Volume 6, Issue 1 (XXXIV)
January - March 2019

ISSN 2394 - 7780

ज्ञान-विज्ञान विमुक्तये
UGC
University Grants Commission
Journal No.: 63571

International Journal of

Advance and Innovative Research

(Conference Special)

Indian Academicians and Researchers Association
www.iaraedu.com

NATIONAL CONFERENCE ON CYBER INTELLIGENCE, CYBER FORENSICS & INVESTIGATION (CICFI 2018 - 19)

ORGANIZED BY

Department of Computer Science and Information Technology

Jnan Vikas Mandal's Mehta Degree College

Navi Mumbai

&

Hexa Digital Forensic Corporation

22nd & 23rd March, 2019

In Association with

Knowledge Partners

Publication Partner

Indian Academicians and Researcher's Association

ABOUT THE COLLEGE

Jnan Vikas Mandal was founded in the year 1974 with a desire to provide education at various levels. It started Mehta Degree College in the year 2001 and received permanent affiliation from University of Mumbai for its various courses and has been re-accredited by NAAC with grade 'A' (CGPA-3.33). College offers B.Sc., B.Com., B.Sc.(C.S.), B.Sc.(I.T.), B.M.S., B.A.F., B.B.I., B.M.M. courses and post graduate courses such as M.Sc. (Chemistry), M.Sc.(By Research), M.Com., M.Sc.(I.T.).

ABOUT BHABHA ATOMIC RESEARCH CENTRE (BARC)

The Bhabha Atomic Research Centre (BARC) is India's premier nuclear research facility headquartered in Trombay, Mumbai, Maharashtra. BARC is a multidisciplinary research centre with extensive infrastructure for advanced research and development covering the entire spectrum of nuclear science, engineering and related areas.

ABOUT MAHARASHTRA CYBER

Maharashtra Cyber was established in 2016 by Home Department, Govt. of Maharashtra Officer of the rank of Special Inspector General of Police is posted to tackle cyber crime and look after cyber security of the government of Maharashtra. Project comprises Technology Assisted Investigation Centre, Technology Assisted Predictive Policing, Cert MH and Centre of Excellence for Capacity building. It is a specialized unit implementing the ambitious Cyber Security Project in state of Maharashtra. It is leading agency in combating piracy of intellectual property on digital Platform.

ABOUT INSTITUTE OF FORENSIC SCIENCE (IFSc.)

The Institute of Forensic Science, Mumbai was established in the year 2009. The Institute is offering Graduate, Post-Graduate and Diploma courses in Forensic Science. The institute is affiliated to Mumbai University, It consists of seven department, namely Dept. of Forensic Science, Dept. of Forensic Chemistry, Dept. of Forensic Physics, Dept. of Forensic Biology, Dept. of Forensic Psychology, Dept. of Digital and Cyber Forensics, Dept. of Law.

ABOUT INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION

Information Systems Audit and Control Association is an international professional association focused on IT governance. ISACA Mumbai Chapter started its operations in a rather informal way in the year 1992 and received chapter status in the year 1996. It has been and continues to be a major supporter of and contributor to the association and foundation efforts.

ABOUT HEXA DIGITAL FORENSIC CORPORATION

Hexa Digital Forensic Corporation is an independent computer forensics company that provides services in digital forensics & investigations, IT security audits, Intellectual Property Rights (IPRs) and providing training in digital forensics and IT security. The firm is also actively extending its services to various law enforcement agencies of Maharashtra state and other states of India.

ABOUT IARA

Indian Academicians and Researchers Association (IARA) is an educational and scientific research organization of Academicians, Research Scholars and practitioners responsible for sharing information about research activities, projects, conferences to its members. IARA offers an excellent opportunity for networking with other members and exchange knowledge. It also takes immense pride in its services offerings to undergraduate and graduate students. Students are provided opportunities to develop and clarify their research interests and skills as part of their preparation to become faculty members and researcher. Visit our website www.iaraedu.com for more details.

PATRONS

Lion. Dr. Ashok Mehta
Hon. President

Shri. M. S. Bhoomraddi
Hon. Executive President

Shri. V. N. Hegde
Hon. Vice President

Shri. V. K. Hunnur
Hon. General Secretary

Shri. K. H. Deshpande
Hon. Jt. General Secretary

Shri. G. N. Haragaball
Hon. Treasurer

ADVISORY COMMITTEE

Shri. R. K. Singh
Head, Media Relations and Public Awareness Section, BARC

Dr. Balsingh Rajput
DCP, Maharashtra Cyber

Mrs. Aruna Mehta
President, ISACA, Mumbai Chapter

Shri. Vicky Shah
Advocate

Convener

Dr. (Mrs.) Leena Sarkar
Principal, Jnan Vikas Mandal

Co-Conveners

Mr. Ramesh Ogania
Founder, Hexa Digital Forensic Corporation, Mumbai

Dr. Pratima Jadhav
Director, IFSc.

Organising Advisor

Dr. John D'mello
A.O., Jnan Vikas Mandal

Organising Secretaries

Asst. Prof. Janhavi Kshirsagar
Coordinator, CS & IT

Asst. Prof. Neeta Khobragade
Coordinator, IFSc.

Asst. Prof. Archana Sanap
Incharge, IT

Asst. Prof. Sunitha Joshi
Incharge, MSc. IT

Treasurer

Asst. Prof. Sanjivani Nalkar

Organizing Committee for the Conference

Asst. Prof. Sarita Sarang

Asst. Prof. Ashish Chavan

Asst. Prof. Sharayu Kadam

Asst. Prof. Mustufa Nullwala

Asst. Prof. Rajshree Pisal

Asst. Prof. Bhagyashree Kulkarni

Asst. Prof. Shakuntala Kulkarni

Asst. Prof. Mamta Pandey

Asst. Prof. Pallavi Deshmukh

Asst. Prof. Ashwini Gangal

Asst. Prof. Tanvi Bhatkar

Asst. Prof. Jael Angel

Guest Editors of Special Issue

Dr. (Mrs.) Leena Sarkar
Principal
Jnan Vikas Mandal's Mehta Degree College
Navi Mumbai

Mr. Ramesh Ogania
Founder
Hexa Digital Forensic Corporation, Mumbai

Mrs. Janhavi Kshirsagar
Assistant Professor & Coordinator, CS & IT
Jnan Vikas Mandal's Mehta Degree College
Navi Mumbai

Mrs. Sunitha Joshi
Assistant Professor & Incharge, MSc. IT
Jnan Vikas Mandal's Mehta Degree College
Navi Mumbai

FROM THE DESK OF CHAIRMAN

I am happy to mention that the department of Computer Science and Information Technology of JVMs Mehta Degree College, Airoli, has put a step forward to organize its first ever Two days National Conference on "**Cyber Intelligence, Cyber Forensics and Investigation**" which is of vital importance in broadening the today's changing scenarios of IT industry and has released the first proceedings of its conference held on March 22nd and 23rd, 2019.

I am proud to state that JVM has been rendering quality services in all the fields by providing excellent infrastructure facilities and well qualified staff. This has made JVM to march confidently towards this competitive world by organizing such conferences from around the nation.

I express my whole hearted congratulations to Principal Dr. (Mrs.) Leena Sarkar for taking keen initiative and her continuous support and cooperation in organizing this conference and making it a successful one.

Hon. Shri. M. S. Bhoomraddi
Chairman
College Governing Council, JVM Trust

FROM THE DESK OF VICE PRESIDENT

At the outset, I would like to congratulate Principal, JVM'S Mehta College and faculty for organizing a first of its kind National Conference on Cyber Intelligence, Cyber Forensics and Investigation, in coordination with Hexa Digital Forensic Corporation on 22nd and 23rd March, 2019. This was a milestone in JVM's history for having organized in such a meticulous way on contemporary issues about digital world and its safety.

This conference was a memorable one, with powerful and relevant "Resource Speakers" having in depth knowledge about cyber related applications. I hope staff and students must have been benefited in this novel field which for sure, will be a sought after subject in the near future.

JVM's management stands firmly behind the organizers in their future endeavors and efforts in imparting the knowledge.

Once again, good wishes to all of you.

Shri. V. N. Hegde
Vice President
JVM

FROM THE DESK OF GENERAL SECRETARY

Seminars, conferences, workshops and refresher courses are the backbone for improving the knowledge among the teaching faculty academically resulting in academical improvement among the student also.

Our JVM'S Mehta Degree College has organized National Conference on Cyber Intelligence, Cyber Forensic and Investigation jointly with Shri. Ramesh Ogania, Founder of Hexa Digital Forensic Corporation and the Science Exhibition by BARC on 22nd& 23rd March 2019 at Airoli, Navi Mumbai.

Dr.(Mrs.) Leena Sarkar, Principal of our college had invited Dr.Balsingh Rajput, DCP, from Maharashtra Cyber as Chief Guest and Shri. R.K.Singh, Head, Media Relations and Public Awareness Section from BARC as Guest of Honour for the National Conference. They both shared their knowledge on the occasion.

We are very grateful to the knowledge partners for the conference i.e. Maharashtra Cyber, BARC, Institute of Forensic Science Mumbai and ISACA (Mumbai Chapter) to have a feather in our cap. Experts & experienced resource persons from reputed organizations and colleges parted their knowledge to the delegates who participated in the conference from different colleges. The National Conference was the first of this type in the vicinity of Navi Mumbai and was a grand success.

I, on behalf of Jnan Vikas Mandal, congratulate all the staff who have made it successful under the guidance of Dr. (Mrs.) Leena Sarkar Principal and as well Shri. Ramesh Ogania, Founder of Hexa Digital Forensic Corporation. It was a unique and grand one.

I have a confidence that organizing such activities every year will motivate and boost the knowledge of teaching staff and standardization of our institute.

Shri V.K.Hunnur
Hon.Gen.Secretary
JVM

FROM THE DESK OF Jt. GENERAL SECRETARY

It was indeed an opportunity to educate ourselves on Cyber Intelligence & Cyber Forensics. The use of technology in common life and experience of individuals was well documented & presented by the experts of the field in various sessions of conference. I feel the JVM in the right path to educate & explore the new avenues in the field of Cyber Intelligence, Cyber Forensics & Investigation in building the safe nation.

Shri. K.H. Deshpande
Hon. Joint General Secretary
JVM

FROM THE DESK OF TREASURER

I feel very proud that the National Conference on Cyber Intelligence, Cyber Forensics and Investigations and Science Exhibition on BARC Technologies was organized at JVM's Mehta Degree College on 22nd & 23rd March, 2019 in close co-ordination with Hexa Digital Forensics Corporation, BARC, Maharashtra Cyber, Institute of Forensic Science (IFSc.) and Information Systems Audit and Control Association (ISACA).

At this point, I extend my best compliments to Principal in particular, Head of the Departments, teaching faculty members, all staff, students and other personalities responsible in making this conference a great success.

Such events will provide opportunity and create imprint on individual about the current advancing technologies, their benefits and its impact on socio-economic development of the country. Best opportunities were provided to hear & interact with national delegates, academicians and industry experts and get acquainted about their research ideas. The young generation was not only exposed to advance technologies, innovative ideas in the field of Cyber Forensics and Investigations and above all helps to make a clear focus in to the field of research aptitude. Never change your originality for the sake of others, because no one can play your role better than you.

The conferences play very important and vital role for the overall development of the student .Lastly, I once again appreciate each one of them for their dedicated and consistent efforts in bringing out the journal on the occasion of first National Conference on Cyber Intelligence and extend my best wishes to one and all.

Shri. G. N. Haragaball
Hon. Treasurer
JVM

CONVENER'S MESSAGE

We at JVM's Mehta Degree College, Airoli, have always thrived to achieve excellence in academics and skill development. In today's technological and web-based world, it is becoming extremely important to understand the threat intelligence, its mechanism, implications and forensics. Keeping this in mind, we planned to organize our first two days National Conference on "Cyber Intelligence, Cyber Forensics & Investigation" so that we can create awareness about cyber threats and maximize cyber security amongst the masses to avoid any unwanted incidents and help the society to build a strong nation. This conference provided a platform for interaction amongst the resource persons and participants to share innovative ideas in this field.

Thus, this National conference intended to be a stepping stone in visualizing the dreams towards a secured future in Digital India.

I express my deep gratitude towards our management members Shri. M.S. Bhoomraddi, Executive President and Chairman, College Governing Council; Shri. V.N.Hegde, Vice President; Shri.V.K.Hunnur, General Secretary; Shri K.H. Deshpande, Jt. General Secretary; Shri G.N.Haragaball, Treasurer, Shri. Satish Khilari and Shri. Avdhoot Akhlekar, management members for gracing the occasion and for their constant support and encouragement.

I am thankful to Shri. Ramesh Ogania, Founder of Hexa Digital Forensic Corporation for joining hands with us for organizing such an informative conference and for inviting highly resourceful speakers.

We were really honoured to have Dr Balsingh Rajput, DCP, Maharashtra Cyber as Chief Guest and Shri R. K. Singh, Head, Media Relation and Public Awareness Officer, BARC as Guest of Honour. We are grateful to both of them for sharing their knowledge and experiences on cyber forensics, investigations and latest technologies.

I am thankful to all resource persons, Shri. Satheesh Kumar Sasidharan (Joint Director, CDAC); Shri. Dinesh O Bareja, (Founder COO, Open Security Alliances, Indiawatch, Principal Consultant of Pyramid Cyber Security and Forensic Pvt. Ltd.); Shri. Ramesh Ogania, (Founder of Hexa Digital Forensic Corporation); Shri. Joseph Gigi (Chief Information Security Officer, BARC); Advocate Vicky Shah; Shri. Ritesh Bhatia (Director, Cybercrime Investigation, V4web Cyber Security); Shri.Rohit Banerjee (Project Management Professional ISACA, Mumbai Chapter); Shri. Vaibhav Sakhare (Senior Digital Forensic Analyst, Technical Head, Pelorus Technologies Pvt. Ltd.) without whom this conference would not have been successful. All the sessions were really enriching and enlightening and have benefited the delegates, academicians, staff and students.

I appreciate the efforts and initiative taken by the department of Computer Science & Information Technology for successfully organizing this national conference.

I also thank Maharashtra Cyber, Bhabha Atomic Research Centre, Institute of Forensic Science, Mumbai and ISACA Mumbai Chapter for being our knowledge partners and YinBuzz, NMTV and FM Gold for being media partners.

I thank Advisory Committee, teaching, non-teaching staff, students, alumni for their hard work and untiring efforts. I thank each and every member of JVM family. I also thank our sponsors and everyone who has helped us in any way in organizing such a wonderful event. I am thankful to all the delegates from different sectors, teachers and students for active participation.

I'm delighted to inform that in such a short span of time we received around 80 papers from various institutes and Universities from India and abroad. They were put through anti-plagiarism check and will be published in UGC approved journal IJAIR. We are thankful to all of you for the overwhelming response.

I am thankful to IARA publications for their ceaseless and meticulous efforts in publishing the proceedings of the conference on time.

As an initiative for skill development and capacity building, we in association with Hexa Digital Forensic Corporation are starting “National Institute of Cyber Intelligence and Investigation”, which will create cyber awareness amongst its students.

Finally, I take this opportunity to convey my thanks to all who have been the part of conference and helped to make this conference grand and successful and helped in creating cyber security.

I hope with the support of you all, we will be able to continue to organize such conferences in future too.

Dr.(Mrs.) Leena Sarkar
Principal & Convener
JVM

FROM THE DESK OF CO-CONVENER

It is a matter of pride and privilege for me to associate with Jnan Vikas Mandal's Mehta Degree College, who had taken keen initiative to start the professional building training project titled "**National Institute of Cyber Intelligence and Investigations".**

I am sure that the deliberations of the conference will come with suggestions from international delegates, industry, academicians and researchers to meet the future challenges in the field of "Cyber Intelligence, Cyber Forensics and Investigations".

I would like to take this opportunity to thank the management and the principal for their endless support.

I would further like to thank the faculties of Computer Science and Information Technology, non teaching staff for their support in making this conference a successful one.

Shri. Ramesh Ogania
Founder, Hexa Digital Forensic Corporation
Cyber Forensics and Cyber Incidents Investigator

CHIEF GUEST OF THE CONFERENCE

Dr. Balsingh Rajput
DCP, Maharashtra Cyber, Mumbai

Dr. Balsingh Rajput, serving as IPS in Maharashtra Cyber, was the Chief Guest for the Two Days National Conference "Cyber Intelligence, Cyber Forensics and Investigation" held on 22nd and 23rd March, 2019.

Dr.Balsingh Rajput mainly described how cyber crime is becoming a major concern and how it is affecting humankind. He focused on how cyber crime is increasing simultaneously with the advancement in technology. He also described different security trends and ways to prevent cyber crime. Moreover, he explained these topics with numerous examples thus revealing the darker side of technology and appealed to all citizens to share Cyber Intelligence information they get from surroundings with law enforcement officials for National Security purpose.

Dr. Balsingh Rajput
DCP, Mumbai, Maharashtra

GUEST OF HONOUR OF THE CONFERENCE

Shri. R. K. Singh
Head, Media Relation and Public Awareness Section, BARC

Shri R.K. Singh, an Electrical Engineer, joined Bhabha Atomic Research Centre in 1986 after graduating from 29th batch of BARC training School. He has worked for Design, development, installation, commissioning & maintenance of control instrumentation of 100 MWth Research Reactor, DHRUVA. Shri Singh has been on deputation to Narora Atomic Power Station (NAPS) for rehabilitation and commissioning of control instrumentation after fire incident. He has worked for design, installation & commissioning of Physical Protection Systems. He has developed Advanced Instrumentation for flow visualization and Vector field mapping of Advanced Heavy Water Reactor (AHWR) components and Pressurised Heavy Water Reactor (PHWR) components.

Shri. R.K. Singh, Head of Media Relations and Public Awareness Section, BARC Mumbai, was the guest of honour for the "Two Days National Conference" held on 22nd and 23rd March, 2019 at J.V.M's Mehta Degree College, Airoli, Navi Mumbai. Shri. R.K. Singh gave the audience insight on the role of Cyber Forensics and Investigations that are prevalent in today's situations and how and by what means one can control or take preventive actions. He also focused on how to spread awareness in public about the Cyber Crimes. He elaborated on how to enhance security and create mass awareness among the youth.

Organizing such conferences will help in bringing the awareness amongst the masses regarding the security issues in Cyber and Crime related issues in the Cyber space. It also promotes the staff and students to involve in more research activities to find out the solution to avoid such crimes happening in the society.

Shri R.K.Singh
Head, Media and Public Awareness Section
BARC

Resource Persons
for
Two Days National Conference
on
Cyber Intelligence, Cyber Forensics and Investigation

Shri. Satheesh Kumar Sasidharan
Joint Director, CDAC

Mr. Satheesh Kumar Sasidharan was invited as a Resource Person for Two Days National Conference on “Cyber Intelligence, Cyber Forensic & Investigation”. Mr. Satheesh Kumar Sasidharan has more than 15 years of experience in the field of Information Technology. For the last 11 years he has been working in the area of Cyber Forensics as a forensics expert as well as an R&D Engineer in CDAC Trivandrum. His area of specialization is Smart Phone Forensics. With his leadership, different commercial forensics tools were developed and deployed in the market. He is also a cyber forensics trainer for various Law Enforcement Agencies in India.

In his talk, he explained Smartphone Forensics and Disk vs Phone forensics. He spoke about real life case study – about satellite phones and terrorist attack. He explained the role of ITU (International Telecommunication Union) in world of Cyber Security. He also explained how various files can leak information from our system, files like Manifest file give details about list of permission, Android data Partition, structure of directory in our mobile phones, file systems information, etc. He also demonstrated how one can use SQLite files for data analysis to decode file system, also from damage phone data retrieval is possible using technologies like Micro Ray & Electron microscope. He concluded the session by showing the list of some tools used for computer forensics and cell phone forensics investigation.

Mr. Satheesh Kumar Sasidharan
Joint Director, CDAC
Thiruvananthapuram

Mr. Dinesh O Bareja
Founder & COO: Open Security Alliance and IndiaWatch.in
Principal Consultant: Pyramid Cyber Security & Forensic Pvt Ltd.

Mr. Dinesh Bareja was invited as a Resource Person for the Two Days National Conference on "Cyber Intelligence, Cyber Forensic & Investigation". Mr. Dinesh Bareja is an Information Security Management professional working in IT/IS domain for more than a decade. He handles projects in India as well as overseas. As he has an extensive business experience in trading, manufacturing and IT sector he brought a unique blend of techno commercial expertise to offering advisory and strategic consulting services in Cyber Security.

He gave in-depth knowledge about Cyber Warfare and Cyber Terrorism. He explained the concept of Connected Warrior- a Techno Soldier, have inbuilt communication system, gesture controls and real time information. He explained the law HIPAA (Health Insurance Portability and Accountability Act) which has been implemented in USA and importance of it. He also introduces the Darkweb to the audience, along with STUXNET which is for advanced persistent threat attacks. He concluded the session by summarizing how Common Man, Government, Academia and Industry can contribute toward Cyber Security.

He concluded the session by summarizing how common man, Government, Academia and Industry can contribute to Cyber Security.

Mr. Dinesh O Bareja
Founder & COO: Open Security Alliance and IndiaWatch.in
Principal Consultant: Pyramid Cyber Security & Forensic Pvt Ltd.

Shri. Ramesh Ogania
Founder, Hexa Digital Forensic Corporation
Cyber Forensics and Cyber Incidents Investigator

Shri. Ramesh Ogania is a Founder of Hexa Digital Forensic Corporation. He delivered an insightful speech on Cyber Intelligence investigation and Counter intelligence techniques. He discussed the types of Cyber Intelligence sources which are mapped with cyber threat intelligence for information security.

He focused on intelligence life cycle. He also discussed various tools like social media enumeration and correlation tools which supports the social media platforms i.e. Linkedin, Facebook, Twitter, Google plus, Instagram that uses facial recognition to correlate social media profiles across different site on a large scale.

Further, he discussed Counter intelligence techniques which are used for virtualization of investigation system and tools and VPN for investigation online and showed two live investigation cases in which Cyber Intelligence techniques are used.

Shri. Ramesh Ogania
Founder
Hexa Digital Forensic Corporation
Cyber Forensics and Cyber Incidents Investigator

Shri. Joseph Gigi
Chief Information Security Officer
Bhabha Atomic Research Centre (BARC)

Shri. Gigi Joseph was invited as a Resource person for the Two Days National Conference on **"Cyber Intelligence, Cyber Forensics and Investigation"** held on 22nd & 23rd March, 2019.

Shri. Gigi joined Bhabha Atomic Research Centre (BARC) in 1992 (36th BARC Training School Batch) and currently holds the position of a Scientific Officer (H) & Chief Information Security Officer (CISO) at BARC. Shri. Gigi has more than 25 years of experience having expertise in Cyber Security, Networking and Telecommunication areas. Few achievements of Gigi are in Design & Development of Secure Network Access system (SNAS), an indigenous integrated cyber security system. Shri. Gigi was honored with '**Homi Bhabha Science & Technology Award**' for the year 2012.

Shri. Gigi elaborated on wide range of topics such as the Apps banned by the Government of India, features of mobile phones, Internet of Things (IOT), Online data, Digital slavery, Tangled phishing attacks, Forensics Analysis, Brain machine interfaces (BM), Banking Malware, Mobile spying, Smart watch. He also gave a brief insight about malwares and how to detect them. His lecture was highly informative.

Shri. Joseph Gigi
Chief Information Security Officer

Avocate Vicky Shah

Advocate Vicky Shah was a resource person for "Two Days National Conference" held on 22nd and 23rd March, 2019 at J.V.M's Mehta Degree College, Airoli, Navi Mumbai.

Advocate Vicky Shah is author, trainer and speaker who started his career as a trainer to law enforcement agencies in India for Cyber Crime Investigation Techniques in October 2004 with NASSCOM and DSCI. He was invited as Speaker by the Reserve Bank of India to address the High-Level committee Meeting on Governance, Risk and Compliance and have been acknowledged for inputs in the Gopal krishnan Report published on 21st January 2011 on the website of Reserve Bank of India. He was included in the panel of Legal expert for advising Office of Controller of Certifying Authorities (CCA), Government of India on Legal matters relating to Information Technology Act and he is also on IRCTC legal panel from March 2016.

Advocate Vicky Shah addressed the audience on 23rd March, the second day of the national conference. Various real life incidents related to cyber crime and methods to safeguard one's personal documents were explained by him. Cyber crime and related legal issues which a common person could face due to their negligence in safeguarding personal documents were also discussed by him in detail.

Advocate Vicky Shah

Mr. Ritesh Bhatia
Founding Director
Cyber Crime Investigator
Cyber Security & Data Privacy Consultant

Mr. Ritesh Bhatia is a Cybercrime Investigator and Cyber security & Data Privacy Consultant. He is the Founder-director of V4WEB Cyber security and has investigated and solved complex cases on cyber crime for the corporates, government organizations, law enforcement agencies and individuals in India and abroad. His views on trending cybercrimes and cyber security have often been sought and published by many media houses including Times of India, Indian Express, Hindustan Times and DNA. He has appeared on national television channels and radio stations such as CNBC, NDTV, Times Mirror Now, India TV, AajTak, Zee News, Radio City, Red FM, and Radio Mirchi to highlight the dangers in the cyber space.

Mr.Ritesh Bhatia delivered a speech on Dark Net and Dark Web. He started with introduction to internet, dark web and deep web. He explained how we can use dark net. He also explained difference between surface web and dark web by giving examples. He also talked about the different types of markets available on dark net. where things such as Drugs, Counterfeit Currency, Forged Papers Passports, driver's licenses, citizenship papers, fake IDs, college diplomas, immigration documents, Ammunition, and Explosives Weapons, Hit men, Human Organs etc are available.

He concluded by talking extensively about the disadvantages and advantages of using the Dark net. He also explained what problems one can face if they try to use dark net for illegal activities.

Mr. Ritesh Bhatia
Founding Director
Cyber Crime Investigator
CyberSecurity & Data Privacy Consultant

Shri. Rohit Banerjee
ISACA, Mumbai Chapter

Shri. Rohit Banerjee, a seasoned professional in IT Governance, Project Assurance and Program Management. He was one of the speakers for the Two Days National Conference held on 22nd and 23rd March, 2019 at J.V.M's Mehta Degree College, Airoli, Navi Mumbai.

Shri. Rohit Banerjee elaborated on how cyber crimes take place and highlighted the measures to prevent them. He also discussed extensively on areas of cyber forensics and criminal investigation. He explained the different forensic techniques and technological advancements with multiple case studies, thus revealing the darker side of technology

He discussed about various courses and training programmes for information security. He made the audience aware of the importance of security and the measures to ensure it. His talk was packed with information and was highly helpful for the audience.

Shri.Rohit Banerjee
ISACA, Mumbai Chapter

Mr. Vaibhav Sakhare
Sr. Digital Forensic Analyst & Technical Head
Mumbai, Maharashtra

Mr. Vaibhav Sakhare is working as a senior Digital Forensics Analyst and Head of Digital Forensic Division, Mumbai from 2015 and is a reporting analyst for examination of digital evidence referred by private organization and Government Agencies. He has technical expertise on various Digital Forensic Tools. He is a certified Examiner in Computer Forensics from EnCEOpentext, from Pasadena, California. He has completed his Diploma in Cyber Law from Government Law College, Mumbai. He has reported more than 250 cases related to the examination of digital evidence referred to DFSL by Investigating Agencies which includes economics crimes, data theft, internet crimes etc.

Mr. Vaibhav Sakhare shared his knowledge with the research paper presenters and the students. He explained various tools and technology like JTAG(Joint Test Action Group) used for verifying designs and testing printed circuit boards after manufacture, Chip-Off Forensics the process in which BGA memory chip is removed from a device and prepared so that a chip reader can acquire the raw data to obtain a physical data dump, ISP(In-System Programming) which is applied to forensics which is best practice of connecting to eMMC or eMCP flash memory chip for the purpose of downloading a device's complete memory contents. Further he explained details about Gait Analysis, which is used to study the human motion using the eye and the brain of observers, augmented by instrumentation for measuring body movements, cloud analysis and new trends of Exhibits Forensics. Further, Mr. Sakhare concluded by highlighting the challenges in Cyber Forensics due to the rapid advancement in technology.

Mr. Vaibhav Sakhare
Sr. Digital Forensic Analyst & Technical Head
Mumbai, Maharashtra

International Journal of Advance and Innovative Research

Volume 6, Issue 1 (XXXIV): January - March 2019

Journal - 63571

UGC Journal Details

Name of the Journal :	International Journal of Advance & Innovative Research
ISSN Number :	
e-ISSN Number :	23947780
Source:	UNIV
Subject:	Multidisciplinary
Publisher:	Indian Academicians and Researchers Association
Country of Publication:	India
Broad Subject Category:	Multidisciplinary

International Journal of Advance and Innovative Research

Volume 6, Issue 1 (XXXIV) : January – March 2019

CONTENTS

Research Papers

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

CYBERCITY AS MILITARY ARENA

Dr. Anjum A. Tadvi
Superintendent of Customs (Preventive)

ABSTRACT

The present paper is in respect of use of Cyberspace to attack states and how it is slowly turning to an arena for military action. Human beings have a natural tendency for conflict. We have fought the animal world during evolution and after that conquered other territories such as land, lakes, sea, air, and space. The new area that has been the new human interest is the cyberspace. Countries and organizations are jostling each other in a bid to outdo the capabilities and powers of each other. The fate of the Nuclear plant of Iran is well known, and it speaks of volume how one nation or group of people can make or break an entire project or an entire country. Cyber engineers outdid the Iranian bid to have its nuclear weapons without a war or Physical attack on its plant. Hackers made attempts to influence elections in the US. It is also understood that elections held in France and Germany held recently were affected by the hacking. Cyberspace has therefore emerged as the 'fifth battle space' and is consequently a new but not entirely separate component of a multi-dimensioned struggle environment which also includes land, sea, air, and space. Cyber warfare is thus a description of the operational activity carried out by the armed forces, law enforcement, and intelligence agencies in current times. NATO has already recognized cyberspace as a domain of conflict. The NATO Secretary General had recently stated that 'nowhere is the fog of war greater than in cyberspace. Thus countries are recognizing that the new territory for war is going to be Cyberspace and not the physical battlefield.

Keywords: Cyberspace, Cybertech

INTRODUCTION

Cyberspace is gradually touching all aspects of human activity, It is turning into a borderless country where the only division is the difference between the military and civil elements and activities related to the same. Some events do overlap each other, and thus caution is required in the national interest. Cyberspace has blurred the physical and geographical boundaries and the difference in time between the nations. The national rules and laws do not thus apply, and states are required to fight off the battle on the new ground where even a militarily weak enemy may be a powerful opponent in Cyberspace.

It is observed that Cyberspace is turning into a battle fought between states and sometimes with non-state opponents. 'Cyberwar' is a series of sinister activities where the enemy/ attacker remain faceless. It has replaced the concept of cold war and proxy wars. Nations are employing an increased used on organized armed force in the name of cyber warfare. The same is employed to gain the upper hand in geopolitical purposes. Countries also find themselves amid conflict with other states or with non-state actors which may be terrorist, extremist and organized criminal groups. Cyberspace is gradually turning into a battle space, a 'domain' of quasi-military operations. Everything is done to protect the national interest and safety and in tit for tat action.To fight these wars, the need for 'cyber weapons 'arises. These weapons are nothing but a quick entry into a weak system or an opportunity gained by better technology. Action and its effect after that follow the entry into the system: The opportunity is arrived by the finding flaw in the system, a bug, or vulnerability in an ICT system. In some cases, advanced technology helps to exploit the flaw or gain entry into the system. Malware, Trojan and Ransomware cannot be ruled out. In certain cases theft of data, destruction of data, Industrial espionage, election manipulation, loss of personal or important data and temporary or permanent disruption of services or systems cannot be ruled out. The disruption of services can be conducted at military, space and nuclear sites which can spell catastrophe for the nation and world. Thus any action or technology that can assist in maligning, disrupting, destroying, data theft and placing of bug etc in systems can be a cyber weapon. Though this description is very brief, it does very little to ponder over the kind of challenge these weapons present. Some 'weapons' are exclusively for military purpose whereas, others are for 'dual-use,' i.e., affecting both military and civil applications. The third kind is for civil technologies and is not weapons in the true sense as they only exploit vulnerabilities for commercial ends. The character of cyber weapons require both the offense and defense tools and thus continue to evolve. Countries are in a race to prepare weapons on Cyberwarfare and label them as deterrence ones. The race is thus unending like the arms race seen earlier. Nations are facing a catch-22 situation where they cannot shy away from acquiring Cyber weapons and trying them on their nemesis in a bid to test the same. The bid to create more and more Cyber weapons has led to a dilemma where all countries are feeling insecure against others.

ISSN 2394 - 7780

The insecurity of the nations is not misplaced as in current scenario most of the industries of national interest such as Oil, Electricity, Nuclear capacities, Space, High Seas drilling, Defense equipment, and Civil aviation manufacturing have been sold or outsourced to private agencies who are not prepared to face a military type attack on their plants and installations. The Privatization of weapons, military goods and nukes have attracted the attention of Non-Government actors and can spell doom for the nation if these Private partners are not protected. With such a big challenge facing the nations, a sort of arms race to defend these installations has, and an era of new arms race albeit in Cyberspace is seen. Use of technology has done away the difference between nuclear and non-nuclear weapons and access to the same has become a matter of accessing the systems in its weak moments to these illegal players.

With technological development, most of the countries have experienced increasingly dependence on Cyber technology. The technological advances have brought these nations more vulnerable to Cyber attacks. It is expected that future attacks on the military will be by using cyber attacks. The same may involve making the radars non-functional, disrupting the working of Submarines and planes and with cyber attacks on the military camps involving temporary disruption of messaging, communication and electricity etc. Attacks from states may start with very fast paced attack on military and disruption of its movement and communication. This may then be followed by the actual attack if any. Nations are thus gearing up for such eventuality and digital techniques for camouflage and concealment of critical networks and key personnel is being employed as a measure of abundance precaution and defense preparedness.

CONCLUSION

Military operations in cyberspace are a new phase of human experience as a cyber conflict is unlikely to produce clear and durable results that are seen during military operations. A major challenge that the world faces is the Space system which is based totally on Cyber technology as all Satellites whether Military or Civil ones are working on Cybertech. Most of the worlds business, trade and information are based on these Satellites. Due to their dependence on Cybertech, they are vulnerable to attacks. Further, most of these Satellites are owned by Private sector and thus more likely to be a threat as was seen in the case of privately-owned Inmarsat satellite telecommunications system upon which global shipping and airline industries depend and due to the hacking of its system. many shipping liners suffered losses as it started giving false and wrong signals about the traffic. The U.S. and allied military forces rely on Inmarsat's worldwide L-band Tactical Satellite (L-TAC) and similarly, other nations too have their Satellites privately owned to help the Armed forces and national airline carriers to gauge the route etc. A Cyberattack on such important will thus be a nightmare for most of the nations. Cyberspace is slowly turning into a military arena where wars are being fought on daily basis. The same may explode in days to come and thus it is necessary for all nations of the world to come together to formulate some plan to control the same.

REFERENCES

1. The Virtual Weapon (2017), Lucas Kello
2. 'Cyber war is real'(2010) Clarke and Robert Knake
3. Cyber War Will Not Take Place(2013) Thomas Rid
4. Cyber Security Review. 26 Mar. 2017.
5. Bloomfield, Lincoln P., and Allen Moulton. Managing International Conflict: From Theory to Policy: A Teaching Tool Using CASCON. New York: St. Martin's, 1997. Print.
6. Carr, Jeffrey. Inside Cyber Warfare. 2012. Print.
7. Chapple, Mike, and David Seidl. Cyber Warfare: Information Operations in a Connected World. Burlington, MA: Jones & Bartlett Learning, 2015. Print.
8. Choucri, Nazli. Cyberpolitics in International Relations. Cambridge, MA: MIT, 2012. Print. 6. Choucri, Nazli. "Explorations in Cyber International Relations: A Research Collaboration of MIT and Harvard University." SSRN Electronic Journal. Print.
9. Choucri, Nazli, Christi Electris, Daniel Goldsmith, Dinsha Mistree, J. Bradley Morrison, Michael Siegel, and Margaret Sweitzer-Hamilton. "Understanding & Modeling State Stability: Exploiting System Dynamics." SSRN Electronic Journal. Print.
10. Clarke, Richard A., and Robert K. Knake. Cyber War: The next Threat to National Security and What to Do about It. New York: Ecco, 2012. Print.

ISSN 2394 - 7780

11. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure. Washington, DC: Executive Office of the President of the United States, 2009. Print.
12. Kaplan, Fred M. Dark Territory: The Secret History of Cyber War. New York: Simon & Schuster, 2016. Print.
13. Madnick, Stuart E., Xitong Li, and Nazli Choucri. "Experiences and Challenges with Using CERT Data to Analyze International Cyber Security." SSRN Electronic Journal. Print. 96
14. Madnick, Stuart, Nazli Choucri, and Jeremy Ferwerda. "Institutional Foundations for Cyber Security: Current Responses and New Challenges." SSRN Electronic Journal. Print.
15. Popp, Robert L., and John Yen. Emergent Information Technologies and Enabling Policies for Counter-terrorism. Hoboken, NJ: Wiley-Interscience, 2006. Print.
16. Reed, Thomas C. At the Abyss: An Insider's History of the Cold War. New York: Ballantine, 2005. Print.
17. NATO. "The History of Cyber Attacks - a Timeline." NATO Review. Web. 26 Mar. 2017.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

CYBER TERRORISM: INDIAN PERSPECTIVE PROBLEMS, ISSUES AND STRATEGIES

Adv. Arun Ramchandra Gaikwad
Research Scholar, Swami Ramanand Teerth Marathwada University, Nanded

ABSTRACT

Terrorism - the unlawful use of violence and intimidation, especially against civilians, in the pursuit of political aims. The traditional concepts and methods of terrorism have taken new dimensions which are more destructive and deadly in nature.

Cyber-terrorism is the togetherness of terrorism and cyber-space. Cyber-terrorism is generally understood to mean unlawful cyber attacks and threats of cyber attack against the information stored in computer and computer networks when done to intimidate a government or its people in the furtherance of social, economical and political objectives.

The cyber terrorism is ultimate danger to quick innovation improvement in information and communication technology. Potential targets are frameworks which control the country's resistances and foundation. cyber-terrorists target the computer systems that control financial transactions , telecommunications networks, electric power grids, air traffic, military command systems and attack on democratic system.

Terrorist groups have been conducting more passive forms of information cyber warfare. It is reported that these terrorist groups are using the Internet to conduct their operations by employing email and file encryption and steganography, as well as conducting web defacement attacks.

In India no clear act of cyber terrorism has occurred yet. We need to be prepare for acts of cyber terrorism as the increasing social critical assurance on information system will make information communication technology system and services as well as embedded information and communication technology an interesting target for future terrorists.

Keywords: Cyber terrorism, cyber attack, cyber warfare , terrorist , information technology

INTRODUCATION

we first need to look at the definition of terrorism which shall encompass the cyber terrorism definition. Unfortunately there is no generally agreed international definition of terrorism,

Information technology Act 2008 define cyber terrorism

Punishment for cyber terrorism.–(1) Whoever,–

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by–

(i) denying or cause the denial of access to any person authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant, and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

ISSN 2394 - 7780

The definition of “cyber-terrorism” cannot be made exhaustive as the nature of crime is such that it must be left to be inclusive in nature. From the above definitions it can easily concluded that

"cyber- terrorism" refers to two elements:

(i) Cyber Space; and

(ii) Terrorism.

This means that the term necessarily refers to any dangerous, damaging, and destructive activity that takes place in cyber-space.

The synergy between terrorism and cyber space has given birth to deadly combination and thus coined a new term cyber terrorism .

Cyber space and terrorism it may either

(A) spreading terror using cyber space.

(B) terrorizing the cyber space

As terror is a psychological condition of human and other living creature, the first one i.e. spreading terror using cyber space is most appropriate . even terrorizing cyber space finally leads to terrorizing the users of cyber space i.e. human beings.

Cyber terrorism is a controversial term. Some author’s choose a very narrow definition ,relating to diplomats by known terrorist organization of disruption attacks against information systems for the primary purpose of creating alarm and panic.

CYBER WARFARE

Cyber warfare can also be described as intranet based conflict involving politically or socially or ideologically motivated attacks on information and information systems . cyber warfare attacks can disable official websites and networks , disrupt or disable essential services, steal or alter classified data , and cripple e-government ,financial and other critical system , among many other possibility.

Cyber warfare is normally between sovereign states , or corporation. In cyber Warfare normal all or most staragic IT infrastructure to disable or destroy

A common term linking ‘Cyber Warfare’ and ‘Cyber Terrorism’ is the “ Cyber Attack” the base action associated with both ‘Cyber warfare’ and ‘cyber terrorism’ and other forms of cyber assault or malicious actions.

CYBER ATTACK

‘Cyber Attack’ can be defined as malicious computer code or other deliberate act designed to alter, disrupt, deny, degrade or destroy information resident in computers and computer networks or the computers and networks themselves.

Cyber Attack refers to “an attack, via. Cyberspace, targeting an enterprise’s for the purpose of disrupting, disabling, destroying or maliciously controlling a computing environment/infrastructure or for destroying the integrity of the data or stealing controlled information.

METHODS OF ATTACK

Terrorist organizations generally use the Internet for publicity purposes. The worldwide web and steady developments of web 2.0 have given an opportunity to the public to easily access and publish information of Internet by terrorists has been described for many years as a growing trend. Terrorist publicity on the Internet is disseminated through several types of platforms. video sharing websites such as YouTube, online Social Network services such as Facebook; and through traditional online forums and blogs. Forums are the most common way of promoting terrorism on the Internet since they provide a platform where people with the same way of thinking gather together.

The main advantages for those terrorist groups to own their own forum is to have a total control over censorship, namely the communications between its members: messages and threads can be modified, deleted. They also have total freedom over the choice of the running platform, hosting location, activity logs and user access control, so members can be banned or promoted based on the way they behave Online social network services used by terrorists are the latest growing trend; more and more supporters of terrorism appreciate the freedom to exchange or comment on any terrorist action without restriction from any forum administrator as described above.

ISSN 2394 - 7780

The increasing number of terrorist sympathizers using Social Network services has already revealed that the terrorist community is not so united and supportive as it seemed to be. There are several disagreements about claims of attacks, or even the purpose of an attack; The increase in the number of terrorist accounts on Twitter raises the issue of identification of individuals or groups Internet users or terrorist sympathizers are initially attracted to the terrorist environment through video sharing websites such as YouTube where videos showing terrorist attacks are displayed.

The YouTube accounts refer to a URL of a terrorist forum where people can click to access the forum, and they can join the forum by sending an email to its administrators. When the "junior member" joins the forum, they will be tested to fulfill basic tasks. They will be then assessed, and based on good results, will be granted a higher rank such as "member," "confirmed member," "senior member," etc. At the same time they will also be granted more privileges, for example they could be given the task to administrate new comers on the forum. After a certain time one of the top administrators will ask the "senior member" to meet physically in order to further assess and validate that person as a good candidate. Following this crucial meeting the "new recruit" is introduced to a very small network of much radicalized individuals via VoIP such as Skype or Paltalk. This is where the candidate is entrusted with sensitive information, including where attacks are planned or targets designated

Initially, Al-Qaeda type groups were reported as using Steganography to hide messages in pictures and/or movies. Though Steganography is an obfuscation method and cannot be considered as an encryption technology, it serves the purpose of hiding a message from plain sight which in turn ensures relative privacy and is one of the aims of encryption. This Modus Operandi was highly probable but has never really been proven to be widely used. The size of the information that can be hidden in a picture is very limited

DARKNET

In the early 2000, some developments have seen emerging alternate networks running in parallel to the Internet. The original purpose of these was to help people under oppressive regimes and without free-speech to be able to communicate giving them increased anonymity and the ability to bypass their national surveillance. Such networks provide traffic anonymization between a client and a server but also permit to develop/host Hidden Services such as web services, file exchange, blogging, chatting hidden from the Internet. Consequently such an opportunity has attracted not only oppressed people but also criminals and terrorist that found through those networks a new way of exchanging information, and spreading knowledge, etc.

Today there are two main anonymous network: TOR (The Onion Router) the oldest, and I2P. Unlike social networks and forums/blogs where terrorist groups use to advertise, claim attack responsibilities and recruit on the Internet, the darknet networks are used to provide specific content such as videos and training materials that can be found on TOR Hidden Services

FULL VPN

As communication and exchange between members of a terrorist cell or organization is crucial, some existing devices can be leveraged to better enforce anonymity. For instance by having a full VPN service across the members and having all communications going through this VPN central point. Nowadays devices such as NAS (Network Attached Storage) are now providing a number of additional services which are easy to install on top of providing storage. We can imagine having such a NAS installed in a safe or unsuspected location or in a nursing place with a broadband ADSL access.

If sufficient trust is placed by a terrorist organization on the NAS device, this device can be configured to enable VPN only communications, and through this channel provide additional dedicated VoIP (Voice over IP) telephony, email servers, web server, video server, file sharing/ storage, any other kind of application needed by the cell and/or group to function and prepare an attack. This has the advantage of being accessible not only by laptops and workstations but also by smartphones that are all now supporting VPN functionalities. This allows the cell/group members to use the different services without having to actually do a real phone call or exchange of information outside the VPN and thus they remain undetectable.

CHALLENGES TO INDIA'S NATIONAL SECURITY.

Existing Cyber Security Initiatives

Administraive Structyre –General

Under ITA2008, administrative structure for information security management is managed by the ministry of communication and information technology and the ministry of home affairs in the central government supported in certain instances by the ministry of home in the respective state government. There is also an inter-ministerial committee to oversee the requirements when required..

ISSN 2394 - 7780

COMPUTER EMERGENCY RESPONSE TEAM (IND- CERT)

Indian cyber Emergency Response Team (IND-CERT), previously called CERT-IN woks as a division of the Ministry of Communication and Information Technology(MCIT), Government of India and is a key authority for regulation of Cyber Security in India. This has been created to enhance the security of India's communication and Information Infrastructure through proactive action and effective collaboration.

Under Section 70B of ITA 2008 IND-CERT is expected to perform the following functions.

(a) Collection, analysis and dissemination of information on cyber incidents.

(b) Forecast and alerts of cyber security incidents.

(c) Emergency measures for handling cyber security incidents.

(d) Coordination of cyber incidents response activities.

(e) Issue guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

(f) Such other functions relating to cyber security as many be prescribed.

In order to discharge these functions, IND-CERT has been bestowed with quasi-judicial powers. Accordingly, it is empowered to call for information and give direction to the service providers, intermediaries, data centers, body corporate and any other person.

Additionally, IND-CERT is designated under Section 70A as the "National Nodal Agency" for protection of what is termed "Critical Information Infrastructure".

Under Section 70 of the Act, Government has the power the designate any Critical Infrastructure System as a "Protected System". This would render any attempt to unauthorized access such a system punishable with imprisonment of up to10 years. This also means that all designated "Protected Systems" are also "Critical Information Infrastructure."

Thus IND-CERT has been provided the responsibilities for securing both the Government infrastructure assets that fall in the category of Critical Information Infrastructure as well as the Private IT Infrastructure irrespective of whether it is critical or not.

SECRETARY,MINISTY OF COMMUNICATION AND INFORMATION TECHNOLOGY (MCIT)

Ministry of Communications and Information Technology (MCIT) is the ministry which implements ITA 2000/8. Administratively it is headed by a Secretary all the rules and notifications under the ITA 2000/8 are issued under the signature of the Secretary. Though he reports to the Minster of State and the Cabinet Minister who oversees the functions of the Ministry, he is the top official supervising the affairs of the ITA 2000/8 administration.

Secretary of MCIT also is the competent authority to exercise the powers given under Section 69B to monitor and collect "Traffic Data" from IT users and User organizations. Such data may include IP address or Computer log records with any person or organization in India.

SECRETARY,MINISTRY OF HOME AFFAIRS

Under Section 69 conferred to certain powers are conferred to intercept, monitor or decrypt any data. The power under this section are exercised by the Secretary, Ministry of Home Affairs either in the Center or in the respective states. It is under these powers that the Government of India has been demanding the access to encrypted information in Blackberry service.

All ISPs and MSPs need to take note of these powers and ensure that they are complied with.

CONTROLLER OFCERTIFYING AUTHORITIES

The Controller of Certifying Authorities has been set up as an independent statutory authority to issue such licenses and also monitor the activities of all the licensed Certifying Authorities. The CCA is also a quasi-judicial authority and is the adjudicator for disputes concerning a subscriber of a digital certificate and a certifying authority.

CYBER REGULATION ADVISORY COMMITTEE

Under section 88 of ITA 2000, it had been envisaged that a Cyber Regulations Advisory Committee (CRAC) would be set up to advise the Central Government generally as regards any rules or for any other purpose connected with this Act. Accordingly a committee has been constituted with has representation from different

ISSN 2394 - 7780

Ministries in Central Government as well as the Police Heads from a few States, the CCA and representatives from industry organizations etc.

COMPLIANCE OFFICERS AND NODAL OFFICERS

Under section 69 the central government or a state government direct any agency of the appropriate government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted and information transmitted received or stored t may direct any through any computer resource.

Similarly under Section 69A, the central government may direct any agency of the Government or intermediary to block access to public of any information generated, transmitted, received, stored or hosted in any computer resource. The powers under this section is exercised by an official who is appointed by the Secretary, MCIT who may be considered as a regulatory officer of the MCIT for the purpose.

Also under Section 69B the Central Government may monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource.

At the Government departments, there s a need to designate an official as a "Nodal Officer" to receive and respond to any information required by the agencies appointed for implementing the security provisions under the Act and also to respond to any queries received from the Public. A system similar to the designation of Public Information Officers under the Rights to Information Act would therefore be required to put in place by the Government departments.

SECURITY AUDITORS AND CONSULTANTS

ITA 2008 has envisaged many security aspects to be implemented at the user level. It envisages that there could be direct and vicarious liabilities on the organizations and its Employees and Directors. Under Section 43A, organizations are to put in place "Reasonable Security Practices". Under section 67C companies have to put in place appropriate "Data Retention and storage policies". Under section 85 and section 79, companies are expected to put in place appropriate security systems that can constitute "Due Diligence".

In order to meet these liabilities, it will be necessary for companies to make an appropriate "ITA 2008 Non Compliance Risk Analysis" and undertake appropriate measures to mitigate the risks. This requires "ITA 2008 Auditors" to conduct an appropriate ITA 2008 Compliance audit and to work with appropriate consultants to ensure compliance.

RECOMMENDATIONS

Internet becomes away to engage in War. That is why cyber war or net war may be called War in the Information Way or I-Way. Taiwan against China, Israel against Palestine, India against Pakistan, China against the USA and so on are some example of Cyber war in I-Way or Superhighway.

For prevention and control of cyber terrorism the national internet security standards must be strong and of world standard.

Especially the Government agencies must choose LAN (Local Area Network) for internal communications and they must adopt their own secret and confidential fiber method about their activities to fight against virus, worm, denial of service attack, attack hacking in net ways which are possible tools and modes of cyber terrorism.

Other most important techniques required to prevent and control attack by terrorists in cyberspace is regular updating of antivirus software, changing passwords and updating of operating system.353

Very important need of the day is awareness, information technology education and training among people who use net and government agencies and even who use non-governmental computer system.

The IT Act, 2000 indirectly prohibits cyber terrorism. But in this regard we need specific and clear law with specific definition of cyber terrorism, legal provisions with specific punishments keeping International and jurisdictional aspects in mind in the era of Global communication convergence and mobile technology.

Change is inevitable and therefore the dilemmas that advancement in technology poses cannot be avoided. the reality is that the criminals have modified their strategies and have started hoping on the advanced technology, and to subsume them the society, the legal, and therefore the enforcement authorities, the non-public companies and organizations will get to modification their mechanism to combat it.

The legal systems round the globe are, with each passing year, attempting to implement new measures to combat cyber act of terrorism. However, with a lot of innovative ways that of operating within the cyber area, a

ISSN 2394 - 7780

lot of loopholes are shaped which can get to be crammed in by the countries by amending the procedures and the laws in effect to tackle cyber act of terrorism. Moreover, a unified international framework ought to be in situ to combat this world issue. Further, the public ought to be created conscious of the threats and the ways that and means that of dissemination and the way to deal just in case of terrorist attacks. All these measures can go an extended method in establishing a secure cyber area desired by the voters

Nothing in this world is perfect. The persons who legislate the laws and by-laws are also not perfect. The laws therefore enacted by them cannot be perfect. Indian cyber laws have emerged from the womb of globalization. It is at the threshold of development. In due course through exposure to varied and complicated issues, it will grow to be a piece of its time legislation.

REFERENCE

- Cyber crimes and society study martials of pgdclcf ded national law school of India university
- Cyber crimes and society study martials of pgdclcf ded national law school of India university
- Cyber crimes and society study martials of pgdclcf ded national law school of India university
- Information technology act 2008 sec 66f

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

BLUETOOTH TECHNOLOGY & HACKING THREATS!

Ramesh Ogania[1] and Dr. Leena Sarkar[2]
[1]Cyber Forensics Professional & Cyber Law Consultant, Founder, Hexa Digital Forensic Corporation
Associate Professor & Principal[2], Department of Chemistry, J. V. M's Degree College, Navi Mumbai

ABSTRACT

"It is very necessary to know Security aspects of Any Technology before adopting it"

We found that Mobile Computing is growing rapidly and manufacturers of mobile computing devices are embedding new features in their latest products. Bluetooth is the basic feature of mobile computing now. We may rarely find any mobile computing devices, not embedded with Blue tooth feature, whether it is Mobile phone or PDA or TAB or Laptops.

Bluetooth Wireless technology standard was launched in the year 1998. This low-power solution will permit upto eight Bluetooth enabled devices to function with each other without line-of-sight restriction, even through walls. It utilizes short-range radio to exchange information among networked devices, enabling effortless wireless connectivity between mobile phone, mobile PCs, and handheld computers. The Bluetooth technology simplifies access to other networks. This is done by recognizing and connecting to different types of networks through a Bluetooth connection. Bluetooth wireless technology is an open specification for a wireless personal area network. It provides limited range RF connectivity for voice and data transmissions between information appliances. To connect two or more Bluetooth Devices pairing is required. "Pairing" means the Handshaking process between devices to authenticate further sharing of data. Passkeys require to pair, but are not always necessarily required! Nowadays Bluetooth technology is no longer short range radio technology.

Through this paper, we have explained Bluetooth Technology and Its Vulnerabilities identified so far, types of Bluetooth attacks, Tools used for Bluetooth attack or Bluetooth Hacking, Risks involved in using Bluetooth technology, precautions for using Bluetooth technology, and the difficulties which may arise during Forensics and Investigation of Crime incidents where Bluetooth technology is used.

Keywords: Bluetooth, Bluetooth Technology Pairing, The SNARF attack, The BACKDOOR attack, The BLUEBUG attack, Bluejacking attack, Bluestumbler, Bluebrowse, Bluejack, Bluesnarf, Bluebug, SpoofTooph, Vcard Blaster, PwnTooth, Challenges in Bluetooth Forensics, Precautions for Bluetooth users, GSM, CDMA, IMEI, Mobile phones, PDA.

INTRODUCTION TO BLUETOOTH TECHNOLOGY

It is named after tenth-century Danish King Bluetooth which invokes images of Viking conquests and plundering; notwithstanding this, the good king Harald Blatand is credited with uniting Denmark and Norway during high reign. Similarly today Bluetooth unites technologies. Bluetooth wireless technology is an open specification for a wireless personal area network. It provides limited range RF connectivity for voice and data transmissions between information appliances. Bluetooth wireless technology eliminates the need for interconnecting cables and enables ad-hoc networking among devices.

Bluetooth wireless technology will allow seamless interconnectivity among devices. Computers and personal digital assistants (PDAs) will share files and synchronize databases remotely; Laptop will access e-mail by linking to nearby cellular phones, and wireless headset will permeate the cellular phone market to simplify hands-free operation.

Bluetooth is a low-cost, low-power, short-range radio that communicates data and voice in point-to-multipoint networks from 10 meters or 32 feet (up to100 meters or 328 feet with an amplifier). Bluetooth transfers data at rates of up to 721 kilobits per second. Bluetooth is a technology designed to manage the complexities of network management, data security, device synchronization, power consumption and basic connectivity between cellular phones, laptop computers, and personal digital assistants (PDAs).

The technology can send and receive e-mail on a mobile computer via a mobile phone, even when the devices are not within line-of-sight. All bluetooth-enabled devices can be set up so that they automatically exchange information and synchronize with one another. For instance, if we accept an appointment on your handheld device, the appointment is automatically accepted in our desktop PC as soon as the two devices are within range of each other. The technology is expected to make the electronic world less dependent on connecting cables. For example, computers will be able to exchange data quickly with wireless phones and handheld devices. Cell phones are expected to be able to download voicemail onto a computer hard drive for storage. Computers may

ISSN 2394 - 7780

be able to play music through wireless speakers positioned across the room. Motorola has developed a Bluetooth car kit that will enable a hands-free wireless car phone to transfer calls to a nearby cellular handset. It will also make Bluetooth clip-on products for its wireless phones, and it is developing Bluetooth chips for incorporation into a variety of devices.

To connect to other blue tooth device, pairing is required. Pairing is the process of handshaking between two or more blue tooth devices.

Pairing: *"Paring" means* the *Handshaking* process between devices to authenticate further sharing of data. *Passkey*s require to pair. To connect two or more Bluetooth Devices Paring is required. *But is not always necessarily required!* Pairs of devices may establish a trusted relationship by learning (by user input) a shared secret known as a *passkey*. A device that wants to communicate only with a trusted device can cryptographically authenticate the identity of the other device. Trusted devices may also encrypt the data that they exchange over the airwaves so that no one can listen in. The encryption can, however, be turned off, and passkeys are stored on the device file system, not on the Bluetooth chip itself. Since the Bluetooth address is permanent, a pairing is preserved, even if the Bluetooth name is changed. Pairs can be deleted at any time by either device. Devices generally require pairing or prompt the owner before they allow a remote device to use any or most of their services. Some devices, such as mobile phones, usually accept OBEX business cards and notes without any pairing or prompts.

Flaws: Serious flaws in Bluetooth security lead to disclosure of personal data.

There are serious weaknesses in the authentication and/or data transfer mechanisms on some Bluetooth enabled devices. Specifically, three vulnerabilities have been found:

Firstly, confidential data can be obtained, anonymously, and without the owner's knowledge or consent, from some Bluetooth enabled mobile phones. This data may include the entire phonebook, calendar and the phone's IMEI.

Secondly, it has been found that the complete memory contents of some mobile phones can be accessed by a previously trusted ("paired") device that has been removed from the trusted list. This data includes not only the phonebook and calendar, but media files such as pictures and text messages. In essence, the entire device can be "backed up" to an attacker's own system.

Thirdly, access can be gained to the AT command set of the device, giving full access to the higher level commands and channels, such as data, voice and messaging. This third vulnerability was identified by Martin Herfurt, and they have since then started working together on finding additional possible exploits resulting from this vulnerability.

Finally, the current trend for "Bluejacking" is promoting an environment which puts consumer devices at greater risk from the above attacks.

Vulnerabilities in Bluetooth: There are some technical weaknesses found in Bluetooth technology. One can use, some of these techniques to get access to the Bluetooth enabled devices. Following are the some of the Vulnerabilities which hackers can use to hack or access the data.

The SNARF attack: It is possible, on some makes of device, to connect to the device without alerting the owner of the target device of the request, and gain access to restricted portions of the stored data therein, including the entire phonebook (and any images or other data associated with the entries), calendar, real-time clock, business card, properties, change log, IMEI (International Mobile Equipment Identity , which uniquely identifies the phone to the mobile network, and is used in illegal phone 'cloning'). This is normally only possible if the device is in "discoverable" or "visible" mode, but there are tools available on the Internet that allow even this safety net to be bypassed.

The BACKDOOR attack: The backdoor attack involves establishing a trust relationship through the "pairing" mechanism, but ensuring that it no longer appears in the target's register of paired devices. In this way, unless the owner is actually observing their device at the precise moment a connection is established, they are unlikely to notice anything untoward, and the attacker may be free to continue to use any resource that a trusted relationship with that device grants access to. This means that not only the data can be retrieved from the phone, but other services, such as modems or Internet, WAP and GPRS gateways may be accessed without the owner's knowledge or consent. Indications are that once the backdoor is installed, the above SNARF attack will function on devices that previously denied access, and without the restrictions of a plain SNARF attack, and possibly the other services will prove to be available also.

ISSN 2394 - 7780

The BLUEBUG attack: The bluebug attack creates a serial profile connection to the device, thereby giving full access to the AT command set, which can then be exploited using standard off the shelf tools, such as PPP for networking and gnokii for messaging, contact management, diverts and initiating calls. With this facility, it is possible to use the phone to initiate calls to premium rate numbers, send sms messages, read sms messages, connect to data services such as the Internet, and even monitor conversations in the vicinity of the phone. The latter is done via a voice call over the GSM network, so the listening post can be anywhere in the world. Bluetooth access is only required for a few seconds, in order to set up the call. Call forwarding diverts can be set up, allowing the owner's incoming calls to be intercepted, either to provide a channel for calls to more expensive destinations, or for identity theft by impersonation of the victim.

Bluejacking *attack*: Although known to the technical community and early adopters for some time, the process is now known as "Bluejacking" has recently come to the forefront in the consumer arena, and is becoming a popular mechanism for exchanging anonymous messages in public places. The technique involves abusing the Bluetooth "pairing" protocol, the system by which Bluetooth devices authenticate each other, to pass a message during the initial "handshake" phase. This is possible because the "name" of the initiating Bluetooth device is displayed on the target device as part of the handshake exchange, and, as the protocol allows a large user defined name field - up to 248 characters - the field itself can be used to pass the message. This is all well and good, and, on the face of it, fairly harmless, but, unfortunately, there is a down side. There is a potential security problem with this, and the more the practice grows and is accepted by the user community, and leveraged as a marketing tool by the vendors, the worse it will get. The problem lies in the fact that the protocol being abused is designed for information exchange. The ability to interface with other devices and exchange, update and synchronise data, is the raison d'etre of Bluetooth. The bluejacking technique is using the first part of a process that allows that exchange to take place, and is therefore open to further abuse if the handshake completes and the "bluejacker" successfully pairs with the target device. If such an event occurs, then all data on the target device becomes available to the initiator, including such things as phone books, calendars, pictures and text messages. As the current wave of PDA and telephony integration progresses, the volume and quality of such data will increase with the devices' capabilities, leading to far more serious potential compromise.

Tools: There are some tools available to hack in to the Bluetooth Devices

- **Bluestumbler** - Monitor and log all visible Bluetooth devices (name, MAC, signal strength, capabilities), and identify manufacturer from MAC address lookup.
- **Bluebrowse** - Display available services on a selected device (FAX, Voice, OBEX etc).
- **Bluejack** - Send anonymous message to a target device (and optionally broadcast to all visible devices).
- **Bluesnarf** - Copy data from target device (everything if pairing succeeds, or a subset in other cases, including phonebook and calendar. In the latter case, user will not be alerted by any bluejack message).
- **Bluebug** - Set up covert serial channel to device.
- **SpoofTooph**: Spoofing, obfuscating and cloning Bluetooth Device Profiles or ids. This tools is new tool developed by JP dunning and presented in DEFCON 2010. This device can be used for obfuscation, impersonation and observation of searchable Bluetooth devices. It also clone the profile of any Bluetooth device.
- **Vcard Blaster**: vCardBlaster is capable of sending a constant stream of vCards over Bluetooth. Users can select a single target or attack all devices in range vCards can be specified or generated by vCardBlaster. vCardBlaster can be used to preform a DoS (Denial of Service) Attack on a Contact List.
- **Blueper:** Blueper is capable of sending a constant stream of files over Bluetooth. Users can select a single target or attack all devices in range. Files can be specified or generated. User can specify file size.
- **PwnTooth:** Suite of Bluetooth attack tools. Designed to automate multiple attacks against multiple targets. Comes bundled with tools like: 1. Bluetooth Stack Smasher, 2. BT_AUDIT, 3. Bluesnrf, 4. Blueper/vCardBlaster. http://www.hackfromacave.com/

Long range Bluetooth Antenna: When Bluetooth invented in early 1998 it was Short range low-power wireless personal area networking technology but now it is no longer short range technology you will find long range antenna which Equipped with an extremely powerful, highly sensitive Bluetooth transmitter, the device can achieve an unparalleled ***range of up to 30 km*** with professional installation. And it can be easily attaches to any computer with a USB port, giving it long-range capabilities. And it works seamlessly with Windows, Mac

ISSN 2394 - 7780

and Linux supporting virtually any Bluetooth profile available. Uses include standard data, streaming data, headsets communication (like Skype calls), and stereo headphone communication, amongst others.

Challenges in Bluetooth Forensics: Cyber Forensics professionals and examiners may face many challenges while investigating any incident where perpetrator uses Bluetooth technology.

Bluetooth device even if paired with other device it is not storing device details except name and MAC id which is easily spoofable.

If hacking incident has executed from long range device antenna than it is very difficult to catch perpetrator. Sometimes Bluetooth device does not record processes executed in the device.

It is very difficult to prove ownership of the device with perpetrator based on only device name and MAC id. In case of Mobile it is not linking or storing with IMEI number or GSM/CDMA service number.

Sometimes the victim may face prosecution if his/her device is used remotely by perpetrator using Bluetooth technology.

Precautions for Bluetooth users : Some of precautions recommended in general for users of Bluetooth embedded mobile device are as follows:

1. Always Keep Bluetooth Service of your device in OFF mode, you should switch ON only if necessarily needed.
2. Never use Simple Pass Key Like 0000 or 4444 which can be easily guessed.
3. Never Use Bluetooth device in Public places like Markets, Cinema Hall, College Campus, Railway Stations, Bus stops.
4. Never Share Bluetooth service with unknown person.
5. Always delete paired device list after exchange of data is over and repaired the device again if needed.
6. Do not install illegitimate software in your device it may have Trojan Virus which enables Bluetooth or all services for hackers without your knowledge.

CONCLUSION

Bluetooth Technology is low power, low cost technology for wireless communication and has to be used with due diligent precautions.

REFERENCES

1. http://rfdesign.com/
2. http://www.bluetooth.com
3. www.bluetooth.com
4. http://www.hackfromacave.com/
5. **Hacking Bluetooth enabled mobile phones and beyond** By *Adam Laurie Marcel Holtmann Martin Herfurt*
6. Thanks to all developers & Companies other than above mentioned list whose products name have appeared in this paper.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

FORENSIC INVESTIGATION OF DRONE

Needa Ashraf Petkar
Department of Digital & Cyber Forensics, Institute of Forensic Science, Fort, Mumbai

ABSTRACT
Due to emerging drone technology, there is an increase in crime committed. This is because of its carrying capabilities, affordability, and easy accessibility. Thus, forensic analysis of drones and its devices is necessary. This paper aims at identifying, extracting and analyzing the shreds of evidence using some basic scripts and forensically sounds tools so that it could be used as digital evidence.

Keywords:- Drone Forensics, adb, Android Backup Extractor, Autopsy, DAT File Structure, Drone, DROP, Forensic Workstation, FTK Imager, Hex Editor, IDA-Pro, JD-GUI, Mobile Forensics, NMAP, TXT File Structure, UAV.

INTRODUCTION
UAVs (Unmanned Aerial Vehicles) or Drones is a small pilotless aircraft. Widely used in the military, photography/videography. Working of the drone can be divided into two parts: first being the drone itself and second being the controller. Some drones, no longer require a controller but use GPS transmitters to follow any direction.

Various crimes are been committed using drones. Some of which includes delivery drugs and cell phones to prison [5], across the border [6], attaching guns or chainsaw [7], attack on personnel [9], privacy invasion, terrorist activities[1], vandalize billboards, disrupt sports events, and so on. Digital evidence that can be obtained is ID of the drone, location of the use of drones, image/video captured, logs and the software used. Realm of this paper is to obtain information and analyze it by using some scripts, open source tools and static and live forensic techniques.

FORENSIC PROCESS FOR DRONE INVESTIGATION
It includes main steps such as Device Acquisition, Evidence Identification Accessing the data, Data Analysis, Reporting and Presenting the evidence. Forensic Tools normally take snapshots of the systems at a particular point of time. Operational Analysis of a UAV or drone requires the understanding of

1. Various systems interacting with each other during a flight.
2. Operation of a single UAV over various multiple flights.
3. The logistics behind the operation over a long period of time.

All the components of the device have to be analysed in order to obtain the desired result. Forensic Image of drone and application is to be acquired and later scan by fsck.f2fs for file system errors.

DEVICE ACQUISITION
1. Animals- Dutch National Police use Eagles to captures drones[13].
2. Ballistic- Capturing drone using nets or shooting down by a gun[13].
3. Client-Based Attacks- Vulnerabilities in the UAV application can be found using reverse engineering.
4. Cloud-based attacks- Cloud-based control software is used to manage UAVs and vulnerabilities can be found.
5. Jamming- Jam directional instructions or positional data being received by UAV.
6. MalDrone- It remotely installs malware onto a flying UAV and hijacks the operations[8].
7. Skyjack- It is a program that detects UAVs, deactivates connected client and connects itself to UAV as owner[14].
8. Spoofing- RF or GPS spoofing techniques is used to relay false information to make it land.
9. Water- US fire departments have used hoses to take down drones[13].

EVIDENCE IDENTIFICATION
An investigator has to think in 3 particular ways in order to acquire forensic evidence, which are, Physical, Process and Flow.

ISSN 2394 - 7780

A. Physical

Evidence obtained immediately& physically, including Drone/UAV, Battery, Sensors, Flight Controller, Ground Control Station/Base Station (GCS), Management/Analysis System, etc.

B. Process

Depending on the steps required to make the drone functional as well as the type of activity the drone is involved, each step and component leaves behind evidence and generates intelligence. Various parameters to be kept in mind are shown in fig.1.

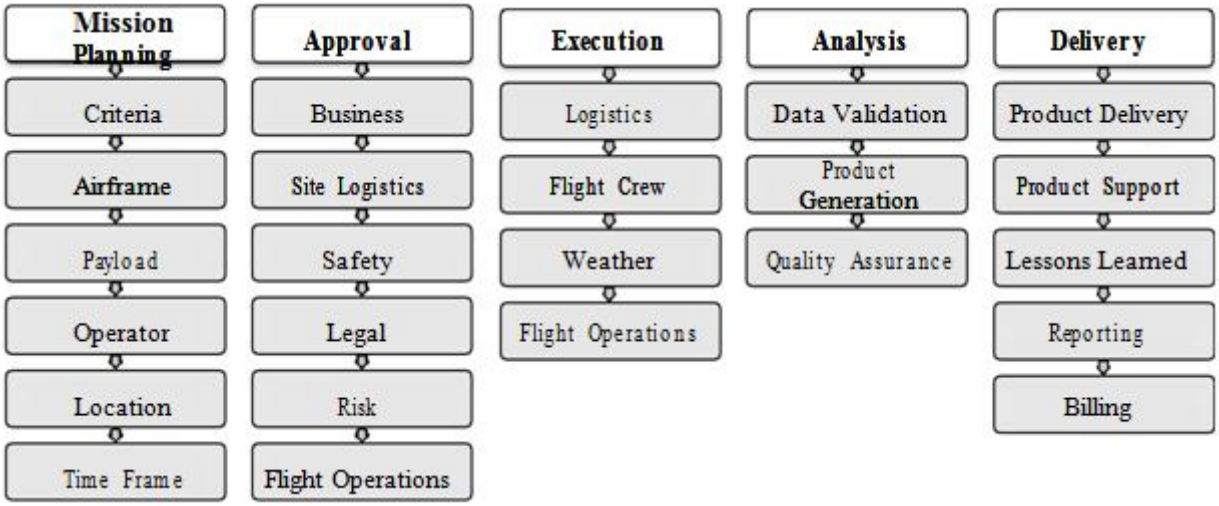


Figure-1: Drone Implementation Process

C. Flow

It is the way through which the data flows to and from the drone[4].

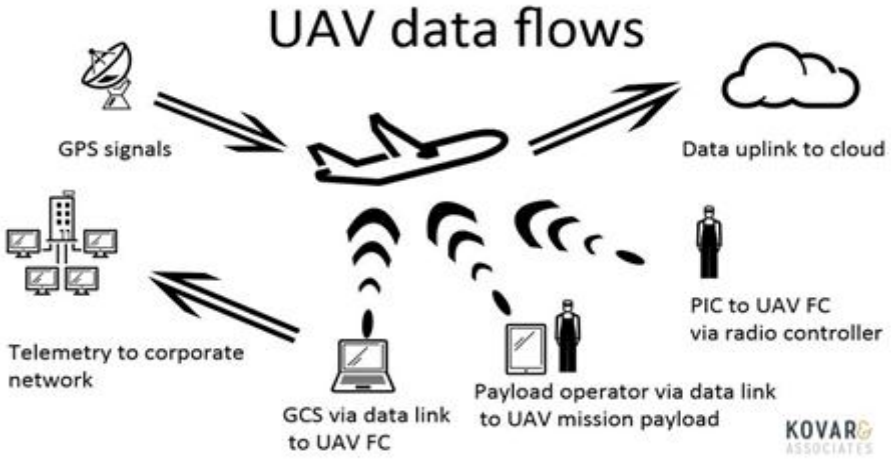


Figure-2: UAV Data Flow

DATA COLLECTION

Evidence from a Drone or UAV can be collected in two ways,

Normal Data Collection

It includes mechanisms or tools provided by the Vendors /Suppliers. These tools or mechanisms help in obtaining data from Drone as well as mobile applications if any. The methods include,

1. Tools from Vendors, Suppliers.
2. Data synchronisation with Third Party Apps or Sites provided by the Vendor/ Supplier.
3. Viewing the digital media on the computer through USB or direct mounting.
4. This method is sufficient in some situations but is not forensically sound because,
5. Access to all sources of data may not be possible.
6. Data tampering may take place during collection.

ISSN 2394 - 7780

B. FORENSIC DATA COLLECTION

It is the use of a forensically sound method to extract data using tools. Some of which includes scripting tools (Bash, Perl, Python, C), open source tools (Winhex, Hex Editor, NMAP, Autopsy, FTK Imager, exifTool, fsck.f2fs, dex2jar, JD-GUI, DatCon)

ACCESSING THE DATA

A. ANDROID BACKUP

It is the backup of the mobile/tablet which is used as a ground control station (GCS). The GCS contains information about camera feed (live), GPS, battery information, user commands-takeoff and landing, owner data, application data and usage logs, etc. Logical backup can be executed using adb backup-all and Android Backup Extractor is used to extract the backup file to a .tar file [10]. It is then decompressed to a directory containing each application files. It is recommended to create a physical image of the android device

B. ANDROID STORAGE

The mobile device's non-volatile internal storage contains the user data. The device is to be connected to the forensic workstation and then the files can be analysed within the computer.

C. DRONE STORAGE

1. Drone, non-volatile internal storage contains flight records. This can be acquired in three ways.
2. Forensic Workstation can be used to manually access the files.
3. Physical image of the internal storage can be acquired using disk dump utility (dd).
4. The internal SD card is pulled out and forensically acquired.

5. External SD Card

Gimbal camera system uses an external SD card to store images and videos. From Gimbal rig, extract the microSD card and insert it into Cellebrite write-blocker. Generate MD5 hash and store it. Dump the entire disk using dd into an image file and verify the hashes. Open the image file in FTK Imager and extract the content into a folder. Use Autopsy for cross-validation. These files contain images, videos and metadata.

DATA ANALYSIS

A. Black Box

Blackbox is similar to airplanes' blackbox. It is important evidence, containing every detailed element with different messages to let us know what took place at a particular instance. It includes Battery Serial Number, Battery Status, Battery Voltage, Flight Controls, Flight Status, Gimbal, Message Config, Message Console, Message-ID, Motor Status, Position, Telemetry, and Vision Positioning.

B. Flight Data

There are two files for flight data- TXT file (Mobile application) and DAT file (Drone), acting as the electronic flight recorder. Proprietary format is used to encrypt and encode both the files. Decryption and decoding of these files, yields data about flight status, GPS, motor, remote control and other information.

DAT Files

These follow a common naming conventionofFLY###.-DAT (#=number). It contains data relating to flight status, location, and sensor readings. Files are extracted from the Drone's SDcard. DatCon tool yields better output, converts binary DAT file into CSV file[2]. The first bytes of the file represents header, date and time. The data packets depend on the type of data is being written. After the message byte, there is a 4bytes internal bus clock tick number.

EXIF Data

It provides camera and location data of the picture taken [4]. To analyse EXIF Data, exifTool is used [12]. Basic script is written to automate extraction of GPS coordinates and the time-stamped flight log. The script executes exifTool on all files, providing GPS data to 6 decimal places. It is filtered to obtain a 'GPS position' and 'Create Date'.

TXT Files

These follow the standard naming convention of FlightRecord_YYYY-MM-DD_ [HH-MM-SS].txt. The date and time correspond to the drone flight initialisation. It contains data regarding battery levels, flight status, location, etc in form of packets. These packets decrypted and decoded using IDA-Pro. Its file structure is ascertained using reverse engineering. The application's .dex file is converted to .class (jar) file using des2jar and is decompiled using JD-GUI, allowing viewing all the java class files.

ISSN 2394 - 7780

Manual Inspection within the Android App and Hex-Editor help in understanding the structure. The last bytes of the files contain information of the device and flight, geotag of the place it took off. Owner's name will be seen in the next bytes. It is followed by 4 identification numbers-Inertial Measurement Unit (IMU), Camera serial number, Controller Circuit Board and Battery.

C. GROUND CONTROL STATION/ LAUNCH POINT EVIDENCE

The controller can be a mobile device or a radio controller. Evidence includes Laptops, Cell phones, Tablets, Removable Media, Default Settings, Launch Points, Dates, Owner Name, Account and other UAVs. Using the above-mentioned data, we can plot the path the user has used for flying. SN Number is a unique identifier for each component.

D. SENSOR DATA

Sensors attached to Drone for multi-functionality includes LIDAR, Optical, Thermo, WiFi, NVIR, GPS, etc. Metadata can also be obtained and provides insight into the locations where it had been, the potential objectives of the drone, etc. Some of the data is stored to the cloud, Facebook, Youtube, Data Mapper, Airware, Vendor specific websites, etc. The packet payload within DAT File contains data of sensor and telemetry.

1. Advanced Battery Payload contains detailed information about battery capacity, current, temperature and voltage for individual cells.
2. Battery Payload contains the overall battery level.
3. Flight Status Payload contains flight states, flight time(ms) and GPS related errors.
4. Gimbal Payload contains cameras positioning data.
5. GPS Payload contains 3-axis acceleration, altitude, gyro, location, magnetometer, velocity, etc.
6. Homepoint payload shows coordinates for homepoint.
7. The Motor payload contains the speed and load of all motors.
8. Remote Control payload contains the status of elevator, rudder and throttle.

STRATEGIC ANALYSIS

Here, the various perception of drone components usage is being analysed, whether the person has two or more drones and they share some of the same components. Launch point's specific for the drone, whether the location is a home, office, or any commercial facility, etc, are the questions that can reveal some interesting information. Basic scripts are used to obtain the following information:

1. Details of all devices those were turned on between any intervals of time from within a database.
2. Location of the device at a specific time
3. Information on the devices that share a common battery[4].

OPEN SOURCE TOOLS

1) DatCon is a java based tool, capable of parsing DAT files[2].
2) dji-log-parser is a browser operated tool and able to parse older TXT format[10].
3) DROP (Drone Open Source Parser) is a command line forensic tool. This tool uses Python 3.4 and is based on reverse engineering DatCon [3].
4) Healthy Drones is an online service to convert TXT files into CSV Files.
5) NMAP and Wireshark for Network monitoring.

CHALLENGES

Some of the challenges that are normally faced include integration with other tools, creating an alert system with an ability to set triggers for performing appropriate actions when new data is added, machine learning for patterns and connections. Some of the data is transmitted and stored in the cloud (user's as well as the manufacturer's account). Manual extraction of this data is extremely complicated.

CONCLUSION AND FUTURE WORK

It is possible to forensically identify and acquire locations, flight times and other relevant data which can add value to a potential case. With regards to forensic analysis of drones, little work has been published. As technology grows, better forensic methods for acquisition and analysis have to develop. Further work has to be

ISSN 2394 - 7780

conducted for different types of drones present today. Work has to be done in reverse engineering the firmware. The Tool has to be developed to map the route of drone from launch point to land site.

ACKNOWLEDGEMENTS
I would like to express my deepest gratitude to my parents, family, friends, and colleagues for the continuous support, especially Mr Ramesh Ogania, my professor and Mr Prasad Borvankar, my mentor, for providing valuable insights pertaining to this domain.

REFERENCES

1. M.Azhar , T. Barton and T.Islam, "Drone Forensic Analysis Using Open Source Tools", *Journal of Digital Forensics, Security and Law*: Vol. 13 : No. 1 , Article 6, March 2018.
2. DatCon. https://github.com/BudWalkerJava/DatCon
3. D. Clark, DROP-DRone Parser. https://github.com/unhcfreg/DROP
4. D.Kovar, Drone Forensics, 2015. https://files.sans.org/summit/Digital_Forensics_and_Incident_Response_Summit_2015/PDFs/ForensicAnalysisofs UASakaDronesDavidKovar.pdf
5. H.Smith, "Courts Crack down on drones delivering drugs to UK Prison" in *Independent*, 2007.
6. K.Davis, "Drug drone operator sentenced; just wanted pot", 2016.
7. "KILLERDRONE!Flying chainsaw", https://www.youtube.com/watch?v=6Viwwetf0gU
8. MalDrone - http://garage4hackers.com/entry.php?b=3105
9. M.D Shear and M.S Schmidt, "White House Drone Crash Described as a U.S. Worker's Drunken Lark", 2015.
10. M.Franklin, dji-log-parser. https://github.com/mikeemoo/dji-log-parser
11. N.Elenkov, Android Backup Extractor. https://github.com/nelenkov/android-backup-extractor.
12. P.Harvey, Exiftool. https://github.com/exiftool
13. S.Hillary, 2016, "Six ways to disable a drone", Techtank. https://www.brookings.edu/blog/techtank/2016/03/16/six-ways-to-disable-a-drone/
14. Skyjack. https://github.com/samyk/skyjack

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

SOCIAL MEDIA FORENSICS WITH MOBILE FORENSICS

Manali Dhanawade
Pelorus Technologies Pvt Ltd. Andheri (East), Mumbai

ABSTRACT
This paper deals with a new challenge for digital forensic experts – the forensic analysis on social networks being used tremendously on the mobile phones. It is intended to find information on social media via mobile phone extraction. It covers the basics of social media, but not the very basics of investigative techniques. Mobile devices are an important evidentiary piece in digital investigation. In this paper, we report the results of our investigation and analysis of social media and instant messaging services being run on mobile devices. This deals with the analysis of various social media accounts being operated from the mobile devices.

I. INTRODUCTION
The forensic field is constantly changing, with the rapid development of technologies. Traditional forensic science has provided a foundation for legal proceedings for more than 100 years. This traditional forensic science has influenced a number of areas due to the increasing number of computer crimes. Digital forensics practitioners can learn much from the traditional forensic process. The distinction between digital forensics and traditional forensics started to become apparent the late 1980s responding to the growth of computer crimes. Since then, digital forensics has always referred to a method of collecting criminal evidence from any digital medium, in order to present it in a court of law. In the early digital forensics stage, investigators used the suspects‟ computers itself to obtain evidence. However the integrity of the evidence may be lost during the investigation process as the computer itself could alter the evidence. It is no longer practical to use the suspects‟ computer to obtain evidence. As a result, a number of digital forensic tools have been developed to help investigators do their work effectively and in a forensically sound manner. There are no standard tools for collecting or processing evidence from social networking environments. Even though there are a number of vendors now offering forensic tools, forensic investigators may face problems choosing the right tools when they may not fully understand the tools[1]. In the 2G and 3G era, Short Message Service (SMS) was a service broadly used by mobile phone users. However, it is very different in the 4G era, where SMS is used less and social media as well as social messenger applications keep emerging. Social media applications and social messenger applications are online media which can be used free of charge by users to share and exchange information in the form of text, picture, audio, or video through the Internet. Various well-known social messenger applications usually come with interesting features such as normal chat, private chat, message notification, location sharing, contact sharing, file sharing, and status updating systems. Based on statistical information in 2019, it is estimated that there will be around 2.77 billion social media users around the globe, up from 2.46 billion in 2017. The increased number of active users and the development of internet technology can give the opportunity for some individuals, groups of people or organizations to commit cybercrime [2]. Blackmailing, identity theft, transaction fraud, and other types of criminal acts using computers or smartphones are all considered as cybercrimes. Many kinds of social messenger applications are now available on Google Play Store and can be downloaded for free. Therefore, the fast growing market of social messenger applications raises concerns about privacy and security. .

II. RELATED WORK
A. MOBILE DEVICE FORENSICS
The initial research work in this field has focus on acquisition techniques and general forensic analysis of smart devices. It has also been observed that the heterogeneity in device hardware, software, ports, connectors, and so on poses a significant challenge to forensic investigators because Small Scale Digital Devices (SSDs) are more proprietary than the traditional personal computer [4]. Ayers, Brothers, and Jansen (2014) define mobile forensics as, “the science if recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods.” This is not an easy criterion to attain because of the constant release of upgrades and rapid changes of mobile device‟s operating systems versions, hardware, software and features requiring a mobile forensic tools company to continually update and keep up the forensic tools capability and compatibility with the newest models of mobile devices.

Kent, Chevalier, Grance, and Dang (2006) suggested Four Step Forensics process (FsFp) that can be used as one of the basic digital forensic investigation models. FSFP contains four phase processes: Collection, Examination, Analysis and Reporting as can be seen in Figure

ISSN 2394 - 7780

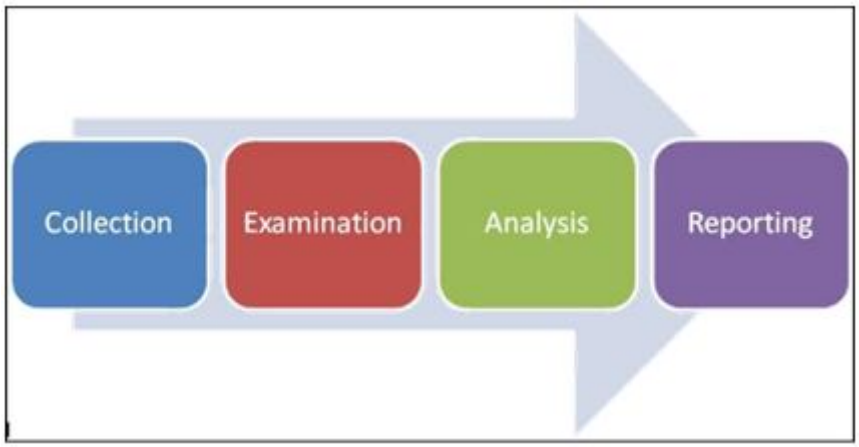


Figure-2.1: FSFP Forensic Investigation Model

MOBILE FORENSICS INVESTIGATING TOOLS

In the investigating process for combating cybercrimes that utilise smartphones and other mobile devices, gathering evidence in a forensic manner is required but challenging. With the general users of mobile devices and the intense use of social media applications on smartphones, the amount of smartphones evidence in each case can be an extremely high.

Technology has significantly contributed o criminal investigation. Various tools have been used to assist the forensics investigation including identification and examination processes. The tools enable forensic investigators to examine the evidence more effectively and in a forensically sound manner. One of the vital elements the digital forensics investigators needed in order to perform an effective forensics investigation is to have knowledge of the right tool for each criminal case scenario. Digital forensic tools that are utilised for investigation must be reliable and relevant in order to make evidence legally admissible in the court. In the following section, tools, which can be used for social media forensics investigation on Android phones will be evaluated and some information about their capabilities and limitations will be provided. Currently the two main mobile forensics tools that have been used in most police institution around the world are Cellebrite UFED and MSAB XRY.

This paper aims social media forensics with mobile forensic extraction with Cellebrite UFED for research and is used by law enforcement agencies and educational institutions. Cellebrite „Universal Forensics Extraction Device‟ (UFED). Cellberite UFED is a handheld device with optional desktop software, data cables, adapters and ther peripherals. The UFED additionally has integrated subscriber Identity Module (SIM) reader. Various mobile operating system (OSs) can be extracted by this tool, including iOS, Android, and Windows Mobile, and thousands of models of phones, tablets, drones and GPS devices.

The Cellebrite UFED enables the retrieval of subject data such as phonebook contacts, all types of multimedia content, SMS and MMS messages, call logs, electronic serial numbers (ESN), International Mobile Equipment Identity (IMEI) and SIM location information from both non-volatile memory and volatile storage via logical(“all visible stored data on mobile devices”), file system (e.g., directories and files), or physical extraction enables it to recover deleted information, decipher encrypted data, and acquire information from password protected mobile applications such as Facebook, Skype, Whatsapp and browser-saved passwords. UFED Cloud Analyzer assists law enforcement agencies and enterprises to enhance their investigations by extracting and displaying information from cloud-based data sources such as, Dropbox, Facebook, Twitter, Gmail, Google Drive, Google Contacts, Google Search History, IMAP, Instagram, etc. UFED Cloud Analyzer reduces the time required to solve cases: Real-time access to an extraction of private user data from key cloud-based data sources, such as social media, web mail and cloud storage sources, etc. Normalization of forensically extracted data into a common view so users can quickly search, filter and sort data.Creation of customized reports for easy review and data sharing. Data export into other analytics tools for further investigation.

B. SOCIAL MEDIA

The popular social media sites like Facebook and Myspace had studied the views on trust and privacy concern regarding sharing of information and new relationships. It is clear there is no much difference as privacy is concerned. It was found that majority of Facebook members were willing to share information than members of Myspace. Whereas Myspace members are more willing to interact with other new members of the site. This

ISSN 2394 - 7780

suggests that given in any social media platform, privacy and trust do not really matter when exchange of information or relationship building between the members.

According to (Lin& Lu,2011) one of the major factor people join social networking sites is for fun or enjoyment, and the other aspect is friends and real benefits of it. It was also known that men and woman have different influencing factors when it comes to joining social networking sites. One of the top reason is, woman is influenced by number of their peers in social media. Whereas men had no impact of friends or families, to join in a social networking site.

C. CYBERCRIME AND SOCIAL NETWORKING SITES

Cybercrime and social networking sites (Williams, Edwards, Horsley, Burnap, Rana, Avis & Sloan, 2013) focuses on social media users with the ability to monitor social media facts streams for signs of high tension which can be examined in order to detect deviancies from the „norm‟ (levels of interconnection/low tension). O'Keeffe & Clarke, 2011) explained spending time in social media Network sites is among the most common activity among the current generation of children and youngsters. Gaming sites, simulated worlds and video sites such as YouTube; and blogs offer youth a gateway for entertainment and interaction. This had grown tremendously in recent years. It is vital that parents become conscious of the environment of social media sites, given that not all of them are safe backgrounds for children and adolescentshis item takes a serious look at the means that public insights of cybercrime are made and uncertainties about it are produced. It discovers the varying conceptualizations of cybercrime before finding tensions in the making of criminological awareness that are causing the rhetoric to be chaotic with realism. It then differences the tradition of cybercrime with what is actually going on in direction to know the support gap that has unlocked up between public demands for Internet safety and its deliverySocial Media Forensic is a fragment of the Network Forensics. It is seen that various social sites such as Facebook, MySpace, Twitter, LinkedIn, etc. has been under various attacks and threats in the past. Attacks on social networking sites can take place from within the network/system or from outside the network[6]. Attacks like retrieving cookie information takes place from within a system where as attacks like Denial of Service (DoS) or DDoS takes place from outside the system. These sites are unguarded to many types of cyber-attacks. Researchers now a days study the point of vulnerability of these social networking sites, which can be termed as Social Network Forensics.

RESEARCH METHODOLOGY

Social Network Forensics and identified the importance of applications that can collect evidence from Social Networking Sites (SNSs) in a forensically sound manner. The approach to be used by the proposed study in identifying the most effective tool for SNS forensics will be tested and analysed by using three chosen forensic tools from the literature review. Namely – Cellebrite‟s UFED 4PC and UFED Cloud Analyser Bryson & Stevens (2002) aim to provide examiners with a number of concepts that assist in making a sound, rational decision to select forensic tools, as opposed to emotional, reactive, or externally motivated factors. The concepts proposed in this study help examiners to identify the strengths and weaknesses of the tools. Although this research argues that forensic examiner‟s knowledge and the methods used are more important than the technical efficacy of the tools, the principles of the study can also be applied to Social Network Forensics. “Computers may be running completely different operating systems and file systems in the future.. It is crucial to check functionality and abilities of the tools in multiple operating systems, and with different case scenarios.

DESIGN OF STUDY

The aim of the study is to conduct research concerning capabilities o elected forensics tools to develop potential and crucial data evidence from social media applications on smartphones in relation to social media-enabled crime investigations. By evaluating each tool information may be gained to improve the investigation processes. The selected forensic tools that were identified will be accessed and compared through an analysis of the data results. Those tool was examined over various Android version Smartphones. On each Android Smartphone, the social media applications Facebook, Twitter, Instagram, Gmail, Hangouts via the account package being extracted from the mobile devices.

In this study, there is a need to collect, analyze and interpret quantitative and qualitative data in one study, a mixed methodology consists of mobile forensics and social media forensics. The data will consist of how many instances of specified planted social media status (posts), photos, chat messages and videos in Android smartphones hat can be gathered by the selected mobile forensic tool.

In this research, all smartphones will be wiped before the evidence is planted. The step minimizes and eliminates unused excess data that can hamper the extraction process. Cellebrite UFED that is employed in this

ISSN 2394 - 7780

research is UFED 4PC and UFED Physical Analyzer and UFED Cloud Analyzer. UFED has more extraction type options, such as logical extraction, file system extraction, and physical extraction.

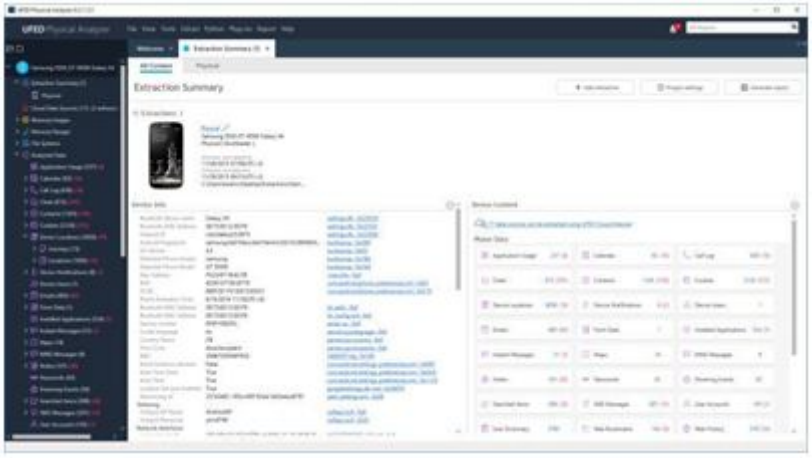


Figure-3.1**:** UFED Physical Analyser

Figure-3.2: UFED 4PC

Data Analysis chieving reliable outputs and results, with precise data analysis procedures are necessary for trustworthy findings. The first step is to acquire physical extraction of the android smartphones and get their ufd files. Here in this extraction the it includes all the hidden deleted data and all that the user does with its phone.

The second step is running the physical analyzer and exporting the account packages that are created with various accounts and on various applications being logged on. The third step is analyzing the output results for determining the tool capability.

Cloud Analyzer

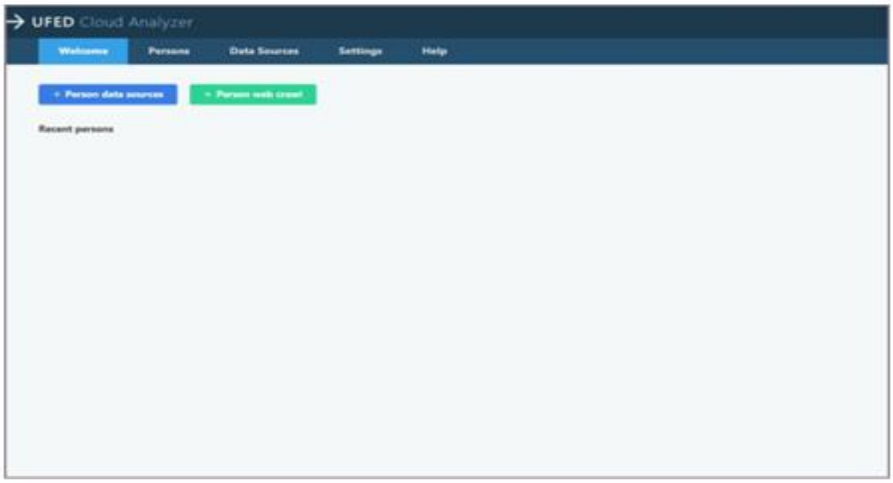


Figure-3.3: UFED Cloud Analyser Welcome Page

ISSN 2394 - 7780

The account package being exported during the physical extraction needs to be imported into the Cloud Analyzer UCAE files exported from UFED Physical Analyzer.

Once you have imported the data sources, the following window appears.

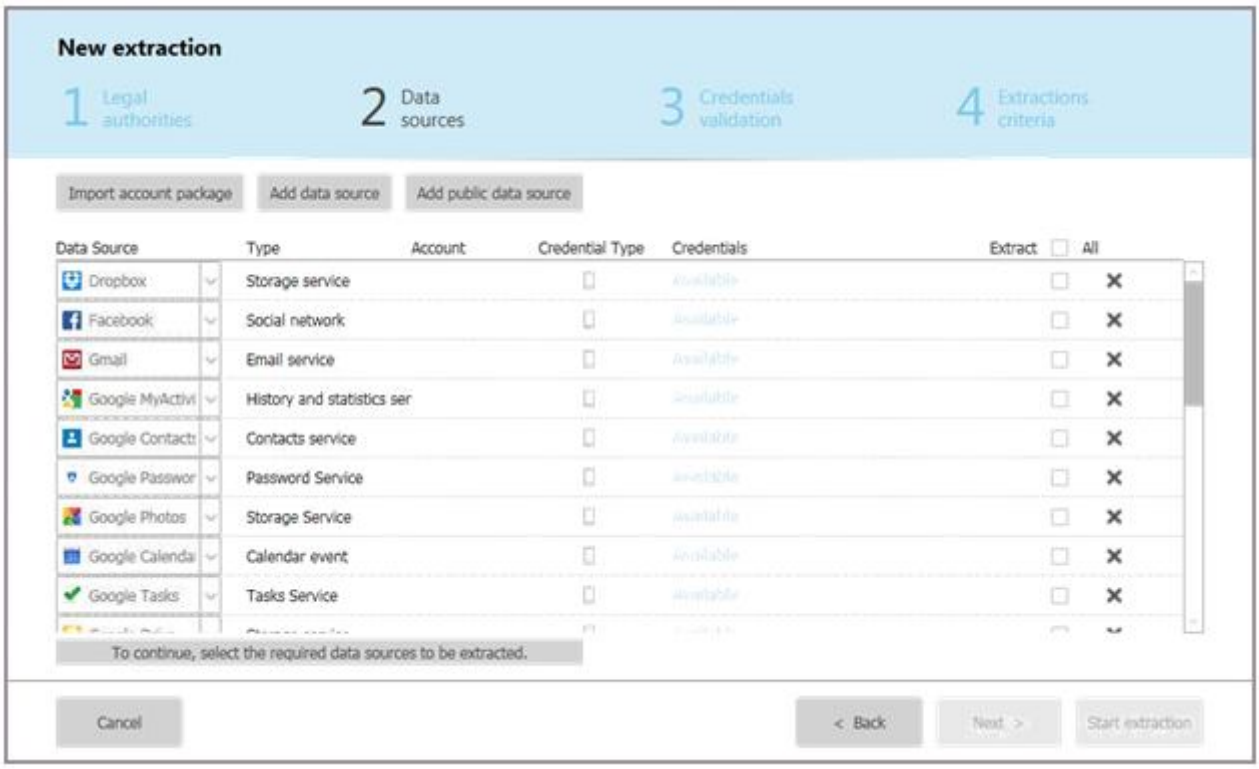


Figure-3.4: UFED Cloud Analyzer Importing Account Package Extract check box for each required data source (or select All).

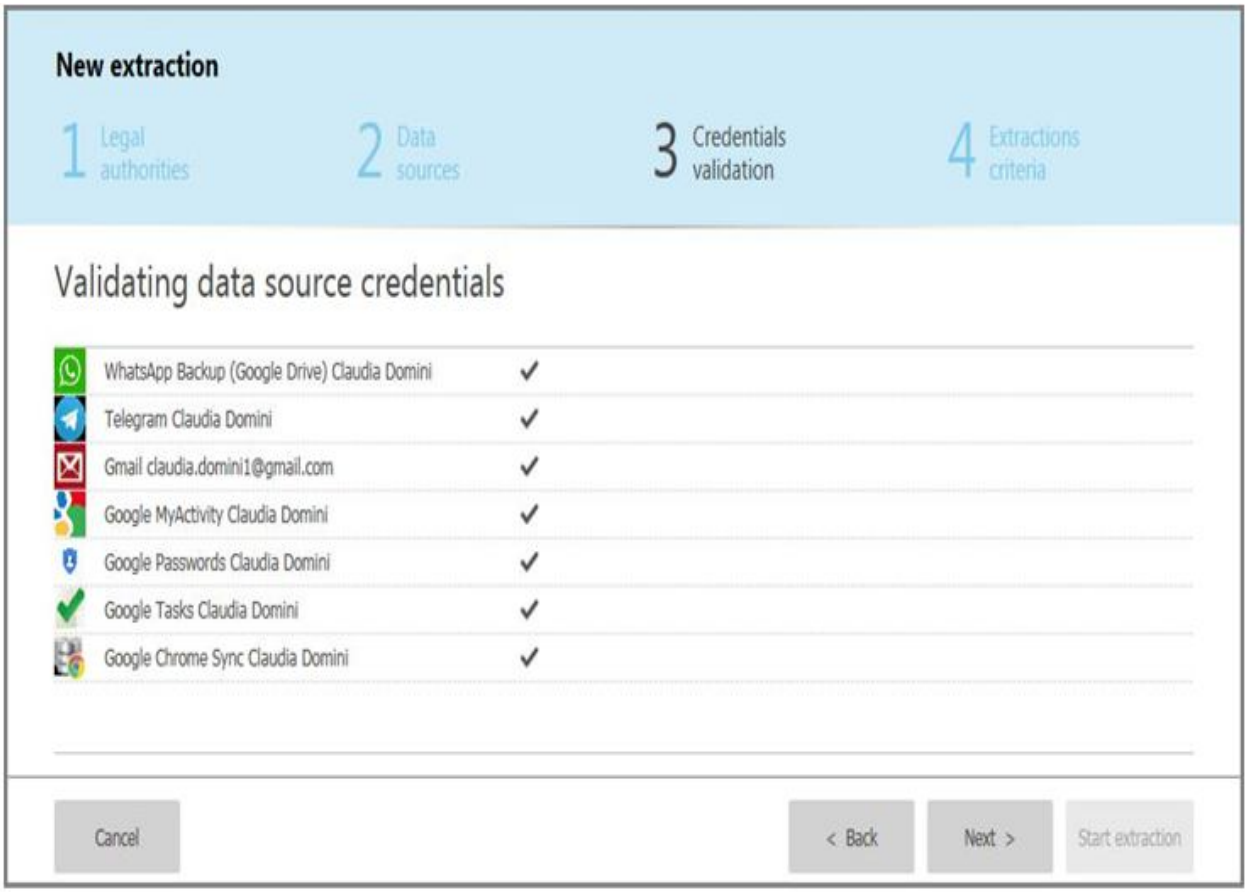


Figure-3.5: Validating credentials

ISSN 2394 - 7780

Clicking Next establishes a connection for credential validation with the cloud data source.

UFED Cloud Analyzer validates the selected data source credentials.

Some sources, will require additional validation steps:

a. If two-factor authentication is required, Two factor authentication

b. If CAPTCHA is required, see CAPTCHA

c. If a token has expired, it is sometimes possible to obtain the credentials using the Password collector

4. When the data source credentials have been validated,

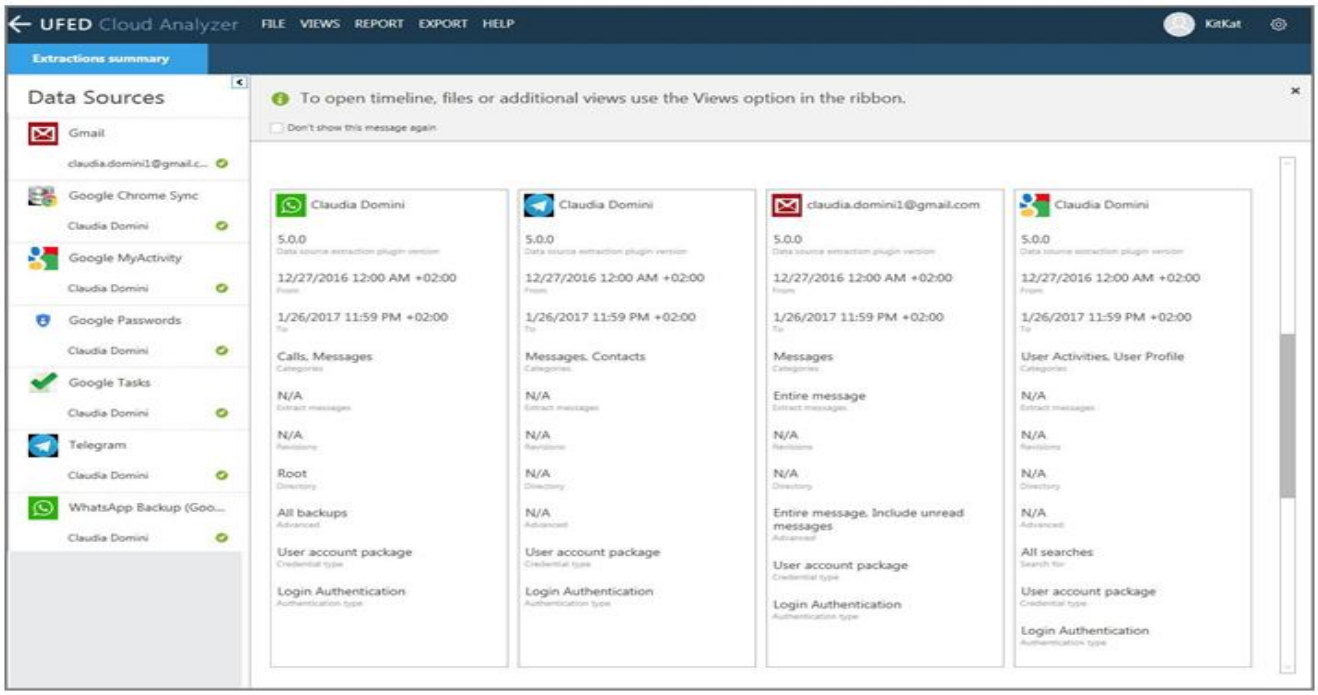


Figure-3.5: Various data Sources uploaded to the Cloud

The date range is related to the time the content was posted or uploaded to the cloud data source. The supported Content categories relate to the data artefact type, which may contain additional artifacts that are extracted as well. UFED Cloud Analyzer enables investigators to extract login credentials from account packages. Login credentials (aka "login keys") can be extracted from iOS and Android mobile devices and PCs.

The password collector helps investigators overcome expired tokens and gain access to apps which are not directly supported by UFED Cloud Analyzer.

Select the Password collector and proceed with the extraction. After the extraction is complete, click Views > Profile in the top bar. A list of the applications and their credentials will be shown.

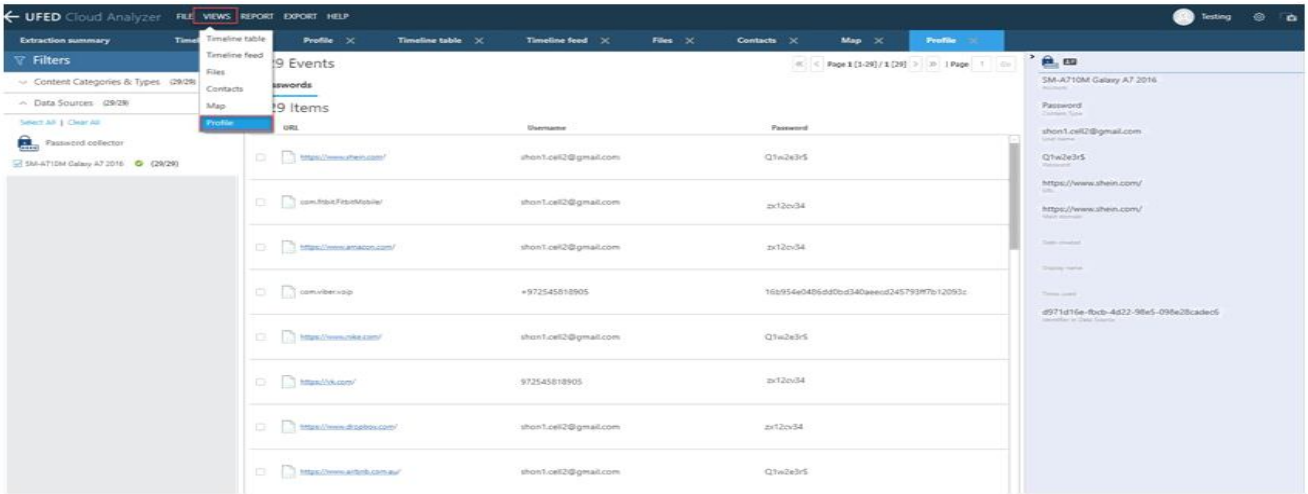


Figure-3.6: Password Collector

ISSN 2394 - 7780

Two factor authentication

Generally, two factor authentication is not required if using an account package originating from a phone extraction.

UFED Cloud Analyzer supports two factor authentication for the following data sources:

Coinbase:

Dropbox: After entering the credentials and clicking Next, you need to enter the Dropbox: verification code sent via SMS.

Facebook: UFED Cloud Analyzer recognizes that 2 factor authentication was enabled by the person. As part of the authentication process, after typing the person's user name and password you can enter the pin code to complete the authentication process. See Google Chrome sync: After entering the credentials and clicking Next, you need to enter the passphrase as specified in the Chrome encryption options.

Google: After entering the credentials and clicking Next, you need to enter the Google verification code sent via SMS

iCloud: You can access the iCloud device backup even when two factor authentication is applied by the user. When using the iCloud credentials to access the backup, you can select to which device you would like to send verification. The device can be selected from a list of authorized devices previously defined by the user. This provides better control over the process and reduces the number of alerts to the user.

Telegram: After entering the phone number and clicking Next, you need to enter the

verification number sent via SMS. If an account package originating from a phone extraction is being used, two factor authentication will not be required.

Facebook authentication

To use two factor authentication (Facebook):

Enter the user credentials and click Next. The following window appears

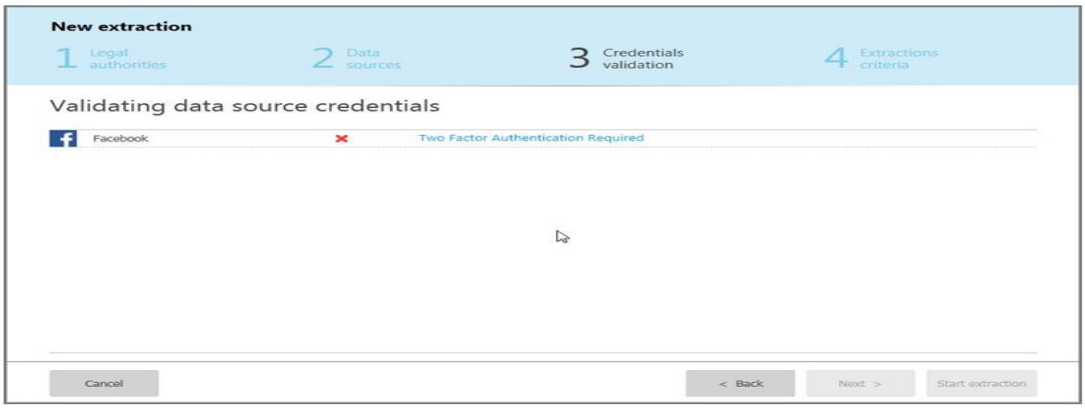


Figure-3.5: Click Two Factor Authentication Required

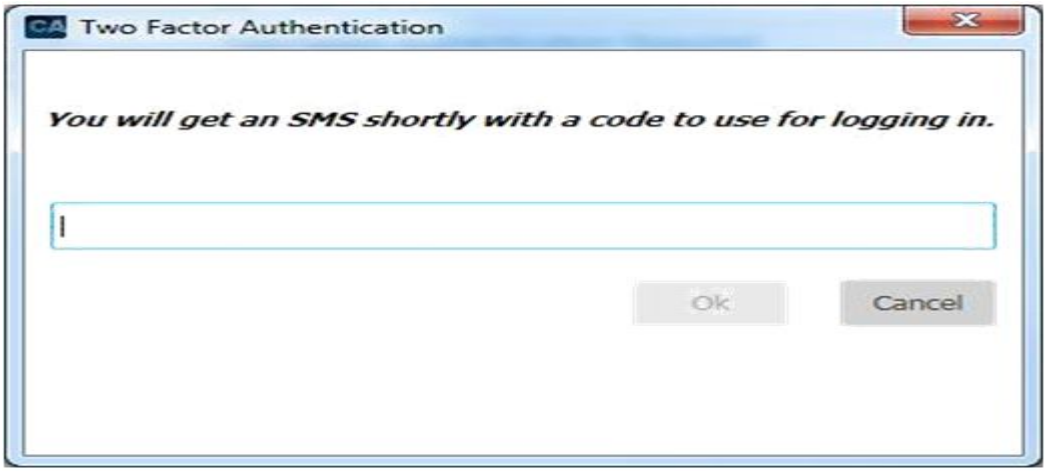


Figure-3.6: Verification code

ISSN 2394 - 7780

In case if the Account package is not extracted and the data sources are added anthan the investigator needs to enter the credentials manually. Here if the user has secured his account by the two factor authentication than various other ways are their for the authentication as shown above since the phone is being seized the investigator itself can get the data or the code and enter the it whereas the investigator can enter the credentials being obtained from the password collector which shows all the usernames and the credentials being obtained while extracting the device and getting a pathway to get the data and analysis of the various applications that has been logged on by the user and its activities done till the last login. Here various data be it instant messaging apps such as Whatsapp, Instagram and VIber data takes its data from the last google drive backup.

You can extract WhatsApp application backups of Android devices from Google Drive and WhatsApp application backups of Apple devices from iCloud. While the conversations are stored locally on the device, WhatsApp users can back up their content to the cloud and restore it on new devices. The backup contains all relevant information including chats and call log history. The frequency of the backups is defined by the user.

You can access the information stored on the cloud by relying on login information from the mobile device. The login information contains two elements, the Google/iCloud login information required to access Google Drive/iCloud Backup and a device key required to access the WhatsApp messages. If the Google login information has expired, you can use the credentials for the Google account, but to obtain the message you will also need the device key which is available in the account package generated by UFED Physical Analyzer. Without the device key, you can access the WhatsApp backup, however you will only have access to media files (photos and videos) attached to the message, without the message itself.

The Primary account is a WhatsApp Backup account of a mobile device from which the extraction was performed. It includes chats, calls and media files. The Other account is a WhatsApp Backup account to which only the Google credentials are available, and it includes only media files.

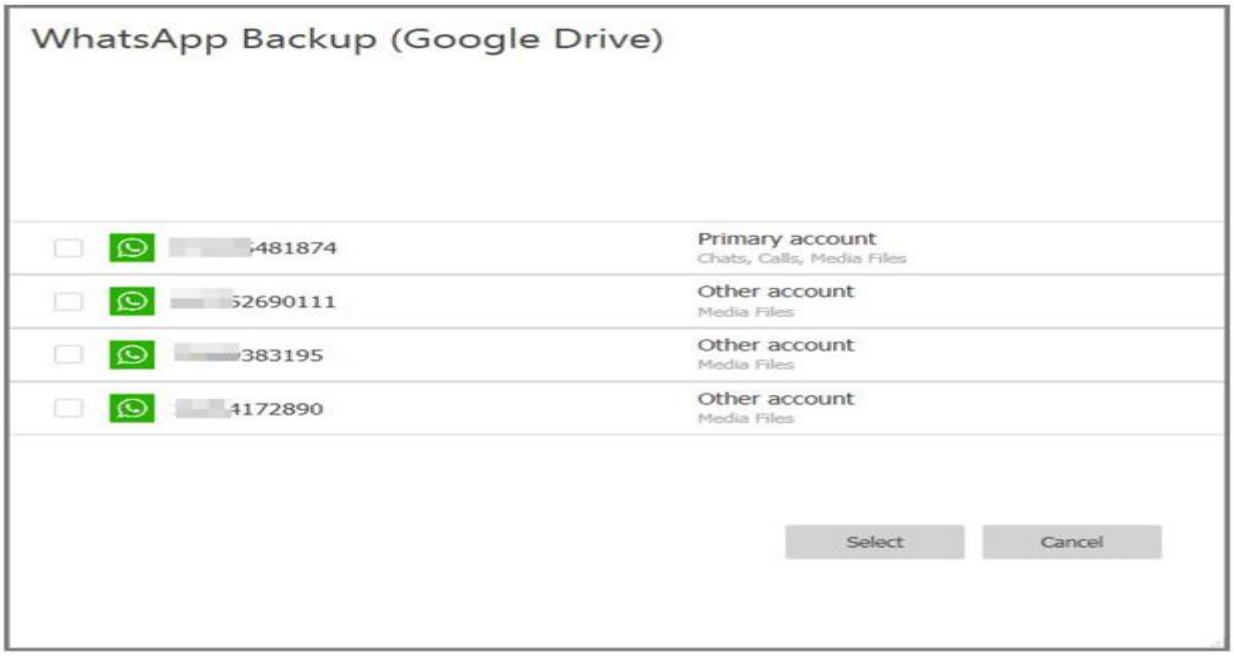


Figure-3.7: Whatsapp Backup

IV LIMITATIONS OF THE RESEARCH

The research evaluates two prominent mobile digital forensic tools‟ capability in the case of social media investigation on smartphones. When social media are involved in a crime, the investigator needs to choose digital forensic tools to examine, gather, and analyse the evidence from digital devices such as tablets, computers, and smartphones. Each of those devices is unique. They have been developed in their own particular ways. For that reason, for an investigator it is necessary to understand which digital forensic tools are capable to be used for investigating social media-enabled case evidence. Nowadays, the most frequent digital device that has evidence in a social media-enabled case is smartphones. Dealing with smartphones is not a simple task due to each of them having unique characteristics. Not only the evidence is distinctive but also the mobile forensic tool that is used for examination of smartphones has its own functionalities and limitations. In order to appropriately perform a forensically sound investigation, it is essential to identify those characteristics and limitations.

ISSN 2394 - 7780

CONCLUSION

The results and analysis of the research findings presents discovered relationships in the findings based on the test scenarios. The main focus of paper is on reporting the test results and presenting the tool assessment results in a visual format with the purpose to provide clearer visualisation of each smartphone forensic tool‟s capability and limitations in a social media investigation. Also presents the comparison data Cellebrite‟s UFED various tools that can allow the investigator to identify and then utilise the forensics tool effectively. Hence, by understanding each of tool‟s ability, it can reduce the investigation time and improve the extraction of evidence. In social media-related crime investigation process, understanding the capability of each forensic tool can help the investigator to work more effective when examining social media applications. As has been noted in the prior section, the mobile device forensic tools that are evaluated in Cellebrite UFED 7.1, performed variably the test scenarios. The recent version of each tool can be expected to improve and therefore can examine a greater variety of smartphones.

REFERENCES

1. Social Network Forensics: Evidence Extraction Tool Capabilities JUNG SON MNZCS, Postgrad Dip. Computing (UNITEC, NZ), Dip. InfoTech (AUT, NZ), Cert. Computing (AUT, NZ)
2. Android Forensics Analysis: Private Chat on Social Messenger G. B. Satrya, P. T. Daely, and S. Y. Shin IT Convergence Engineering Kumoh National Institute of Technology {gandevabs, 20156130, wdragon}@kumoh.ac.kr
3. Social Networking Applications on Mobile Devices By Noora Al Mutawa, Ibrahim Baggili and Andrew Marrington.
4. Forensic artifacts of the ChatON Instant Messaging application By Asif Iqbal 1, Andrew Marrington 2 , Ibrahim Baggili 3 Athena Labs 1 , Zayed University 1, 2, University of New Haven 3 Dubai, UAE asif@babariqbal.com, andrew.marrington@zu.ac.ae, ibaggili@newhaven.edu
5. Social Media Investigation: Mobile device Forensic Tools Capabilities By Stephanie Kartikamutiara Brennadiva
6. Social Network Forensics: Survey and Challenges by Urjashee Shaw Department of Computer Science and Engineering & IT, Assam Don Bosco University Guwahati, Assam, India Email: urjashee09@gmail.com , Dolly Das Department of Computer Science and Engineering & IT, Assam Don Bosco University Guwahati, Assam, India Email: dollydas.0901@gmail.com, Smriti Priya Medhi Department of Computer Science and Engineering & IT, Assam Don Bosco University Guwahati, India Email: smriti.medhi@dbuniversity.ac.in
7. Study on Effect of Social Networking Sites on the Young World of Cyber Crime by Sajeesh Hamsa Symbiosis Center for Management Studies, Symbiosis International (Deemed University), Pune; Dr. Archana Singh Symbiosis Center for Management Studies Symbiosis International (Deemed University), Pune; Prof. Nehajoan Panackal Symbiosis Center for Management Studies, Symbiosis International (Deemed University), Pune.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

TECHNIQUES USED FOR DATABASE SECURITY

Anindita Ghosh
Student, Institute of Forensic Science, Fort, Mumbai

ABSTRACT
Database security provides controlled, protected access to contents of database to preserve it's confidentiality, integrity and quality from threats that put documental assets at risk and can be occasioned in the form of fraud or unauthorized access, changing data values for reasons of sabotage, disclosing confidential data inappropriately etc. This paper will tackle methods of database security.

Keywords: security, Encryption, blockchain technology, cipher text, digital signature.

I. INTRODUCTION
Databases are the jugular veins of a business and hackers unleash attacks to gain access to sensitive information, extract value, steal backups and produce irregularities in databases. Database security begins with protecting the physical system that hosts DBMS and anything that prevents DBMS to achieve it's goals is considered a threat to database security. Some threats are:

- Insider threats
- Authentication, authorization& Access-Control (AAA)
- Privilege abuse- Legitimate/ Excessive/ Elevation
- SQL Injections
- Weak Audit Trail
- Database Platform Vulnerabilities
- Database Communication Protocol vulnerabilities
- DOS attack.

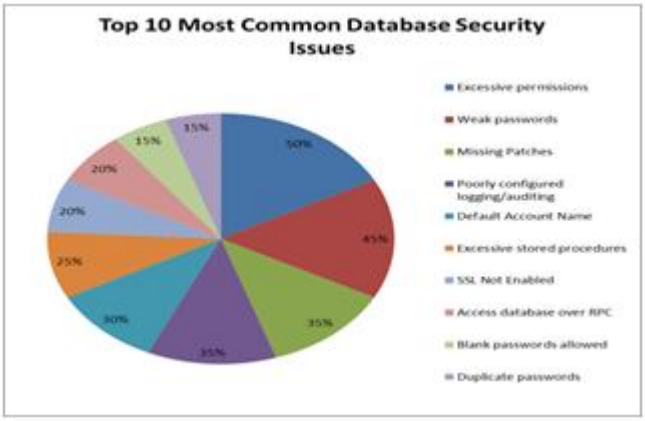


Fig-1: Threats to Database security

II. TECHNIQUES USED FOR DATABASE SECURITY
The key elements required to be preserved include integrity, authenticity, utility, confidentiality and non-repudiation.

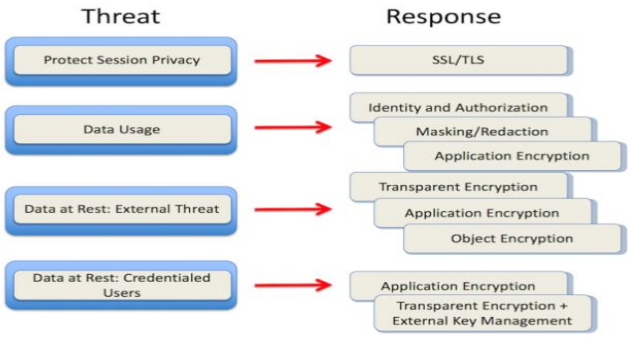


Fig-2: Measures to handle threats

ISSN 2394 - 7780

A. USING PASSWORDS

Using passwords to restrict excessive access can also be stated as the Principle of least privileges. Users are only granted the least amount of permissions for their legitimate purpose, thus preventing chances of legitimate Privilege abuse. The PoLP states that a request to a resource should be served with only minimum amount of privileges required to render the requested in a particular abstraction layer of any computing environment [1]. Application layer passwords need strong use of accounts that is having specific account to each service type and assign permissions accordingly. Restricting access to data through stored procedures allows to control data being submitted through procedure parameters, makes SQL injection attacks harder and doesn't expose databases.

B. ACCESS TYPE

There are two methods of access type-Remote access and local access.

- **LOCAL ACCESS ALLOWS THE WEB**

application and web database to be hosted on one server. This increases database vulnerability because intruder gets access to both database and web application if admin account for the server is compromised.

- **ON THE OTHER HAND, REMOTE**

access allows a secure connection establishment from anywhere with a remote computer network. It allows authorising users to work remotely, device provisioning and support and prevents access of every data object to unnecessary websites. It follows the norm that data should be treated on a "need to know" basis. It also includes not linking accounts, or store databases in directory with public sharing access as the relatively non-critical data provides back door to critical data elsewhere. Isolating data in discrete chunks with different users further help in protecting databases.

C. USE OF WEB APPLICATION FIREWALL (WAF)

It protects data from denial of service attacks, data or session hijacking, SQL injection attacks, XSS, as it filters, monitors and blocks HTTP traffic to-and-from web applications. It can either be network-based, host-based or cloud-based and is deployed as hardware appliance or through a proxy or server plug-in. Rule base is a set of rules that governs the content allowed through the firewall that work on Top Down principle, used to analyse 7 layer web application.

Top Down approach is essentially the breaking down of a system to gain insight into it's compositional sub-systems in a reverse format [2]. Rule bases have Source-Destination-Service-action format having 3 security models (SM);

- Blacklist/Negative SM
- Whitelist/positive SM
- Hybrid SM.

D. DATA & DATABASE ENCRYPTION

Encrypting doesn't avoid intrusion but hides personal and sensitive information, preventing information leak. For example: Passwords are hashed-&-salted (using algorithms like MD5, salts are keys specific to websites) for even more security. Encrypting all the database backups and avoiding its storage in publicly accessible locations like web folders, temporary partition ensures that the hacker cannot access the configuration files. The Three methods for database encryption:

1. **APPLICATION PROGRAM INTERFACE**

API that uses a code to edit relevant parts and encode the application layer i.e. encryption is done before data enters the database which makes it time consuming.

2. **PLUG-IN METHOD**

It attaches an encryption package onto DBMS and it allows for column level encryption, access control and auditing.

Each encryption package uses a 32-bit integer as a key identifier and if the specific plug-in supports key rotation, then encryption keys can be rotated to create a new version of the key.

3. **Transparent Data Encryption**

TDE requires the installation of an encryption/decryption engine directly into database engine as it performs real time I/O encryption & decryption of log files in order to protect data "at rest".

ISSN 2394 - 7780

TDE uses a DEK, which is a symmetric key secured by using a certificate stored in the master database of the server; or an asymmetric key protected by EKM module. For easy availability during recovery, DEK is stored in the database boot record [3].

TDE uses AES and 3DES algorithms to encrypt data without changing existing application.

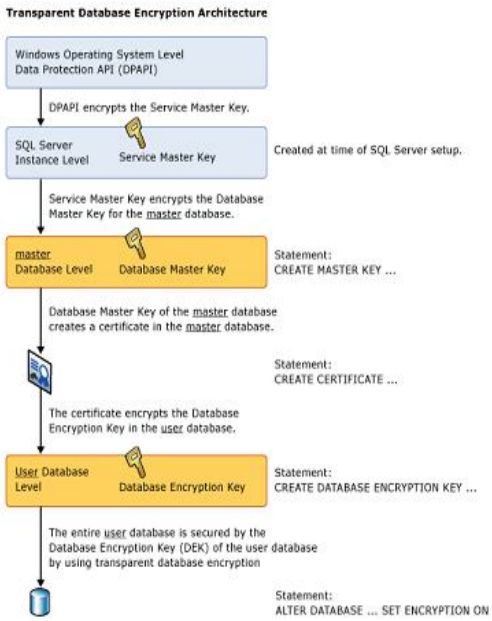


Fig-3: Transparent Database Encryption Architecture

E. MONITOR AND AUDIT DATABASE

Monitoring access and conducts of database users ensures no odd activity implying a leak. Keeping a constant check on unknown IP addresses password protection and regular audits help finding inactive accounts or any unauthorized user manipulating information, enable future accountability for current undertaken actions and problems with access control.

F. PROGRAM UPDATES

Some updates are introduced to patch severe exploits which may leave the database, or the server vulnerable to threats. A timely deployment of current service packs & critical security hotfixes keeps the program fool-proof and up-to-date on any recent issues or loopholes that programmers have fixed and advances the database performance.

G. TOKEN-BASED ACCESS CONTROL

A security token or authentication token is a smart card reader or an electronically activated switch that permits authorized access to network service. It might be in the form of smart card or embedded objects as in key fob. In this process, user enters their credentials i.e. the token and the token is signed with an encryption.
The server verifies the information by matching the encrypted sign to the security algorithm.

If the server finds, the sign hasn't been tampered, the request is validated. In the contrary, the users request is denied.

Tokens offer access to a specific resource for a limited time period and are stored on user side, this process is more scalable and supports multi-server platform. Once the user logs out, the token is destroyed .

H. BIOMETRIC AUTHENTICATION

Biometric is the measurement and statistical analysis of an individual's physical and behavioural characteristics. The authentication system relies on unique biological characteristics and compares a digital image captured to the stored biometric data to confirm authenticity. Biometric features used are:

4. **RETINA SCANS- THIS SYSTEM CAPTURES**
an image of the blood vessel pattern in the light sensitive surface lining of an individual's eye for comparison.

5. **IRIS RECOGNITION- THE UNIQUE**
complex pattern within the ring shaped area surrounding the pupil and the eye colour shows variation that are unique to every individual on scrutinizing.

ISSN 2394 - 7780

6. **FINGERPRINT SCANNING- IT INITIALLY**
identifies the candidate's common unique points, known as minutiae, in both the base and the input images and ratios of relative distances are as the comparing function.

7. **FINGER VEIN ID- THIS SYSTEM**
compares data on the basis of the vascular patterns on a person's finger.

8. **FACIAL RECOGNITION- THE SENSOR**
maps individual's facial features by extracting landmarks by projecting structured light on the face and compares the measurements of the probe image captured to the template retained in the database.

I. *BLOCKCHAIN TECHNOLOGY:*

Block chain is a decentralized, distributed digital ledger of records, called blocks that are linked by cryptography. Each block comprises of cryptographic hash of the previous block, a timestamp and transaction data [5].

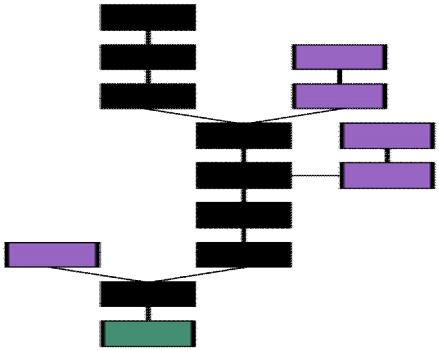


Fig-4: The main chain (black) , genesis block (green), Orphan blocks (purple)

This system is decentralized i.e. it doesn't upload data to the cloud or any single location, rather divides the data into small chunks that gets distributed across the network creating a distributed consensus system in the digital online world. Intruding into any one node will not result in data loss as each computer/ node has complete copy of the ledger [6].

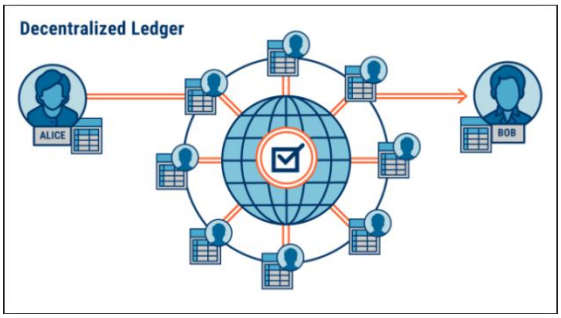


Fig-5: Decentralized ledger

Block chains offer encryption & validation. No third party is required to process transaction and each network participant has a private key that is assigned to the transaction agent which is kept as a password or personal digital signature & a public key stored with other agents, , thus maintaining the integrity of the database. Public keys are never tied to real world entities. [4]

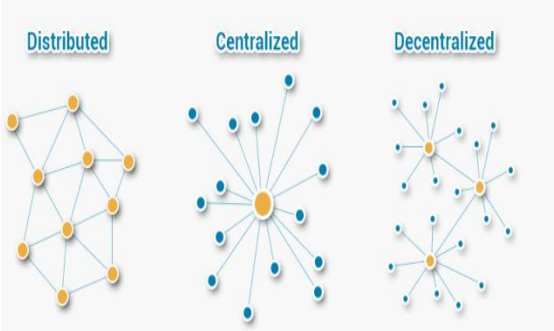


Fig-6: Blockchain Networking systems

ISSN 2394 - 7780

WORKING

9. **VALIDATE ENTRIES- BLOCKCHAIN USES**

cryptographic proof mechanism. Each transaction sent is protected by a digital signature to 'public' key of the receiver, which is digitally signed by private key of sender. Receiver verifies the digital signature implying ownership of sender. Transaction is then broadcast to every node in the network & is recorded in public ledger after verification.

10. **SAFEGUARD ENTRIES- IT STORES THE**

cryptographic digest of the file, linked to the user's submission time. Only the digest is stored & not the document i.e. the signature and timestamp associated with the document validates the data without any single centralized entity or third party interference.

11. **PRESERVE HISTORIC RECORD- IT**

implements Decentralized Internet of Things (IoT) platforms for secured and trusted exchange of data and record keeping. In such an architecture, Blockchain serves as the general ledger of IoT topology.

Types of blockchain:

12. **PUBLIC BLOCKCHAIN- THE ORIGINAL**

distributer ledger structure with no access restrictions, allowing anyone with internet to send, receive and audit transactions & become a validator.

13. **PRIVATE BLOCKCHAIN- THE CLOSED**

network blockchain in which only specific, pre-chosen entities, that are invited by network administrators can create new transactions on the chain. It allows record keeping procedure without sacrificing autonomy and running the risk of exposing data.

14. **CONSORTIUM BLOCKCHAIN- THE PART-**

Public part-private blockchain is semi-decentralized, which allows access to more than one validator and each validator can operate a node on such network. It restricts users' reading rights and allows limited set of transaction nodes.[5]

EXAMPLE

1. X wants to send money to Y.
2. Online Transaction is represented as block.
3. Block is broadcast dicretely to every node in the network.
4. Nodes in the network approve transaction after confirming authenticity.
5. Block is added to the chain which provides transparent record of transaction.
6. Money is moved from X to Y.

J. DIGITAL SIGNATURE

Digital signatures allows to sign digital media. It is a mathematical technique used to validate the authenticity of the sender [6]. Signing algorithms like e-mail programs create one way hash of electronic data which is to be signed. The signing algorithm encrypts the hash value using private key. Message is encrypted to cipher text at sender's side using encrypting algorithm, which cannot be deciphered easily unless by the authorized user. Digital sign is appended with data and sent. The receiver decrypts the document hash using signer's public key. The program calculates a new hash for the document and compares it to the decrypted hash to confirm integrity. Granularity of digital signature is dependent on dynamic alteration of the database.

III. CONCLUSION

In this paper we talked about various security threats posed to databases. Authorisations, encryption, updating and restricted access control by various techniques to alleviate such threats are used to augment and enhance database security.

REFERENCES

1. W. contributors, "*Principle of least privilege*", En.wikipedia.org, 2019. [Online].Available :http://en.wikipedia.org/ wiki/Principle_of_least_privilege. [Accessed: 28- Feb- 2019].
2. E. Meslin, "*The Value of Using Top-Down and Bottom-Up Approaches for Building Trust and Transparency in Biobanking*", www.ncbi.nlm.nih.gov, 2010. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/ articles/PMC2865393/. [Accessed: 25- Feb- 2019].

ISSN 2394 - 7780

3. A. ku and V. to, "*Transparent Data Encryption (TDE) - SQL Server*", Docs.microsoft.com, 2019. [Online]. Available: https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-2017. [Accessed: 25- Feb- 2019].
4. F. Olleros and M. Zhegu, *Research handbook on digital transformations*, Revised ed. Cheltenham: Edward Elgar, 2016, p. 226.
5. M. crosby, P. Pattnayak, S. Verma and V. Kalyanaraman, "*Applied Innovation Review (AIR) - UC Berkeley Sutardja Center*", UC Berkeley Sutardja Center, 2016.[Online].Available:https://scet.berkeley.edu/applied-innovation-review/. [Accessed: 25- Feb- 2019].
6. J. olenski, "*How do Digital Signatures Work? A Look Behind the Scenes*", Globalsign, 2015. .Available: https://www.globalsign.com/en-in/blog/how-do-digital-signatures-work/. [Accessed: 26- Feb- 2019].

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

SOCIAL MEDIA INTELLIGENCE AND INVESTIGATION

Mamta Deepak Pandey
Assistant Professor, JVM'S Mehta Degree College, Navi Mumbai

ABSTRACT
This paper is all about latest member of the intelligence family. Joining IMINT, SIGINT, HUMINT, and others are 'SOCMINT' – social media intelligence. In an age of ubiquitous social media it is the responsibility of the security community to admit SOCMINT into the national intelligence framework, but only when two important tests are passed. First, that it rests on solid methodological base of collection, evidence, verification, understanding and application. Second, the moral hazard it entails can be legitimately managed.

Keywords: SMI (Social Media Investigation) or SOCMINT (Social Media Intelligence), OSINT, IMINT, HUMINT, SIGINT

INTRODUCTION
The term "social media intelligence" was first introduced by David Omand, Jamie Bartlett, and Carl Miller at Demos, a London-based think tank. They defined the term for the Centre for the Analysis of Social Media (CASM) in a 2012 paper. Here, we discussed how intelligence is the key to social media, and how social media intelligence is an expansion of social media monitoring and social listening. Now, social media intelligence may be a crucial layer on high of social listening. It is a comparatively new area in digital marketing and plays an important role in the way to use social [knowledge] a lot of effectively.

SMI (Social Media Investigation) or SOCMINT (Social Media Intelligence) refers to the collective tools and solutions that enable organizations to observe social channels and conversations, respond to social signals and synthesize social information points into meaningful trends and analysis supported on the user's needs. Social media intelligence permits one to gather intelligence gathering from social media sites, from open and closed social networks. This type of intelligence gathering is a part of OSINT (Open- Source Intelligence).

Social media is now an important part of intelligence and security work, but that technological, analytical and regulatory changes are needed before it can be considered a powerful new form of intelligence.

Use of social networking sites by Indian web users, especially younger generations, has grown exponentially in every recent year. This has thrown many challenges to the Indian law enforcement agencies. They need to understand its implications in prevention, prediction, detection and investigation on crimes and maintenance of law and order. By properly integrating social medial strategies in its police work, Indian law enforcement agencies

can leverage upon the opportunity offered by social media apart from tackling the challenges it poses. Monitoring of social media content has become necessary in the backdrop of its misuse in certain incidents in India. Police departments in many countries have already adopted a comprehensive and integrated approach to use social media for their benefit and Indian Police can ill afford to ignore this powerful media.

Today social media is a place where people post almost everything. The casualness of people's social profiles has increased the possibility of information leakage making social networks a new place of communication for scammers who execute fraud. Social media also helps cyber investigators to get hold of the cyber criminals.

The intelligence family has been growing. From IMINT (Imaginary Intelligence), HUMINT (Human Intelligence), SIGINT (Signals Intelligence) to SOCMINT (social media intelligence), security is now all ready to clean up cyber threats.

In this age when social media is abundant, it is the concern of the security communal to acknowledge SOCMINT into the national intelligence agenda, but only if two vital tests are approved. First, that it should be based on strong operational foundation of assemblage, proofs, authentication, and submission. Second, that the moral hazard it entails should be one which can be legitimately managed. Below there is outline for how this can be done. Listing down a few social media intelligence tips for Fraud and Criminal Forensics.

1. TOOL, TIPS AND TRICKS FROM ONLINE SOCIAL MEDIA
Investigators often miss or underutilize the social media resources in investigating cyber criminals. Like in any other communities, where frauds and criminals exist, in the social media community also, frauds do exist. Hence, in every community, investigators need to know the tools and tips against cybercrime protection.The

ISSN 2394 - 7780

undercover investigation officers are now in a world where internet caching data and face recognition algorithm make it possible for them in finding out the location of posting an image a decade ago. The engaging of geolocation and social networking allows investigators to find out newer tricks of an investigation.

2. FACEBOOK: WHERE CRIMINALS FIND EASY ACCESS TO DATA EXPLOITATION

Over thousands of social networking sites, Facebook has the most population of over 1.1 billion profiles. With 200 million status updates every day, Facebook account settings, data backup, and common frauds take place regularly. Recent updates of Facebook like the Poke apps for iOS, archive, etc. adds more value to the understandings of investigators.

3. OBLIGATIONS CONCERNING ONLINE SOCIAL MEDIA

The interlocking of geolocation and mobile devices help investigators find new investigation tools and techniques. While doing so there are risks related to privacy associated with the public and private data related to social media and networking. The social media activities of employees and their available data on the public platform are threats and challenges to cybersecurity.

4. WHAT CYBER INVESTIGATORS SHOULD RECOGNIZE ABOUT COVERING IDENTITY ON THE INTERNET?

Cyber investigators should know how criminals hide their identity on the internet. Hiding one's identity is an opportunity for the investigators, while the same becomes a challenge when the same applies to cybercriminals. Using different methods of hiding their identity while working on the internet allows the cyber police to involve in secret online research while availing a path for the cybercriminals to involve in sneaky interaction in persistence to evil on-going.

5. OPEN SOURCE INTELLIGENCE (OSINT)

Investigators should make use of open source intelligence (OSINT), which involves gathering and acquiring information from open sources and then using it to reform legal intelligence. Since online marketing has speeded up all over the internet, so OSINT is now a serious factor for both investigators as well as cybercriminals. Investigators need to differentiate between the comments and interferences of big online gossips and discussions.

LATEST SCANDAL BY THE USE OF SOCMINT IN INDIA

If the Cobrapost investigation which exposed that many film industries celebrities were willing to pass views of political parties as personal opinion for money shook your conscience, there is not much we can do to restrict them from doing, because the relevant Indian law is silent on this matter. The investigation revealed that more than 30 Indian film and TV industry actors/ artistes have agreed to spread the propaganda of political parties through their social media accounts for the sake of money. "Taking money for tweeting on behalf of political parties is certainly unethical, but it is not illegal. The Information Technology Act, 2000 is totally silent on this," Pavan Duggal, one of the nation's top cyber law experts, told IANS. What the investigation unearthed was simply the tip of the iceberg. The rise in popularity of social media platforms actually opened up a comparatively new advertising economy driven by "influencer marketing". Marketing firm Mediakix estimated that influencer marketing on Instagram alone could reach $2 billion by the end of this year from $1 billion in 2017. While Instagram has over a billion monthly active users globally, its parent company Facebook has over 2.3 billion monthly active users and over 16 million people log in to Twitter daily. WhatsApp is another powerful platform which has over two hundred million users in India.

The kind of reach that these social media platforms have offers some plan concerning however huge the influencer promoting business might be. Important here to say that it is not just celebrities who are the stars in this game, while celebrities with huge following running into millions on social media are referred to as macro influencers, even some people with less number of followers can earn huge sum of money as influencers. They are known as micro influencers. With a large array of social media analytics tool available online, it is not difficult to identify the proper influencers for their advertising programmes. "In the beginning, celebrities were used as influencers for complete endorsement and promoting purposes. However, after social media, now everyone seems to be a star and everything is business as well as politics," social media expert Anoop Mishra told IANS. In countries just like the US, it is mandatory to put proper disclosure on paid posts. But only a few follow the rules. In India, because of lack of user awareness, it is even harder to differentiate between a paid post and a private opinion. With the elections around, political parties are not complaining more. A prime WhatsApp executive recently even warned political parties against abusing its platform. "More than ten thousand official WhatsApp groups have been created by a leading political party to slam its rivals on social media."Political discourse goes to be impacted by social media influencers. There is no two opinions

ISSN 2394 - 7780

concerning it," Duggal said, adding that the consequences of this may be terribly serious as social media platforms are being used to create a highly-polarized atmosphere in the country. Just as social media corporations have come back up with transparency rules for political ads, they should have similar features for influencers so that people can distinguish between commercial space and personal space. "Manipulation of social media platform for private gains should be brought under the ambit of law without putting barriers on free speech.

CONCLUSION

The opportunities that the explosion of social media use offers are remarkable. SOCMINT ought to become a full member of the intelligence and enforcement family. At the heart of this process are the twin demonstrations of necessity and legitimacy.

To meet the challenge of necessity, a new, applied academic discipline – social media science – must be developed. This requires new relationships with business and academe, and concerted, long-term investment to build technological, methodological and presentational capabilities. Those disciplines best equipped to understand and explain human behaviour – the social and behavioural sciences, political science, psephology, anthropology and social psychology – must be made to interweave with the massive knowledge approaches necessary to know social media. Only through this fusion can data-led explanations of human behaviour even be humanistic explanations of human behaviour. But technology and capability is simply half the image. To meet the challenge of legitimacy, the public must broadly understand and accept why, when and with what restrictions SOCMINT is undertaken. Any Government that wishes to conduct SOCMINT must adopt an explicitly articulated approach grounded in respect for human rights and the associated principles of accountability, proportionality and necessity.

REFERENCE

- Pescovitz, David (January 9, 2006). "Facebook prank on police". Boing Boing. Archived from the original on January 11, 2006.
- Jadhav, Adam; Shane Graber. Students learning dangers of internet 'confession'; Sophomore could also be expelled for Facebook page".
- Amy L. Ashbridge (April 26, 2007). "SUNY Cobleskill student says his web posting troubled officials". The Daily Star. Archived from the original on July 16, 2011.
- Amos, Meredith (March 1, 2006). "Baylor U. students outraged by off-campus party". The Lariat
- Larsen, Lindsay (February 2, 2007). "U. Connecticut law school party causes stir over stereotypes". The Daily Campus.
- Aggarwal, N., Agarwal, S.: Mining YouTube metadata for detecting privacy invading harassment and misdemeanor videos. In: Privacy, Security and Trust (PST).
- Aggarwal, N., Agarwal, S, Sureka, A.: Using common-sense knowledge-base for detecting word obfuscation in adversarial communication. In: Workshop on Future Information Security (FIS).
- Ramakrishnan, N., Butler, P., Muthiah, and S.: 'Beating the news' with embers: forecasting civil unrest using open source indicators. In: Proceedings of the twentieth ACM SIGKDD International Conference on data Discovery and data processing, KDD 2014, pp. 1799–1808.
- ACM New York.
- Agarwal, N.: A focused crawler for mining hate and extremism promoting videos on YouTube. In: twenty fifth ACM Conference on machine-readable text and Social Media (HT), pp.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

FIGHTING DATA GLUT WITH FILE SYSTEM ANALYSIS

Puneet Gawali
Student, Digital Forensics & Information Security, Gujarat Forensic Sciences University, Gandhinagar

ABSTRACT
File system plays an important role in Digital Forensics as the trails left behind when a system is compromised can be studied, identified and analysed which could be crucial for any of the forensic analyst in getting the lead during investigation. In the world of Digital Investigation, File System plays an important role and investigation of these files is important task. This paper gives us the overview of which tool gives the most of the evidences, as in how the attack has been performed.

Keywords: Tools, Investigation, File System, Analysis, Artefacts

I.INTRODUCTION
This paper provides overview of how file systems provide a mechanism for users to store data in a hierarchy of files and directories. A file system consists of structural and user data that are organized in such a way that the computer knows where to find them. The file system in OS is usually organized into directories for efficient usage. The directories may have files or other directions. For file management an OS does these activities; keeping the track of users, location, status and information, allocate and de-allocate the resources and take the decision that gets resources. A file is actually contains a sequence of bits, bytes, records and lines whose significance is defined by a file users or a file creator. The related record or information of a file is stored on a secondary storage device like optical disk, magnetic disk and magnetic tapes. The important features of file system are inventor, name, partition identifier, native operating system, based sector allocation, file allocation, namespace, maximum files and maximum file name size, maximum volume size and date handled. The access date is the date when a file is last time accessed although the access may be a simple move or open. Type of file system determines how the data is stored on disk and how much memory is allocated to this file system, through this paper I will be performing overt attacks on windows, and the artefacts found after this attacks would be used in the analysis as in which tool yields the better result this would help the analyst to decide beforehand as to on which tool he should work on to solve the case effectively.

The process of digital forensics can be seen as follows:

Figure1: Digital Forensic Process

1. Identification – the first stage identifies potential sources of relevant evidence/information (devices) as well as key custodians and location of data.
2. Preservation – the process of preserving relevant electronically stored information (ESI) by protecting the crime or incident scene, capturing visual images of the scene and documenting all relevant information about the evidence and how it was acquired.

ISSN 2394 - 7780

3. Collection – collecting digital information that may be relevant to the investigation. Collection may involve removing the electronic device(s) from the crime or incident scene and then imaging, copying or printing out its (their) content.
4. Analysis – an in-depth systematic search of evidence relating to the incident being investigated. The outputs of examination are data objects found in the collected information; they may include system- and user-generated files. Analysis aims to draw conclusions based on the evidence found.
5. Reporting – firstly, reports are based on proven techniques and methodology and secondly, other competent forensic examiners should be able to duplicate and reproduce the same results.

II. FILE SYSTEMS

File systems provide a mechanism for users to store data in a hierarchy of files and directories. A file system consists of structural and user data that are organized such that the computer knows where to find them. In most cases, the file system is independent from any specific computer.

NTFS

Short for NTFS file system, NTFS is a file organizational system that stores and accesses information located on Microsoft Windows NT, Windows 2000, Windows XP, Windows 7, and Windows 10. NTFS offers better methods of data protection and file recovery than the previous FAT file system versions.

FAT

Short for file allocation table, FAT is a method of keeping track of the contents of a hard drive used by early Microsoft operating systems that was first introduced in 1977. The table is a chart of numbers that correspond to cluster addresses on the hard drive. Below is a listing of the different types of FAT that have been used and the operating systems using them.

FAT32

Enhanced File Allocation Table utilizing a 28-bit binary system, first used in Windows 95 OSR2 and Windows 98, that saves disk space by using 4 k cluster. See FAT32 page for extended information about FAT32.

GFS

Short for Global File System, GFS was first developed at the University of Minnesota and now maintained by Red Hat. GFS is a File system that spans across a cluster and allows multiple computers to act as a unified machine.

HFS

Short for hierarchical file system, HFS is a file system used to store the files on floppy disks, CD-ROM discs, and hard drives of older Apple Macintosh computers. Since OS X was introduced, Apple no longer supports the ability to write to or format HFS disks.

III. RESEARCH METHODOLOGY

The file content can be encrypted to keep it secure from unauthorized access. This can be done by the application that creates the file. Before any file is been written to disk the OS encrypts the file and saves the cipher text to data units. The non-content data such as the file name and when the file was last accessed are not hidden or encrypted. Sometimes an entire volume can be encrypted, encrypted data can prove a tough task to an investigator. EFS is available in all versions of Windows developed for business environments from Windows 2000 onwards. In general, no files are encrypted but encryption can be enabled by users on an individual file, directory, or drive basis. Some EFS settings can also be mandated via Group Policy in Windows domain environments, when an operating system is running on a system without file encryption access to files generally goes through OS-driven user authentication and access control lists. But, if an attacker acquires physical access of the computer, this hindrance can be easily avoided. Other way for instance would be to remove the disk and put it in another computer with an OS installed that can read the file system; another, would be to just reboot the computer from a boot CD containing an OS that is suitable for accessing the local file system. The globally accepted solution to this is to store the files encrypted on the physical media.

BLOCK SIZE

Suppose you have a classroom with 50 students, and you have students sitting in 25 spaces and books, other stationaries kept in the middle of the other 25 spaces. You technically have 25 half-spaces available, but you can't make sit 25 more students there. The similar scene arises with a file system that uses fixed-size blocks. Fixed size can contain data only up to the block size. You can't share a block with multiple files. And for the cost of lost flexibility and wasted space, the file system gains simplicity. Another file system, like NTFS, store

ISSN 2394 - 7780

small files directly in the index record (e.g., MFT or Master File Table) to avoid consuming an entire cluster. This is extremely crucial when the maximum block (cluster) size can be as high as 64kb. Sorted out file systems like ZFS can use variable block size.

SLACK SPACE

Slack space is the leftover storage that exists on a computer's hard disk drive when a computer file does not need all the space it has been allocated by the operating system. The analysis of slack space is an important aspect of computer forensics. To understand why slack space plays an important role in e-discovery, one must first understand how data is stored on computers that have hard disk drives. Computers containing hard disk store data in a sealed unit that contains a stack of circular, spinning disks called platters. Each platter is composed of logically defined spaces called sectors and by default, most operating system (OS) sectors are configured to hold no more than 512 bytes of data. Consider if a text file that is 400 bytes is saved to disk, the sector will have 212 bytes of extra space left over. When the hard drive of computer is brand new, the space in a sector that is not used – the slack space – is blank, but that changes as the computer gets used. When a file is moved to trash, the operating system doesn't erase the file, it simply makes the sector the file occupied available for reallocation. A new file that is only 200 bytes be allocated to the original sector, the sector's slack space will now contain 200 bytes of leftover data from the first file in addition to the original of 212 bytes of extra space. That remaining data, which is called latent data or ambient data, can provide investigators with clues as to prior uses of the computer in question as well as leads for further inquiries. In 2016, for example, the Federal Bureau of Investigation (FBI) revealed that it had reviewed millions of e-mail fragments that resided in the slack space of former Secretary of State Hillary Clinton's personal servers in order to determine whether or not the servers have improperly stored or transmitted classified information. Technically if we take a closer look, a file's slack space is the difference between its logical and physical size, logical size of a file is determined by the file's actual size and is measured in bytes. The physical size of a file is identified by the number of sectors that are allocated to the file. In lot of operating systems, including Windows, sectors are clustered in groups of four by default which means that each cluster has 2,048 bytes. Now, the logical size of the blue file below is 1280 bytes. This file was provided a cluster of four 512-byte sectors, which means the physical size of the file is 2,048 bytes. The difference of 2,048 and that of 1,280 is 768, which means that the blue file's slack space is 768 bytes.

METADATA

Metadata is often described as "data about data" and is used to provide information about a specific file or document. Computer forensics experts use metadata to understand what activities were transpiring on a digital device such as a computer. Most metadata fields are hidden and not easily seen or accessible by the end user. Sometimes individuals make an effort to alter or purge metadata. When a person tries to cover his or her tracks by tampering with metadata, inconsistencies across various metadata points can sometimes reveal clues of evidence tampering or destruction of crucial discovery. Only an expert skilled in forensic examinations has the necessary skills and experience to testify credibly in a court of law about computer evidence tampering. It is important that you retain a skilled and experienced forensic expert to preserve the metadata through forensic imaging or other industry accepted forensic methods and perform the necessary metadata analysis for your matter.

INFORMATION HIDING METHODS

A. Hidden Files and Folders

Possibly the most simple method of information hiding a person could use is hidden files or folders. All Microsoft Windows operating systems allow a user to set properties for a file or folder. Taking this into consideration, a criminal could simply store whatever information they choose in a file or a folder of files and mark the file or folder as hidden from the Windows file properties dialog box. Since this is the simplest method of information hiding, it is also the most easily detectable method of information hiding.

B. Deleted Files

According to Davis et. al., "one of the most common tasks requested in any investigation is to find and recover the files that have been deleted from the system. This will often be a prime indicator of what the suspect is trying to hide if you find mass deletions before your imaging occurred". Multiple factors are taken into account when designing file systems. For the final user of the system, more often than not they are concerned with the speed and throughput of the system as opposed to the security. Taking this into consideration, the designer of the operating system has a couple of options when implementing the way the file system will handle deleted files. First, the operating system can overwrite the data on disk and remove it completely, or the operating system can mark the file as unallocated in the FAT or MFT.

ISSN 2394 - 7780

C. Hidden/Deleted Partitions

As with files, it is also possible to mark a partition as hidden or deleted. Hidden partitions, although possible, are almost useless when hiding information for criminal purposes. This is because most common file systems have standardized ways of dealing with hidden partitions. Every operating system as well as any partition manager will recognize these partitions even though they are hidden, and some Linux distributions mount these hidden partitions by default. The method for marking a partition as hidden manually is rather straightforward. If a user flips the fifth most least significant bit in the partition ID, the partition is hidden.

Deleted partitions are a little more useful for information hiding. All operating systems make use of a master boot record (MBR) which is located in the first block on the drive and contains a pointer to a boot loader that either allows the user to choose from multiple operating systems installed or loads an operating system from a partition on a drive. All file systems are accessed through the MBR. The MBR also contains a partition table for each partition that has information about the partition on the drive. It is possible for a user to delete the partition table, or entries in the partition table, using various utilities freely available. The deleted partitions still remain on the disk just as deleted files/folders do, so it may be possible to recover or reconstruct these partitions using most computer forensic tool kits.

D. Bad Clusters

The file is split up into segments based on the size of the clusters used by the FAT file system. The segments are then placed in unallocated spaces as identified by the file allocation table. This process mimics the normal allocation done by the file system except that there is no entry for the file in the directory entries. As each segment of the file is placed in unallocated clusters, that cluster is marked as “bad” in the file allocation table. This can be done directly because the start position of the file system can be found based on the type of FAT. To keep track of the clusters that compose the hidden file, each “bad” cluster is recorded in a configuration file and encrypted. This technique tries to completely hide a file in unallocated clusters manually, by avoiding the default behaviour of file allocation. By doing this, there will be no directory entry for the file, and the file clusters can be manually marked as “bad” in the file allocation table.

E. Steganography

Steganography means “concealed writing” and refers to many types of information hiding.For the purposes of this paper, let us consider image steganography.This is perhaps the most complex and useful information hiding technique.Also, it is the most difficult to detect and uncover.An image file is usually large in size compared to a text or short audio file, thus image files can be used to plant steganography that will go undetected to a typical user. According to Kessler, “the most common steganography method in audio and image files employ some type of least significant bit substitution or overwriting”. If a user wanted to hide a short text file or something similar in an image file, changing the least significant bit changes very little in the image and it is not very likely that a human could detect the alterations. This is a very simple implementation of image steganography.

IV. OBJECTIVE

The main objective of the paper is to conceal data of windows 7(compromised machine) and the analysing it using autopsy to find evidence of hidden data. In this the tools used would be:

VMware workstation pro: where the windows 7 is loaded as virtual machine

ADS (alternate data stream) technique is used to concealed and hide data

AUTOPSY is used to analyse the file system: in which timeline analysis, hash, keyword search, web artefacts, data carving, EXIF image location, etc information can be retrieved

Various screen shots of the analysis conducted can been seen in the below given screenshots

Figure-3.1: Windows Registry Editor

ISSN 2394 - 7780

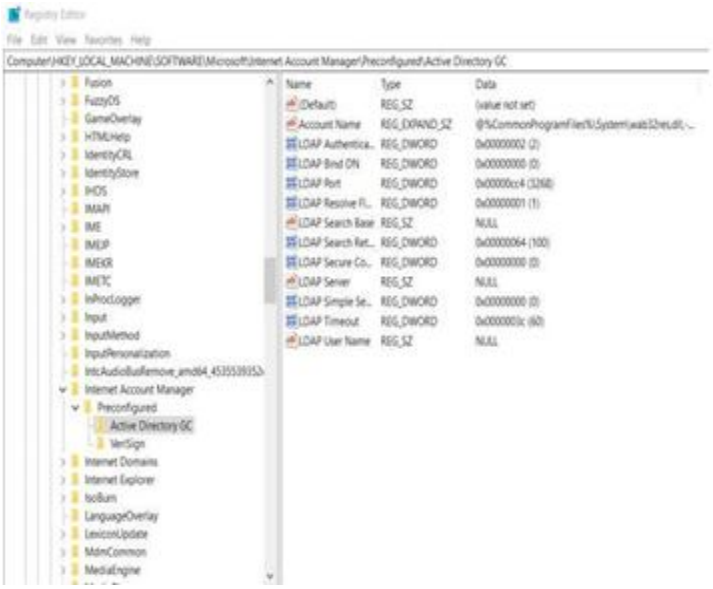


Figure-3.2: Internet History

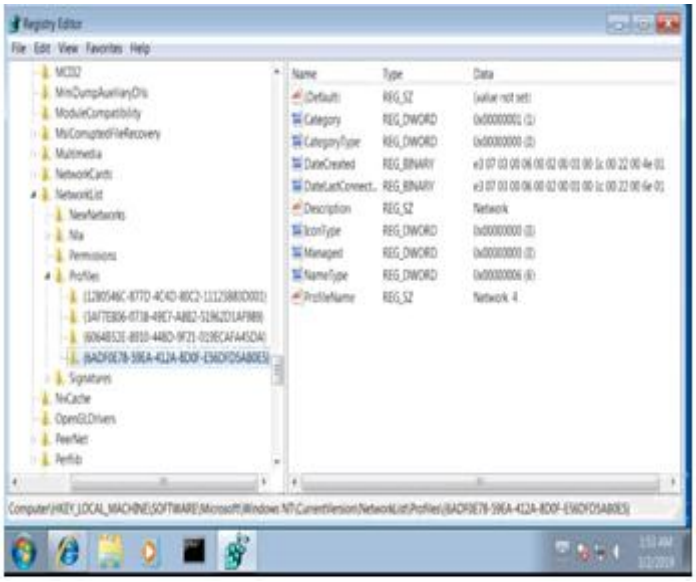


Figure-3.3: Wifi Connected Network 4 Forensics

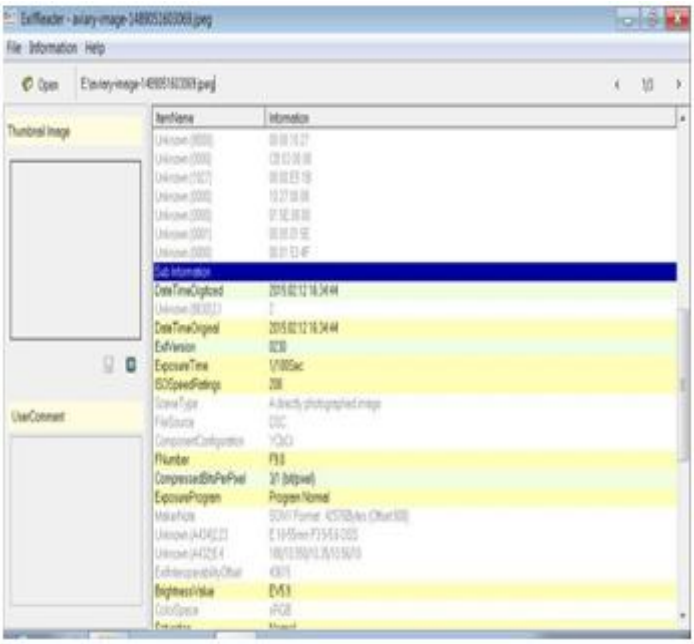
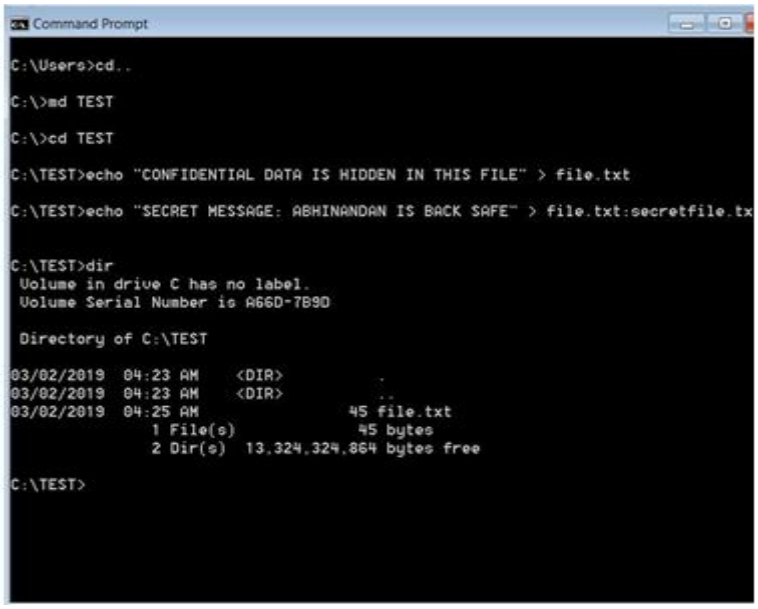


Figure-3.4: EXIF Reader To Detect Location And Device

ISSN 2394 - 7780



Figur-3.5: Using ADS To Hide File

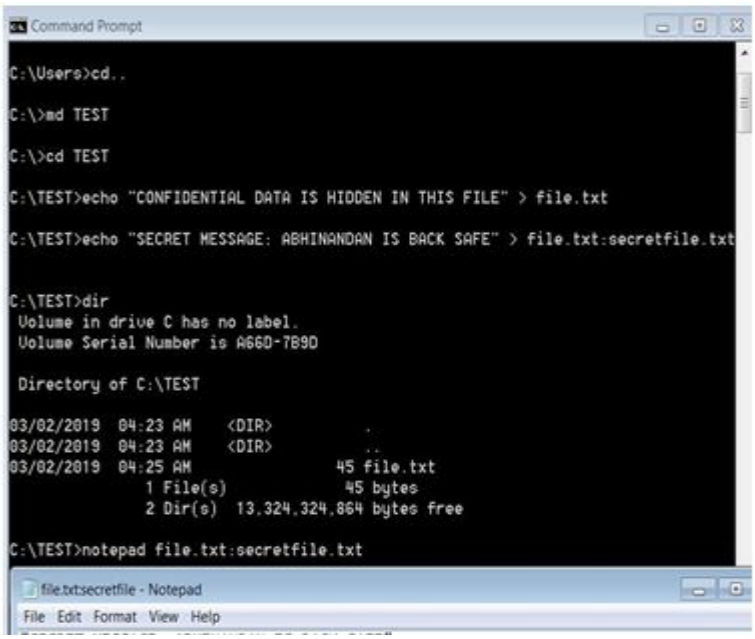


Figure-3.6: ADS Hiding

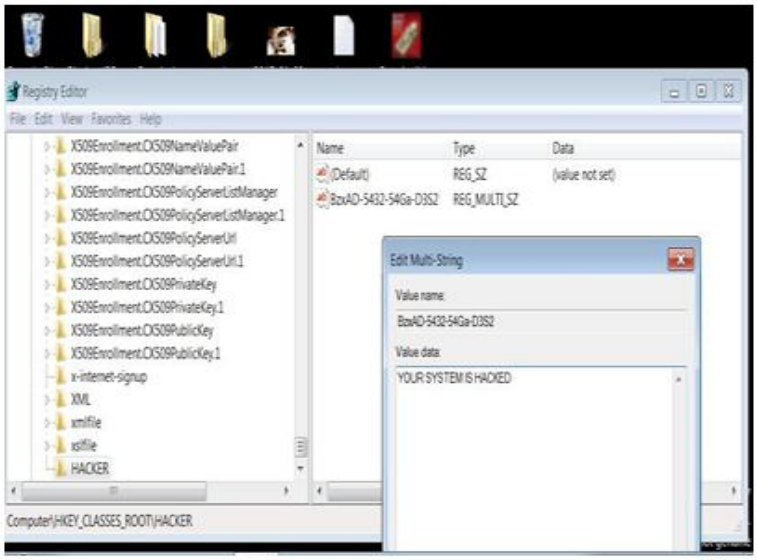


Figure-3.7: Opening The Hidden Message Through Registry

ISSN 2394 - 7780

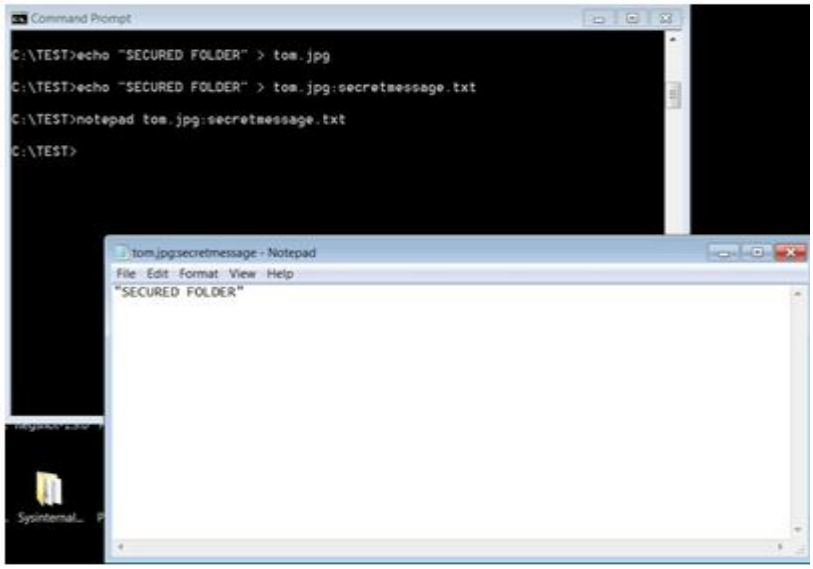


Figure-3.8: Steganography

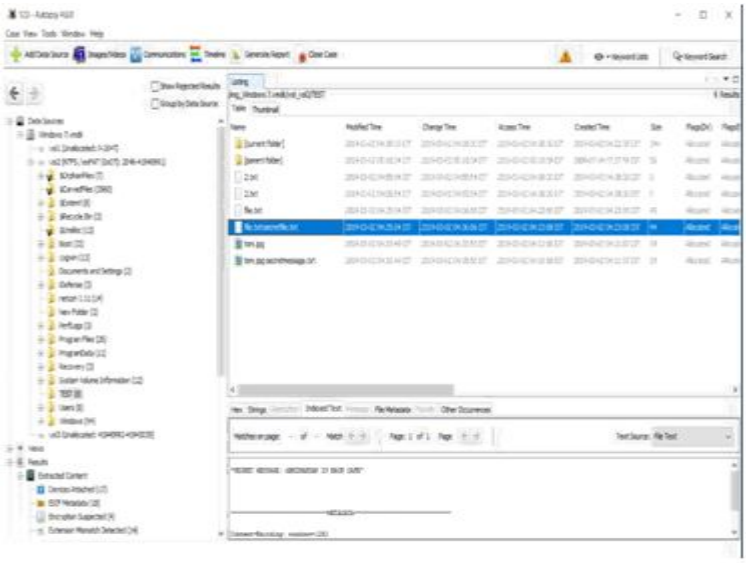


Figure-3.9: Results Seen In Autopsy

V. CONCLUSION

Most modern tool kits provide methods for detecting, recovering, and viewing most all types of information hiding. Thus, the investigator's job is made much easier with the advent of these tool kits. However, as these tool kits make detecting the common methods of information hiding more trivial, it is plausible that new and more innovative ways of information hiding will be developed to circumvent the current methods and thwart the tool kits capabilities. It can be concluded that almost every possible action or step taken in the compromised machine can be detected in autopsy tool, due to hidden data usually is stored in the file system without any structure or metadata it is hard to recover them, thus it can be taken as most efficient tool in understanding and carrying out file system forensics. This paper emphasizes the knowledge and importance of file systems for digital forensics, as several techniques to hide data such as slack space and hidden attributes are used by attacker.

REFERENCES

[1] Carrier, B.D., File System Forensic Analysis, Addison Wesley Professional, 2005

[2] Cheong Kai Wee, Analysis of hidden data in the NTFS file system, forensic focus, 3-8, 2011

[3] Role of File System in Operating System by Faheem Hafeez College of Information Technology, University of Punjab

[4] Methods of Information Hiding and Detection in File Systems By Jeremy Davis, Joe MacLean, David Dampier Department of Computer Science and Engineering, Mississippi State University, Mississippi State, MS

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

SOCIAL MEDIA FORENSIC AND INVESTIGATION

Vallari Pramod Tawade
JVM'S Mehta College, Navi Mumbai

ABSTRACT
Now-a-days, mobile devices are increasingly used to access social media and instant messaging services, which allow users to communicate with others easily and quickly. With rapidly increasing use of social media and instant messaging services, misuse of these services conducting different cybercrimes such as cyber stalking, cyber bullying, slander spreading and sexual harassment have been increased. Therefore, mobile devices can be consider as an important evidentiary piece in digital and forensic investigation. We report the results of our investigation and analysis of social media and instant messaging services in Firefox OS.In recent years, it has been examined that three social media services (Facebook, Twitter and Google+) as well as three instant messaging services (Tinder, Whats app, kik) is playing vital role in analysis and social media investigations.

Keywords: Firefox OS forensics; mobile forensics; social media forensics; instant messaging forensics; mobile applications investigation,Whats-app,Facebook,investigator,Computer security,Online social network application.

INTRODUCTION
Recent years have seen a massive increase in the number of online social networks such as MySpace, Facebook, Twitter and Whats app which facilitate a high degree of user personalizatio nation and user intercommunication

Computer forensics is used as an investigative tool in order to allow the investigator to determine what has occurred, when it occurred, where it occurred, why it might have occurred and hopefully who is responsible. All of this information is required to ensure that there is sufficient evidence to prosecute criminals. The main challenges among the process of computer forensics include performing the analysis and reporting the results to ensure that the evidence is consistent and reliable for prosecution of criminals in a court of law.

In this paper, we present a comprehensive digital forensic investigation model specifically for online social networks. The model is separated into two environments which are physical and digital environments that reflect the scene of investigation. The novelty of this work is therefore the development of this model, along with development of a tool that will support online social networks investigation and analysis process.

INVESTIGATION
Identification: This activity will be carried out by implementing the prototype to be developed. Firstly identify any evidence or supporting information which is available on online social network. For example the name of a suspect and a victim will be given to enable us to conduct a thorough investigation of a case. For the case of auditing, we need to identify the person that will be audited.

Searching: Based on the relevant data gathered from the investigation process, we will run a thorough search that enables us to discover relevant data automatically. There are a large number of different types of data that can be collected and used as evidence or supporting information that might be extracted from an online social network, as follows:

Filtering: The filtering activity will scale down and focus the investigation on relevant information and discard any irrelevant information.

Capturing: Information collected through filtering will be captured in the best way to ensure the integrity of the data is sustained. The data itself will be analysed in the next process.

ANALYSIS
A thorough analysis will be carried out based on the information collected from the previous activities. This activity will be supported by a module in the prototype to be developed.

Hypothesis: This activity consists of developing a hypothesis for the case to support any discovered evidence.

Reporting: The reporting activity will involve documenting the analyzed data and evidence gathered from the previous process, as well generating a detailed report of a suspect (or audited person) and others related to the case.

ISSN 2394 - 7780

BODY

Forensic investigation of social networking applications

Social media applications such as Facebook, LinkedIn, Tinder and Twitter provide facilities including email, blogging, instant messaging and photo sharing for social and commercial exchange.There has been a rapid growth in the use of social media and networking applications by both individuals and organisations. And an increasing number of organisations use Facebook ,Whats-app and Twitter as part of their marketing campaigns.

Although social networking applications are mainly used for personal purpose,some organisations actively encourage their employees to use them within the work environment to potentially improve productivity via enhanced information sharing above and beyond the corporate network.social media can provide employee with formal and informal ties to information sources both within and beyond organisational boundaries. However, some organisations might not fully appreciate the potential for misuse that social networking applications may provide.

If organisations do allow employees to use social networking applications within the work environment then it would be prudent to set out guidelines for such in the organisation's computer usage policy, to ensure that employees are provided with explicit guidance.

Misuse of social media may occur in many different forms, from defamation of individuals, to nurses violating patient rights through misuse of social media and data loss occurring to organisations resulting from inappropriate use. Forensic investigation of social media may be required for a variety of different purposes, from gathering evidence for use in a criminal trial to use in corporate disciplinary panels for employees that have breached company policy.

FORENSIC PROCEDURE

Typically, an individual employee or police officer may encounter suspected misuse of a social networking application (or details relating to a suspected criminal act) and then report such suspected misuse to the relevant authority (either their manager in an organism, or the local police force).

Initially, digital evidence might be obtained from the web pages of the social networking application containing the material associated with the suspect-ed misuse, assuming that these can be accessed (that is, not on 'private' pages). In an organisation, a next step might then be to obtain digital evidence from the employee's computer (or in a police investigation, the individual's computer) that might be involved in the suspected of misuse of the social networking application. In addition, it might be necessary to obtain digital evidence from the computer of the employees (or individuals) who were affected by such misuse.

"Forensic investigation of social media may be required for a variety of different purposes, from gathering evidence for use in a criminal trial to use in corporate disciplinary panels"

Given the number of computing devices that could potentially be used to update material on social networking applications (personal computers, laptop computers, tablets, mobile telephones, personal digital assistants and computer games consoles), it may be necessary to examine a range of computing devices that may have been used by in misuse of the social networking application. In instances involving police investigations a request might be made to the provider of the social networking application for the relevant digital data relating to suspected misuse. In some instances (for police investigations) the server computers sup-porting the social networking application might need to be forensically examined.

EVIDENCE ACQUISITION

In terms of the ease of acquisition of digital evidence from social networking applications, the following order of potential sources of acquisition might typically be adopted.

First, relevant social networking application web pages (if such can be accessed). Significant changes may be made to a web page at any time from when the message or post was initially made, to the time when the investigator attempts to make a copy of the page. For example, a victim might allege harassment on a Facebook web page where there is a message stating "I will see you soon!" and the icon of a firearm next to it. When the investigator accesses the page the person posting the message has changed their icon to be a bouquet of roses. The investigator has to be suitably knowledgeable and qualified to identify what elements are mutable, and where the necessary additional evidence of an offence can be found from other sources, such as:

UÊ / iÊÃÕÃ«iVÌ½ÃÊV «ÕÌ }Ê`iÛ Vi¬Ã®]Ê

assuming the suspect can be identified and located.

ISSN 2394 - 7780

The potential difficulty with acquiring digital evidence from this source (or sources) is that social media can be accessed across a variety of platforms from mobile phones, tablet computers, e-readers and traditional desktops both at both or work.

UÊ / iÊÛ VÌ ½ÃÊV «ÕÌ }Ê`iÛ Vi-Ã®°Ê

Unlike an email-based investigation, social media is essentially about publication, and future modification of the post or web page means that although the victim's machine can be useful for the investigation, service provider logs potentially provide the best evidence.

Typically social networking service's server computers and relevant Internet service provider's server computers would only be available for police investigations, whereas the other sources would typically be available for both internal corporate and police investigations.

Where an incident involves potential evidence displayed on a social media website the most convenient method of recovering the evidence may be to visit the website and take copies of the relevant content. The forensic investigator should record the address of the website, or the specific web page within the site. When carrying out any evidence recovery it is essential that an audit trail of all activity carried out by the forensic investigator is recorded in a log.

CONCLUSION

We described existing digital forensics investigation models and frameworks and found these to generally involve the process of identifying, preserving, analyzing and presenting digital evidence. For the purposes of general investigation (e.g. analysis of a hard disc), there are various tools available because they are produced according to general investigatory requirements. However, to conduct investigations in online social networks, these tools are not suitable because they do not provide specific functions and options as discussed in the previous section. To deal with these shortcomings, there is a need to establish a standardized forensic investigation process for these networks, thus we have developed a comprehensive online social network digital forensic investigation model and we will develop an application prototype to fulfil the essential requirements of online social network digital forensic investigations. And then we have designed the application prototype by developing the algorithms to ensure that the objective of systematic investigation and analysis process as described in our model is accomplished.

Since this is an ongoing project, we intend to work further in a number of directions. We will carry out a number of case studies to validate the design of the application prototype. Subsequently, we will develop the design and we will carry out evaluations of the prototype to make sure the purpose of developing this model is fulfilled and that the functionalities meet the essential requirements of the online social networks digital forensic investigation model.

REFERENCE

1. ScienceDaily2010.http://www.computerforensicsworld.com/www.sci encedaily.com Accessed on 21.10.2010
2. http://www.computerworld.com Accessed on 22.10.2010
3. http://www.computer-forensics.privacyresources.org Accessed on 22.10.2010
4. Lele RD. Computers in Medicine (Progress in Medical Informatics) By R D Lele (Tata McGraw-Hill Publishing Company Limited.
5. http://www.basistech.com Accessed on 22.10.2010

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

SOCIAL MEDIA INTELLIGENCE AND INVESTIGATION

Amit Jaynath Upadhyay
Jnan Vikas Mandal's Mehata Degree College

ABSTRACT

Social media has become one of needs of daily life today. We are in the age of social media it has given us an opportunity to express our feelings , can communicate with people throughout the world. Social media is fairly easy to operate and cheap. It includes information in audio mode, video mode , images and graphical ways. It is also a good source for a good complaining related to health , against corruption and awareness about envornment.

So ever-increasing part of the population makes use of social media in their daily lives, social media data is in many di erent disciplines.

Literature analysis through which we can identify challenges addressed and solutions proposed. The research revealed that the volume of data was most often treated as a challenge by researchers. Other categories have received less attention. Based on the results of the literature searc and we discuss the most important challenge for researchers and present potential solutions. The findings are used to extend the existing framework on social media analytics. The article provides benefits for researchers and practitioners who wish to collect and analysis social media datas.

INTRODUCTION

It is one of the useful and powerful tool of digital intelligence and itself now a major source of information of polices , securities anintelligence authorities on the identities, location, movement, financing and identities of suspects.The growth in use of social media for human being help .Social media has evolved over the last decade to become an important driver for acquiring and spreading information in di erent domains, such as business, entertainment, science ,crisis management, Bun and politics, One reason for the popularity of social media is the opportunity to receive or create and share public messages at low costs ubiquitously.

This is the time of social media today we are using Facebook, Whatsapp , twitter, Instagram etc These are the sources of transfering data, audio, video, images and has enhanced our live styles.

Understanding the content of the social media presents an opportunity for public bodies to better understand ,and respond the public to whom provide service.

Now a days social media has got a great power and a way to express thougths. It is having a power through we can communicate with people throughout the world.

Social media is a web-based technology for facilitatimg social interaction between a large group of people.

Social media is a growing rapidly and becoming important part of everyday life, because of the latest technological revolution. This fast growth is due to the increasing usage of smart phones like BlackBerrys, Androids and iphones.

The mobile versions of the social media are easy to access and have made it user friendly. As well as the Map services made it usage through mobile to find directions and places easily.

Social media is having a vital role in the student's life. It is easier and convenient to access information and commucative vs social media. Teachers and students are connected to each other and can make good uses and these technology.

Most popular Social Media Site is Facebook. All the celebrities, politicians , players of the whole world are connected to social media and have a craze of followers. Thay communicate with their fans and are very popular throughout he world.

ISSN 2394 - 7780

Principle

1.There must be sufficient, sustainable suitable cause: the first and overarching principles forces the big picture to be taken in to account, the overall perposes that could justify the acquition by a public body capabilities to gather, understand and use social media data.

2. There must be integrity of motive: This principle refers to the need for integrity throughout the whole 'intelligence' system from the statement and justification of access , accessing the information itself.

3. There must be right authority, validated by external oversight: There is a general principle that there must be an audit trail for the authorizations of actions that may carry moral hazard.

4. Resources to secret intelligence must be a last resort if more open sources can be used.

Social Media problems:

There are many problems related to social media intelligence.Some of them are as follows:

Challenges

First there was the Blue Whale Challenge, then the Momo Challenge and now a new challenge called the Bird Box Challenge is taking over the internet and influencing the impressionable minds. For parents, it adds to the burden of managing their kids' social media usage as it presents a very clear threat to not just their emotional wellbeing but even their life. We talked to experts to find out how parents can deal with this increasing menace of social media challenges and how to monitor your child's social media usage.

Momo Challenge: It is a challenge spread by adults on Facebook and media outlets claiming that children and adolescents are being enticed by the user named it as momo to perform a series of dangerous tasks with violent attacks as well as suicide.

Bird box challenge: An online game that encourages young people to harm themselves and in some cases even suicide has been reported.

Blue whale challenge: In this challenge, people have to make a picture of blue whale fish in the hand and the last as well as final step was to attempt suicide.

Online hacking

In computer networking, hacking is a technical effort to manipulate the normal behavior of network connections and connected computers. Hacking and hackers are most commonly related with programming attacks on networks and on computers.

Three types of hacking

1. White hat hacker
2. Grey hat hacker
3. Black hat hacker

ISSN 2394 - 7780

1. White hacking
A white hat hacker is a computer security specialist who breaks into protected systems and networks to test and accesses their security.

2. Gray hacking
The term grey hating refers to a computer hacker or computer security expert who may sometimes violate laws and typical ethical standards.

3.Black hat hacker
Black hats trys to break into computer systems to steal credit card information and to steal valuable sensitive information to sell in the black market.

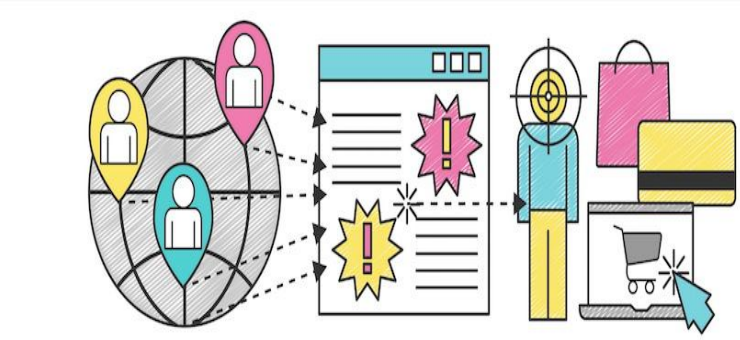
SOCIAL MEDIA EFFECTS ON HEALTH
It is very harmful for health if not operated properly. Some are as follows:

- **Addiction to social media:** People who are addicted to social media may experience negative side effects such as eye strain, social withdrawal and lack of sleep.
- **Stress:** If you spend more time researching problems and arguing with people, you may experience stress and understanding power of brain which can have a negative impact on your health.
- **Emotional connections:** Social media help you connect with many people and stay in touch with those with who you are already close. Connecting with people has proven knowledge benefits
- **Information:** You can find a amount of health-related information on social media. This can be quite helpful to the people. you take advice without doing proper research and it will also be harmful.
- **Eye problems:** You can get eyestrain from staring at screens for too long distance.
- **Lack of exercise:** Social media might harmful for doing exercises.

ISSN 2394 - 7780

Solutions

- There are many solutions of problems related with social media.
- Use of social media should be limited,
- It should be operated with responsibility and eith a positive aspects.



- people need a strong social media presence nowadays, and if you aren't online the main social networking sites, you're missing out on a LOT, but you need to know how to handle it all.
- Don't become dependent on such sites. Instead, find yourself some offline hobbies, friends, and ways to recreate so that you don't become addicted to the Interne
- You need to ask yourself does online friendship really workYes, and no – just as the link to this post describes, do read the interesting conversation that goes on about it in the post.
- It all depends on how you build relationships with your online friends. Check their profiles before making friends with them, another point most people forget to do.
- Also, don't entirely depend or only have online friends. Move out and meet offline friends and be with them, so that the awkwardness doesn't remain.
- If you are on the social networks just to waste time, you can never get anything worthwhile done. In case you have to deal with people who bore you, and you are one of the polite ones, you need to change!
- After one or two replies, excuse yourself from the conversation and get away. If you continue talking, they will continue asking or talking. So, the choice is always in your hand.
- When you are forever online working and visiting several social media and social networking websites in day, you tire your brain and lack the attention and focus.
- Yes, if you have the free time, these social networks are good, or else, they can reduce your efficiency and productivity, besides harming your entire days work and routine.
- Thus, time yourself and remain focused in what you need to do first – everything else can come up later. Setting your priorities is essential, which ensures you only work to achieve your target.

CONCLUSION

As every coin has two sides hence social media is good but operators should operate ,it with responsibility not to miss use it ever. As a user of social media its, our duty to use it for only good perpose and we can get benefit of social media 100%.Social media is good and will continue to beand it may be harmful, unless something is done about it. it has power over people is dangerous and often goes unnoticed. People should care otherwise if not addressed or taken care, of social media could cause national and international problems. Social media will growth and increase many internet users. Even if the user is not affected by social media and they are still in danger.

REFERANCES

- https://www.google.com
- https://www.google.com/search?client=firefoxd&q=social+media+intelligence+aand+inon
- https://www.google.com/search?client=firefox-b-d&q=social+media+intelligence+advantages
- https://www.google.com/search?client=firefox-b-d&q=social+media+intelluigence+intro

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

A SURVEY ON COMPUTER FORENSIC ANALYSIS AND INVESTIGATION ON COMPUTER EVIDENCES

Renukadevi C[1] and Jagadevi Gudda[2]
Assistant Professor[1], Department of Computer Science, S. L. N Eng. College Raichur
Assistant Professor[2], Department of Electronics, S. B. College of Science, Kalaburagi

ABSTRACT
This paper discusses information essential to understanding the role of forensic analysis. The topics covered help you understand that certain rules must be followed when dealing with evidence and why evidence must be properly collected, protected, and controlled to be of value during court or disciplinary activities. The terms discussed and concepts presented are essential to understand in your preparation for the Security. Understanding the process of conducting an investigation will not only assist one but will also help in the discovery of potential violations of laws or corporate policies. The paper discusses about the collection and study of preservation of evidences, and hence to discover the importance of a viable chain of custody means and there by exploring steps in investigating a computer crime or policy violation.

Keywords: Forensic, security, investigation, policies

1. INTRODUCTION

Computer forensics is certainly one of the popular buzzwords in computer security.

The term forensics relates to the application of scientific knowledge to legal problems. Specifically, computer forensics involves the preservation, identification, documentation, and interpretation of computer data, as explained in Warren G. Kruse and Jay Heiser's[1] Computer Forensics: Incident Response Essentials (Boston: Addison-Wesley, 2002). In today's practice, computer forensics can be performed for three purposes:

• Investigating and analyzing computer systems as related to a violation of laws

• Investigating and analyzing computer systems for compliance with an organization's policies

• Investigating computer systems that have been remotely attacked. It is important to note that computer

Forensics actions may, at some point in time, deal with legal violations, and investigations could go to court proceedings. It is extremely important to understand this concept, because even minor procedural missteps can have significant legal consequences.

1.1 EVIDENCE

Evidence consists of the documents, verbal statements, and material objects admissible in a court of law. Evidence is critical to convincing management, juries, judges, or other authorities that some kind of violation has occurred. The submission of evidence is challenging, but it is even more challenging when computers are used because the people involved may not be technically educated and thus may not fully understand what's happened. Computer evidence presents yet more challenges because the data itself cannot be sensed with the physical senses.

1.2 STANDARDS FOR EVIDENCE

Evidence must meet these three standards

• Sufficient The evidence must be convincing or measure up without question.

• Competent The evidence must be legally qualified and reliable.

• Relevant The evidence must be material to the case or have a bearing on the matter at hand.

1.3 TYPES OF EVIDENCE

All evidence is not created equal. Some evidence is stronger and better than other, weaker evidence. There are several types of evidence:

• **Direct evidence** Oral testimony that proves a specific fact (such as an eyewitness's statement). The knowledge of the facts is obtained through the five senses of the witness. There are no inferences or presumptions.

• **Real evidence** (also known as associative or physical evidence) Tangible objects that prove or disprove a fact. Physical evidence links the suspect to the scene of a crime.

ISSN 2394 - 7780

• **Documentary evidence** Evidence in the form of business records, printouts, manuals, and the like. Much of the evidence relating to computer crimes is documentary evidence.

• **Demonstrative evidence** Used to aid the jury and may be in the form of a model, experiment, chart, and so on, offered to prove that an event occurred. Harold F. Tipton and Micki Krause's Information Security Management Handbook[2].

1.4 THREE RULES REGARDING EVIDENCE

There are some rules which guide the use of evidence, especially if they could result in court proceedings:

• **Best evidence rule** Courts prefer original evidence rather than a copy to ensure that no alteration of the evidence (whether intentional or unintentional) has occurred. There are instances when a duplicate can be accepted, such as when the original is lost or destroyed by acts of God or in the normal course of business.

• **Exclusionary rule** The Fourth Amendment to the United States Constitution precludes illegal search and seizure. Therefore, any evidence collected in violation of the Fourth Amendment is not admissible as evidence.
• **Hearsay rule** Hearsay is second-hand evidence—evidence not gathered from the personal knowledge of the witness. Computer-generated evidence is considered hearsay evidence

2. PROCEDURE OF ACQUIRING EVIDENCE

When an incident occurs, you will need to collect data and information to facilitate your investigation. If someone is committing a crime or intentionally violating a company policy, they will likely try to hide the fact that they were involved. Therefore, collect as much information as soon as you can. Obviously, as time passes, evidence can be tampered with or destroyed. When an incident occurs and the computer being used is going to be secured, there are two facts to consider: should it be turned off, and should it be disconnected from the network?

On the other hand, it is possible for the computer criminal to leave behind a software bomb that you don't know about, and any commands you execute, including shutting down or restarting the system, could destroy or modify files, information, or evidence.

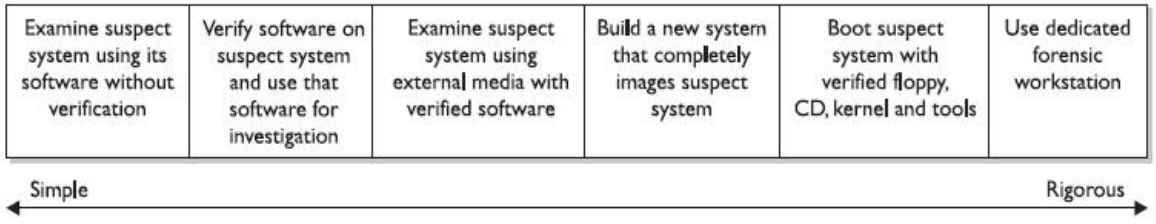
Further, if the computer being analyzed is a server, it is unlikely management will support taking it offline and shutting it down for investigation.

Steps show the relationship between the complexity of your investigation and both the reliability of your forensic data and the difficulty of investigation from simple to rigorous.

1. There are many investigative methods from simple to more rigorous.
2. Examine suspect system using its software with its investigation
3. Verify software on suspect system and apply software for investigation
4. Examine suspect system external media with verified software
5. Build a new system that completely images suspect system
6. Boot suspect system with floppy disc , kernel, CD and tools
7. Use dedicated forensic workstation.

2.1 IDENTIFYING EVIDENCE

Evidence must be properly marked as it is collected so that it can be identified as the particular piece of evidence gathered at the scene. Properly label and store evidence. Be sure the labels can't be easily removed. Keep a log book identifying each piece of evidence (in case the label is removed), the persons who discovered it, the case number, the date, time, and location discovered, and the reason for collection. This information should be specific enough for recollection later in court. Log other identifying marks, such as device make, model, serial number, cable configuration or type, and so on. Note any type of damage to the piece of evidence



ISSN 2394 - 7780

2.2 PROTECTING EVIDENCE

Protect evidence from electromagnetic or mechanical damage. Ensure that evidence is not tampered with, damaged, or compromised by the procedures used during the investigation. Protect evidence from extremes in heat and cold, humidity, water, magnetic fields, and vibration. Use static-free evidence protection gloves as opposed to standard latex gloves. Stealth evidence in a proper container with evidence tape, and mark it with your initials, date, and case number.

2.3 TRANSPORTING EVIDENCE

Properly log all evidence in and out of controlled storage. Use proper packing techniques, such as placing components in static-free bags, using foam packing material, and using cardboard boxes. Be especially cautious during transport of evidence to ensure custody of evidence is maintained and it isn't damaged or tampered with.

2.4 STORING EVIDENCE

Store the evidence in an evidence room that has low traffic, restricted access, camera monitoring, and entry logging capabilities. Store components in static-free bags, foam packing material, and cardboard boxes.

2.5 CONDUCTING THE INVESTIGATION

When analyzing computer storage components, it is important to use extreme caution. A copy of the system should be analyzed—never the original system, as that will have to serve as evidence. A system specially designed for forensics examination should be used. Conduct analysis in a controlled environment with strong physical security, minimal traffic, controlled access, and so on. Remember that witness credibility is extremely important. It is easy to imagine how quickly credibility can be damaged if the witness sis asked,"Did you lock the file system" andcan'tansweraffirmatively.Or,"Whenyouimagedthisdiskdrive,didyouuseanew system?" and one can't answer that the destination disk was new or had been completely formatted using a low-level format before data was copied to it.

2.6 ANALYSIS

After successfully imaging the drives to be analyzed and calculating and storing the message digests, the investigator will now begin the analysis. The details of the investigation will depend on the particulars of the incident being investigated. However, in general, the following steps will be involved:

• Check the Recycle Bin for deleted files.

• Check the web browser history files and address bar histories.

• Check the web browser cookie files. Each web browser stores cookies in different places.

CONCLUSION

From this paper we have come to a conclusion that investigating and analyzing computer systems as related to a violation of laws, investigating and analyzing computer systems for compliance with an organization's policies and Investigating computer systems that have been remotely attacked. Also above paper we discussed about the types different types of collecting evidences along with their procedures and standards available for evaluation and hence how to conduct investigations in real time.

REFERENCES

1. Computer Forensics Heiser Jay G Kruse Warren G Ii
2. Computer Forensics: Incident Response Essentials
3. http://www.forensicsciencetechnician.net
4. The international journal of forensic computer ... - ijofcs

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

PROTECTING WEB APPLICATION'S VULNERABILITIES FROM SQL INJECTION ATTACK

Sadaf Shaikh[1] and Ujwala Sav[2]
Student[1] and Assistant Professor[2], Information Technology, Vidyalankar School of Information of Technology, Wadala (E)

ABSTRACT
Security and privacy of database-driven web applications are extremely multifaceted against web intruders. One of the most dangerous cyber-attacks is the SQL-Injection, which simply creates huge loss to the organization and commercial vendors. SQL is a code injection technique used to attack data-driven applications, in which malicious SQL Statements are inserted into an entry field for execution. Since an SQL Injection vulnerability could possibly affect any website or web application that makes use of an SQL-based database, the vulnerability is one of the oldest, most prevalent and most dangerous of web application vulnerabilities. By leveraging an SQL Injection vulnerability, given the right circumstances, an attacker can use it to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQL Injection can also be used to add, modify and delete records in a database, affecting data integrity.

To such an extent, we need to protect the web applications from vulnerabilities of SQL injection with the help of data encryption techniques. This research paper proposed web application protection from SQL injection attack by using master key and AES algorithm.

Keywords: SQL Injection Vulnerabilities, Database Security, Encryption, AES Algorithm.

1. INTRODUCTION

SQL injection is a basic attack that can be used either to gain unauthorized access to the database or to modify the database illegally. This is the most common attack used to retrieve the confidential information from the database such as Credit card details, etc. SQL injection happens when a hacker or an attacker inserts malicious data in the input field. The main reason for SQL injection attack –end user input string is not validated properly and is passed to the database without validation [10]. SQL injection attacks are too much vulnerable that it can bypass any security levels such as Firewall, encryption, and traditional intrusion detection system. Basically, a web application is three tier architecture, the Application tier at the user side, Middle tier which converts the user queries into the SQL format, and the backend database server which stores the user data as well as the user's authentication table. SQL injection attack is application level security vulnerabilities. Most of the web Application used over the internet or in the enterprises is vulnerable to the SQL injection attack. Although the vulnerabilities that lead to the SQL injection attack are due to the lack of effective technique for detecting and for preventing them. Programming practices such as defensive programming and sophisticated input validation techniques can prevent some vulnerability. A novel idea to prevent SQL injection is to use encryption algorithm. An encryption algorithm can be used to encrypt all the user data that has to be sent over the network to the database.

2. LITERATURE REVIEW

2.1 SQL INJECTION

SQL Injection is one of the many web attack mechanisms used by hackers to steal data from databases. It is perhaps one of the most common application layer attack methodology used today. It is the type of attack that takes advantage of improper implementations of your web applications that allows hacker to inject SQL commands into say a login form to allow them to gain the access to the data held within your database [12]. In essence, SQL Injection arises because the fields available for user input allow SQL statements to pass through and query the database directly. Web applications allow legitimate website visitors to submit and retrieve data to and from a database over the Internet using their preferred web browser. Databases store data needed for websites to deliver specific content to visitors and render information to clients, customers, suppliers, employees and a host of stakeholders. User credentials, financial and payment information, secret passwords, company statistics may all be resident within a database and accessed by legitimate users through off-the-shelf and custom web applications. SQL Injection attack is the hacking technique which attempts to pass SQL commands through a web application for execution by the backend database. If not implemented properly, web applications may result in SQL Injection attacks that allow hackers to view and collect information from the database.

ISSN 2394 - 7780

Take a simple login page where a legitimate user would enter his username and password combination to enter a secure area to view his personal details or upload his comments and details in a forum. When the legitimate user submits his data, an SQL query is generated from these data and submitted to the database for verification. If valid, the user is allowed access the system. That is, the web application that controls the login page will communicate with the database through a series of planned commands so as to verify the username and password combination. On verification process, the legitimate user is granted appropriate access. Through SQL Injection, the hacker may input specifically created SQL commands with the intent of bypassing the login form barrier and seeing what lies behind it. This is only possible if the inputs are not properly implemented (i.e., made invulnerable) and sent directly with the SQL query to the database. SQL Injection vulnerabilities provide the means for an attacker to communicate directly to the database [12].

3. TYPES OF SQL INJECTION VULNERABILITIES

The SQL injection attacks can be done through various techniques. Some of them are specified below:

3.1. TAUTOLOGY ATTACK

The main objective of tautology-based attack is to inject code in conditional statements so that they are always evaluated as true. Using tautologies, the hacker wishes to either bypass user authentication or insert inject-able parameters or extract data from the database [12]. A typical SQL tautology has the form, where the comparison expression uses one or more relational operators to compare operands and generate an always true condition. Bypassing authentication page and collecting data is the most common example of this kind of attack. In this type of attack, the attacker exploits an inject-able field contained in the" WHERE" clause of query. Attacker transforms this conditional query into a tautology and hence causes all the rows in the database table targeted by the query to be returned. **For example: - SELECT * FROM user WHERE id= '1'or '1=1'- 'AND password= '12345'; "or 1=1" the most commonly known tautology.**

3.2. LOGICALLY INCORRECT QUERY ATTACKS

By providing incorrect data in the input field, the database might return some important information about the database, its fields and the database name. Continuously usage of this attack might compromise the security of the database [10]. The main objective of the Illegal/Logically Incorrect Queries based SQL Attacks is to gather the information about the back end, database of the Web Application. When a query is rejected, an error message is returned from the database which includes useful debugging information. This error messages help attacker to find vulnerable parameters in the application and consequently database of the application [8].

For Example:

1. Original URL:http://www.toolsmarketal.com/veglat/? id_nav=2234556

2. SQL Injection: http://www.toolsmarket-al/veglat/? id_nav=223456

3. Error message showed: SELECT name FROM Employee WHERE id=223455\ '. From the message error we get the name of table and fields: name; Employee; Id by the gained information attacker can organize more perfect attacks. The Illegal/Logically Incorrect Queries based SQL attack is considered as the basis step for all the other attacking techniques.

3.3. UNION QUERY

In this technique, attackers join injected query to the safe query by the word UNION and then can get data about other tables from the application.

For Example: Following executed from the server:

SELECT name, phone FROM tbl_user WHERE userid=$id1

By injecting the following Id value into:

$id1= 1 UNION ALL SELECT credit Card Number, 1 FROM Credit CardTable

Then we will have the following query:

SELECT name, phone FROM tbl_user WHERE userid1 =1 UNION ALL SELECT creditCardNumber, 1 FROM Credit CardTable This will join the result of the original query with all the credit card users to the attacker.

4. RESEARCH METHODOLOGY

We propose a technique to prevent all the SQL injection attacks by using encryption techniques.

ISSN 2394 - 7780

- Master Key Generation
- AES Algorithm

4.1 SQL SERVER AND DATABASE ENCRYPTION KEYS

Encryption keys are used by SQL Server to help secure data, credentials and connection information that is stored in a server database. There are two kinds of keys: **Symmetric and Asymmetric** Keys in SQL Server. Symmetric keys use the same password to encrypt and decrypt data. Asymmetric keys use one password to encrypt data (called the public key) and another to decrypt data (called the private key).

SQL Server has two primary applications for keys: a service master key (SMK) generated on and for a SQL Server instance, and a database master key (DMK) used for a database. The Service Master Key is the root of the SQL Server encryption hierarchy. The SMK is generated automatically the first time the SQL Server instance is started and is used to encrypt a linked server password, credentials, and the database master key. Whereas, the database master key is a symmetric key that is used to protect the private keys of certificates and asymmetric keys that are present in the database. It can also be used to encrypt data.

4.2 CREATE MASTER KEY

```
CREATE MASTER KEY ENCRYPTION BY PASSWORD = '23987hxJ#KL95234nl0zBe';
```

The following example creates a database master key for the current database. The key is encrypted using the password **'23987hxJ#KL95234nl0zBe'.** The master key is encrypted by using the AES_256 algorithm and a user-supplied password.

4.3 AES ENCRYPTION

AES or Advanced Encryption is a cipher i.e. a method of encrypting and decrypting information. Since 1977, the US government used a cipher called DES (Data Encryption Standard) to protect sensitive, unclassified information. A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack.

The AES algorithm was ultimately selected and declared a Federal Information Processing Standards or FIPS standard by the NIST (National Institute of Standards and Technology) in 2001. AES belongs to a family of ciphers which is known as block ciphers. A block cipher is an algorithm that encrypts data on a per-block basis. The size of each block is usually measured in bits. AES, for example, is 128 bits long, which means AES will operate on 128 bits of plaintext to produce 128 bits of ciphertext. AES requires the use of keys during the encryption and decryption processes. AES supports three keys with different lengths: **128-bit, 192-bit, and 256-bit keys**. The longer the key, the stronger the encryption. So, AES 128 encryption is the least strong, while AES 256 encryption is the strongest.

4.3.1 HOW IS THE AES ENCRYPTION ALGORITHM USED IN SECURE FILE TRANSFERS?

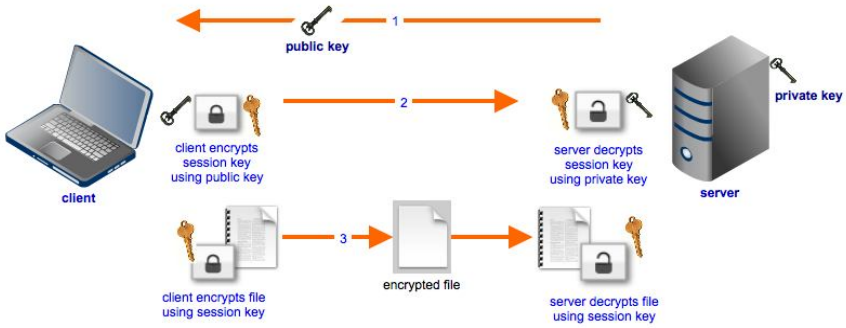


Figure-1: [Source: https://www.jscape.com/blog/aes-encryption]

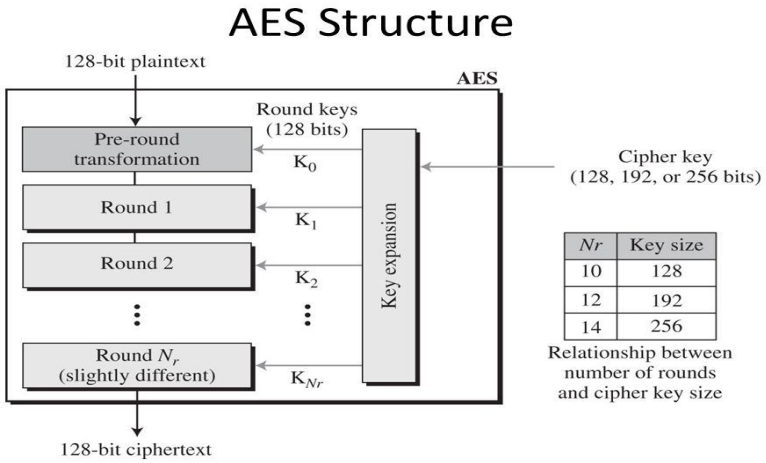
4.3.2 FEATURES OF AES

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

ISSN 2394 - 7780

4.4 STRUCTURE OF AES

AES is an iterative rather than Feistel cipher. It is based on 'substitution–permutation network'. AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix − The number of rounds in AES is variable and depends on the length of the key. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.



Nr	Key size
10	128
12	192
14	256

Figure-2: [Source: https://scanftree.com/cryptography/advanced-encryption-standard]

AES comprises three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. Symmetric (also known as secret-key) ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know -- and use -- the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of cipher text.

For encryption, each round consists of the following four steps:

- **Substitute bytes**: SubBytes mean substitution of byte of the state array by searching in lookup table which is called substitution box or S-box. S-box is a 16*16 lookup table and it contains 256 different values. The S-box table contains all possible values for 8-bit sequence that means in decimal 0 to 255. Each byte of the state array is the input of this SubBytes step and the input byte is alternated by a corresponding value. The AES S-Box is shown in the Table below.

	0	1	2	3	4	5	6	7	8	9	0a	0b	0c	0d	0e	0f
0	63	7c	77	7b	f2	6b	6f	c5	30	1	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	4	c7	23	c3	18	96	5	9a	7	12	80	e2	eb	27	b2	75
40	9	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	0	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	2	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	6	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	8
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	3	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure-3: [https://www.commonlounge.com]

ISSN 2394 - 7780

- **Shift rows:** The ShiftRow function performs byte wise circular shifts on last three rows of the state. In this function, first row is not rotated, but second, third, and fourth rows are rotated by one, two, three bytes respectively. This rotation provides diffusion property of the AES algorithm.

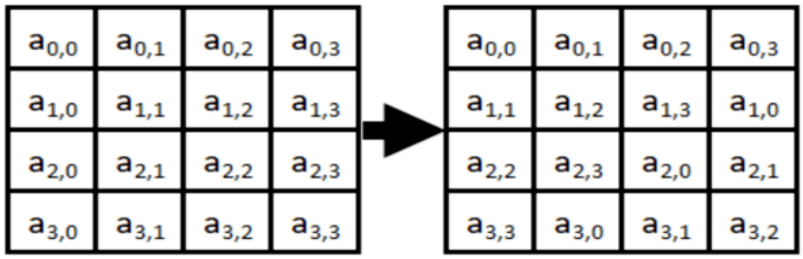


Figure-4: [https://www.commonlounge.com]

- **Mix columns:** From the Mix Column operations, there is a transposition of linear transformation made to join the 4-byte in each column. The task of this step is to take 4-byte as input and outputs 4-byte, where every input bytes have an effect on all the output 4-byte. Each column is transformed using fixed matrix operations; this is composed of multiplication and addition of the entries.

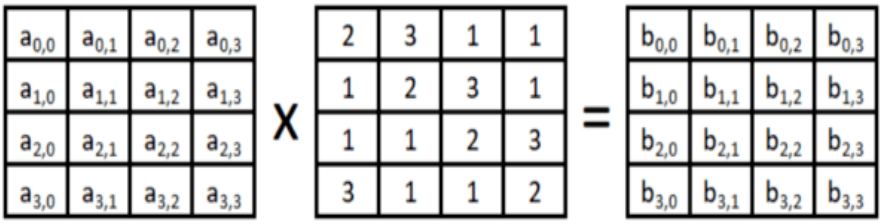


Figure-5: [https://www.commonlounge.com]

- **Add round key:** For every round in the AddRoundKey step, a subkey is generated from the main key by means of Rijndael's key schedule. The subkey is inserted by combining every byte in the state with it related byte in the subkey by means of bitwise XOR. For the first word of the round key, the value used in the exclusive-or is the result of passing the last word of the previous round key through the g function.

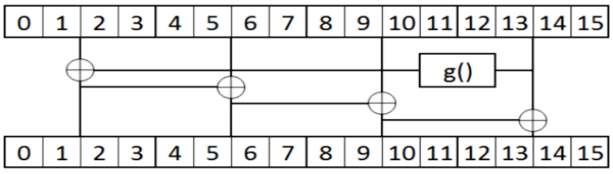


Figure-6: [https://www.commonlounge.com]

5. RESULT AND ANALYSIS

In this research, smartsniff tool is used to protect web applications from SQL injection attack. If the data is in plain text format, it becomes easier for the hacker to exploit the data, but, if the data is in Encrypted format (Cipher) it is unreadable. Using **Smartsniff** tool, all the active Unencrypted packets were captured and the details were displayed in the separate window.

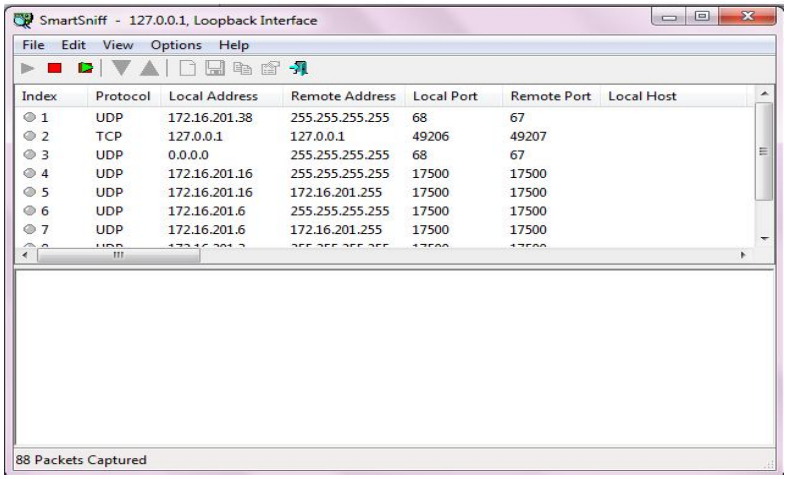


Figure-7

ISSN 2394 - 7780

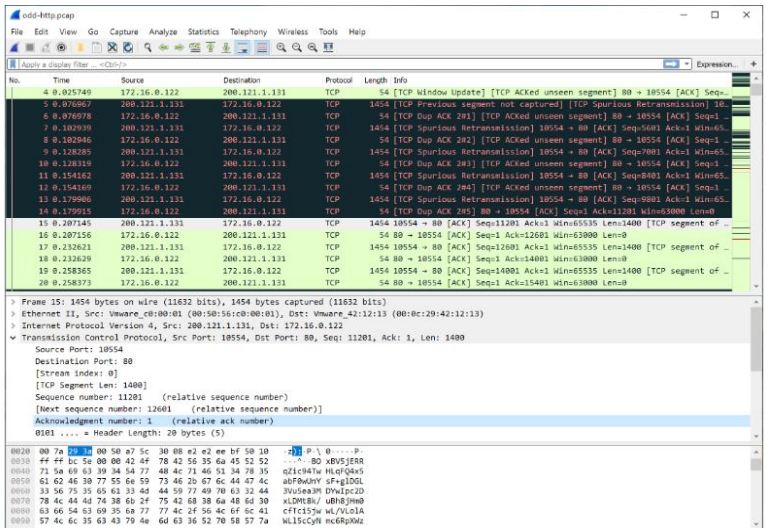


Figure-7.1

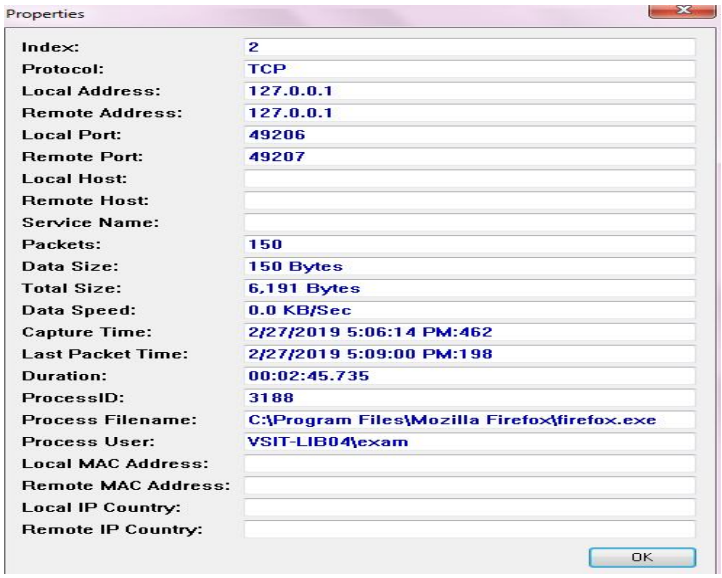


Figure-7.2 [Information about the captured TCP packet]

CONCLUSION

We have studied the existing Advanced Encryption Standard and its implementation. We have also done the analysis and comparison of the captured unencrypted packets over the network using various tools. Many methods have been used to avoid SQL Injection attacks but no feasible solution is available. Encryption algorithms play important roles to protect original and confidential data from unauthorized access. This paper covered the different types of vulnerabilities and most powerful and widely supported AES algorithm for SQL Injection prevention.

REFERENCES

1. Zainab S. Alwan et al, International Journal of Computer Science and Mobile Computing, Vol.6 Issue.8, August- 2017
2. International Journal of Computer and Communication Engineering, Vol. 2, No. 5, September 2013
3. Li Qian, Zhenyuan Zhu, lun Hu, Shuying Liu - 2015 International Conference on Estimation, Detection and Information Fusion (ICEDIF 2015)
4. Inyong Lee a , Soonki Jeong b , Sangsoo Yeoc , Jongsub Moond,□, A novel method for SQL injection attack detection based on removing SQL query attribute values, Mathematical and Computer Modelling 55 (2012) 58–68
5. A Survey on SQL Injection Attacks, Detection and Prevention Techniques, IEEE20180

ISSN 2394 - 7780

6. SQL Injection Prevention Using Query Parsing, International Journal of New Innovations in Engineering and Technology (IJNIET)
7. Generation of SQL-injection free secure algorithm to detect and prevent SQL-injection attacks, Kanchana Natarajana , Sarala Subramanib, Department of IT, School of Computer Science & Engineering, Bharathiar University, Coimbatore-641046, Tamilnadu, India
8. Hong Ma, Tsu-Yang Wu , Min Chen, Rong-Hua Yang, and Jeng-Shyang Pan, A Parse Tree-Based NoSQL Injection Attacks Detection Mechanism, Journal of Information Hiding and Multimedia Signal Processing c 2017 ISSN 2073-4212 Ubiquitous International Volume 8, Number 4, July 2017
9. Chaturvedi et al., International Journal of Advanced Research in Computer Science and Software Engineering 6(3), March - 2016, pp. 106-110
10. International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106, Volume-5, Issue-7, Jul.-2017
11. Gregory T. Buehrer, Bruce W. Weide, and Paolo A. G. Sivilotti, Using Parse Tree Validation to Prevent SQL Injection Attacks
12. Dinu P S1 , Deepa S Kumar2 , Dr. M. Abdul Rahman3, Preventing SQL injection Attacks Using Cryptography Methods, International Journal of Scientific Research Engineering & Technology (IJSRET), ISSN 2278 – 0882 Volume 4, Issue 5, May 2015
13. Web Security by Preventing SQL Injection Using Encryption in Stored Procedures, Deevi Radha Rani, B.Siva Kumar, L.Taraka Rama Rao, V.T.Sai Jagadish, M.Pradeep, Deevi Radha Rani et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (2) , 2012,3689-3692
14. USING HASH ALGORITHM TO DETECT SQL INJECTION VULNERABILITY *Maki Mahdi, Ahmed Hashim Mohammad, INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS ISSN 2320-7345
15. SQL-injection vulnerability scanning tool for automatic creation of SQL-injection attacks, A. Bashah Mat Ali et al. / Procedia Computer Science 3 (2011) 453–45
16. Ako Muhamad Abdullah, Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data, Publication Date: June 16, 2017
17. Isaac Kofi Nti* , Eric Gymfi and Owusu Nyarko, Implementation of Advanced Encryption Standard Algorithm with Key Length of 256 Bits for Preventing Data Loss in an Organization, Nti et al., Int J Adv Techno 2017, 8:2 DOI: 10.4172/0976-4860.1000183

WEB REFERENCES

1. https://www.brainkart.com/article/AES(Advanced-Encryption-Standard)-Structure_8408/
2. https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard
3. https://www.commonlounge.com/discussion/e32fdd267aaa4240a4464723bc74d0a5
4. https://docs.microsoft.com/en-us/sql/t-sql/statements/create-master-key-transact-sql?view=sql-server-2017
5. https://sqlity.net/en/2373/create-database-master-key/
6. https://docs.oracle.com/goldengate/c1230/gg-winux/OGGSE/encrypting-data-master-key-and-wallet-method.htm#OGGSE-GUID-9401E5C0-D574-4A5C-A61B-3DCFDD275CF0

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

A PERSPECTIVE ON MASS SURVEILLENCE OF A SMART CITY IN INDIA BASED ON INTERNET OF THINGS (IOT)

Arti Gavas
Assistant Professor, Information Technology, Anna Leela College of Commerce and Economics, Shobha Jayaram Shetty College For BMS, Kurla (E)

ABSTRACT

We live in age of mass surveillance and big data is mixed with ever increasing power of Artificial Intelligence makes all our actions being recorded and stored like never before. This information is being mined to identify social media trends for targeted advertisement. But it is also been used to predict riots, election outcomes, disease epidemics and to track crowds (CCTV footages) in real time.

A computer forecasting systems that sweeps through the data that we post on social media every day. It mines the posts from Facebook twitter and it analyses them with restaurant apps, traffic maps, currency rates and even food prices. Systems mine big data from trends rather than analyzing individual's information. For ex. Mass cancellation at restaurant bookings and in an hospital's parking lot filled up. The system can predict that there is probably outbreak of food poisoning or flue. But such systems do have its limits. It can't mine the public data to forecast social events before they happen. It can't predict the spontaneous events like crowd stamped, terrorist attacks. Real time CCTV footage at public places can be used to track the individual faces and individuals actions to forecast such spontaneous events up to some extents. This is where Internet of Things and AI can be helpful in crowd analysis. It can help spy abnormal patterns in crowd and ultimately saving lives.

Sophistication in technology has greatly reduced hustles and bustles of our life Internet of Things is that sophistication in technology where all those activities which can be mechanized in some way can be made possible through it. It has increased world connectivity enormously. IoT technology is proving itself a transformative technology in mass surveillance.

The aim of this research paper is to introduce power of IoT in mass surveillance and to evaluate future avenues with IoT based smart cities. It also aims at highlighting the scenario regarding analyzing and making sense out of data which is obtained through mass surveillance for wellbeing of humanity.

Keywords: Mass Surveillance, IoT, Artificial Intelligence, smart city, sensors, proliferation of IoT devices, Challenges in IoT.

OBJECTIVES

1) To provide insight into mass surveillance and predicting future events through Computers.
2) To study different computer based systems currently available to forecast future chain of events.
3) To define IoT and to illustrate various capabilities of IoT devices.
4) To design IoT based new model/ framework for Smart Cities in India.

RESEARCH METHODOLOGY

1) The research methodology adapted for aforementioned objectives to fulfill is basically a literature review and evaluation of secondary data available on web resources.
2) Literature review gave the insight about various IoT based mass surveillance systems available currently.
3) It also provided a deep awareness that IoT devices produces enormously huge amount of data which needs proper data storage, data mining and data interpretation techniques.

INTRODUCTION

1) Mass Surveillance to forecast future chain of Events using Computers

Mass surveillance deals with the complex observation of a world population in order to supervise people in crowd. Such surveillance is generally done at public places like railway stations, banks, shopping mall, food courts, hospitals, education hubs etc. Surveillance can also be performed on social media sites too. The surveillance is generally performed by government agencies and it is carried out with each nation's laws and judicial systems. The legal issues and various permissions to carry out such surveillance varies county by country.

Mass surveillance is a necessity in today's vulnerable world. It can be used to predict terrorism, crime or social unrest, public health issues etc. Some mechanism can be deployed to prevent such unpleasant happenings. On

ISSN 2394 - 7780

contrary mass surveillance is perceived as violating privacy rights or freedoms. It is often criticized for being monitoring and controlling tool at public places.

Computing devices play vital role in acquisition of data, storage of data, dissemination of data, analyzing of data and presenting data for general prediction to specialized prediction. So far separate but mostly general purpose computing devices were the choice to perform aforementioned steps in order to get proper mass surveillance data repository. IoT can have single specialized computing device which can perform all of these steps. Such devices can acquire data using various sensors, they can simultaneously send this data on cloud storage, they can communicate with other computing devices for data dissemination.

2. Existing computer based systems in India for mass surveillance

- Central Monitoring System (CMS): This system is basically a data collection system which facilitates Government of India to eavesdrop to phone conversations, intercept e-mails and text messages, and supervises posts on social networking sites and also to track Google searches.
- DRDO NETRA: This system is actually a network which can track your communication online on a real time basis by yielding data from various voice-over-IP services, including Google Talk and Skype. This system is monitored and controlled by the Research and Analysis Wing.
- NATGRID: It is an intelligent system which links the databases of various ministries and Departments of Government of India.

All of the above systems use the power of computing devices for acquiring the data from various sources and disseminating information to the various sources. Most of these systems require human intelligence to conclude the intelligent meaning out of this gathered data. We can bring IoT techniques in this practice to develop AI based Expert Systems.

3. Defining INTERNET OF THINGS (IoT)

The internet of things (IoT) are the physical objects that we use in our daily life which have computing ability to think and act in real world with the help of sensors, actuators and processors while being connected to the internet and being able to identify themselves and discoverable to other devices.

3.1Capabilities of IoT devices with respect to Surveillance.

IoT devices can form an intelligent network citywide which can have capabilities like intelligent identifying, locating, Tracking, monitoring, and managing things 24x07. Various evolutions in technology, increasing computing power, increased storage capacity, and battery backups are strengthening this IoT networks more. Moreover these capabilities are becoming available at low cost and low size. This trend is also facilitating the growth of tremendous small-scale electronic devices with identification/communication/computing capabilities, which could be entrenched in other devices, systems, and facilities.

3.2 IoT exhibits following capabilities to perform mass surveillance

1). Broad Perception

IoT can use various types of sensors like temperature sensors, moisture sensor, humidity sensors, RFID sensors; smell sensors to capture different input types, there is not be a limit on types of input that IoT devices can capture.

2). Accessible Transmission

IoT devices use existing underlying transmission networks to communicate over the internet with other such devices. It uses standard protocols and standards to communicate.

3). Intelligent Processing

Along with sensors IoT devices contains processor which can process the acquired data intelligently. Also it has internet connectivity which can be used to connect to various databases while processing.

4). Tracking mobile asset

Assets can be equipped with position sensors and communication interface to turn them into IoT devices. Such assets can track themselves.

5). Effective fleet management

Vehicles can have location sensors and internet connectivity which can be harvested to schedule effective fleet management. Vehicles and drivers can be assigned to specific route based on business requirement in real time.

ISSN 2394 - 7780

6). Traffic information system

These types of system can sense the traffic conditions like congestion, accident, emergency etc, and can communicate to traffic police or to the hospitals.

7). Sensing environmental changes

Such types of systems can sense physical and chemical changes in the environment. They can process the data collected by various sensors in environment and can produce intelligent reports describing the action to be taken.

8). Remote Controlling

IoT based Drone systems are the best systems to collect data from such areas where human can't reach due some kind of physical limitations of environment. Such devices can be used as remote sensing devices which can withstand any types of harsh environment to collect data.

9). Intelligent Appliance control

IoT devices can get indication from ones' gesture. In mass surveillance IoT devices can focus on any objectionable behavior to record real time footage more clearly for further investigation.

10). Formation of Ad Hoc Network

Several IoT devices can collectively form an Ad-hoc network during emergency or during disaster management in a city. They can simultaneously collect data, process data as well as disseminate the data to appropriate destinations like police stations, hospitals, city centers, educational hubs etc.

4. IoT based framework of Smart Cities in India for mass surveillance

4.1 At Banks

Every office is covered under CCTV surveillance now days. Banks also have several CCTVs deployed at various angles. If robbery situation is detected by any employee of the bank, he/she will press the security alarm. Using location of alarm and gesture of employee the IoT based CCTVs can focus and zoom in at appropriate place where robber is standing to record real time footage. Simultaneously it can send an emergency message or can make an emergency call in such situations to police.

4.2 At Railway Stations

Railway stations are already doing mass surveillance using CCTVs. These CCTVs can be made smarter with the help of IoT enabled capabilities. Intelligent Cameras can sense the future events like stampede situation or terrorist attacks by facial expression of someone amongst mass. It can compare those possible terrorists' faces with the database available on internet and can inform concern authorities about it.

4.3 At Road Traffic

IoT enabled devices can be deployed at roads to observe the smooth functioning on road. They can detect abnormal speed, direction or any abnormal behavior of a driver. For example if driver is about to get a heart attack or epilepsy, there will be a sudden change in direction and way of driving. IoT enabled cameras can detect it and can pass on the message to hospitals and doctors informing about potential patient in a city.

4.4 Framework Diagram

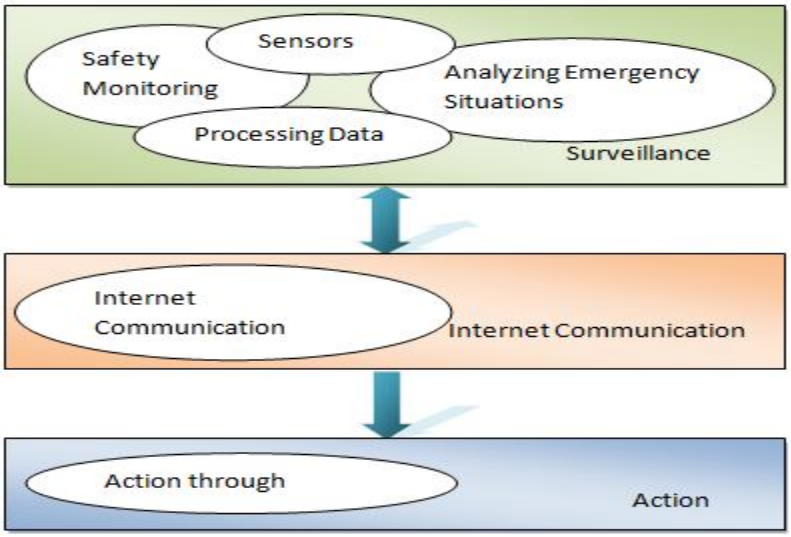


Fig: 3 stage architecture of IoT based Mass Surveillance

ISSN 2394 - 7780

FINDINGS AND RECOMMENDATIONS

Due to enormous sophistication in technology proliferation of digital devices is predicted to be exponential. With the advancement and maturity of distributed intelligent information processing technologies, IoT systems will be able to make clever sensing broadly obtainable through information sharing and association. The regular establishment and improvement of the standards system will definitely bring IoT into our day to day life. The IoT brings an opportunity for the mass surveillance services, thus enhancing the commercial and social potential future of mankind.

CONCLUSION

The IoT includes several technologies such as Artificial Intelligence, information technology, communication technology, advanced embedded electronics, cloud computing etc. IoT is deploying newer information repository and knowledge economy which needs to be analyzed against social wellbeing. But the challenges from research areas, business areas, and the government will keep us investigating newer and clever technologies like AI or IoT. The main challenges in IoT devices development is getting the information from heterogeneous sources, in reducing costs of devise, reducing power requirements of such devices, improving data storage and processing power and in improving overall efficiencies. Another challenge IoT has brought is lack of fundamental theory support, vague architecture, and not fully formed standards.

To make Indian metro cities as IoT based smart cities a number of demonstration application projects such as the smart city and the intelligent transportation system in public IoT applications, intelligent emergency systems, and intelligent supervision in industry applications to ensure safety and security to be practiced. The future of IoT will be expected to be united, flawless, and pervasive. Finally, the expansions of IoT as an intelligent surveillance system can be proceeding with interoperability, energy sustainability, privacy, and security. IoT is turning out to be an foreseeable trend of development of information industry, which bound to bring new changes to our lives.

BIBILOGRAPHY

1) A Vision of IoT: Applications, Challenges,and Opportunities With China Perspective
[Shanzhi Chen, Senior Member, IEEE, Hui Xu, Dake Liu, Senior Member, IEEE, Bo Hu, and Hucheng Wang

2) Privacy and The Internet of Things: Perspectives on Mass Surveillance in the United States
[Nishant Jain CPSC 610 4/25/18]

3) An Efficient Algorithm for Media-based Surveillance System (EAMSuS) in IoT smart city framework
[Vasileios A. Memos, Kostas E. Psannis, Yutaka Ishibashi, Byung-Gyu Kim, B.B Gupta]

4) Designing the Internet of Things (Book)

[Adrian McEwen, Hakim Cassimally]

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

IOT BASED SMART AUTOMATION USING DRONES & HOME MONITORING OWL

Pinki Pandey
JVM's Mehta Degree College, Navi Mumbai

ABSTRACT
Drones are defined as Unmanned Aerial Vehicles (UAVs). In other words drones are flying devices that are autonomously programmed or remotely controlled, either by a remote control or a ground station, and are categorized as networked robotic technologies. Unfortunately, drones haven't had a big impact on agricultural practices, at least until recently. A lot is happening lately on the subject of drone applications in agriculture and precision farming but drones is mostly use in Military fields.
The first drones were applied for military functions long before the looks of IOT devices.

Drones as military weapons were strong, fast, durable, using a classic, or jet engine.

The operate of home security system share an excellent deal in common good home security system as trycreate to form a sensible and safe home and make your family feelsafer and secure. One of the big differences is that drone security system cannot hover around the property 24/7 because the battery cannot sustain long hour surveillance.

INTRODUCTION
'IOT' was formulated as the term 'Internet of Things' was coined by Kevin Ashton.IOT can be any device and this device contain sensor with the ability to collect and transfer data over a network the embedded technology in the object help them to interact with internal status and external environment which in-turn help in decision making.
The application of hardware and software with regard to smart drones depends on the setup of the device and the purpose. It is differentiated between autonomous and single person/shared control, also-called swarm UAVs. Six of Earth's seven continents square measure for good settled on an outsized scale. The overall solution is determined necessary was a set of "dashboard-driven connected services utilizing an IOT backend" that would accomplish several key things:

TYPES OF DRONES
1. single-rotor helicopter
2. multi-rotor
3. fixed wing hybrid VTOL
4. fixed wing

TYPES OF SENSORS USED IN DRONES
There are differing types of sensors which will be employed in a drone to record differing types of changes and collect a spread of knowledge.

1. Speed and Distance Sensors
These sensors will be wont to discover the speed of the drone or activity the gap between drone and another object, without actual physical contact with the object.

This can be tired many ways, such as:
- Sonar-pulse distance sensing
- Light-pulse distance sensing
- Magnetic-field change sensing

2. Infrared and Thermal sensors
The potential uses for infrared sensors, especially in cameras, are vast and include search and rescue, surveillance, crop and forest health, pipeline inspection, leak detection etc., depending upon the precision of the sensor.

Infrared isn't visible to the human eyes however one will most likely feel it typically as radiated heat once its intensity is high.

A thermal camera will therefore sight areas of upper temperatures.

ISSN 2394 - 7780

It will reveal warming sections of electrical instrumentation in varied devices like switch-gears and substations.

A drone will facilitate to sight these sections from a distance and increase the security of human personnel.They can even be used for vision and police work.

3. Image sensors

An image detector will sight and convey info regarding what constitutes a picture.

It is done by changing the variable attenuation of sunshine waves into signals.

They are utilized in the cameras that the drones carry to make a digital image of the photographs taken by the drone.

They can be used for various purposes such as thermograph, creation of multispectral images, sensor arrays for x-rays and other highly sensitive arrays for astronomy.

4. Chemical Sensors

A chemical detector, in kind could be a is a self-contained device, will be connected drone in order to provide information about the chemical composition of any atmosphere.

With the modification within the chemical composition of the setting, analyte molecules inside the device interact selectively with the molecules present on the environment.

NEW TECHNOLOGY USED IN DRONES

AIR MAP

Air Map is the leading provider of aeronautical data & services to UAV's.AirMap is the leading global provider of aeronautical data & services to unmanned aircraft, or drones.

Use Air Map to keep up situational awareness, request digital authorization, get traffic alerts

Air Map offers these features and more:

- Toggle between multiple map styles
- Discover airspace rules and advisories by sorting out a location or panning and zooming Air Map's responsive vector maps
- set up a flight path to specific period, altitude, and airspace requirements
- hook up with any supported DJI drone to fly and toggle camera settings directly from the Air Map app
- controlled airspaces
- Send digital flight notice to collaborating U.S. airports
- Get time period traffic alerts for close manned craft

ISSN 2394 - 7780

CAMERA

TRNDLabs has just launched the SKEYE Nano Drone, this company launch smallest camera in the world. Its measures just 1.57" 1.57"0.87.
Their cameras technologies, delicacies may are available little packages.

The camera clocks in at modest zero.3 megapixels – 300,000 pixels with full video capability.

BOM DETECTION

Add to that, effective cameras and this makes the drones suitable for purposes of bomb detection. Thus, these aerial vehicles are apt for making us aware of unexploded bombs and soldiers save lives.

Parachute

It enables automated parachute recovery in case of battery failure. Convenient clip-on solution will allow M210 to be packed in its carry case without any modifications.

APPLICATION OF DRONES

DRONE DETECTION FOR CRITICAL INFRASTRUCTURE

Unprotected critical infrastructure such as nuclear and electrical power plants, refineries and energy and water utility companies are easy targets for unauthorized drawn activity and thus if left unprotected pose a threat to public safety. In the worst case a drone attack with explosives it is extremely important to detect and feed of attack in these areas

HAREWARE

The drone detector is predicated on the Aaronia IsoLOG 3D antenna, a real-time spectrum analyzer (XFR V5 PRO, RR or RF Command Center) and a special software plug-in for theRTSA Suite software.

Combining of these parts permits for 24/7 observation and recording with uninterrupted knowledge streaming.

The system saves extensive measure time, and is both compact and flexible.

It will be established at nearly anywhere you wish to protect.

ISSN 2394 - 7780

DISASTER MANAGEMENT

Natural and artificial disasters destroy environments, usually creating conditions therefore tough that relief employees square measure unable to access areas and supply help.

Drones have the ability to take on roles where relief workers and manned vehicles fall short and it is also help to identify on which area affected or safe. After natural disaster or terrorist attacks, in this area that are not possible to reach, drones can supplies such as water and food to peoples needs.

- Hazardous chemical spills
- The need for mapping
- Assessing structural damage
- Delivering emergency infrastructures and supplies
- Extinguishing wild fires

LAW ENFORCEMENT

Drones used to assist in monitoring criminal and illegal activities and also used to track the smugglers, terrorist or illegal drugs transportation. Many country started to use drones for reduce traffic on a road. law enforcement leading the pack in acquisitions.

If your local department doesn't have a UAS, it's likely that the conversation about acquiring one has already started.From accident reconstruction to look and rescue, the utility of the technology cannot be overstated.

Here square measure 5 applications for drones in enforcement.

- Traffic accident reconstruction
- Search and rescue
- Active shooter response
- Surveillance and crowd monitoring

MINING

Drones have well-tried themselves within the mining trade as associate economical replacement for ground based mostly survey ways.They go on the far side mensuration, allowing for aerial photo and video capture for a wide variety of uses.

Drones in mining can be used for constant measurement and assessment of the physical material. With unique cameras, drones in mining can be useful in volumetric data capturing of ore, rock and minerals storage which is extremely difficult to measure manually.

Airbotics drone is quite famous in mining which provides an industrial grade on-site drone solution used by mining companies for measuring materials, surveying operations, and general security. It is fully autonomous and stored in on-site housing that can swap cameras and batteries on its own.

TELECOMMUNICATIONS

To ensure service reliability frequent inspection of Telecommunication towers is very vital. In this drones can play an important role where they can quickly assess the damage so that repair teams could be deployed to restore service. With the advent of drone, the service has become more easy, danger-free and less time-consuming.

WILDLIFE STUDY &PRESERVATION

Drones may also be used for watching life while not heavy the animals.

In recent times, the use of drones by wildlife sanctuaries to monitor the activities of animals has increased, especially for species of animals that are on the verge of extinction and preserving them is a prime concern.

Drones have served as a deterrent to poachers.They provide unexampled protection to animals, like elephants, rhinos, and big cats, a favorite target for poachers.With its thermal cameras and sensors, drones have the ability to operate during the night.This enables them to monitor and research on wildlife without causing any disturbance and provides insight on their patterns, behavior, and habitat.

ISSN 2394 - 7780

INTERACTIVE HOME MONITORING OWL

Ulo creates a novel bond, like no other device. It redefines the approach you act with objects: associate organic communication. The language of our eyes is one in every of the foremost powerful and effective tools of non-verbal communication.Smart home security system, as strive to your family feel safer and secure.Ulo could be a cute police investigation camera, a pet raptor interacting with you thru eye expression. Home surveillance system in many aspect, such as 24/7 monitoring, motion detection, impact on privacy, regulation, etc

Eye expressions area unit AN economical, natural and universal thanks to connect instantly with Ulo.

- A - 2 Round 1,22" LCD screen
- B - 1 Hidden surveillance camera (1080p HD / 30 fps) & Motion Sensor under the two-way mirror beak
- C - 1 Mono Microphone
- D - 1 Capacitive button
- E - 1 Neodymium magnet under the rotative base
- F - 4 Adhesive neodymium magnets (⌀20mm/⌀0.8in)
- G - 1 Wifi 802.11ac module
- H - 1 Orientation sensor
- I - 1 Li-Po rechargeable battery
- J - 1 micro-USB to USB cable (65cm/25.6in)
- K - 1 Speaker

ISSN 2394 - 7780

CONCLUSION

Internet of Things shapes a human life with good connectivity and ultimate functionality and helps in improving end user experience.

In any case, executive authorities shall market the use of drones well, because the majority of people is poorly informed and relates drones to military. Thus negative connotations exist in people's minds, representing a barrier that needs to be overcome in order to be accepted by society. Positive applications, such as search-and-rescue, border patrol, firefighting missions etc. can lead to a safer life and save lifes. Communicating clearly and transparent about all related sensitive threats and risks shall create trust and understanding. In agriculture, there is a quite research and development has been done. The economy of eastern countries is still depends on the agriculture.

The implementation of drone will reduce the time and efficiency of the production which leads the higher production. At the same time the cost of the IOT implementation needs to be reduced. This will enable the small farmers to utilize the smart agriculture. The farmer needs to be educated or the agriculture studies could have separate subjects about the current development of IOT and the connected smart world. The fully customizable modular approach needs to be enabled in the agriculture software for adopt the vast area of the agriculture segments. Most of the IOT products running on the electricity; but the new technologies need to be inventing like sensors running on the bio gas for implementing the IOT on the rural area.

Now a days the mobile networks are focusing on urban areas compared to the rural area. So we need to find the new technology that can enable ad-hoc joining of the rural area in the existing mobile networks with the small device. The investment time-consuming.

In the Ulo surveillance camera the Alert Mode is easily and quickly enables during times in which the user's smartphone is no longer a part of the Wi-Fi network. Ulo lasts 2 days on a single charge, laying flat or mounted. Added features include night vision, waterproof design, and flexible compatibility with a number of devices.

REFERENCE

- TED XBGU
- https://www.allerin.com
- https://www.kickstarter.com
- https://www.dronethusiast.com
- https://blog.marketresearch.com/8-key-military-applications-for-artificial-intelligence-in-2018
- https://unsplash.com/search/photos/drone

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

THE NEED OF RESPONSIBLE AND ETHICAL FRAMEWORK IN ORDER TO USE SOCIALMEDIA INTELLIGENCE FOR BETTERMENT OF MANKIND

Amey Patankar
Inspector, Central Tax and Customs, GST East Commissionerate, Bengaluru Zone, Bachelor of Engineering, (EXTC), Mumbai University

ABSTRACT
IN today's modern times, the data in form of personal, social is available on the internet through various social networking websites which has a great potential to impact the lives of millions of people. Unaware of its adverse impact, many a times, disaster like situation arises where taking control of situation becomes a herculean task as masses, media, sometimes private organizations or governments are involved directly or indirectly. In this paper, various possible guidelines or techniques are discussed which could be used while analyzing social media data or while using certain tools. I sincerely hope that these methods prove to be effective and the power of social media intelligence be used in good manner for a larger base of human population.

INTRODUCTION
Since May 2018, there have been 29 cases of persons being lynched to death in India where no political angle was involved, neither religious dispute nor even cast, neither jihad nor naxalism. These misfortunate killings were because of a rumor about a child lifting gang which was spread like a wildfire throughout India and which alleged that many kidnappers have entered the state and safety of children is under potential threat. In the state of Tripura, government appointed announcer to dispel the rumor himself was lynched to death.

In such case, who shall be held responsible for such killings? It is clear that mere announcements urging people not to believe in such rumors by the government will not help. Our authorities need to tackle such 'never faced before' situations and emergencies arriving out of Social media using intelligence derived from same Social media with methodological and ethical framework within which it will be used.

What is Social Media Intelligence?
Social media intelligence (SMI or SOCMINT) refers to the collective tools and solutions that allow organizations to monitor social channels and conversations, respond to social signals and synthesize social data points into meaningful trends and analysis based on the user's needs. Social media intelligence allows one to collect intelligence gathering from social media sites, using both intrusive or non-intrusive means, from open and closed social networks.

Why is it necessary?
If we look at the necessity of SOCMINT through economical angle or in respect of a organization say E-commerce company, it is absolutely necessary for them to have data fetched from various websites like Google, Face Book, Twitter etc giving them valuable information about trends and mindset of people (rather customers). The tools used thereby give such information to the owners of the company which is further applied to make change in the product or services and thus enhancing the profit of the company.

Success of the SOCMINT does not depend on the accuracy of the data or information it has provided but its usefulness in the process of Decision making. Otherwise, it may result in doing harm or collateral damage to the suspects who are actually innocents.

Access of the data
After any incident or major event in India, for eg. Mumbai attacks, Elections or natural calamity, the social media is flooded with various responses in form of opinions, images, videos, hash tags etc. This flood of information in the form of large data sets cannot be used directly. Various selection and filtering tools are used.

What is missing in this process is specific direction. The new methods suggested as below.

A. Collaboration of data from various actors- Using SOCMINT cannot be a role of a single actor. Gathering it from various agencies which may include response from the public, data from government authorities, from private organizations and then applying it in such a manner which is of huge benefit to the masses. Example can be cited of Facebook Disaster Map where in a situation of calamity, people affected can use the app and mark themselves 'safe', which is such a valuable information for agencies involved in rescue mission. Location of those who have marked themselves 'safe' and those who haven't can guide the search operation provided that the data passes through filters of veracity and reliability.

ISSN 2394 - 7780

B. Prediction and Forecasting-

Many social media apps and websites have predicting capabilities based on the inputs of the users and live information available through satellites. Google maps has proved to be a useful application while navigating through crowded cities like Mumbai, Delhi etc. It gives the live update of the traffic and congestion to the driver enabling him to consider alternate route and thus saving on fuel, time, fatigue.

C. Public Service Design and Delivery-

Indian population largely relies on railways for commuting from place to other. Indian railways has spread its wings in the social media platforms such as Twitter in order to provide best of the services to the passengers. In case of emergency or issues like maintaining cleanliness in the train coaches, the tweets by passengers are viewed seriously by the authorities and corrective measures are taken. Same should be followed in respect of issues in the cities to bring it in the notice of the civic authorities. Ideal administration would never afford to ignore the hashtags such as #potholes, #accident, #roadblock etc.

Processing and Analysis-

Usually social media data sets are huge, even after collecting the information from various partners, analyzing it is the greatest challenge. Especially when it comes to 'Human emotions', the usual methods do not give satisfactory results. A situational, cultural perspective is needed to analyze such collected data. For example, during the elections, sentiments of the people regarding the election process or a certain political party have to be analyzed. In this case, considering the cultural and location aspect, the lexicon or community specific words need to be paid attention to. This helps to understand the 'context' of the public concern which further helps to find the exact sentiments of the people towards the given process. Context should not be misinterpreted failing to which may give rise to a critical situation.

The authorities should balance between 'protecting privacy and security of the concerned people' and 'being able to analyze people's sentiment' throughout the process.

Assessing the impact and its evaluation-

Analysis of Social media datasets always give insight to the authorities thus enabling them to find the outcomes of the policies and suggesting measures to improve the same. This is the most important feature which enables the process of constant improvement.

When a certain project is proposed by the government or any institute which is harmful to the environment, people have powerful tool of social media to express the discontent. This not only helps the government to identify the opinion of the masses but also gives them idea of how much of the concerned population is affected by the decision. The popular example is of opposing to the flyover construction in Bangalore, India through twitter by tweeting #steelbeda movement. It is to note that regional lexicon is considered here to understand sentiments of the masses.

Another popular movement which attracted attention of all is #metoo movement has originated in western countries few years ago. But it gave courage to Indian women to express their grievances and thus helping authorities to attend the issue accordingly.

If we have to analyze the outcome of such events, it should be noted that tweets have to be filtered based on the five important public concerns namely lack of information, partisanship, distrust of institutions, personal economic impact and other, unclassified concerns. Since other measures of expressing their views were unavailable or ineffective for eg. Interviews with press or Protest because such measures can be manipulated by fake and paid crowd or lack of attention by media, the potential for social media as a near real-time measure of public opinion of policy reforms is realized.

Innovative methods and Technologies-

The data sets obtained through social media need not always be analyzed using traditional tools and techniques. It has to be beyond the regular methods thus enabling flexibility and context-specific implementation. Data responsibility decision trees, framework of moral values can be used to translate principles into a series of questions. Further, a transparency report showing with whom data is being shared and toward what public benefit could help allay concerns about government misuse of private-sector data assets.

The techniques of analyzing the social media should also collaborate with other inputs as open source intelligence (aka OSINT), Human intelligence (aka HUMINT), imagery intelligence (IMINT) and Signal intelligence (SIGINT).

ISSN 2394 - 7780

CONCLUSION

It is ascertained that Social media intelligence has significant effect on the society and it offers remarkable opportunities. The potential must be tapped by the government by engaging law enforcement agencies and giving legal framework to the SOCMINT.

The same may be added in the academics and also as a part of training in the industries. After all, all the major fields like social and behavioral sciences, political science, psychology, anthropology and social psychology are related to SCOMINT directly or indirectly. This will give the common masses chance to learn, understand and accept the challenges and limitations that come with SOCMINT.

Ultimately, peoples' active and wise involvement in the process is crucial as any social (refer *latin* Socius) process originates from them and for them. Which shall ultimately bring betterment to whole mankind.

REFERENCES

- Paige Maas, "Facebook Disaster Maps: Methodology," Facebook, June 7, 2017,
- https://research.fb.com/facebook-disaster-maps-methodology/
- Google, website- https://impactchallenge.withgoogle.com/india2013
- Wikipedia, website- https://en.wikipedia.org/wiki/Social_media_intelligence

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

GDPR IMPACT ON INDIA

Saili Parab, Aditi Mestry and Sanika More
Institute of Forensic Science, Fort, Mumbai

ABSTRACT
This paper aims to provide an overview of the new rules put forth by European Union (EU) to give EU citizens more control on their personal data, that is General Data Protection Regulation (GDPR) and its impact on India and its businesses related to European Union.

Keywords: GDPR, European Union, India, Business, Data Privacy, Personal Data Protection Bill.

INTRODUCTION
GDPR stands for General Data Protection Regulation. The General Data Protection Regulation is the set of passed by the European Union in 2016, for how companies manage and share personal data and to give EU citizens more control over their personal data. It aims to simplify the regulatory environment for business so both citizen and businesses in the European Union can fully benefit from the digital economy. In fact, The GDPR only applies to the European Citizens but due to the global nature of the internet, almost every online service is already affected. The reforms are brought up to bring in the laws and obligations especially those of personal data, privacy and consent across Europe to cope up with the speed of this internet-connected age. Here, GDPR sets a very high bar for obtaining personal data from the user than ever before. Any company any time collects personal data for any EU citizen, the company needs to take an explicit and informed consent from that person. The user also needs a way to withdraw the consent, and they can request the data from a company which has to verify the consent. Essentially, our lives revolve around the internet like from social media to banks, shopping and now even governments, and every service involves the collection of personal data. [4]

Under GDPR, these organizations have to be very careful about the data collection as well as the consent of the person should be explicit or they may have to face severe forfeits for not doing so. GDPR's penalties are severe enough to get the whole industry's attention. The maximum fine is set at 4% of the company's global turnover (or $20 million or greater). GDPR applies to organizations within the European Union, as well as any organization outside the European Union which offers goods or services to the citizens or businesses in the European Union. There are two types of data-handlers to whom the legalization applies to, they are ‘processors' and ‘controllers'. The definitions of each are given in Article 4 of the General Data Protection Regulation. “The Public body or agency which alone or jointly with others governs the processes and means of the processing of personal data is said to a ‘controller’”, while "The public body or agency which processes personal data on behalf of the controller is said to the ‘processor’". GDPR is the result of a determination of the European Parliament and other governmental bodies to strengthen the data protection for those living in the EU, while also providing greater uniformity to existing data laws. Residents of the EU will gain a greater measure of control over their data (and how it is used), by organizations inside as well as outside the EU. [4]

MAIN CONTENT
The impact of GDPR on India and Indian individuals is an outcome of the approach adopted by the businesses around the world. Due to India's weak data protection laws, Indian e-services industry would become less competitive and lose its European markets. Indian companies would be required to implement sufficient safeguards, as per the terms of GDPR, to prevent a transfer of personal data outside EU boundaries. This would further increase compliance costs. The GDPR has its application outside EU which means that the Indian companies not aligned with GDPR cannot do the business with the EU entities. The ‘adequacy requirements' under the GDPR permits only countries with adequate protection to data subjects, in respect of privacy and protection of their data subjects, to receive data of Europeans. The types of data considered personal under GDPR includes name, address, photos, IP address. It also includes sensitive personal data as genetic data and biometric data which could be processed to uniquely identify an individual. [3] Article 3 (Territorial scope) of the General Data Protection Regulation makes it clear that the regulation will be applied regardless of whether or not the processing takes place in the EU. Indian companies won't be able to do business with the EU if they do not comply with the GDPR or if not there is a risk of huge penalties on failure to comply with it. The commerce around the world including India have determined not to limit the changes made to update their privacy policies and compliance with GDPR, to their users located in the European Union. Due to this decision businesses are making these safeguards accessible worldwide that has been directed by pragmatism and administrative issues, rather than implementing country-specific policies. A note must be made that these rights are only accessible by Indian Nationals under contract. Pursuing protection under GDPR will not be able to

ISSN 2394 - 7780

Indian nationals. Thus, any implementation for breach will essentially be under contract and also available, under Privacy laws of India. Although this is not a supreme solution, the choice of complying with GDPR by the commerce around the world and India has resulted in an unexpected benefit for Indian national. [1]

The recent case recorded under GDPR was filed against Google. France's data protection regulator, National Commission on Informatics and Liberty (CNIL), has issued Google a €50 million fine (around $56.8 million USD) for failing to comply with its GDPR obligations. This is the biggest ever GDPR fine yet to be issued by a European regulator and the first time one of the tech giants has been found to fall foul of the tough new regulations that came into force in May 2018. CNIL said that the fine was issued because Google failed to provide enough information to users about the data consent policies and didn't give them enough control over how their information is used. According to the regulator, these violations are yet to have been rectified by the search giant. Under GDPR, companies are required to gain the user's "genuine consent" before collecting their information, which means making consent an explicitly opt-in process that's easy for people to withdraw. [6]

RESULT

The necessities for GDPR compliance need to carefully analyzed by Indian companies. They need to review policies, procedures, existing privacy programs, conduct data discovery exercises and maintain documentation in order to demonstrate visibility of the personal data processed. It needs to impart data privacy training to employees or subcontractors. Also, implement processes to perform data protection impact assessments (DPLAs), manage data subject requests, privacy by Design, etc. Review/update contracts signed with third-party vendors. Organizations should focus on changing the technologies they use and should consider. Pseudonymisation and encryption required while processing personal data. Reviewing and updating configurations of data loss prevention (DLP), Security Information and Event Management (SIEM) and other technical solutions. Equipping the security ecosystems with effective identity and access management (IdAM) solutions. They need to review data retention schedules, cross-border data transfers, privacy bills, permission, etc. They need to analyze the logging of monitoring and incident management solutions. The Indian companies need to invest in systems to carry out data discovery exercises to determine what/how/where PII is handled within the association to enter the GDPR regime smoothly which will help Indian companies. [2]

India is also propagating stronger data protection laws as was evident in the Supreme Court's ruling on the right to data privacy. The Indian Draft bill on data protection draws inspiration from GDPR but has its limits. Just like the GDPR, the draft bill prescribes differing ranges of penalties for contraventions of different provisions. For some contraventions, the maximum penalty is Rs 5 crore, or up to 2% of the global turnover of a company in the previous year, whichever is higher. For some contraventions, including contravening the provisions on cross-border transfers, consent, and grounds of processing, penalties extend to Rs 15 crore or 4% of the global turnover in the previous financial year, whichever was higher. [2]

CONCLUSION

After defining the concept of General Data Protection Regulation and its impact on European Union and India and also its businesses, a conclusion can be drawn that the GDPR is not only affecting the members of European Union but also any other country which is associated with the European Union. To comply with the GDPR almost all the famous and recognized companies, as well as Indian companies, had made changes in their privacy policies. Also, the Personal Data Protection Bill is proposed in India which has taken inspiration from GDPR but is not as strict as GDPR. The processing of the personal data of individuals (data principals) by government and private entities (data fiduciaries) incorporated in India and abroad is regulated by this bill. Also, if the Indian companies don't comply with GDPR then those companies won't be allowed to do any kind of data transaction with the European Union.

REFERENCE

1. Rödl & Partner "Indian Data Privacy laws and EU GDPR" published on May 24, 2018. Available:www.roedl.com/insights/india-eu-gdpr-data-privacy-law
2. Sivarama Krishnan "How can Indian organizations prepare for the GDPR regime?" Available:www.pwc.in/consulting/cyber-security/blogs/how-can-Indian-organisations-prepare-for-the-gdpr-regime.html
3. Deepti Susan Thomas "GDPR and its impact on Indian firms "updated: October 30,2018 . Availablewww.deccanherald.com/business/economy-business/gdpr-and-its-impact-indian-700371.html
4. Russell Brandom "Everything you need to know about GDPR" updated: May 25,2018.Available:www.theverge.com/2018/3/28/17172548/gdpr-compliance-requirements-privacy-notice

ISSN 2394 - 7780

5. Shivpriya Nanda and Zain Pandit "GDPR: Why does a law enacted in Europe affect business in India?" updated: May 31, 2018. Available: https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/gdpr-why-does-a-law-enacted-in-europe-affect-businesses-in-india/articleshow/64365950.cms
6. Intelegain Tech trends, "Technology; France commences post-GDPR era with approx.$56 million fine against Google," [online] updated: January 29,2019. Available: http://techtrends.intelegain.com/technology/france-commences-post-gdpr-era-with-approx-56-million-fine-against-google/

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

DIVING INTO DARK WEB

Mustufa Nullwala[1] and Dr. Leena Sarkar[2]
Assistant Professor[1] and Principal[2], JVM's Mehta Degree College, Mumbai

ABSTRACT
The Deep Web is so big for search engines to drape it up entirely. It is the long tail of what's left out of the whole Internet. The Deep Web is a warehouse of databases and other services available on web that are never indexed by traditional search engines like Google, Yahoo and Bing for a reason. Government files, public and private sector intra network are some examples of content found there. Dark Web is the encrypted internet where illegal activity takes place. The dark web subset of deep web is the World Wide Web content that exists on darknets, overlay networks which use the public Internet but require specific software, configurations or authorization to access. Dark Web is definitely used for nefarious purposes more than the standard Internet; there are many legitimate uses of the Dark Web as well. Legitimate use includes things like using various technologies to anonymize reports of domestic abuse, government regulations, military operations, and other crimes that have serious consequences for those calling out the issues. This paper gives overture on the dark web which shows what profligate things available on it which can be vicious to human life and how one should take proper precautions to use it.

Keywords: Deep web, Dark web, Cybercrime, Dark net Market.

INTRODUCTION
The internet is biggest network existing around the world. It is divided into 3 parts surface web, deep web and dark web. The content you surf over the internet using search engines like Google, Yahoo, etc. are the part of the surface web, statistically surface web is only 4% of the whole internet remaining 96% of the internet is deep web. This section is very vast on the internet and it is not accessible via regular search engines. Deep web has thousand terabytes information. The internet looks like an iceberg, upper base is a surface web and beneath major submerged part of an ice berg is deep web which one can consider as filthy caves dare to enter. Technologically, deep web pages are not indexed by basic search engines coming to dark web; it is a danger corner of a deep web mostly used for illegal activities like drugs trading, arms and ammunition supply, illegal transactions and many more things one cannot imagine. Dark web is known by various terms like cyber attacker paradise, black dark market, etc. In market, there are special operating systems and browsers to access dark side of the internet. Operating systems like Kali Linux, Parrot, etc and browsers like TOR, WHONIX, etc. Websites surfing over TOR browser usually have an extension ".onion". There are people who misuse it for doing criminal activities like tracking people's location, stalking them, doing things like force someone to watch one video while at the same time everything else on your computer is frozen.

I. TECHNOLOGIES USED TO ACCESS DARK WEB
Accessing dark web is easy, but easier to get caught, so better precautions have to be taken. Dark web is subset of deep web contain hidden market; accessing it can be done by using TOR browser which is most widely used. Dark net sites mostly belong to onion domain.

First of all compelling towards security very seriously you have to get VPN (Virtual Private Network) for surfing Dark net websites. VPN act as a secure tunnel. One also should have knowledge that you cannot fool ISP and law enforcement people that they will not be able to track you. They are master at it so don't make cakewalk for then. Using VPN your activities will reach hidden from government agencies people, all information flowing through VPN will be encrypted. VPN also help you to protect you own personal identity, files from your computer. After that you can't access dark web using common browser, specifically browsers have been designed for this purpose. One of the famous browsers of dark internet world is TOR official website is available to download it.

After installing it, you will be able to gain access to onion domain websites securely also having a good level of anonymity one can go through a list of dark net websites also known as block market sites of deep web apart from dark sites one can get tons of knowledge of hacking like penetration testing, gain control area computer system, backdoor programs, launch man in the middle attacks, ARP poisoning and many more.

II. OUTRAGEOUS THINGS AVAILABLE ON DARK WEB
Dark web is not only place where evil thing takes place; sometimes it is also used for good activities. Apparently as name given to it dark web most of the time it is used for dreadful activities. List is long but some of the activities one can do or things you can buy are:

ISSN 2394 - 7780

- Selling fake brand product
- Selling buying weapons illegally
- Dealing of drugs
- Hacking of social networking sites
- Making face drivers license or passport
- Blank credit cards
- Exploiting and creating mirror website of e-commerce website
- Stolen cars
- Wi-Fi hacking
- Stealing Netflix accounts
- Dealing with bit coins
- Fake college degree
- Hacking of government data

III. CYBER CRIME IN DARK WEB

Cybercrime is the crime that involves a computer and a network. Cybercrimes are defined as an offence which are done by individuals or groups with criminal motive with intention to harm the victim physical or mentally. The cybercrime has become the high profile crimes and their types are hacking, unwanted-surveillance, extortion, child pornography and child grooming, some are private or confidential, some are psychologically and physically.

Now-a-days, the dark web is highly preferred for cybercrimes; dark web is a part of internet which is not indexed by the search engine. This dark web has the hotbed for the criminals to have the activity of frauds, hacking or many more. It becomes easier to snag a data or a share of billions of dollars without stepping out of your place. Research says that powerful malware, readymade phishing pages and password crackers for popular brands, and an incredible hacking tool are also sold on the dark markets for just few dollars.

Most powerful items found were remote access Trojans (RAT).This malware allows the scammers to take the full advantages of the victim and full remote control of their victim's computer. It also discovered RATs on the android operating system, which is written in python and visual basic. The notorious malware Black shades RATs was found which infected over half a million devices and its creator in jail. This also allows hackers include infected computer in a botnet. Another dominant cyber-attack vector is Phishing, it surprise the enterprising hackers which sells the readymade spoof pages for hundreds of popular brands which are ranging from Apple and Netflix from Wal-Mart, Dunkin Donuts of mine craft and League of Legends. Statistics shows that how much customers are targeted by these thieves, gets the package of identifying information that enables for theft.

IV. EASILY ACCESSIBLE PLATFORM ON DARKWEB

To become a hacker doesn't need to bother to learn hacking, one can easily configure their password cracking tool to attack their target sites with the help of dark web. Readymade configuration files or list of sites also proliferate on the dark web markets for $2 to $3 each.

Using existing platform available on dark web, the theft and hacks of the data becomes the cybercriminal's bread and butter. As we see that, it enables our personal information in its raw form for the use of bank account, credit card account which criminals get easy to theft the data using tools. Cybercriminal can be individual or in group. An individual cybercriminal make a half of million dollars yearly simply by trafficking, hacking or stealing the data.

V. CONCLUSION

In this evolutionary world, cyber securities have been a major concern. Current researches and studies have continuously highlighted the existence of dark net, the rationale behind all the criminal activities. The dark web will continue to scale up and mesmerize everyone who uses the internet. It contains a captivating amount of knowledge that could help us evolve technologically. And of course, it has disadvantages too which can exploit human life in many ways. The dark net is giving a way to enormous illegal activities providing platform and

ISSN 2394 - 7780

also forcing the law enforcing entities worldwide to use new unconventional methods to track these cyber criminals. Regardless of, if the Dark Web exists or not, the aforementioned activities will still occur. So as an end user perspective, we should take a protection of our personal data seriously. Ignorance will create vulnerabilities to our personal as well as professional life. Dealing with dark web, one has to do in-depth deep web security study. When an ordinary computer wants to interact with criminal underground, dark web is the best known place for it. Anonymity it provides, but not always guaranteed. Dark web is no place to trust, majority of underground markets are built on crime and fraud basis. In certain conditions, user can use virtual machine operating system, reason for this is to quantify the protecting base operating system and protect it from viruses and malware which will target the virtual operating system.

VI. REFERENCES

- https://www.thesslstore.com/blog/2018-cybercrime-statistics/
- https://hackernoon.com/the-dark-web-is-democratizing-cybercrime-75e951e2454https://www.deepdotweb.com/2018/11/23/important-forensic-tools-used-in-harvesting-the-deep-web/
- https://mybroadband.co.za/news/internet/129288-23-outrageous-things-you-can-buy-on-the-dark-web.html
- https://www.ranker.com/list/things-you-can-buy-on-the-dark-web/mike-rothschild
- https://hackernoon.com/the-dark-web-is-democratizing-cybercrime-75e951e2454
- https://www.thesslstore.com/blog/2018-cybercrime-statistics/
- https://www.wikihow.com/Access-the-Deep-Web
- https://us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html
- https://darkwebnews.com/help-advice/access-dark-web/
- https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html
- https://www.deepwebsiteslinks.com/how-to-access-the-deep-web/#diffdeepwebdarkweb
- http://thehiddenwiki.org/
- https://www.independent.co.uk/life-style/gadgets-and-tech/news/telegram-app-drugs-sell-channels-bots-crime-graffiti-dropgangs-dark-web-a8814671.html
- https://online.norwich.edu/academic-programs/masters/information-security-assurance/resources/infographics/deep-web-crime-requires-new-forensic-approaches

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

DARKWEB FORENSICS INVESTIGATION

Tushar P. Jadhav
JVM Mehta College, Navi Mumbai

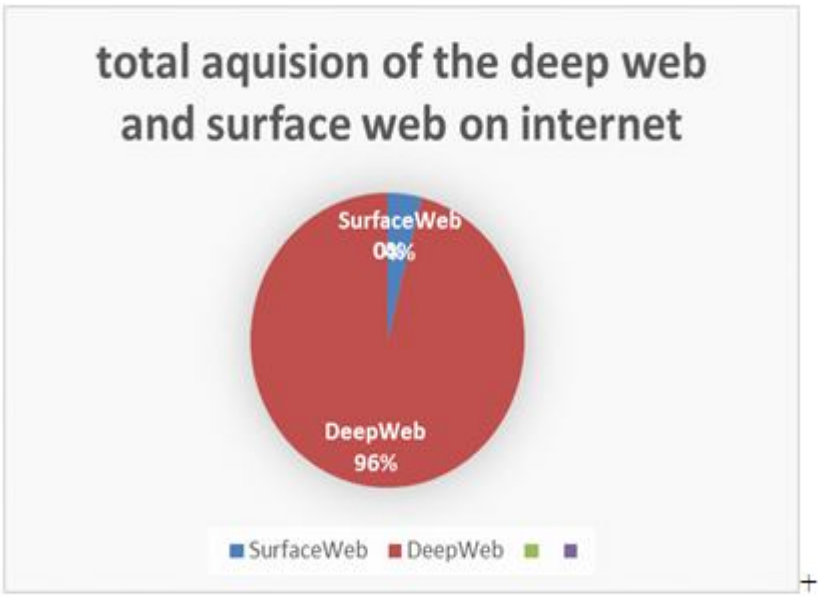
ABSTRACT
Search engine such as Google, yahoo and Bing cannot index the deep web content. The dark web is lies within the deep web. Dark web are intestinally hidden and does not index by the standard browsers. Darkweb are free and open source technology .The dark web content are accessible only by The Onion Router. Tor hides the IP address and identity of the users. Tor is the virtual market of trading goods such as weapons, drugs narcotics, human body parts etc. The murder hiring services, childpornography, hacking are done by using darkweb. Because of these it become difficult for forensic expert to investigate the criminals. Dark web uses crypto currency for money transactions. Bitcoins are used as the currency over the darkweb the online trade are carried out by using the bitcoins. Bitcoin wallet is the best evidence for forensic investigators

Keywords: Surface web, deepweb, darkweb, bitcoins, TOR browser, Onion sites.

INTRODUCATION
Today, the whole world relays on internet. So the safety and security of internet users depends on the reliable and secure infrastructure. This infrastructure is handled by cyberspace. As compared with technical implementation and execution, cyberspace is best medium for social interaction. As per latest research, 90% US companies are targeted for cyber-attack. Hackers hack 3 billion Yahoo accounts in 2016. According to Uber, 57 million Uber riders and driver information was hacked.

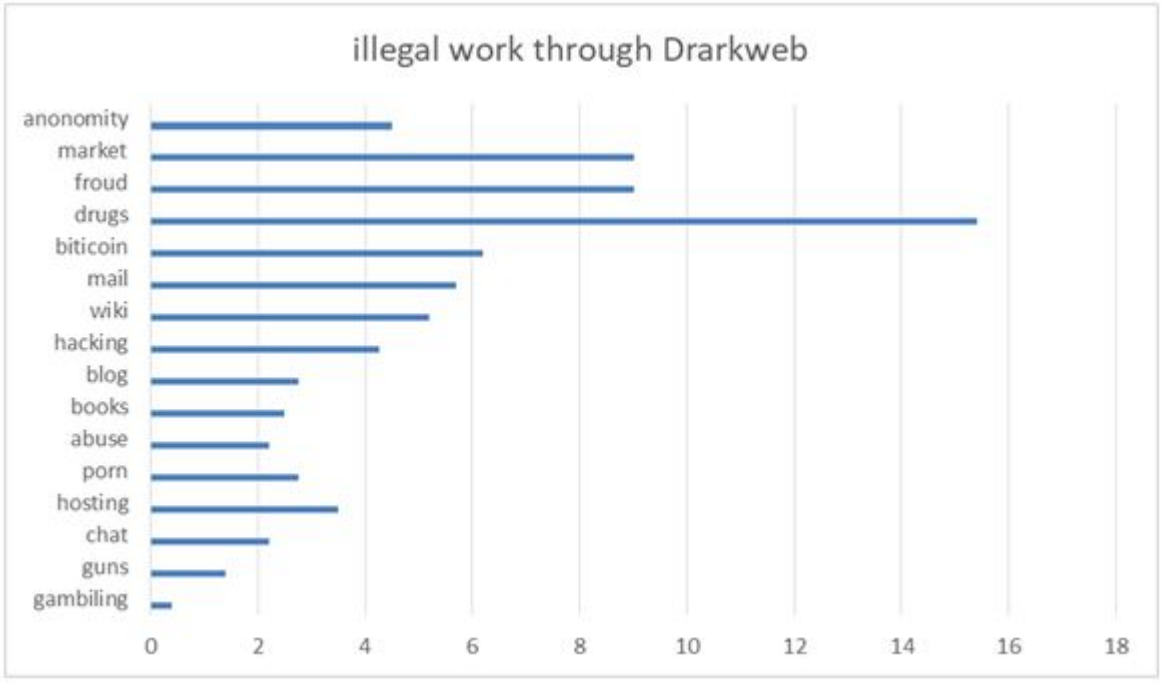
In 1970, the Dark net concept was introduced and used in Government Military and academic network purpose. The TOR is the one of the biggest form of dark web and was developed by three scientist named as Paul……it was originally implemented by USA defence advance research project agency.

Internet has surface web and deep web as subtypes. We can indexed the surface web contents by using different search engines like Google, yahoo, Bing etc. the engines like Google, yahoo, Bing etc. The deep web contents cannot be searched by normal web search engine. Dark web exist inside the deep web. We cannot access the dark web by using normal standard browser, we need to use only TOR browser. TOR allows it's user to internet anonymously. TOR hides the IP address, system details and also all information related to Internet Service Provider.



In the above diagram, the blue portion denotes the surface web and contains 4% of information accessed through normal Google search. Although 96% of deep web content does not available through standard web browsers and is denoted by the brown portion. According to the latest researches the number of dark web users are increasing day by day. Dark web are usually accessed through TOR browser. TOR browser helps the domain to host the website at free of cost . The website hosted under TOR browser has the .onion extension and TOR browser web content are accessed only through the url . Following diagram represent the illegal work performed using the dark Web and its percentage (according to 2015 stats)

ISSN 2394 - 7780



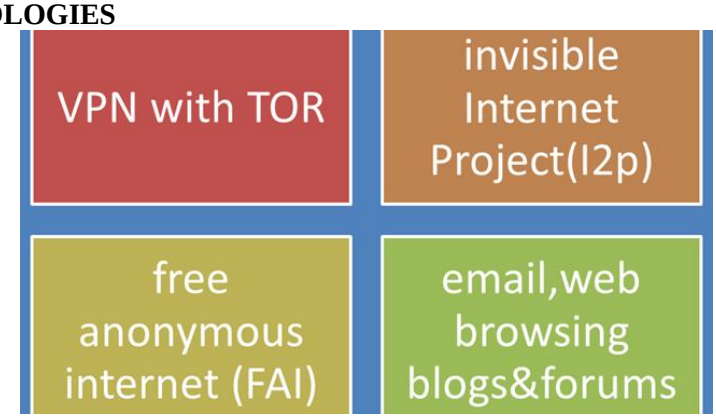
Graph represents the name of the illegal activities carried through the tor browser.

HOW TO ACCESS DARK WEB AS AN INVESTIGATION

Following are the steps and terminology, used for dark web investigation.

- Buy a VPN and download the TOR browser from www.torproject.org.TOR browser must be downloaded from official tor website ; because tor browser are mostly used in the hacking and criminal activity purpose. If you will access the tor browser using VPN no government, hackers and firewall will restrict you on browsing and searching activity on internet .
- Install the TOR browser on your pc or mac, double click on downloaded file and extract to destination folder.
- Start TOR browser, TOR browser provides you a good level of security and anonymity. By following above steps you are eligible to gain access to .onion web sites . For safer access we should close all other application and browser that are connected to the internet
- Do not change the tor browser's window size, because feds have the programs that can match identities such as the matching online time.
- You must turn off the JavaScript from tor browser setting.
- You must disconnect the webcam and other cameras from computer system because government and hackers can easily get in your system through webcam. Disconnect your microphones and also don't use your real email id for signing purpose. You must use anonymous email-Id and password.
- Never used your real name, photos, passwords that you used before on the dark web because it is the fastest way to track you.

DARK WEB TECHNOLOGIES



ISSN 2394 - 7780

VVPN WITH TOR
It gives the extra level of privacy and security from hackers. It hides all browsing details from government and ISP.

INVISIBLE INTERNET PROJECT
It is the anonymous network within network it protect from third party internet service provider (ISP).We must use (I2p) for privacy and security purpose.

FREE ANONYMOUS INTERNET
It uses block Chain technology to create secure, private, peer to peer alternative to regular World Wide Web. It has its own currency based on Bitcoin code. It allow to post the media on the browser with privacy.

EMAIL, WEB BROWSING & BLOGS AND FORUMS
The entire web database of the tor browser are saved on the email database, the dark web have its own anonymous web mail service called as the TorMail . Web browsing are carried out through the private deep web. .onion URLs blogs and forums are also darkWeb technology that is used in sharing data media and personal blogs.

HOW DARKWEBWORKS?
Surface web contains total 4% of the internet and rest of the 96% are deep web. Inside the deep web, the darkweb exist. Dark Web is a publicly visible web site with hidden IP address , which are accessible through Tor browser .The privacy of the users of dark web are preserve via layered technology called as the onion routing . Onion routing has many VPN throughout the VPN the requests are send to server for accessing the information. All these process are carried out through the onion routing each layer of onion routing has its own security and encryption standards.

All illegal websites are hosted by the dark web's TOR browser. In the dark web the a single host acts as the server and client. The data transfered to machine to machine without hosting on the web servers. The peer to peer server are access are occurred in dark web technology on the tor browser we can buy domain for hosting website with free of cost.

Due to layered architecture of the Darknet no one can track the real location and identify. Users data are passed through the large amount of the intermediate server, which protects user's identity and guaranties anonymity. Transmitted information can be decrypted only by a subsequent node in the scheme .The complicated system of dark net makes it almost impossible to reproduce the node path and decrypt information layer by layer. Due to high level of encryption websites are not able to track your geo location and IP address, also users are not able get information about host.

Communication between the dark net users is highly encrypted, it allows users to talk, blog, and share files confidentially. Darknet is also used for illegal activities such as sailing of drugs, stolen credit card details: human body parts, narcotics, illegal trade child pornography, exchangeof pedophiles and terrorists, etc.

Dark web uses crypto currency for money transactions. Bitcoins are used as the currency over the darkweb. The online trade are carried out by using the bitcoins .

DARKWEB INVESTIGATION GUIDELINES
According to my research paper following are the guidelines for Darkweb forensic investigators

- Track the vulnerabilities of the TOR browser.
- Depending on the type of investigation the private investigators should try to hack the database of the infected site on which crime is held. because database is the essential tool for investigator's
- Searching through dark web can help to locate the criminals
- Searching method should be online because it gives more information than field search.
- To gather the data from dark web create the web crawler. Web crawler is programming script which is used to open the web page and copy the text and tag from each page.
- Determine the structure of the darkweb market space.
- Investigate the market space vendors ,we identify the vendors of market space using data collected from web crawler
- Keep track and follows their victims moments and habits ,like frequenty accessing social media account with GPS system

ISSN 2394 - 7780

- Keep record of install software on victims pc

CONCLUSION

Darkweb technology is used for good purpose as well as the criminal activities. Darknet are used in the military and securing, confidential data and it is used for the hacking purpose also. Forensic investigators used dark web for tracking the criminals. Darkweb is good platform for hosting the website because it gives domain free of cost. Darkweb provides the peer to peer web hosting so no third party server can maintain your data. darkweb provides security and encryption for private browsing. According to my research paper I will suggest that the bitcoin wallet of criminal is the best evidence for forensic investigators. Because it will give the bank details of the criminals.

REFERENCE

1. https://articles.forensicfocus.com
2. https://investigatinginternetcrimes.wordpress.com
3. www.iacpcybercenter.org
4. www.researchgate.net
5. www.zdnet.com
6. https://en.wikipedia.org/wiki/Dark_web

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

DARKWEB: THE DARKER SIDE OF INTERNET

Nivedita Tiwari
G. N Khalsa College, Matunga

ABSTRACT

The internet has become one of the essential requirements for freedom of speech, and freedom in general. This freedom is sometime a threat to countries and governments, so they restrict or ban it. As the technology is growing day by day there is an increase of bitcoin currencies and the use of dark web. DarkWeb also called as Darknet is the portion of internet which cannot be accessed by our everyday search engines. No matter how scary the dark web is, no matter how much Tor helps people, the dark web will probably always have a reputation involving only criminal activity. Dark web has given new face to the crime. Also Dark web when combined with bitcoins it makes things very easy especially for the terrorism group.Things like legal weapons and drugs are sometimes used for non-legal purposes. Although the current news still going on which states that RBI has banned all the banks which were dealing with virtual currencies still we cannot say that this will help to eradicate the terrorism or the unnecessary activities completely.

Banning however will not serve our actual purpose. Hence The bottom line is we cannot completely eradicate the DarkWeb but we could definitely track the user to some extent with the help of Forensic tools.

1. INTRODUCTION

This paper gives a review on how to track users using DarkWeb with the help of Forensic tools. The internet has many faces. The global access to internet has transformed our societies in many ways. Recent report states that the overall use of internet in India today is significantly higher than China.While the majority of us use search engines like google, yahoo, bingo etc to learn,research and interact, there is a less innocent side to the online world. Only 56% users of the world are onto the innocent side of the world. Rest all other users uses Internet especially for illegal activities. The dark web is the one which paves way for the terrorism.

Dark Web consists of online content that can not be accessed through standard search engines.The general population are unaware about the information present onto the Darkweb as they are intentionally hidden from the regular search engines.

It is also called as darknet. The dark web is a subgroup of the deep web. Both dark and deep web pages can be found on search engine results pages but deep web pages can be accessed by anyone with a browser who knows the URL. Dark web pages, in contrast, requires special software with the correct decryption key, as well as access rights and knowledge of where to find the content. It is always said that “You can get everything what you want but you won’t get it for free”.You need to pay something to get something. Sometimes paying is in the form of losing your identity, losing your data etc.

When using dark web one can hide their identities.

Famous examples for the Dark Web sites include the Silk Road and its offspring. The Silk Road was a website for the buying and selling of recreational drugs, and a lot more scary things besides.

People operating within closed societies and wants to get hidden from the government agencies can use the Dark Web to communicate with the outside world.

The dark web requires special software to access.Online marketing are on its trend. However we can say that “Monday Sale” is now currently becoming “Cyber Monday” only the difference is the marketing are done with the help of virtual currencies onto the darkweb. On contrary Darkweb supplies more of the illegal things.

2. LAYERS OF THE WEB

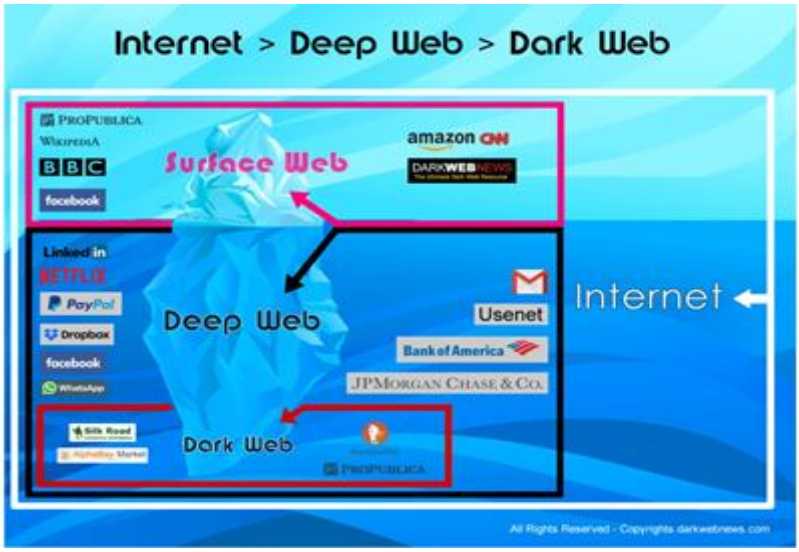
Surface web: This is what people use today It's where we are now. We can enter a search term into a common search engine like Google or Bing and receive results based on our search terms. Best for the everyday users of the Internet. However there are also illegal activities going onto the suface web as well but not as high as DarkWeb. Hence Surface web is the top, visible layer of the web.

Deep web: The deep web consists of all manner of information that cannot be indexed (or searched) by familiar search engines. For example, suppose you want to visit Shimla from your current location.You would like to book your tickets and hotels using makemytrip website.You searched for the same by entering the required details.The result returned to you is called as Deep Web as these searches are not indexed by google but by the website database.

ISSN 2394 - 7780

Also there are ways hackers could easily manipulate the database so certain precautions should be taken while accessing the websites.

Dark web: The dark web is a subsidiary of the Deep Web intentionally hidden and inaccessible. You need a specialized browser to access it. You can almost find anything you needed onto the Dark web. Dark webpages are hosted on darknets. Dark web provides you with the sites that cannot be accessed by the regular search engines which we use.You can say that many a times users information are put on sale on the Dark web. A bit more computer knowledge is required to find way into and around the dark web, which is generally a collection of mostly illegal information, products, and services that don't hold interest for the average user.



3. TWO DARKNETS

a. DarkNet

There are two darknets, with the TOR darknet being the more popular of the two. TOR gives the users anonymous access to both the regular web and the Darknet. Dark websites on TOR use the onion domain name Darknet surfing is usually faster with TOR, and the cloaked population is very high in the TOR virtual world.

TOR stands for 'The Onion Router'.

b. I2P or The Invisible Internet Project

I2P is a network layer, that allows peer to peer communication anonymously.The connections are achieved by encrypting user's traffic. It is generally used when the speed of the performance is slower and is more exclusive than TOR; you cannot use I2P browsing to see regular web pages. I2P is published under multiple license and it is free and opensource.

4. WHAT ARE BITCOINS?

Bitcoin was the first popular cryptocoin. The bitcoins can be stored offline on a person's local hardware. This is called as "cold storage", and it protects the currency from being taken by others. When the currency is stored on the hot storage(or onto the internet),there is a high risk of it being stolen.

On the other hand, if a person loses access to the hardware that contains the bitcoins, the currency is gone forever.

5. HOW BITCOINS WORK

Bitcoin is a digital payment system where the payment are done anonymously using digital currency.Bitcoin is not affiliated to any bank or government.You can give another name for bitcoin as physical gold coin. Their value is as similar to the nuggets of gold in your pocket. Bitcoins can be used to purchase goods and services online, or you can secure or save them and hope that their value increases over the years as the price of bitcoins goes on fluctuating.

Trading of bitcoins are performed from one personal wallet to another. A wallet is a small personal database that allows you store your bitcoins on your computer drive smartphone, tablet or in the cloud.

6. COMMERCE ON THE DARK WEB

All commerce sites on dark web conduct transactions in bitcoin , but that doesn't mean it's safe to do business there. The inherent anonymity of the place attracts scammers and thieves.

ISSN 2394 - 7780

The commerce sites present onto the Darkweb have the same features as any e-retail operation, including reviews, shopping carts etc, but there are important differences.The most important feature is quality control. On the Darkweb both buyers and sellers are anonymous, and therefore the credibility of any ratings system is doubtful one. Ratings can be easily controlled, and even sellers with long track records have been known to suddenly disappear with their customers' crypto-coins, only to set up shop later under a different name.

Most e-commerce providers offer some kind of service that keeps customer funds on hold until the product has been delivered. Every communication on Darkweb is encrypted,and hence even the simplest transaction requires a PGP key.

Completing a transaction whenever purchasing illegal goods doesn't gives you the guarantee that the goods will arrive.

6.A STAYING ON TOP OF THE HACKER UNDERGROUND

It is important to be on top of what's happening in the hacker underground. You should use the dark web for situational awareness, and keeping an eye on what's going on.

7. TOOLS FOR ACCESSING THE DARK WEB

To access the dark web, you need to download special browser clients, of which the most popular one is Tor. Tor does two things: First it connect users to the subset of networks that make up the dark web and secondly it anonymize every step by encrypting who are you,what is your location,and what you're doing.

Downloading Tor or any other browser does not indicate that the user is engaging in any sort of illegal activity; infact on the other hand, many people are finding these tools(Tor) useful as it concerns about your privacy .

Once you've downloaded and installed Tor, your browsing is made anonymous, which is crucial for visiting any part of the dark web. However using dark web doesn't guarantees you cannot be untraceable. In fact, many people are caught engaging in illegal stuff on the dark web. Using these tools makes it difficult to track you , but not impossible.

Although downloading these encryption tools and clients is definitely not illegal, using them sends up red flags about you. People who wants to break the law often start from here, so law enforcement keeps track of these users.

8. USERS OF THE DARK WEB

The dark web has somewhat of disagreeable reputation. Imagine if all online transaction are done onto the dark web it would then be a cake walk especially for the terrorists.The feature of anonymity that it provides is definitely a huge draw for those looking to procure drugs, weapons, and other illicit items, but on contrary it has also been a safe haven of sorts for people who need to hode themselves and share information without detection.

9. THE SILK ROAD

One example of the dark web that wasn't entirely legal was the "storefront" also called as the Silk Road. The Silk Road was a large marketplace within the dark web, which was famous for the buying and selling of illegal drugs, but also a wide variety of illegal goods and information. Goods can be purchased using only Bitcoins, which can be transferred anonymously through networks that make up the dark web.

10.NONCRIMINAL USE OF THE DARK WEB

Although visiting the dark web can be considered as an illegal activity, some people desperately need to remain anonymous because their lives may be in danger or the information they possess is sensitive or even volatile. Many a times journalists are tend to use the dark web to contact sources anonymously.You are most likely to be on dark web only because you don't want your identity to be revealed or your location to be revealed.

11 APPEAL OF THE DARK WEB

Dark web is not only a place where you can just drop by online informally it does take some doing and a certain level of technological experiences.

a. Anonymity

The Dark Web's offers the feature of anonymous browsing and is definitely a cake walk or a huge draw for people who are looking to sell drugs, weapons, and other illegal items.So while visiting the Dark Web you can certainly think of all the illegal activities.

b. Privacy and the Dark Web

Privacy concerns are on many people's minds, especially it is always thought that our activities are possibly monitored by various ways. The Dark Web could be used for people who want to stay unnamed or hidden and

ISSN 2394 - 7780

private, for whatever reason — perhaps you definitely don't want others to know what all activities you are performing onto the web.

It's quiet important that there should be no doubt between the dark web and the tools you are using to access it to stay ano nymous.These two are completely different from one another. Tor is one of the most frequently used software by the people who want to remain anonymous.

c.Privacy, Safety, and Anonymity

It is inpredictable that how long the Dark Web will continue to grow and evolve; the appeal to remain anonymous is growing high day by day and one cannot completely resist it. More people are actually concerned about their completely legal online activities, communications, etc. are being tracked, and therefore tools such as Tor which help them to attain privacy also grow in popularity.

12.FUTURE WORK WITH THE HELP OF FORENSIC TOOLS

The most basic thing one can do is to ban the use of Tor and I2P or ban the use of virtual currencies(which is recently done by RBI).The combination of Bitcoin and Dark web can evolve the nature of terrorism to a great extent.

One possible thing we can do to track DarkWeb users is to find out which all machines are downloading the Tor software as Tor is the famous software used for hiding their identity. As we got to know that illegal trade on DarkWeb is carried out with the help of bitcoins forensic tools can also help us to find the transactions of bitcoins done by a particular IP address.These bitcoins are associated with Blockchain technology. The block chain technology keeps a digital record of the transaction done by bitcoins.The Block technology stores the transaction record onto the hardware of the user which cannot be tampered at all. Once we track the user of Tor and its transaction of bitcoin through their hardware device it would be easy to get the location of the IP and the user as well. Also with the help of network forensic tools such as NetIntercept and NetworkMiner tool which is used to capture the packets transmitted onto the network one can capture the packets transmitted by the system which is under inspection and decrypt the information.

13. REFERENCES

1. https://www.izoologic.com/2017/07/05/introd uction-deep-dark-web/

2. https://darkwebnews.com/help-advice/access-dark-web/

3. https://searchsecurity.techtarget.com/feature/T or-networks-Stop-employees-from-touring-the-deep-Web

4. Dark Web Kristin Finklea Specialist in Domestic Security

5. Balduzzi M., Ciancaglini V. "Cybercrime in the Deep Web"

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER SECURITY AND ITS IMPACT AT THE WORKPLACE

Dr. B. Jyoti
Associate Professor, Department of Electronics, Bi Bi Raza Degree College for Women, Kalaburgi

ABSTRACT
This paper discusses about the criminal activities and their security aspects at work place. The principle of scarcity says that we value an asset higher when it has a scarce availability, while we tend to think that what exists in abundance has little or no value. It is possible that this theory explains why we do not give importance to the information that we generate as users. Possibly, this is the reason why cybercrime has turned into one of the most profitable criminal activities of these times, and this situation will continue as long as we ignore how much data our email address or ID number can provide anyone who asks for them. Things get worse when cybercriminals target companies. The corporate information and why do hackers attack when you are working? Their methods and use

Keywords: Hackers, social engineering, phishing, cyber crime

1. INTRODUCTION

The data of the clients is an important part of the economic activity. That is why protecting information should be one of the priorities of companies, but in most of them it is not yet. The Internet has given us a window of business opportunities that sometimes makes it difficult to make out genuine threats. This means that, in terms of cyber security, companies are reactive and not active, which means that they only look for solutions when they have been strike by an attack instead of preventing it by carrying out cyber security policies .

HACKERS ATTACK AT WORKPLACE

Remember, how was your first day of work? Surely, it was not one of the easiest. You had to learn the names of your colleagues or not. The principle of scarcity says that we value ability higher when it has an inadequate ease of use, while we tend to think that what exists in loads has little or no value. Many times its viable that this hypothesis elucidates that we do not give significance to the information that we breed as users. That is the reason why cybercrime has turned to continue as long as we ignore how much data our email address or ID number can provide anyone who asks for them. Things get worse when cybercriminals target companies.

THE CORPORATE INFORMATION AND WHY DO HACKERS ATTACK WHEN YOU ARE WORKING?

The data of the clients are an important part of the economic activity. That is why protecting information should be into one of the most profitable criminal activities of these times, and this situation will one of the priorities of companies, but in most of them it is not yet. The Internet has given us a window of business opportunities that sometimes makes it difficult to perceive real threats. This means that, in terms of cyber security, companies are reactive and not active, which means that they only look for solutions when they have been hit by an attack instead of preventing it by the implementation of cyber security policies .

But none of that information had to do with how to protect yourself from cyber attacks or how to perform your job more safely. And why is that a problem? Because every day we receive dozens of emails from customers, suppliers and advertisers; we manage orders through or third-party applications; and in short, we carry out tasks proper to the activity we perform without the necessary security training. The next click might end with the ransom of the equipment and the encryption of the data stored in it. Cybercriminals are aware of the lack of security training of most users.

WHAT METHODS DO THEY USE?

This is how social engineering and phishing works take advantage of it, just as they do with the uncontrolled things that many workers have in their offices. Lack of awareness and hurry to make up the perfect context for an attack with high probability of success. And part of that success is determined by the methodology that cyber criminals use, like for example, social engineering and phishing. Lack of awareness and rushing makes the perfect setting for an attack with high probability of success.

METHODS PHISHERS USE

An exercise of persuasion. This is how you could define what people do when performing social engineering. Through a set of psychological techniques But none of that information had to do with how to protect yourself from cyberattacks or how to perform your job more safely. And why is that a problem? Because every day we receive dozens of emails from customers, suppliers and advertisers; we manage orders through corporate or

ISSN 2394 - 7780

third-party applications; and in short, we carry out tasks proper to the activity we perform without the necessary security training. The next click might end with the ransom of the equipment and the encryption of the data stored in it. Cybercriminals are aware of the lack of security training of most users.

WHICH METHODS HACKERS USE?

This is how social engineering and phishing works take advantage of it, just as they do with the frenetic rhythm that many workers have in their offices. Lack of awareness and rushing make up the perfect context for an attack with high probability of success. And part of that success is determined by the methodology that cybercriminals use, like for example, social engineering and phishing. Lack of awareness and rushing makes the perfect setting for an attack with high probability of success and social skills, the social engineer aims to gain sensitive information. An example of social engineering could be receiving the mail of someone who supposedly is your manager. In the mail, he asks you to send certain confidential information that you have or, depending on your responsibility, to make a bank transfer to an account number that provides you with the excuse that it is necessary to make that payment as soon as possible. It seems that the CEO Scam is quite obvious, but the reality is that it has achieved a high level of sophistication, so it is a fairly common attack among companies. Also, this example can be even more terrifying if possible. On the one hand, it is making you think that the mail comes from a manager (social engineering); on the other hand, it could not only ask you to make a What happens when the threats come from within the company? money transfer, but also download a malicious file that can compromise your company's infrastructure (phishing).

Like this case, cybercriminals create every day new ways to carry out attacks using social engineering and phishing. In this scenario, learning to recognize a cyber threat becomes a need for all the people who work with electronic devices connected to the Internet. A phishing attack may seem obvious, but the reality is that it is more common than most imagined.

WHAT HAPPENS WHEN THE THREATS COME FROM WITHIN THE COMPANY?

"The truth is out there". Do you remember? That's what they said in the X-Files series, letting us know that we had to look for the dangers outside, but how wrong they were. When it comes to cyber security, the people who make an attack possible do not have to wear a hooded sweatshirt or be in front of their computer at dawn. They can wear a suit and tie or have an office schedule.

They may be the people you spend more time with than your family. It is possible that they are your work mates. According to a study that IBM published in 2016 60% of attacks came from within an organization. From that number, 44.5% of the attacks were perpetrated by evil, while 15.5% of those attacks originated by accident, which means by a worker who has allowed access to the company's infrastructure without wanting to.

CONCLUSION

From the study it is clear that things get worse when cybercriminals target companies and the bad news is that you do not just have to defend yourself from what is out there, the good news is that there is a small percentage of those attacks that occur by accident. Cyber security is not expensive compared to the cost of having a cyber attack and these situations can be avoided by complying with the basics in cyber security.

REFERENCES

1. https://opendatasecurity.io/
2. https://twitter.com/ODSops
3. opendatasecurity.com
4. https://www.researchgate.net/publication/321528686_A_Recent_Study_over_Cyber_Security_and_its_Elements/download

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

REVIEW OF E-GOVERNANCE POLICIES AND ITS SECURITY ISSUES

Dr. Swati Vitkar[1] and Dhanraj Jadhav[2]
Assistant Professor[1], SIES (NERUL) College of Arts, Science & Commerce, Nerul
Assistant Professor[2], BSc (IT), Narsee Monjee College of Commerce & Economics, Vile Parle (West), Mumbai

ABSTRACT
It was considered that much more thrust is required for secure e-government in the country to promote inclusive growth covering electronic services, products, devices and employment opportunities. Moreover, electronics manufacturing in the country should be strengthened.

In order to transform India into a society economy and knowledge digitally empowered, the Indian Government has launched the Digital India programme.

Digital India is partially implemented and now it started showing the changes in some sectors, by taking benefits of the modern ICT. Implementation of e-Governance in India can redefine and restructure outdated processes and procedures. The main aim is to provide citizen-centric service delivery which is hassle free and fast. There are lot of Privacy and Security Issues in implementation of e-Governance. Lack of awareness about privacy and security issues are also discussed in this paper.

Keywords: Security, E-governance, Digital India, ICT, Digital India

I. INTRODUCTION

e-Government initiatives in India took a wider dimension in the mid 1990s for broader sectoral applications, with emphasis on citizen-centric services. The main government ICT initiatives include, among others, some of the most important projects, such as the computerization of railway, land registry computerization, etc., which mainly focused on the development of information systems. Later, many states began ambitious individual e-government projects aimed at providing electronic services to citizens.

Although these e-government projects were centered on the individual, they could do less than the desired impact because of their limited features. E-governance solutions are expensive and complex solutions which would be built brick by brick over a time period, involving numerous solution providers. In order to have a successful solution for e-governance, governments should adopt middleware standards that are common across the entire e-governance solution. In addition to middleware standards, government should adopt certain technology standards. Such middleware and technology standards enable development of scalable and robust solutions and cut down the cost of development and maintenance of solutions for e-governance. Implementation of e-Governance in India can redefine and restructure outdated processes and procedures by taking advantage of the modern ICT. The main aim is to provide citizen-centric service delivery which is fast and hassle free.

E-KRANTI: NATIONAL E-GOVERNANCE PLAN 2.0

The e-government program nationally known as the National e-Government Plan began in 2006. There was a 31 Mission Mode Project under the National e-Government Plan covering a wide range of domains, viz. agriculture, land registries, health, education, passports, police, courts, municipalities, business taxes, treasuries etc. 24 mission mode projects have been implemented and began delivering range, either full or partial services envisaged.

The government of Narendra Modi, soon after its victory in May 2014, announced the Digital India prgramme with the objective of "Transforming India to the Digitally Empowered Society and Knowledge Economy. The focus of the programme is IT + IT = IT "India Today and Information Technology is equal to India Tomorrow".

Indian Government is playing very important role by introducing its flagship programme called DIGITAL INDIA. Through, DIGITAL INDIA various IT enabled services are provided. Its main vision is to transform India into a digitally empowered society and knowledge economy.

This was powerful vision being made by a leader who had caused a tectonic political change through meaningful use of social media and digital engagement of citizens and voters. The McKinsey Global Institute research does amazing predictions - a 2014 report, the Institute noted that India Digital positioned our country with the biggest opportunity yet to accelerate economic growth. In the next 10 years, the use of technology in India through India Digital could pump anywhere between USD 500 billion and $ 1 trillion in the economy - which represents anywhere between 20% and 30% the current GDP of India, and is as much as the proportion that the manufacturing sector Current Scenario: makes to the GDP of India.

ISSN 2394 - 7780

Digital India will transform India and its democracy through a more effective citizen-government engagement, transparency in public administration, taking the government to the people and citizens.

II. VISION OF DIGITAL INDIA

This programme is centered on three key areas

- Digital Infrastructure as a Core Utility to Every Citizen
- Governance and Services on Demand
- Digital Empowerment of Citizens

The proof of the vision and goals of Digital India, lies in the way it should specifically transform the lives of the 1.2 billion Indians. If the 3 areas of vision for the program - the infrastructure as a service to all citizens, governance and demand services that promote government efficiency and the digital empowerment of citizens. Information and services can be accessed without delays - and this will empower the citizens and boost the economy forward. The key task now before the government is to create a policy and implementation ecosystem for technological transformation of the country. This will require a legislative environment where they will allow all stakeholders to work and perform their functions, and supported investment, detailed implementation plan.

III. TECHNOLOGY TO TRANSFORM GOVERNMENT

One of the defining attributes of the Modi Government so far has been its relentless focus on increasing the efficiency and effectiveness of government. The results of this approach in the government bureaucratic efficiency and execution is already very visible in progress in several projects over the past one year. The technology is already being used - whether in control systems or other areas. Among the many structural reforms budgets is the focus on technology-based targeting of subsidies. This effort is probably the best thought through the efforts over the past six decades to address the scourge of leaks and corruption in subsidies.

Technology has a direct relationship with what is in effect a more efficient, transparent and accountable government. Creation of a technology platform for making processes of administrative decisions, moves governments to a new form of greater responsiveness and transparency. Responsiveness means less bureaucracy and more efficient environment and lives of citizens.

A number of other allied benefits accrued including reducing expenditure, enabling data analysis in real time, and ensuring faster movement of information and intelligence to key players in the bureaucracy. Each of these in turn generate Swifter, informed and more accurate and formulation of the policies adopted by the machinery of government decisions. A big problem when policies are usually made by vested interests and lobbyists in the absence of data and facts.

Another promise budget is the transformation of our economy into a cashless economy. A good example of a well executed service governance technologically enabled the government is the Pradhan Mantri Jan Dhan Yojana. The National Payment Corporation of India (CPI) has built a platform, reportedly all banks and telecom operators in the country connected. In 2014, 26 public sector banks and three private sector banks joined this platform that allows customers of any bank access to their accounts, check balance, transfer money, including through even mobile basic features. This is one of many steps taken by the CPI to India in a cashless economy, and once well established, will transform the way the Indian bank, make significant savings for the public purse, while improving the delivery of end line. The priorities mentioned by the Prime Minister in his election manifesto spoke of a "people-oriented system put in place" and "stress in addressing the problems of the people." Nothing would serve the best technology for servicing and repair of damage caused. It reduces red tape, and gives citizens access to information, coupled with expectations of a significant response.

IV. ICT TO BOOST AGRICULTURAL SECTOR

The lack of information or inappropriate information given, when combined with other factors such as environment leads to a huge loss in crop production or crop quality or the selling price of crops and, finally, farmers suffered heavily. Therefore, strategies should be made to provide farmers with any information from seed planting to harvesting and marketing of agricultural products from time to time to reduce waste and promote rural livelihoods and food security.

Since farmers in many parts of India, including Uttar Pradesh and East are becoming familiarize with mobile and internet and getting information on crops, soils, climate, cultivation practices, financing, storage and marketing products etc. Much concerted efforts of government, NGO and the side of the industry is now a demand of time for our farmers to use ICT for development benefits rapid technological advances in

ISSN 2394 - 7780

agricultural production, storage and marketing. It may be shared equally among all communities and sectors of rural society.Agriwatch is an information service which is internet-enabled and it provides the technical information and agricultural market in the form of magazines, newspapers, SMS and a website [5].

The objective of Agriwatch is to address and overcome the lack of information available to farming communities and therefore help them plan better and realize higher value.

Currently to assess damage to crops, officials and civil servants have to harvest crops damaged in six different fields, noting the last seven years to produce the same crop and then calculate damage. The process of granting compensation also extends as the amount is first sent to the insurance company, which in turn sends it to the deputy commissioner who then forwards it to the recipient.

V. TECHNOLOGY TO TRANSFORM THE LIVES OF CITIZENS

The extraordinary story of a 69 years old farmer Dharwad district of Karnataka state gives us a small window into exactly how the lives of 1.2 million Indian citizens can be positively impacted by having access to a delivery platform government services and integrated IT citizens. BM Hanasi, the owner of a seven-acre plot of land left completely baffled Karnataka cabinet after he wrote to the chief minister Siddaramaiah wondering why the government was not using latitude and longitude coordinates of Google Earth and WhatsApp to verify and expedite the crop insurance claims.

With the help of technologically enabled, citizens can save the mire of government bureaucracy and political corruption. A painful procedure for a citizen, otherwise take six months, could become a process in real time through the use of simple, affordable and accessible technologies process. This is a real opportunity and potential of the Digital India - the benefits to the end user service line - and the government has to do everything it takes to take it.

If the focus is on the transformation of government-to-citizen, government-to-business or government-to-government dynamics, there is a need for this program to go beyond statements of direction and speed to a vision of a India virtually integrated - which is already home to 850 million mobile users and 220 million Internet users. Integration practically India

While the physical integration of the country is expensive and time consuming and is a work in progress - Digital India can integrate remote parts of the nation to the rest of the country. The Northeast, Jammu and Kashmir can be integrated more efficiently, economically and in all other forms in a digital network. The possibilities for creating business on the back of these local economies are immense therefore also the possible transformation. In a sense, the ultimate objective of the Digital India is to integrate the country and the economy. By providing efficient, enabling technology platform, citizens in remote areas of the country can participate in and contribute to the economy. The North Eastern states, for example, have enormous potential for information technology led growth and development. With a very high literacy rate (over 70%), and the large number of people fluent in English, the region has great potential for the growth of the information technology enabled services - which is precisely what the eighth Digital pillar of India - "IT for Jobs' is on. Anticipating a country that successfully navigated the transformation of the telecommunications sector and created more than one crore employment for a period of five years through units Business Process Outsourcing.

VI. DIGITAL INDIA BUDGET 2015

The program is expected to cost approximately INR1,130 billion. Timely implementation of schemes and adequate funding are essential. The extent of fiber optic national network was announced, and the program's objective of connecting 2.5 lakh Gram Panchayats in 2016 was only just reiterated.

VII. JOURNEY TOWARDS TRANSFORMATION OF INDIA USING TECHNOLOGY

The ambitious programme of Digital India has started showing its results, although only in some urban areas and metros. How use of various technologies is beneficial in the following sectors :

1) Agriculture

Current Scenario: Farmers are unable to get updated knowledge in farming.

Technology: GIS, GPS, Cloud Technology, Sensors

Benefits: 24 * 7 Expert forum is available and can get experts advice immediately. To enable E-commerce in Agricultural products though vertical portal.

2) Education

Current Scenario: Almost chalk and board traditional system is being followed

ISSN 2394 - 7780

Technology: Skype, Cloud Computing E-Learning, Smart Boards

Benefits: Fast learning, Readily available information.

3) Health
Current Scenario: Expert diagnosis is not immediately available.

Technology: Sensors, Health management software.

Benefits: Correct diagnosis, Fast Treatment,

4) Banking
Current Scenario: e-Banking is not available in rural areas. And all types of transactions cannot be done on-line.

Technology: Specialized banking software and advanced computer network security using cloud computing.

Benefits: Paperless Banking, Fast Transaction, AnyTime, AnyWhere, Safe n Secure money transactions

5) Shopping
Current Scenario: Many shopkeepers would like to follow traditional shopping.

Technology: Websites developed by using JavaScripts, Cascading style sheets, HTML, PHP etc.

Benefits: Cashless Shopping, Variety of items are available, secure, reduced cost, paperless offices, Reduced transportation, improve standard of living.

VIII. CHALLENGES

The challenge for Digital India to provide last mile connectivity to Phase 3 and 4 areas - which are the cities and smaller towns of India. The digitization of these inhibitions require massive investments. It is clear that while government has a role in making investments, most of this investment and innovation must come from a public-private partnership that brings together the strong technological and entrepreneurial ecosystem in India fully into this. It is clear that the success of Digital India depends on innovation policy framework and allowing the government to make - and it is equally important that in addition to being an investor, the government assigned itself a role as a facilitator and plays innovation and investment that role too.

e-Governance also comes with its own set of challenges. Few strategic areas that need to be addressed are as follows: -

15. Ambiguity integrated service delivery
16. Awareness of both officials and public
17. Government representatives awareness about ICT
18. Public Awareness about ICTs
19. Non-acceptability of IT systems
20. Leveraging Private funding
21. Resistance to Re-engineering of Departmental Processes
22. Independent Impact Assessment
23. Localization/Multi-language support
24. Underutilization of existing ICT infrastructure
25. Non-compatibility between government officials and solution architects
26. Lack of Infrastructure
27. Privacy and Security Issues
28. Lack of Reliable Maintenance

IX. PRIVACY & SECURITY ISSUES IN IMPLEMENTATION OF E-GOVERNANCE POLICIES

To run any e-governance policy security solution is very critical. It is imposed through various components like firewall, authentication, mechanisms for audit control and mechanism for authorization [9]. It should provide an automated and role-based, secure, policy-based user management [11]. It needs to be able to centrally define

ISSN 2394 - 7780

and manage security policy for a wide range of e-governance and its applications. It should also have role-based administration model for allocation of administrative privileges and group users according to the needs of the business.

Security should also have a workflow to adapt to multilevel approval hierarchies and should be configurable for the local government / departmental environment, the planning system or other workflow products to collect and process information from the various contact points throughout the government. Security also includes enabling PKI for the existing web-based applications. It should have provision to support authentication and access control for the web (browser) users through ID & passwords which are already used, client-side certificates/RSA secure ID tokens[6]

The privacy issues are also major worries in India. The privacy of the citizen to be maintained while using the online services. During the communication of a resident with a Government agency, it can reveal lot of information, which can be misused by the hacker. Thus, the citizen should be ensured that the information would pass through reliable channels and intricate network. The identity of citizens before they access the services needs to be verified. Cybercrime is used to destabilize the effectiveness of e-Governance. Government systems have been targeted and hacked due to a variety of reasons.

X. CONCLUSION

The journey of the e-government initiatives in India took a wider dimension in the mid-90s for broader sectoral applications, with emphasis on citizen-centric services. Later, many states / UT began several e-government projects. Although these e-government projects were centered on the individual, they could do less than the desired impact. Government of India launched the National e-Government Plan (GNE) in 2006. The 31 projects covering multiple domains Mission mode is initiated. Despite the successful implementation of many projects of e-government throughout the country, e-government as a whole has not been able to make the desired impact and meet all its objectives.

The quality of rural life can also be enhanced by inputs which provide quality information for better decision-making skills. Information Technology can play an important role in facilitating the transformation of rural India to meet these challenges and to bridge the digital divide rapidly growing.

Rapid changes in the field of information technology make it possible to develop and disseminate electronic services needed in rural India. The bottlenecks in the tasks to be addressed immediately. It will help to reduce unemployment and fast development of country in all aspects, which will have great impact on Indian Economy. Also it will help to reduce poverty and help all Indian citizens to become independent and E-Literate. A national strategy needs to be drawn for leading IT penetration in rural India. A national agency with an advisory paper can act as a catalyst in the process.

Lack of awareness about privacy and security is still an issue. Government is yet to apply some new standards in all the organizations to reach international standards. Although there are standards like ISO 27001 and ISO 20000 for IT securities and management. Proper security issues should be handled with care while implementing e-Governance policies.

XI. REFERENCES

1. S.C. Mittal, “Role of Information Technology in Agriculture and its Scope in India”
2. Department of Industrial Policy and Promotion (DIPP), Media Reports, Press Information Bureau (PIB), RNCOS Reports.
3. Dept. of Electronics AndInformation Technology (deity.gov.in) retrieved on 10thMarch 2019, 9.30 pm.
4. Framework for Mobile Governance, Government of India, Department of Information Technology Ministry of Communications and Information Technology.
5. http://www.e-agriculture.org/sites/default/files/uploads/media/Agriwatch.pdf
6. Tidswell, J. E. and T. Jaeger. 2000. “An access control model for simplifying constraint expression”. In Proceedings of the 7th ACM conference on Computer and communications security, Pages 154 – 163.
7. Bhavesh Kataria, “Use of Information and Communications Technologies (ICTs) in Crop Production” 2015 IJSRSET | Volume 1 | Issue 3 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099.
8. Bakshi, S., ‘Corporate Governance in Transformation Times’, IBA Bulletin, 2003.

ISSN 2394 - 7780

9. Schneier, B. and J. Kelsey. 1999. “Secure audit logs to support computer forensics”. In ACM Transactions on Information System Security.

10. Prof. M.C. Sharma, Abhinav Sharma, “Role of Information Technology in Indian Banking Sector”, SHIV SHAKTI International Journal in Multidisciplinary and Academic Research (SSIJMAR) Vol. 2, No. 1, January-February (ISSN 2278 – 5973).

11. Bonatti, P.; S. di Vimercati; P. Samarati. 2000. “A modular approach to composing access control policies. In Proceedings of the ACM Conference on Computer and Communications Security”

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER SECURITY SHOWCASE: AN APPLICATION APPROACH

Rupali Phatak
[1]Department of Computer Science, DBJ College, Chiplun

ABSTRACT
The uncontrolled increase in the use of technology for the betterment of society through various applications is a major issue of the current area. The increase in technology also proves the adverse impact of cybercrime and other similar pitfalls. The literature is focused on the need of cyber security to avoid destructive actions. This cyber security related algorithms are widely used in various applications. Highlighted areas of applications are medical domain, wireless communication, moving objects defense, ATM etc. We focused on the similar concept of applications through exhaustive survey. The techniques of cyber security enlisted in this survey along with their pros and cons.

Keywords: Cyber security, implantable medical devices (IMD), moving target defense (MTD)

I. INTRODUCTION
Cyber security is a technique of disallowing access of any personnel or organizational computers to unauthorized aspirant, identifying irregularity in networking and protecting from code cheaters. Cyber security defends computing devices, data and integrity of computing system present in organizations. Applications of this cyber security are overwhelming the researchers [1]. With this motivation, we have focused on few major areas of concern.

The presented survey is arranged into four sections. Section II focus on moving target defense based cyber security algorithm. Third section illustrates detail comparison of authentication protocols in medical field. The paper is concluded in fourth section.

II. MOVING TARGET DEFENSE
Moving target defense (MTD) system works on networked system. MTD continuously changes the location of object and increases the efforts of attacker [2]. MTD is a fusion of shuffle, diversity and redundancy. Shuffle is applicable for Application layer and focused on TCP/IP infrastructure. Shuffling is responsible for exchanging IP addresses, VM migration, data randomization, proxy relocation, Instruction set randomization etc [3]. Diversity is also applicable for Application layer and topology layer and is mainly focused on topology of network. The diversity can be broadly viewed as path diversity, compiler base diversity, data diversity, software mix, software implementation etc [4]. Another contributor of MTD focusing on both application and topology layer is redundancy. It is responsible for providing multiple replicas of network component [5]. MTD hides the identity of agent by applying shuffling and diversities and provide various replicas. Thus attacker cannot easily find the object. MTD is inapplicable if network gets extended. Thus it is not scalable and adaptive. The combination of MTD and hierarchical attack representation model (HARM) solves this problem of scalability [2].

Table-1: Moving target defense

Methodology	Merits	Demerits
MTD	• Enhance security	• No provision of scalability and adaptability
MTD with HARM	• Qualitative and Quantitative Security matrices	• Not implemented in real world • Various vulnerability incorporated

III. IMPLANTABLE MEDICAL DEVICES (IMD)
Due of this changed lifestyle increase in diseases and weakening of human immunity system justifies the need of IMDs which get implanted into the human body to recover from medical condition and providing artificial functionality to damaged organs. IMDs include cardiac pacemakers and defibrillator, infusion pumps, neurostimulators, body area networks, cochlear implants. Few authentication protocols are explained in this section.

ZP Sec is an algorithm which protects from unauthorized access. Zero power authentications is a technique where a Wireless Identification and Sensing Platform (WISP) and a piezoelectric element circuitry are inserted in the human body. The WISP takes input from RF signals which are handled by programmers. These signals are transmitted from near distance of the patient to get appropriate output from IMD. The IMD sends the signal to the microphones touching the patient and which in turn programmer can sense the signals [6].

ISSN 2394 - 7780

Ultrasound based distance bounding is an extension of Diffi-Hellman algorithm which is used to communicate with IMD using ultra sound. This algorithm uses private keys for communication using encryption [7].

In-vivo Near field communication (NFC) is an embedded techniques implemented in IMDS and smart phones. In vivo NFC tag is present in the implanted IMD which communicates with Ex vivo NFC embedded in smart phones [8].

Cloaker is an external device that communicates with IMDs and programmers that handles the cloaker. The cloaker is mainly used in emergency critical situations. If the cloaker is misplaced or is out of battery it is still responsive [12].

IMD Guard is an external device called guardian which uses throughputs of ECG to get secrete key to share between IMD and guardian. The IMD pings the guardian and waits for T1 time until the guardian sends any response. If the programmer is available, the key is shared among programmer and IMD. Otherwise guardian waits for T2 time and resends [13].

IMD Shield is an external device which is carried on the human body. IMD shield act as a jammer and receiver. It allows only authorized access, if found unauthorized access it jams the signals. It works as a security shield for the existing IMDs [14].

Biometric-based two-level secure access control (BBS-AC) is a procedure which includes two levels of authentications. First level of authentication is biometrics measurements and second level of authentication is based on iris snap [9].

Heart to heart is a cryptographic authentication protocol which uses ECG signal. In this protocol IMD and programmer request the ECG signal at the same time. On the bases of these readings further which readings are to be accepted or rejected is depends on Neyman-Pearson hypothesis testing [10].

ECG-based secret data sharing (ESDS) is a secure technique which uses ECG signals to grand authentication.IMD and programmer need to measure ECG signals synchronously. The data to be shared need to be encrypted using error correcting code (ECC) [11].

Emergency aware access control (ea-ac) protocol states that a wearable proxy device which shares the key with IMD. In case of emergency, IMD detects some failure and sends response to proxy device, which sends emergency signal to the doctor in proximity [15].

Hospital authentication server access control (has-ac) authentication mechanism allows IMDs to share a key with the hospital server within the hospital. Also, the physician from the hospital shares a key with the authentication server [16]. Table 2 discusses merits and demerits of all above protocols.

Table-2: State-of-art authentication protocols

Contributor	Methodology	Merits	Demerits
D. Halperin et al. [6]	Zero power sensible security	• No battery power required • efficient access	• Low signal strength
K. B. Rasmussen et al.[7]	Ultrasound based distance bounding	• Used sound signal • Public key encryption	• Unauthorized access
B. Kim et al. [8]	In-vivo NFC	• Use of smart phone • Signal range 10cm to 1 m • Use of 3G or WiFi network	• Security protocol is handset dependent
T. Denning, [12]	Cloaker	• External device • shared session key • very fast response time	• inefficient approach • Excessive power consumtion
F. Xu et al. [13]	IMD Guard	• Shared key between guardian and IMD • Easy to rekey	• Required skin contact • Man-in middle attack
S. Gollakota et al. [14]	IMD Shield	• Battery life	• Power limitation

ISSN 2394 - 7780

		• Provides enhance security to existing IMD	• If shield is lost Security threatens
X. Hei et al. [9]	BBS-AC	• Two level authentication • Battery life	• Pre-stores biometrics data • Rarely perfect
M. Rostami et al. [10]	Heart-to-heart	• Battery life • Enhance security	• Wearable device • Battery drainage
Zheng et al. [11]	ECG-based secret data sharing (ESDS)	• No public key barrier • Battery life	• Man-in Middle Attack
M. Darji and B. H. Trivedi [15]	Emergency aware access control (EA-AC)	• Access contol • Battery life	• If proxy device is lost then IMD becomes inaccessible
C.-S.Park [16]	Hospital authentication server access control (HAS-AC)	• Authorized access	• No solution for emergency authentication • Drainage of battery • Denial of service attack

IV. CONCLUSION

Focusing on drastic change in lifestyle through use of technology, it is an immense need to maintain the privacy of this usage. Handful contributions are found in the state-of-art cyber security techniques obeying same objective. We shortlisted few major application areas of the cyber security and presented a rigorous study of them. Our work signifies the merits and demerits of all enlisted techniques and will be useful for new researchers working in the same field. The limitations of said technologies need to be removed for more secure lifestyle.

REFERENCES

1. https://www.papermasters.com/cyber-security.html
2. Jin B. Hong, Dong Seong Kim, “Assessing the Effectiveness of Moving Target Defenses using Security Models”, IEEE Transactions on Dependable and Secure Computing 2015
3. J. Jafarian, E. Al-Shaer, and Q. Duan, “Openflow Random Host Mutation: Transparent Moving Target Defense Using Software Defined Networking,” in Proc. of Hot Topics in Software Defined Networks (HotSDN 2012), 2012.
4. A. Newell, D. Obenshain, T. Tantillo, C. Nita-Rotaru, and Y. Amir, “Increasing Network Resiliency by Optimally Assigning Diverse Variants to Routing Nodes,” in Proc. of the 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2013), 2013.
5. S. Al-Wakeel and A.S. S., “PRSA: A Path Redundancy Based Security Algorithm for Wireless Sensor Networks,” in Proc. of IEEE Wireless Communications and Networking Conference (WCNC 2007), March 2007, pp. 4156–4160..
6. D. Halperin *et al.*, ``Pacemakers and implantable cardiac de_brillators:Software radio attacks and zero-power defenses," in *Proc. IEEE Symp. Secur. Privacy*, May 2008, pp. 129_142.
7. K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, ``Proximity-based access control for implantable medical devices," in *Proc. 16th ACM Conf. Comput. Commun. Secur. (CCS)*, 2009,pp. 410_419.
8. B. Kim, J. Yu, and H. Kim, ``*In-vivo* NFC: Remote monitoring of implanted medical devices with improved privacy," in *Proc. 10th ACM Conf. Embedded Netw. Sensor Syst. (SenSys)*, 2012, pp. 327_328.
9. X. Hei and X. Du, ``Biometric-based two-level secure access control for implantable medical devices during emergencies," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 346_350.
10. M. Rostami, A. Juels, and F. Koushanfar, ``Heart-to-heart (H2H): Authentication for implanted medical devices," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, 2013, pp. 1099_1112.
11. G. Zheng, G. Fang, R. Shankaran, M. A. Orgun, and E. Dutkiewicz, ``An ECG-based secret data sharing scheme supporting emergency treatment of implantable medical devices," in *Proc. Int. Symp. Wireless Pers. Multimedia Commun.*, Sep. 2014, pp. 624_628.

ISSN 2394 - 7780

12. T. Denning, K. Fu, and T. Kohno, ``Absence makes the heart grow fonder: New directions for implantable medical device security," in *Proc. 3rd Conf. Hot Topics Secur. (HOTSEC)*, 2008, pp. 5:1_5:7.
13. F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li, ``IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1862_1870.
14. S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, ``They can hear your heartbeats: Non-invasive security for implantable medical devices," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 2_13, Aug. 2011.
15. M. Darji and B. H. Trivedi, ``Emergency aware, non-invasive, personalized access control framework for IMDs," in *Recent Trends in Computer Networks and Distributed Systems Security* (Communications in Computer and Information Science), vol. 420, G. M. Pérez, S. Thampi, R. Ko, and L. Shu, Eds. Berlin, Germany: Springer, 2014, pp. 370_381.
16. C. S. Park, ‘‘Security mechanism based on hospital authentication server for secure application of implantable medical devices,’’ Bio Med Res. Int., vol. 2014, Jul. 2014.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

HUMAN RIGHTS IN CYBER WORLD

Prajakta Amit Patil
F. G. Naik College of Arts, Sci (IT) and Commerce, Koperkhairne, Navi Mumbai

ABSTRACT
This paper focuses on Human Rights in cyber world and their violation by personally and groups as well as due to commission of cybercrimes and applications of laws.

Cyberspace is virtual communicative space created by digital technologies. It is not limited to operation of computer networks, but also encompasses all social activities in which digital information and communication technologies are deployed. Point of global concern arises when we talk about safeguarding human rights in cyberspace. When we talk about human rights and cyberspace, we also talk on the issue of cybercrimes.

Crimes which are done on internet or by making internet a medium are known as cyber-crimes. Many of time cyber criminals perform such crimes which violates human rights of individuals.

The solution which the legal authorities take out to combat this issue is by limiting the content which is being posted on internet which in turn curtails the human rights of the individuals.

Thus, human rights on cyberspace are violated in both ways, by crimes also and by application of laws also.

International organizations have now started to take this issue seriously and laws are being made on this issue.

Keywords: Human Rights, Cyber Space, Cyber Crime, Hacking, Cyber Security, Cyber World

INTRODUCTION:

Whatare the Human Rights and why do Human Rights in Cyber World matter?

Human rights are rights which are provided to an individual by virtue of him being a human being.

The concept of human rights acknowledges that every single human being is entitled to enjoy his or her human rights without distinction as to race, colour, sex, language, religion, political or otheropinion, national or social origin, property, birth or other status.

Human rights are legally guaranteed by human rights law, protecting individuals and groups against actions which interfere with fundamental freedoms and human dignity.

Cyberspace is the virtual communicative space created by digital technologies. It is not limited to the operation of computer networks, but also encompasses all social activities in which digital information and communication technologies (ICT) are deployed.

Human Rights in cyber space is a new field of global concern. With the advent of internet and the popularity which it has gained in the recent years,it is necessary to monitor the cyber space and protect the human rights of people in it.

As we increasingly conduct our lives online – shopping, socializing and sharing information – our digital rights, particularly the rights to privacy and freedom of expression, are becoming more important.

We need to understand how our data is being used by companies, governments and internet giants such as Facebook and Google. Is it being handled fairly and scrupulously, or sold or shared without our consent.

The internet provides you a platform to exercise the right to freedom of expression and information Misuse of this information and violation of our basic human rights in Cyber World has given birth to a new category of crime and criminals i.e., cyber crime and criminals.

Cyber criminals are intruding into the private lives of the individuals thereby infringing the human rights of internet users. Internet is a strong medium of expression of your ideas and thus it should be without any restrictions. To control and supervise criminal activities on internet, human right of expression many at times can be violated.

Human rights in Cyber world

Human rights in Cyber World should not only be articulated as individual rights, but should be recognized both as individual and as collective rights.

1)UNIVERSALITY AND EQUALITY: All humans are born free and equal in dignity and rights, which must be respected, protected and fulfilled in the online environment.Everyone is entitled to all rights and freedoms

ISSN 2394 - 7780

without distinction of any kind, "such as ethnicity, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status".

for e.g

- Persons with disabilities have a right to access, on an equal basis with others, to the Internet.
- Gender equality -Women and men have an equal right to learn about, define, access, use and shape the Internet.
- Net neutrality and net equality - The Internet is a global commons. Its architecture must be protected and promoted for it to be a vehicle for free, open, equal and non-discriminating exchange of information, communication and culture

2) RIGHTS AND SOCIAL JUSTICE: Everyone has the duty to respect the human rights of all others in the online environment.

e. gOn the Internet the right to an appropriate social and international order includes:

Rights includes Protection against all forms of crime, right to enjoy secure connections to and on the Internet

Persons with disabilities have a right to access, on an equal basis with others, to the Internet.

The Internet and the communications system must be governed in such a way as to ensure that it upholds and expands human rights to the fullest extent possible

The Internet as a social and international order shall enshrine principles of multilingualism, pluralism, and heterogeneous forms of cultural life in both form and substance.

3) ACCESSIBILITY: Everyone has an equal right to access and use a secure and open Internet. The right to access to, and make use of, the Internet shall be ensured for all and it shall not be subject to any restrictions except those which are provided by law, are necessary in a democratic society to protect national security, public order, public health or morals or the rights and freedoms of others, and are consistent with the other.

4) EXPRESSION AND ASSOCIATION: Everyone has the right to seek, receive, and impart information freely on the Internet without censorship or other interference. Everyone also has the right to associate freely through and on the Internet, for social, political, cultural or other purposes.

5) PRIVACY AND DATA PROTECTION: Everyone has the right to privacy online. This includes freedom from surveillance, the right to use encryption, and the right to online anonymity, right to data protection, including control over personal data collection, retention, processing, disposal and disclosure.

No one shall be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence. Everyone has the right to the protection of the law against such interference or attacks

6) LIFE, LIBERTY AND SECURITY: The rights to life, liberty, and security must be respected, protected and fulfilled online. These rights must not be infringed upon, or used to infringe other rights, in the online environment.

On the Internet, the right to life, liberty and security includes:

Every one shall be protected against all forms of crime committed on or using the Internet

Everyone has the right to enjoy secure connections to and on the Internet.

Everyone has the right to seek, receive and impart information and ideas through the Internet.

The freedom and pluralism of the media shall be respected.

Freedom of Religion and Belief -includes freedom, either alone or in community with others and in public or private, to manifest his or her religion or belief in teaching, practice, worship and observance.

7) DIVERSITY: Cultural and linguistic diversity on the Internet must be promoted, and technical and policy innovation should be encouraged to facilitate plurality of expression

e.gAll individuals and communities have the right to use their own language

Right to participate in the cultural life of the community

ISSN 2394 - 7780

8) NETWORK EQUALITY: Everyone shall have universal and open access to the Internet's content, free from discriminatory prioritization, filtering or traffic control on commercial, political or other grounds.

9) DUTIES AND RESPONSIBILITIES:

Everyone has duties to the community in which alone the free and full development of his personality is possible.

Everybody has the duty and responsibility to respect the rights of all individuals in the online environment

Power holders must exercise their power responsibly, refrain from violating human rights and respect, protect and fulfill them to the fullest extent possible.

Cyber Crimes affecting Human Rights and Human Rights Protection in Cyberspace
When we talk about the human rights and cyberspace, we also talk on the issue of cybercrimes.

Cyber crime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cyber crime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet.

Also Cybersecurity laws and policies have a direct impact on human rights, particularly the right to privacy, freedom of expression, and the free flow of information.

Policymakers have created several national policies with the intention of protecting the Internet and other information communication technologies (ICTs) systems against malicious actors.

However, many of these policies are overly broad and ill-defined, and lack clear checks and balances or other democratic accountability mechanisms, which can lead to human rights abuses and can stifle innovation.

For example, extreme cybersecurity laws can be used to censor dissidents, monitor communications, and criminalize online users for expressing their views.

Thus the human rights on the cyberspace are violated in both the ways, by crimes also and by application of laws also.

The international organizations have now started to take this issue seriously and laws are being made on this issue.

Cyber laws are formed by International Organizations -

1)To protect the basic needs and interests of individuals in cyber-world

2)To Prevent misuse of Basic Human rights Cyber world are prevented by incorporating Cyber laws .

Under International law, states are legally obliged to respect, protect and fulfill the human rights of their citizens. Governments have the primary responsibility for realizing human rights within their jurisdictions. The duty to protect requires governments to protect against human rights violations committed by other actors, including businesses. States are also obliged to take appropriate steps to investigate, punish and redress human rights abuses which take place within their territory and/or jurisdiction.

However, other actors also have responsibilities under the International human rights regime. The Universal Declaration of Human Rights calls on "every individual and every organ of society" to promote and respect human rights. While these responsibilities do not equate to legal obligations (unless they have been enacted as such under national legislation) they do form part of prevailing social norms which companies and other private organizations should respect.

Thus while the primary responsibilities under the Charter remain with governments, the Charter also provides guidance to governments about how they must ensure that private companies are respecting human rights, and guidelines to companies about how they should behave so as to respect human rights in the Internet environment.

The Indian Parliament passed the Information Technology Act 2000 and amended in 2008 on the United Nations Commissionson International Trade Law (U.N.C.I.T.R.A.L) model Law.

The law defines the offences in a detailed manner along with penalties foreach category of offences. Thus cyber laws are the safe savior tocombat cyber-crime.

ISSN 2394 - 7780

CONCLUSION

As world is becoming too small as everybody is connected to cyber space ,as technology advances ,Cyberspace with its benefits has a darker side also and marks the presence of cyber-crimes which ultimately lead to the violation of human rights.

To overcome and protect human rights in cyber world ,Apart from Governing bodies which implement Cyber laws to prevent cyber crimes , it is everybody's responsibility of protecting individualsand groups against actions which interfere with fundamental freedoms and human dignity.

FUTURE WORKS

The future of human rights in cyberspace depends on the evolution of the laws and its interpretation in continuouslychangingtechnologies. Internationally acceptable laws should be there to safeguard the human rights of the individuals in the cyberspace.

Future work needed in this space for countries to acceptance and implementation "Internationally Acceptable Standard" for Protection of Human Rights in Cyberspace.

REFERENCES

- https://www.religion-online.org/article/human-rights-in-cyberspace/
- https://en.wikipedia.org/wiki/Human_rights_in_cyberspace
- https://www.ohchr.org/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf
- https://www.weforum.org/agenda/2015/11/what-are-your-digital-rights-explainer
- http://ijldai.thelawbrigade.com/index.php/2017/05/24/the-flip-side-of-curbing-cyber-crimes-violation-of-human-rights/
- https://www.humanrights.gov.au/sites/default/files/document/publication/human_rights_cyberspace.pdf
- http://docs.manupatra.in/newsline/articles/Upload/C4971E8F-86E8-48E1-886B-CEF0B774397F.pdf

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

INTELLECTUAL PROTECTION IN DATABASE MANAGEMENT SYSTEMS

Varsha Kshirsagar
Ph.D. Electrical, IITRAM, Ahmedabad

ABSTRACT
Intellectual property (IP) protection is considered as one of crucial tech- nology for the reuse based design methodology in various disciplines.Case study of intellectual property protection in different disciplines gives com- petative advantage over the rivals and healthy competition always responsi- ble for technology improvement.This paper supports balanced discussion of the drawbacks,the motivation ,challenges and answers for problems associ- ated in different disciplines like machine learning,micro-video,big Data in IP protection. IP protection like patent makes positive impact to secure fund from goverment program

1 INTRODUCTION
Intellectual property has high degree of protection. Intellectual property right work as a two way sword,from one side there is increasing awareness and this protection is considered as motivational factor for creation of in-tellectual work and from otherside giving overall protection to intellectual work can be unfortunate to the further process of humanity[1] Rights given to owner for own creation of their minds,result of thought such as writ- ing,painting,scientific inventions.

Intellectual property rights are generic terms of exclusive rights given to the result gained by humans.Anirben Sengupta,et al thought is that the ul- timate goal of Intellectual property is to protect the rights of buyers and sellers.[3] Thabiso ,et al [2] represents Intellectual Property in terms of Ap- propriability which is ability of technological term to protect its innovation Intellectual property needed to balance the public and private right (ex- clusively and exception)for economic significance,to make innovation possi- ble,to ensures quality and making improvement in daily life. IP protection normally through makes positive impact in helping companies for getting fund from goverment program.[?] It is key business asset for economic explo- ration of work which gives remarkable recognition in the form of fame and intensive to the creator .It spurs economic growth and its lucrative. Patent database in any field can give specific direction for new researchers.

2 INTELLECTUAL PROPERTY PROTECTION STRATEGY
Various methods can be used for IP protection and in terms of intellectual asset of company for profitability. There are mainly two types of intellectual Property

i) Formal IP protection methods like patents,copyrights ,trademarks.

ii) Informal IP protection method like trade secrets,non -disclosure agree-ments,lead times,complexity of design,complementary sales and complemen- tary manufacturing and operations [2]

- Copyright is right to stop others from taking full benefit the work without knowledge of owners of copyright maintains balance between interest and rights of the author[1] and its law cover protection of published and unpub- lished work.
- The patent is used for protecting and maintaining ventures IP value and for making profit or creating value for stakeholders.patent are used to get com- petitive advantages and to invent new product it can also used for valuation asset during contract for more profit[2].
- Trademarks are recognizable images and/or words which is used to define and differentiate various product or services.[5] Trademark law is well defined and its registration make it distinctive and relate with quality warranty rep- utation of product

3 LITERATURE REVIEW
In praposed paper we survey the efforts from different disciplines like Big Data,Machine Learning ,Digital Piracy for existing methods for intellectual property protection and focus is made to improve protection in each area.

3.1 IP Protection in the field of Semiconductors
According to the International Technology Roadmap for semiconductors(ITRS), there is productivity gap between previous and existing techniques ,to close this gap industry moved IP reuse based designs and this is important reason for making IP most valuable asset.

ISSN 2394 - 7780

With time IP protection evolved from one form to other for example lay- out design to SoC(system on chip) design which changes aim of IP protection extension with different IP infringement.Here in society of Intellectual Prop- erty IP owner is known as watermark and legal IP user is known as fingerprint and for making these terms effective it is necessary 1) To provide quality 2) maintain credibility of IP owner and legal user 3)It should be robust 4) pro- vide facility of part protection to any portion of IP 5)should provide same treatment to all users 6)allow easy identification of watermark/fingerprint 6)should punctual in desired function ability.

Existing methods such as watermarking, fingerprinting can identify IP piracy but can not prevent IP piracy. design of watermark is lagging in case of robustness ,research on watermak method is open to all so loosing effectiveness of protection [?]most IP piracy is due to Reverse Engineering and to prevent this two new methods Logic encryption and IC camouflaging can be used to prevent Reverse Engineering attacks.[6]

3.2 IP Protection in Big Data Industry

Resent research in IP protection by Juan He,et al.[5] in the field of big data is still in early stage of development.Existing method can be divided into three categories.

(i) Study of copyright,trade mark and other issue in the area of big data. (ii) Study of patented technologies in the field of big data.

(iii) Study of industry development atmosphere of big data.

Reviewing all existing method a lot improvement needed so proposed method explains systematic study of different challenges of big data from vertical and horizontal angles and scrutinizes data collection,storage,analysis and mining and summarizes the risks faced in each data processing.Also covers application of big data in retail industry,logistics industry,health-care industry and concludes protection mechanism of intellectual property in new models[5].

3.3 IP protection in Micro Electronic Media

The aim of this paper is to achive kind of autharisation having feature of portability and easy to accesss and easy to access and to enhance the qual- ity of copyright protection.From the study of data users of online video is growing linearly with advancement in technology such as 3G,4G and creates favorable condition for micro video copyright transaction Existing method for video copyright protection is digital watermarking , in a proposed method dual threading mechanism is used which increases micro-video authorization efficiency by decreasing time required for this process also add encryption for digital watermarking.In order to improve system efficiency of micro-video authorization multi thread processing is used where one thread is added to remove drawback of multithreading.

It obtain the compression Stream of audio and video from a package and reduces time require to process effectively. With technology improvement area of pay mode video is also changing to make this process easy such that trading price set rationally depends on popularity of copyright.This mode of online trading have many benefits such as 1)it is very convenient communication if compared with offline mode2)online transaction for micro-video promote actual quality video to more peoples 3)Increases development online trading mode ,gives more choices for the customers of micro-video 4) Increases healthy competition for more improvement in this field.[?, micro video]

3.4 IP protection in the form of Trademark

Trademark are known images or symbols which represent reputation inno- vation quality of product,perception with known product tilt towards brand piracy,to identify trademark infringement oweners register their trademark and to avoid piracy.In this field images are compared and similarity examined by experts.Due to volume registration of Trademark in patent office manual inspection is not possible.

Trademark Image Retrival is necessary to avoid false registration of sym- bols in patent office to avoid drawback of existing system here neural nework with many layers. [5]

4 RESULT AND DISCUSSION

Intellectual property protection makes innovation possible almost in all fields with remarkable quality.However role of intellectual property more difficult to establish but economic growth always motivates people for intellectual growth

i) In the field of machine learning IP protection Trusted Execution Environ- ment responsible for increasing extra implementation and validation cost.

ISSN 2394 - 7780

ii) Copy right contract should made easy and convenient for both parties.There are limited methods for IP protection at higher abstraction level

iii) Ideal pricing model should be designed depend on popularity of copy right trading.

iv) Micro -video protection method have drawback of increasing cost of CPU,higher error rate compared with single thread.

5 CONCLUSION

With improvement in technology a lot of advancement is needed in the field of IP Protection and for this existing IP can be used as an asset for future work.Fast and crucial growth expected in this field for benefit in almost all digital area.

REFERENCES

1. S.Ravindra Bhatt, Innovation and intellectual property rights law-an overview of the Indian Law, IIMB Management review, 2018(30),51-61
2. Thabiso T. Kgaanyago,Elma vander Lingen Influence of External Funding and Intellectual Property Protection on the Success of Techno- logical Ventures:Case study 2018 Proceeding of PICMET'18 Technology management for Interconnected World.
3. Anirban Sengupta,Dipanjan Roy Reusable Intellectual Property Core Protection for Both Buyer and Seller,2018,IEEE Conference on Con- sumer Electronics (ICCE) .
4. Miodrag Potkonjak,Gang Qu,Farinaz Koushanfar ,Chip-Hong Chang Research on Intellectual Property Protection ,2017 IEEE.
5. Claudio A Perez,Pablo A Estevez,Francisco J.Galdames,Danial A. SChulz Trademark Image Retrival Using a Combination of Deep Convolutional Neural Network ,2018 IEEE
6. Yuntong Qi,Yu Liang,Sanxing Cao The Research of The Copyright for Online Micro-videos with Reference to The Ways of Protection and Ex- change,2017 IEEE

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

ISSUES OF DEEP AND DARKWEB -REVIEW

Nilesh Prajapati
JVM Mehta Degree College, Navi Mumbai

ABSTRACT
This paper discusses about the underlying security issues in webs and their kinds in todays world and tries to either or not to implement dark web and their impact on social media. If you are into computer security then you might have heard about types of web, there are three types of the web such as Surface Web, Deep Web and Dark Web normally people know about Surface Web. Many people believe that Google search engine is capable to find any information based on a particular topic on the internet. But this is our illusion there are also some other Search Engines which helps to access the private or secret information that is not usually accessed via search engine like Google.

Keywords: Surface web, deep web, dark web, search engine

INTRODUCTION
Surface Web: It is used by normal users to access web sites and web content,near about only 4% of World Wide Web content is present on Surface Web.In Surface Web all activity is public so anyone can communicate with any one.You cannot hide your private activities.So if you are doing any illegal activity any legal organizations anyone can track your illegal activities.

Deep Web:A major part of worldwide web content is covered by Deep Web, near about more than 90%.Deep web contains those links which the user will not find by normally searching on google or other search engines.It contains private information such as government database or data of any private organization

Dark web: It is also known as 'Invisible Web'.Its content is not indexed by search engines. And it is hard to keep track off.

WHAT IS DARK WEB ?
Dark web is also known as Darknet,It's a part of Deep web or we can say that it's a subset of Deep Web dark web it maintains the privacy of host.for accessing sites of dark web you need special web browsers such as Tor, I2P, and Freenet, and is often associated with criminal activity of various degrees,including buying and selling drugs, pornography, gambling, etc.

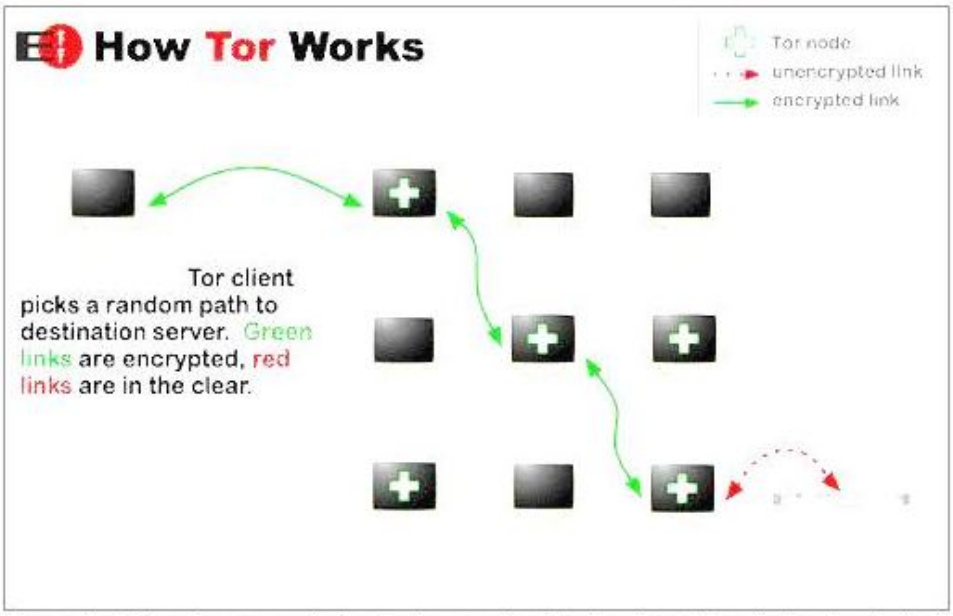
	INDEXING	**NON INDEXING**
RESTRICTED	NULL	DARK WEB
ACCESSIBLE	SURFACE WEB	DEEP WEB

HOW TO ACCESS DARK WEB?
You cannot access dark web by using a normal ISP or Browsers (i.e. use the normal internet connection that you have such as airtel, Jio and Idea and try to open the dark web link in Google Chrome, opera or search for

ISSN 2394 - 7780

that link you will not get any result). For accessing these websites you need a special type of browser and you can access this by Onion Routing. The web sites which you cannot directly access by Google or even by typing on browsers are known as Dark Web.

Normally on the surface web you cannot maintain your privacy. So for that one open source Community has been developed which maintain your privacy and allow you to visit sites privately. So in this scenario, when we want to visit any website we need to buy one VPN and then visit the website so now just because we have a virtual private network ,no government agencies or Internet service provider can track us ,they will not be able to know what we are doing, but its disadvantage is that the company which is providing us VPN will get the information about our activities. So to solve this problem we use the concept of onion routing and we buy multiple VPN's For example if we want to visit google.com the request will first go to the first VPN and that request will go to multiple VPN's one by one and form an complex network at the end it will open google.com and if google.com wants to check from where the request has come it becomes difficult to trace back due to complex routing. Every time it changes its IP address.



Example of Tor data transmission and encryption. Notice the red line indicating the lack of encryption outside the Tor network.

Tor has some websites with .onion domain these websites are like normal websites but the only difference is that this normal websites such as .org , .com is that this website's will normally get opened in Google but these .onion websites only open in Tor so that the host and visitor both are anonymous.

STEPS TO HOST .ONION WEBSITE

step1 :

Install Tor browser and then configure Tor server by setting up to serve HTTP content it is done in the same way as we do to configure our regular web server. While we would value more highly to run a traditional net server at 0.0.0.0 in order that it becomes accessible to the web as a full by its informatics, we can bind our native server environment to 127.0.0.1 to ensure that it will be accessible only locally and through Tor. And also Install Xamp server it allows you to host your website it's a virtual web server.

step2:

- Create a web page with .PHP extension and open it using localhost before that open Xampp Server and start Apache and run the file.
- create one folder where domain will be alotted for your website.
- Go to the folder where Tor browser has been installed in Tor browser folder go to the \Browser\TorBrowser\Tor folder in that you will get one torrc file and open it and write the code you want to write. MiddenServiceDir C:\Users\Hp\Desktop\Tor Browser\Host MiddenServicePort 80 127.0.0.1

- First line represents the path where we will get Domain
- and second displays our IP address and port number

ISSN 2394 - 7780

Step3:
Open the .php file by ip address 127.0.0.1 on local browser you will get the same file which was

open in localhost and then close the tor browser and Then again open Tor browser now you will

get one domain in domain folder which you have created and if you type that domain in tor

browser your site will appear.

THINGS THAT YOU CAN BUY AND SELL USING DARK WEB

1.Drugs Dealing
Individual or dealer-level quantities of illicit and pharmaceuticals of each sort square measure on

the market within the digital underground. The trade route, the now-shuttered drug superstore, did $200 million of business in twenty-eight months.

2. Weapons
Different unauthorized organizations are doing illegal dealings of weapons for illegal activity.

3. Counterfeit Currency
Fake cash varies widely in quality and price, in euros, pounds, and yen all are available. Six hundred dollars can get you $2,500 in counterfeit U.S.notes, secure to pass the everyday pen and ultraviolet-light tests.

4. Human trafficking
It is trading of humans for the purpose of commercial sexual exploitation and forced labor.

5. Human Organs
In the darker corners of the Dark internet, a vibrant and gruesome black market for live organs thrives.Kidneys might fetch $200,000, hearts $120,000, livers $150,000, and a combination of eyeballs $1,500.

THINGS THAT MAKE INTERNET CRIME WORK

1. Cryptocurrency
Digital money, such as bitcoin and dark coin, and the payment system Liberty Reserve provide a convenient system for users to spend money online while keeping their real-world identities hidden.

2. Bulletproof Web-hosting Services
Some web hosts in places like Russia or united States welcome all type of content, create no tries to be told their customers' true identities, settle for anonymous payments in bitcoin, and habitually ignore subpoena requests from law enforcement.

3. Cloud Computing
By hosting their criminal malware with reputable firms, hackers are much less likely to see their traffic blocked by security systems. A recent study instructed that sixteen p.c of the world's malware and cyber attack distribution channels originated within the Amazon Cloud.

4. Crimeware
Less skilled criminals can buy all the tool which is needed to steal the data. There was one hacker who used such a tool which invaded Target's point-of-sale system in 2013.

5. Hackers for Hire
New hackers are hired for illegal activities.

6. Multilingual Crime Call Centers
Employees can play any double-faced role you'd like, like providing job and academic references, initiating wire transfers, and unblocking hacked accounts.

ADVANTAGES

1. Freedom of speech
The right to freely express your opinion on any topic while not fearing about abuse that almost all western countries deem granted (although with these matters, you ne'er extremely recognize what might happen) is sort of a utopia in sure elements of the globe.

2. Political Activism
Oppressive governments are a crude reality in the 21st century. Information could be a terribly powerful weapon to the present quite regimes, and its citizen's movements on the globe Wide net area unit strictly

ISSN 2394 - 7780

monitored to avoid the unfold of revolutionary ideas. Blocking websites, particularly those associated with social media, is a common measure in oppressive environments.

3. Knowledge

The deep web stores the largest virtual libraries you could possibly imagine. It is a good house for researchers, students and lecturers, since what they can find in the deepnet will more probably not be available from standard search engines. Scientific findings that haven't created public and will influence health and social beliefs of enormous populations are often found within the deepest of the net waters. Literature from all ways of thinking that you will not find in the book storefronts are also stored in the deep web.

DISADVANTAGES

1. Phishing and scams

Phishing via cloned websites and alternative scam sites area unit varied, with darknet markets usually publicized with deceitful urls.

2. Illegal and ethically disputed pornography

There is regular enforcement action against sites distributing kiddie porn – usually via compromising the positioning by distributing malware to the users. Sites use complicated systems of guides, forums and community regulation. Other content includes sexualised torture and killing of animals and revenge smut.

3. Terrorism

There is a area unit with minimum of some real and deceitful websites claiming to be employed by ISIL, including a fake one seized in Operation anonymous. In the wake of the Gregorian calendar month 2015 Paris attacks AN actual such web site was hacked by AN Anonymous related hacker cluster GhostSec and replaced with an advertisement for SSRI. The Rawti Shax religious person cluster was found to be operative on the dark net at just the once.

CONCLUSION

The deep net can still perplex and fascinate everybody who uses the web. It contains an bewitching quantity of data that might facilitate United States of America evolve technologically and as a species once connected to alternative bits of knowledge. And of course, it’s darker side will always be lurking too, just as it always does in human nature. The deep net speaks to the fathomless, scattered potential of not only the internet, but the human race, too. Regardless of if the Dark net exists or not, the aforementioned activities still occur. The Dark net simply provides a straightforward thanks to connect with folks of comparable interests, and to facilitate any interaction.

REFERENCES

- 1.https://www.google.com/url?sa=t&source=web&rct=j&url=https://www.researchgate.net/profile
- /Arvind_Singh56/post/Do_you_have_any_idea_about_DEEP_WEB_DARK_WEB_RED_ROO
- M_of_internet/attachment/5b8beec53843b0067537635d/AS%253A666415669473282%2540153
- 5897285612/download/Dark-Web.pdf&ved=2ahUKEwiyy73V5oDhAhXXR30KHVNeA2QQFj
- AAegQIAhAB&usg=AOvVaw3CAIolBuOCgHFgLinb5-sd
- https://goo.gl/images/Aip7UX
- https://www.scribd.com/document/355412798/TorAndTheDarknet-pdf
- https://youtu.be/VJdMG-UbCFw

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

OVERCOMING THE ISSUES IN DIGITAL FORENSIC AND INTERNET OF THINGS

Sharayu Mahesh Kadam
Assistant Professor, Department of Computer Science & Information Technology, JVM's Mehta College, Mumbai

ABSTRACT
The smart devices are used in the major field such as the healthcare, transportation, smart home, and smart city. This technology one-time uncovered too much openness, which may lead to cybercrime from side to side devices. With the IOT constraints and low-security mechanisms applied, the device could be easily been attacked, treated and broken by cyber criminals where the smart devices might be provide incorrect data where it can conduct to incorrect analysis and actuation to the genuine users. To observe with the IOT characteristics, two approaches towards of having the analysis for IOT forensic is wished-for by emphasizing the pre-investigation point and implementing the real-time analysis to make sure the data and possible proof is composed and sealed all over the investigation.

Keywords: The Internet of Things, Digital Forensic, IOT Forensic, Real- Time Investigation.

INTRODUCTION
Term web Things was 1st utilized by Kevin Ashtonin 1999 is an unambiguously classifiable objects (things) and their virtual illustration sinan Internet-like structure We typically assume in terms of computers, tablets and smart phones. It describes a world wherever on subject of something may be connected and communicate in a very "smart mode" by combining straightforward knowledge to provide usable intelligence. With the IOT, the physical world is changing into one huge system with last word goal of rising quality of life.IOT (Internet of Things) could be a difficult automation and analytics system that exploits networking, sensing, big data, artificial intelligence technology deliver complete product for a product or service. These systems enable bigger transparency, control and performance when applied on any industry or system. IOT have applications across industries through their distinctive flexibility and talent to be appropriate in any surroundings. They enhance information assortment, automation, operations, and much more through smart devices and powerful enabling technology.

IOT CHALLENGES
- **Security:** Security is major concern in field of computer technology. With the numerous device connected chances of security usage also increases on failing it will expose data.
- **Privacy:** The IOT creates challenges to privacy, many who transcend the info privacy problems that presently exist Privacy is that the single most significant challenge to the various users. If privacy isn't self-addressed then privacy will be threatened. In terms of the latter, voice recognition or vision options area unit being integrated that may ceaselessly hear conversations or sit up for activity and by selection transmit that information for processes. These data exposes legal and regulative challenges facing information security and privacy.
- **Standards:** Standards can evolve however save lot of project space and development cost. Without standards to guide makers, developers typically style merchandise that operates in troubled ways that on the web while not abundant relevance their impact. A lot of this comes all the way down to price constraints and therefore they have to be compelled to develop a product for unleash faster than competitors.
- **Regulation:** Like privacy, there are a large vary of regulative and legal queries close the IOT, which require thoughtful thought. The technology is advancing far more speedily than the associated policy and regulative environments.
- **Development:** The broad scope of IOT challenges won't be distinctive within countries.

Threats
"Action that takes advantage in security weaknesses with the Associate Nursing passing system and contains a negative impact there on." Originally, threats area unit derived from 2 totally different essences: natural and human. Our focus is on human-related threats, such as:

Identification

Localization and Tracking

ISSN 2394 - 7780

Examples may be GPS hacking and thru web traffic are as follows

- **Profiling:** the gathering of data concerning interests, hobbies, and demographics
- **Privacy:** violating interaction and presentation: assortment of personal info through a public channel open for the market
- **Lifecycle transitions:** usage of private photos and videos on smart gadgets, such as old phones and laptops

Attacks on IOT

1. **Cyber reconnaissance:** wherever associate trespasser uses cracking techniques and malicious code to conduct spying on the targeted user to either gain access to secret data or sabotage the prevailing systems. Cyber-attack like hackers 'weaponries'' everyday devices with malware
2. **Brute force attacks on passwords:** intruders make an attempt to guess the user's passwords with the help of automated software, which makes innumerable attempts until the right password grants the access.
3. **Stalking or tracking:** The every move will be tracked or traced by UID which belongs to IOT device. Tracking a user offers away their precise location in time wherever they want to stay anonymous.
4. **Controlled Attacks:** using Denial Of Services (DOS), Trojans, or viruses are some examples of controlled attacks. In such cases, intruders develop a selected virus that's programmed to perform during a bound manner so as to destroy the host device. Programmers and developers ought to be watchful whereas engaged on current IOT solutions since hackers nowadays have sturdy artillery to launch cyber-attacks in the world.

Sensor and actuators

A sensor carries energy modules, power management modules, RF modules, and sensing modules.

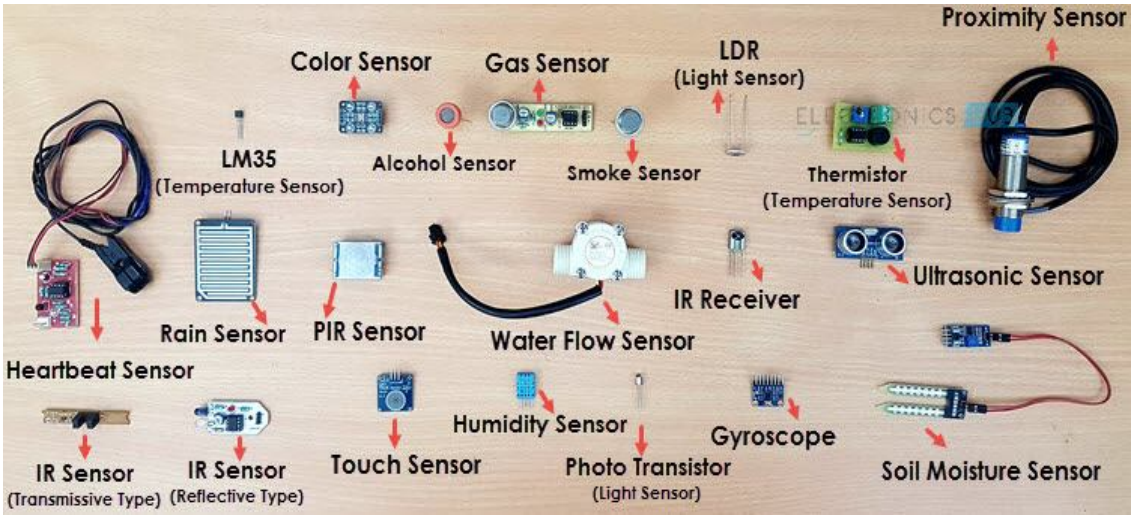
1. An input stage consists of protection circuitry and amplifier.

In some circuits, the amplification is incorporated into the A/D convertor.

2. A/D converter.

3. A Microcontroller takes details from A/D converter, process the data and converts it in a form readable by the user

RF modules manage communications through their signal process, WiFi, ZigBee, Bluetooth, radio transceiver, duplexer, and BAW.



The sensing module manages sensing through assorted active and passive measurement devices. List of measure devices employed in IOT –

1. Accelerometers -temperature sensors
2. Magnetometers -proximity sensors
3. Gyroscopes -image sensors

ISSN 2394 - 7780

4. Acoustic sensors -light sensors

5. Pressure sensors -gas RFID sensors

6. Humidity sensors -micro flow sensors

Data Processing Module
The third building blocks of the IOT device is that the processing module.This is the particular "computer" and also the main unit that processes the information performs operations like native analytics, stores data locally, and performs some other computing operations.

Communication Module
The last building blocks of IOT hardware is that the communications module. This is the half that permits communications together with your Cloud and with 3rd party systems either locally or in Cloud.

Wearable Electronic Devices
Wearable electronic devices area unit tiny devices that may be worn on the pinnacle, neck, arms, torso, and feet.

IOT Hardware – Wearable Electronic Devices

Current smart wearable devices include:

• Head − Helmets, glasses,

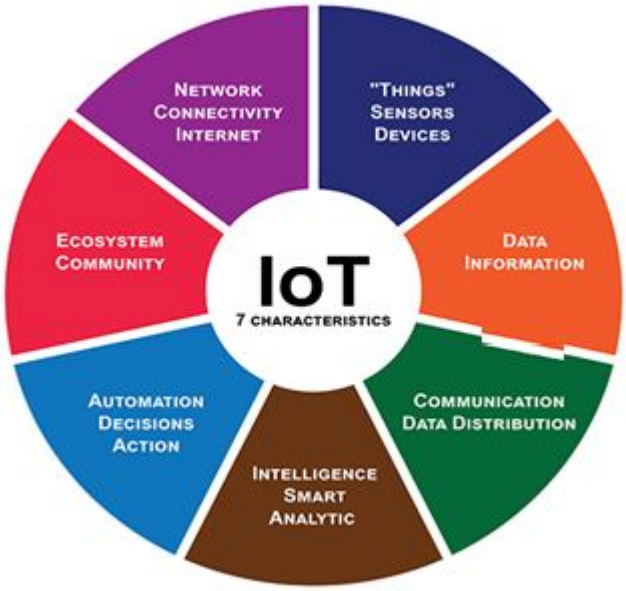
• Neck − Jewelry, collars

• Arm − Wristwatches, wristbands, rings

• Torso – Clothing pieces, backpacks

• Feet − Shoes, Socks

Following are the characteristics of Internet of Things



ISSN 2394 - 7780

1. Connectivity
This doesn't need much further explanation. Devices, sensors, they are connected to associate degree item, to every different, actuators, a method or another network.

2. Things
Physical things exist in the physical world and are capable of beings ensued, actuated and connected. Examples of physical things embody the encompassing setting, industrial robots, goods and electrical equipment. Virtual things exist within the data world and are capable of being hold on, processed and accessed.(Ex)virtual things include multimedia discontent and application software. Devices will contain sensors sensing materials will be connected to systems and things.

3. Communication
Devices gets linked in order that they will communicate and analyze this information.

4. Intelligence.
The face of the intelligence is with the sensing capabilities in IOT devices and therefore the intelligence gathered from information analytics also AI.

5. Action
This can be manual action, action primarily based upon debates concerning phenomena and automation, typically the foremost necessary piece.

6. Ecosystem.
Place of web from a perspective of different system, communities, goals and therefore the image during which the web of Things fits.

DIGITAL FORENSIC TOWARDS IOT

IOT forensics is one of the digital forensic branches where the main investigation process with the IOT transportation. This is a way to know the system carefully and start to investigate the event which is related to IOT. The challenger is likely exploiting the openness of the devices and the communication channel like e-mail, phone call which begin hateful orders to put in danger in a patient's life. Therefore, the forensic investigation methodology is necessary to be performing in the IOT model.

Reviews of Digital Forensic Framework

Digital forensic frameworks have been planned formerly. The frameworks were developed for the conservative computing. On the other hand, none of them are readily and suit for the IOT context. These process need to be ready to cater for the Internet of Things characteristic and its environment. The classification of pre-investigation phase, investigation and post-investigation are being considered based on the process involved in the framework from the previous work.

The Investigation Framework

The IOT devices create big information which contains the likely data where it will contact the investigation procedure. It's difficult to recognize which device had occupied in the event and it will take more time to find which devices start the attacks. All the important parts of data need to be collecting and keep determining the facts about the occurrence. Collecting and preserving the data is the most dangerous steps of the forensic process. The process of proof of withdrawal also might be difficult than the predictable computing as there are various data formats, protocols, and physical interfaces concerned.

Real-Time Approach for IOT Forensic

The Components of Real-Time Investigation

The components of real-time investigation are as follows:

Time Synchronization – As in the real-time approach for IOT forensic, the clock of the IOT devices, data storages, and detection machine are timely synchronize.

Memory and Storage Requirement – Real-time computing requires sufficient memory and storage ability to contain the extreme giving out and memory supplies and timing individuality.

Communication Requirement – Tough and steady communication between the components is very important to make sure that all the possible data can be remove and store up in a timely method.

CONCLUSIONS

Here, attempt has been made to elaborate the framework of the IOT environment. Also security issues related to IOT focusing on importance of security in IOT environment. To, combine IOT with digital forensics, the high degree improvement in forensics has measured. By analyzing retrospectively the gap has been defined.

ISSN 2394 - 7780

REFERENCES

1. Abdmeziem, R. & Tandjaoui, D., 2014. Internet of Things: Concept Building blocks, Applications and Challenges.
2. Alharbi, S., Weber-Jahnke, J. & Traore, I., 2011. The proactive and reactive digital forensics investigation process: A systematic literature review. *International Journal of Security and its Applications.*
3. Borgohain, T., Kumar, U. & Sanyal, S., 2015. Survey of Security and Privacy Issues of Internet of Things.
4. Carrier, B. & Spafford, E., 2004. An event-based digital forensic investigation framework. *Digital forensic research workshop*.
5. Hachem, S., Teixeira, T. & Issarny, V., 2011. Ontologies for the internet of things.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

REVIEW STUDY ON CYBER INTELLIGENCE AND CYBER FORENSIC INVESGATION

Raj M. Kittur
Student, Mechanical Department, Mahatma Gandhi Institute of Technical Education and Research Centre, Navsari, Gujarat

ABSTRACT
It is all started with Threshold (Beginning) of "INTERNET", when people began to use it, they were unaware about the fact that up to what extent it can harm or can be fruitful for mankind. Internet has increased the amount of CYBER CRIMES, CYBER TERRORISM, MAIL SPAMMING, SOFTWARE HACKING, etc. In order to overcome this problem USA Federal Government Agency has decided to establish a fusion between existing agencies and the private sector for real-time use against cyber attacks. CTIIC (CYBER THREAT INTELLIGENCE INTEGRATION CENTER) was created due to blocked efforts in Congress that were stymied over liability and privacy concerns of citizens. Basically, this is the most powerful support to reduce, decrease the crimes related to computers, and also it is helpful in various other fields of investigations such as Intelligence agencies of different countries, also to stop the terrorist activities, etc

Keywords: Cyber Threat Intelligence, Attributes, and its Examine

CONCEPTS OF CYBER INTELLIGENCE

Introduction to CYBER INTELLIGENCE

It is basically an "elusive" concept and is based on the collection of intelligence using open source intelligence (OSINT), social media intelligence (SOCMINT), human intelligence (HUMINT), technical intelligence or intelligence from the deep and dark web. CI's key mission is to research and analyze trends and technical developments in three areas:

1) CYBER CRIME

2) HACTIVISM (use of technology to promote a political agenda)

3) Cyberespionage (advanced persistent threat, APT or Cyber spying)

Types: The UK's National Cyber Security Centre (NCSC) distinguishes/ramifies four types of threat intelligence:

Tactical: attacker methodologies, tools, and tactics – relies on enough resources and involves certain actions to go against potentially dangerous actors trying to do infiltration.

Technical: indicators of specific malware

Operational: details of the specific incoming attack, assess an organisation's ability in determining future cyber threats.

Strategic:high – level information on changing risk (strategic shifts) – senior leadership is required for thorough determination to critically assess (impose) threats.

Benefits of tactical cyber intelligence:

Provides context and relevance to a large amount of data

Empowers organisations to develop a proactive cybersecurity posture and to bolster (to give support)overall risk management policies

Informs better decision - making during and following the detection of a cyber intrusion

Drives momentum toward a cybersecurity posture that is predictive, not just reactive

Enables improved detection od advanced threats

Challenges and Controversies on the value of cyber threat intelligence:

There are also challenges that cyber threat intelligence research is facing, including some controversies on the value of threat intelligence and whether it really works. Different experst have voiced their concerns on whether TI is really effective in its current state. Conversely, others have argued that "Threat Intelligence" can help identity vulnerabilities and ways to resolve them.

ISSN 2394 - 7780

Attribution

Cyber threats involve the use of computers, software and networks. During or after a cyber attack technical information about the network and computers between the attacker and the victim can be collected. However, identifying the person(s) behind an attack, their motivations, or the ultimate sponsor of the attack, is difficult. Recent efforts in threat intelligence emphasize understanding adversary TTPs.

APT (Advanced Persistent Threat) attribution studies:

APT1

APT28

APT29

Blackvine Cyber Espionage group

Dragonfly

ESG Solution Showcase

Waterbug Group

Seedworm

CTI and political risk

Influential geopolitical countries, such as the US, Russia, China and Iran, use cyberspace as an extension of their foreign and intelligence collection policies. To achieve these objectives, they have formed APT units that primarily specialise in the following fields:

Collection of sensitive data from or government computer systems

Electronic penetration or sabotage of critical infrastructure computer syatems

A combination of CTI with risk analysis, which includes a deep understanding of current geoplotical disputes and leadership ulterior political motives, can help analysts understand future cyberwarfare patterns.

CYBER FORENSICS AND CYBER INVESTIGATIONS

Cyber Forensics is the practice of collecting, analyzing and reporting on digital data in a way that is legally admissible. It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally. Cyber forensics follows a similar process to other forensic disciplines, and faces similar issues.

Uses of Cyber forensics

There are few areas of crime or dispute where cyber forensics cannot be applied. Law enforcement agencies have been among the earliest and heaviest users of cyber forensics and consequently have often been at the forefront of developments in the field. Computers may constitute a ‘scene of a crime’, for example with hacking or denial of service attacks or they may hold evidence in the form of emails, internet history, documents or other files relevant to crimes such as murder, kidnap, fraud and drug trafficking. It is not just the content of emails, documents and other files may be of investigators but also the ‘metadata’ associateed with those files. A cyber forensic investigation may reveal when a document first appeared on a computer, when it was last edited, when it was last saved or printed and which user carried out these actions. Most recently, commercial organizations have used cyber forensics to their benefit in a variety of cases.

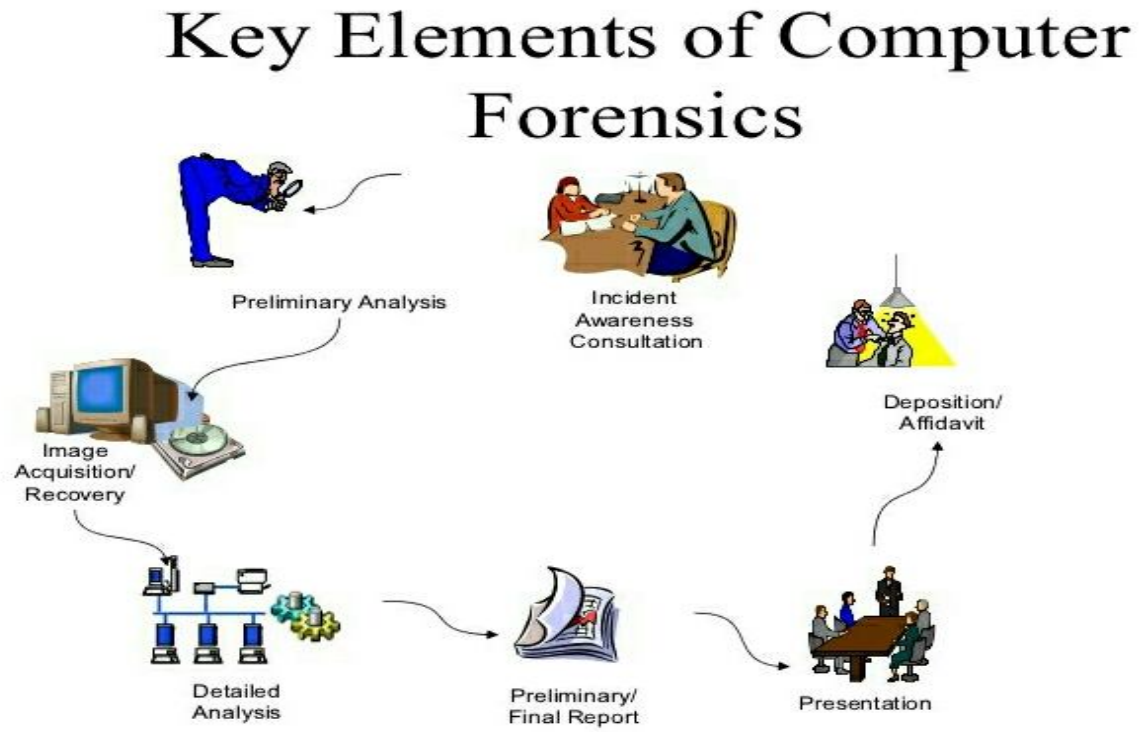
Services they provide

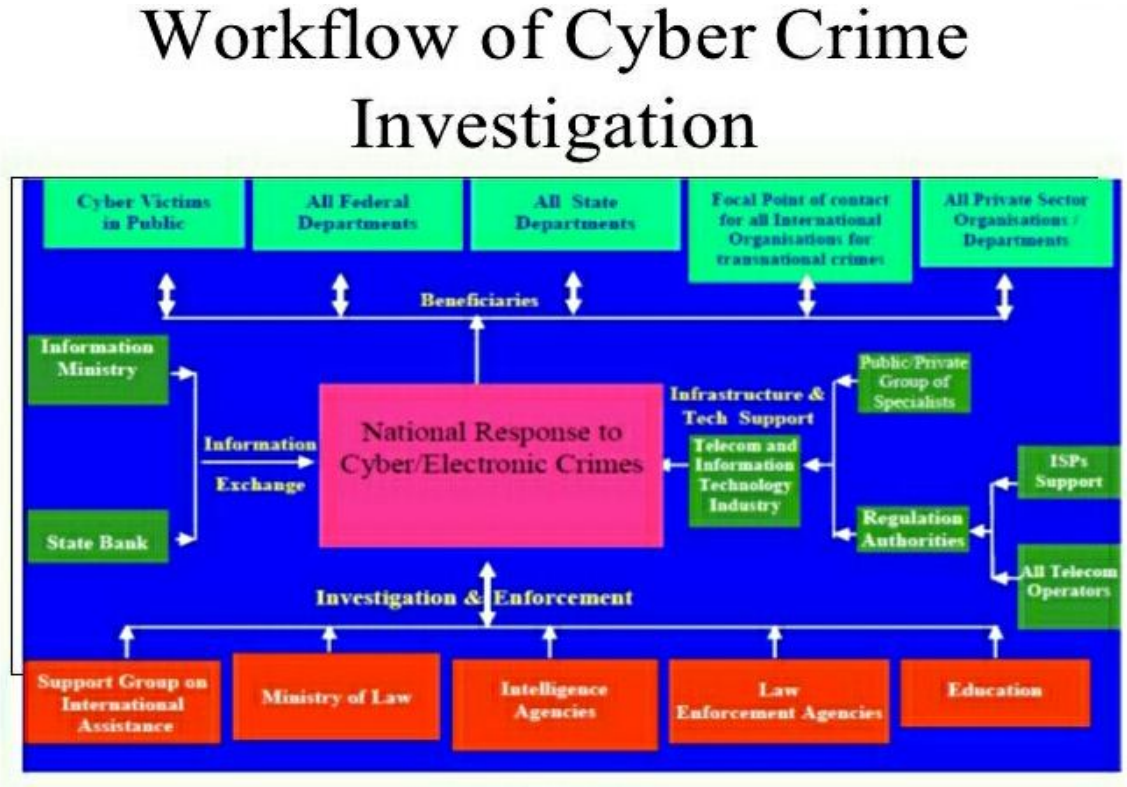
- Data Recovery
- Data Protection
- Email Analysis
- Image Recovery
- Email Protection
- System Protection
- Employee Monitoring
- Email Tracing

ISSN 2394 - 7780

- Fake Email ID's and Social Networking accounts
- Offensive content
- Website/Email hacking

Any other crime involving the use of computers.





The types of Computer Forensic Investigations (CFI)

1) Administrative Investigations and the CCFE (Certified Computer Forensics Examiner) exam

2) Civil Investigations

3) Criminal Investigations

ISSN 2394 - 7780

4) E – Discovery

5) Evidence Management

6) Incident Response and Forensics

7) Intellectual Property Investigations and the CCFE

CRIMINAL INVESTIGATIONS

In computer forensics, criminal and civil cases have different procedures. Criminal laws deal with the offenses against the individuals and the state. The law enforcement body of the state arrests the criminals and its judicial system conducts a trail. After that, the perpetrator is punished with fine, probation, imprisonment, or even capital punishment.

In criminal cases, the forensic scientists with an authorized search warrant can forcibly seize the computer and other devices that may have been used for criminal purposes. When carrying out criminal investigations, the law enforcement agencies must follow the rules. For example, the Fourth amendment to the U.S. Constitution and the Charter of Rights of Canada restrict government "search and seizure" to safeguards the rights of people, including people suspected of crimes. Besides the "Department of Justice" (DOJ) regularly updates the information on search and seizure.

The investigators can determine whether the crime was computer-related by asking some questions, such as:

- What tool was used to commit the crime?
- Did the perpetrator breach someone else's rights by email harassment?
- Was it a simple trespass?
- Was it vandalism or theft?

Following Legal Processes in Criminal Investigations:

U.S. courts accept the legal processes discussed here; however, other countries may have different procedures. The legal processes of criminal investigation depend on the local customs, legislative standards, and the rules of evidence. Generally, criminal cases follow three stages:

1. The complaint
2. The investigation
3. The prosecution

CIVIL INVESTIGATIONS

Civil investigations are not conducted because of crime but because of disputes or lawsuits in which the questions of property or money must be settled. The winning party must receive compensation in the form of payment, property, or services. Also, civil investigations are conducted by private investigators instead of law enforcement agents.

In civil matters, the investigators and a defendant can negotiate over when the computer will be inspected and even what data will be required to check. When conducting the civil investigations, the private investigators use one or more of the following three methods to acquire relevant information.

- Interrogations and interviews
- Record checking
- Physical surveillance

Administrative Investigation

Common types of administrative investigations stem from the corruption and misbehavior of employees, such as sexual harassment, bribe taking, stalking, and racial discrimination within any administrative agency, such as either a government agency or any corporation, which may lead to disciplinary action. The concerned agency, following its rules and regulations, has the legal right to conduct an administrative investigation against those employees who violate these rules and regulations.

At a workplace, the investigators first examine the network and the computer system of the employee in question. In this way, the investigators can find evidence in emails, work management applications, and computer storage devices. External sources, such as social media, can also be helpful.

ISSN 2394 - 7780

Administrative investigations, in fact, are non-criminal in nature. However, some facts found in administrative investigations may involve the law enforcement agencies. For example, one employee committed sexual harassment via emails. When the investigators examined his mailbox, they discovered emails, along with the emails of sexual harassment, proving his connection with terrorist organizations.

Private investigators, detectives, analysts, and clerks all can perform administrative investigations. The law enforcement agents become involved only if the case takes on a criminal nature.

Prerequisites for an Effective Investigation

Before carrying out the investigation, the examiner should recognize the proficiency level of the actors involved in the case, such as police offers or attorneys. To conduct an investigation and manage the computer forensics aspects of the case, the examiner must have DES training and sufficient information about the scope of the case, which includes the computer hardware, operating system, hard drive, and other devices. Also, the examiner should determine whether the necessary resources are available to conduct an investigation. Furthermore, he/she should also make sure that the right tools are available for acquiring and analyzing evidence.

Process Model for Computer Forensics Investigation

Many attempts have been made to develop a universally accepted process model for computer forensics investigations, but all in vain. In fact, the main reason for the failure of process models is that there is no process model developed so far that can be applied to the whole computer forensics field. Instead, the present process models only cover specific areas of computer forensics, such as law enforcement, cloud forensics, or mobile forensics.

Report Writing for High-Tech Investigations

The structure of the well-defined report contributes to reader's ability to understand the information that the report writer is trying to provide. The investigators should ensure that the report's sections are labeled and follow a regular numbering scheme. Also, make sure that the supporting material, such as tables and figures, are labeled and numbered consistently. Avoid using jargon, vague wording, and slang.

Maintaining Professional Conduct

Professional conduct is of paramount importance because it determines the credibility of the computer forensics investigator. Professional conduct includes ethical behavior and legal principles. When conducting an investigation, the examiner must adhere to legal principles and exhibit the highest level of ethical behavior. Professional conduct can be maintained by taking the following guidelines into consideration:

- Maintain confidentiality during an investigation. To do so, don't reveal the case's sensitive information to anyone; only authorized people should be privy to this information, such as other investigators.
- Expand technical knowledge continually.
- Maintain integrity.
- Don't hurry to reach conclusions without considering all the available facts.
- To keep the integrity of fact finding during an investigation, the examiner must avoid bias or prejudice.
- Since the field of computer forensics is changing rapidly, the examiners must stay current with the most recent computer hardware and software, operating systems, forensic tools, and networking.
- Be aware of the most recent investigation techniques.

CONCLUSION

In conclusion I would like to conclude that the whole world which is insecure about their information, data or any other kind of privacy related protection they require is provided by the forensic experts and their methodology of investigation, which will not completely eradicate or destroy this CYBER THREATS, CYBER CRIMES, etc. but up to some extent it will be reduced.

REFERENCE

- https://www.infosecinstitute.com/career-profiles/computer-forensics-investigator/
- https://en.wikipedia.org/wiki/Cyber_threat_intelligence

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

MALWARE INVESTIGATION AND ANALYSIS

Sunitha Joshi
JVMs Mehta Degree College, Airoli

ABSTRACT
The sum and the intricacy of malignant movement is expanding and advancing step by step. Run of the dynamic static code investigation is in vain when tested by differing variations. The prolog of new malware tests each day isn't extraordinary and the malware planned by the aggressors can change as they spread. Along these lines, robotized dynamic malware investigation turns into a generally favored method for the recognizable proof of obscure malware.

In this paper, a computerized malware location framework is displayed dependent on unique malware investigation approach. The conduct of malware is seen in the controlled condition of the famous malware investigation framework. It utilizes the grouping and characterization of inserted malware conduct reports to recognize the nearness of pernicious conduct. In view of the experimentation and assessment it is apparent that the proposed framework can accomplish better F-measures, FPR, FNR, TPR and TNR values bringing about precise arrangement prompting progressively effective location of obscure malware contrasted with the customary various leveled characterization approach.

Keywords: malware, FPR, FNR TPR, TNR

I. INTRODUCTION
Malware risk is a sort of code structured with hazardous goals. The real job of the malware is focusing on the security of clients and their data which made the utilization of noxious exercises consistently developing. Be that as it may, the high-need for risk is presented by the security scientists.

Generally sent customary methodologies, for example, signature-based and static malware examination require manual assessment of the noxious code by the human experts. Tragically, gigantic development in the age of malevolent code drove the antivirus merchants to confront a large number of new malware records each day.

The examination of extensive volume of documents by this method avoided because of jumbling, polymorphism and so forth. Subsequently, a solid and computerized examination is an imperative point to certainly adapt to this danger. With the expansion in promptly accessible and modern apparatuses, utilization of the new age digital dangers/assaults is ending up more focused on, steady and obscure. The propelled malware's are focused on, obscure, stealthy, customized and zero days when contrasted with the customary malware which were wide, known, open and one time. Once inside, they stow away, recreate and incapacitate having assurances. In the wake of getting introduced, they call their order and control servers for further guidelines, which could be to take information, contaminate different machines, and permit observation.

Cloud foundation has been developing pattern for a considerable length of time by giving chances to scale, adaptability and productivity. Despite the fact that clouds developing in the present situation yet there exist essential assaults by the programmers, for example, VM gaps and cloud explicit dangers identified on the earth. Giving security and dependability assume an essential job in the virtualized condition. There are a lot of studies occurring in the virtualized condition which has the primary importance on systems, Virtual machine administrator, visitor virtual machines and Operating System (OS).

Against this foundation, here in this paper, a structure is proposed for malware conduct investigation dependent on virtualization procedures. The location of malware documents in the distributed computing condition utilizing the machine learning approaches is accomplished. The principle commitment is in the decrement of the False Positive rate which inaccurately characterizes pernicious documents.

II. RELATED WORKS
Malware creators have produced a few different ways to recognize the nearness of malware examination frameworks yet powerful malware investigation defeat the majority of the programmers systems, for example, avoidance, confusion, polymorphism and so forth.

A few online devices accessible today are depending on powerful examination systems that create reports which are the human justifiable arrangement. The investigation framework is required to have a proper portrayal for malware, which is then utilized for arrangement either dependent on closeness measure or highlight vectors. In any case, an expansive number of new malware tests landing at against infection merchants consistently require a robotized approach in order to restrain the quantity of tests that require close human investigation. A few

ISSN 2394 - 7780

Artificial Intelligence strategies, especially machine-learning based procedures have been utilized in the writing for computerized malware examination and grouping. The distinctive works did by the creators are examined underneath.

Watson et al. [1] brought up an online cloud irregularity identification framework with the use of one class bolster vector machine. One class SVM plan is utilized at the hypervisor level with using highlights at both framework and system level. Security and strength are real jobs in the cloud framework consequently cloud ought to almost certainly respond to the obscure dangers producing in reality. The proposed strategy includes oddity recognition strategies to beat the identification of obscure dangers. The tale approach utilized here is the one class bolster vector machine helps in use of highlight to distinguish the noxious viewpoint at the hypervisor level. The virtual machine utilized in the test utilizes per VM techniques to play out the investigation which helps in identification of malwares.

Bayer et al. [2] presented a scalable clustering approach that identifies and clusters malware. Extended ANUBIS system is used with taint tracking for analyzing the behavior. The limiting factor of this approach is to trace dependence. Another issue is dynamic data tainting; so the malicious binary could be injected. Some malware triggers only during some actions or events such as setting up time to explore etc. these forms major limitation for this framework. The evasion techniques are also not avoidable in this approach which is again a disadvantage.

Syarif et al. [3] called attention to the investigation of static and dynamic malware approaches. The static technique is accomplished without running framework though powerful while running. This paper features the significant upsides and downsides of every procedure with its distinctive use.

Dilung et al. [4] gave a near structure the presentation of Bare Cloud idea which builds the rate of distinguishing shifty malware however further enhancement can be accomplished presenting more extravagant file system-level occasion follows.

The Bare Cloud make utilization of progressive grouping approaches which harshly arranges malwares into various bunches dependent on the highlights chose. The exploratory outcome gives the more prominent execution when contrasted with alternate strategies and procedures. Testing over the extensive number of malware tests separated the execution and precision among other promptly accessible devices.

Dilung et al. [5] built up a robotized strategy called MALGENE for removing examination avoidance signature. Malgene makes utilization of bioinformatics calculations which finds sly conduct consequently as framework calls.

III. SYSTEM ARCHITECTURE

The principle objective of the proposed framework is to distinguish malware in a computerized path by diminishing the rate of bogus recognizable proof of malware. The utilization of dynamic malware investigation is to recognize the nearness of malevolent conduct. The framework right off the bat catches the execution follows, in this way recognizing the noxious follow.

The engineering perspective of the proposed framework is portrayed in the fig. 1 which for the most part comprises of examination module and the arrangement module. Investigation module mostly does the preprocessing errands, for example, creating information appropriate for the classifier apparatus. While, arrangement modules manage the preprocessed information to play out the correct grouping so as to separate each example into it's relating neighbors.

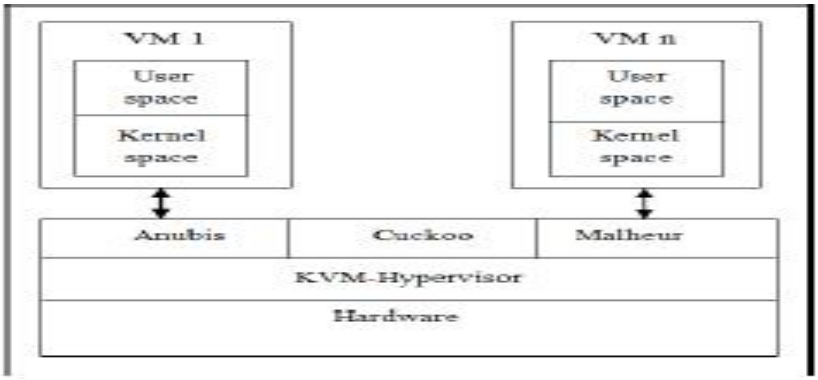


Fig.1. Basic System Architecture

ISSN 2394 - 7780

The key goal of the proposed structure is to recognize malware in an automated way by decreasing the rate of counterfeit unmistakable verification of malware. The usage of dynamic malware examination is to perceive the closeness of pernicious lead. The system directly off the bat gets the execution pursues, as such distinctive the pernicious pursue. The building point of view of the proposed structure is depicted in the fig. 1 which generally involves examination module and the course of action module. Examination module basically does the preprocessing errands, for instance, creating data suitable for the classifier gadget. However, game plan modules deal with the preprocessed data to play out the right gathering in order to isolate every precedent into its relating neighbors.

A.Analysis Module

The preprocessing of malware examination is the execution of malicious follows in the instrumented condition. Here, wild used structures Anubis and Cuckoo sandbox are used to make the social reports of the malware and affable models. These structures continue running over the KVM-hypervisor to keep up a key separation from explanations behind execution to the host machines. The inspiration driving preprocessing step is to pick the most captivating models which are likely going to have threatening behavior. These preprocessed malware tests are then supported to the dynamic malware examination mechanical assemblies used to perceive the proximity of noxious practices.

B.Classification Module

Malware unmistakable verification is practiced through the portrayal of malware which is done using the Malheur gadget. The reliable and accurate request of malware will result in the effective area of malware with the use of novel frameworks portrayed in the further regions.

IV. EXECUTION

The inspiration driving security and adaptability accept an important activity to make usage of dynamic malware examination in dispersed registering condition. To perceive the closeness of threatening code the precedent must be executed and pursued out the features which organize the characteristics of malware tests. The structure uses following approach to finish the examination.

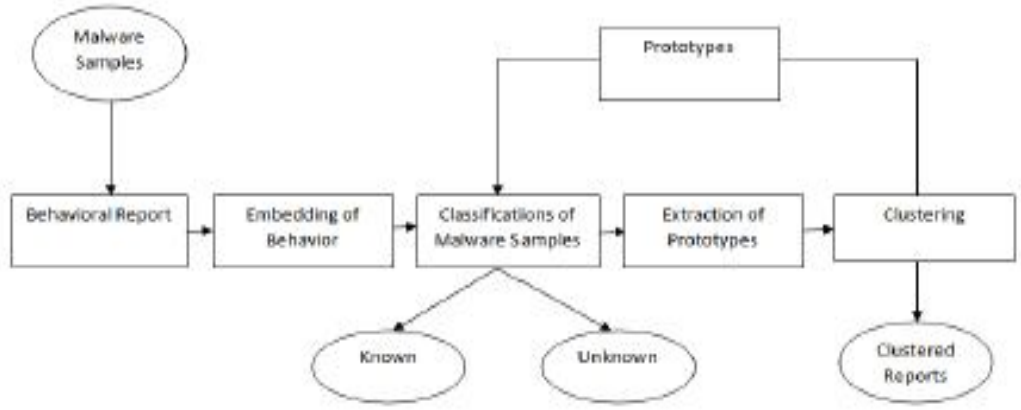


Fig.2. Flow diagram showing overall activities of the system

Grouping and characterization for examination of noxious conduct with the utilization of various leveled bunching and SVM approach [9] are utilized. At first, a report is picked as a model, arbitrarily or settled. Utilizing this model the malware inserted reports are bunched. The bunching of installed reports parcels the given information into important gatherings specifically the groups. Each group split a typical trademark for each item inside it though it fluctuates from different bunches. It helps in the finding of the qualities to the obscure malware information for the bigger measure of tests.

The grouping calculation referenced here speaks to the stream of control between the model age and correlation with the installed reports. The underlying purpose of accepting one report as a model and contrasting and alternate reports, results in the closest neighbors having comparative qualities together. Be that as it may, these aides in the age of groups.

CALCULATION FOR CLUSTERING:

1. Initialize by thinking about every model as a bunch
2. Iteratively find and union the nearby pair of bunches
3. While (min(distance) < dc) (i.e., the Maximum separation between Individuals)

ISSN 2394 - 7780

Do
Bunch the closest models

Refresh separate utilizing total linkage

4. for (x reports)

Do
Allocate closest models to x reject Clusters with lesser than least individuals

The machine learning idea encourages framework to gain proficiency with the highlights of the malware at the state of bunching. The hints of qualities are spared and utilized for the characterization strategy. The strategy is utilized further in the discovery of obscure classes of malware by making utilization of the models got in the primer advances.

Arrangement of obscure malware will require legitimate distinguishing pieces of proof of the given highlights in the standard of conduct which is reachable utilizing bunching and order strategies however it is constrained as the procedure is a clump procedure. Along these lines, the steady examination strategy utilizes officially grouped conduct report with the put away models with another social report of obscure malware. The age of malware expanding this strategy performs order by decreased runtime.

The order calculation given underneath is utilized in the grouping of installed reports into one of a kind bunches. Characterization results free separation of malware into its comparative practices of malware. This is helpful in the recognizable proof of malware follows.

Calculation for Classification:
1. for x reports do
2. Determine the closest model in the preparation information
3. If (closest model is inside the range dr)(i.e., the Radius of a bunch),

Allot reports to the specific bunch else
Reject as obscure

V. RESULT ANALYSIS

The test includes two arrangement of information, for example, preparing and testing. Right off the bat preparing tests are given to the calculations for learning the diverse highlights of malware tests. It is completed in the controlled condition, for example, a sandbox. The execution follows are gathered as a printed report. In any case, the dynamic examination of these malware tests in the sandbox gives spellbinding insights regarding the moves made spot amid the investigation, plainly portraying the distinctive perspectives, for example, arrange, record framework, library, etc exercises.

Malware Name	R	F	P	S	N
QQFarmer .exe	✓	✓	✓	✓	x
cb2b90bfa3 .exe	✓	✓	x	x	✓
cb2c1bc00a .exe	✓	✓	x	✓	x
cb5aab8b5f .exe	✓	✓	✓	x	x
test360343 .exe	✓	✓	x	✓	x
cb5def4900 .exe	✓	✓	x	✓	✓
cb3daa9c3a.exe	✓	✓	✓	x	x
VirusShare .exe	✓	✓	x	✓	✓

Fig.3. List of system activities from Anubis sandbox

ISSN 2394 - 7780

A number of input samples are executed in the sandbox environment and the reports are listed. The analysis time required by the execution of different volumes of samples is compared by taking time as a measure.

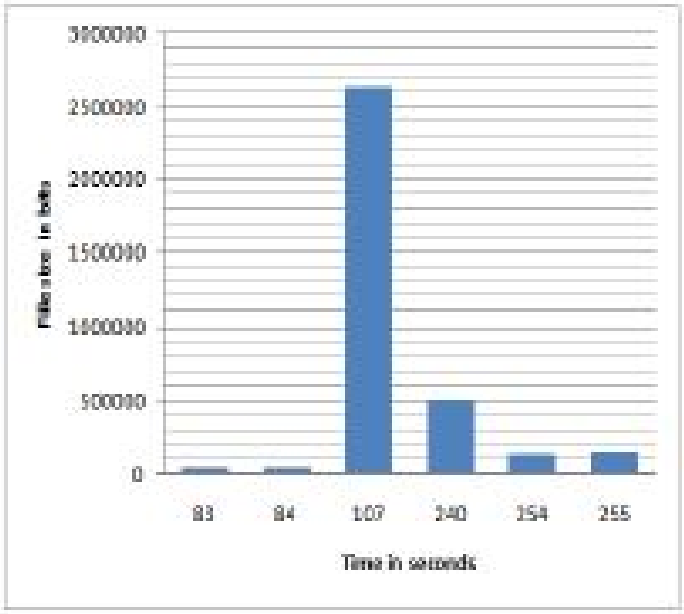


Fig.4. Execution time for files in Anubis framework

The time required for the execution of malware files in Anubis framework is shown in the graph which clearly indicates that even if the size is large it requires greatly less amount of time for execution.

Results for the relative valuation of proposed approaches are shown in Table 6.2 and 6.3 taking F-measure as a major performance metric. The analysis of the components in the framework gives the best result for the related methods. The "prototype-based clustering" gives an F-measure = 0.95 for MIST =1 and 0.936 for MIST= 2. For unknown it reached F-measure is 0.96.

Finally, the evaluation of performance metrics such as TPR, FPR, TNR, and FNR are measured. These metrics compares the number of given samples with the number of output reports which results in the correct identification of malware samples. Following formulas are used to calculate these measures:

Table 1. Comparison of clustering methods

Clustering Method	F-measure
Proposed Method with MIST 1	0.950
Proposed Method with MIST 2	0.953
Hierarchical Clustering	0.881

Table 2. Comparison of classification methods

Classification method	F_k	F_u
Proposed Method with MIST 1	0.981	0.967
Proposed Method with MIST 2	0.972	0.954
SVM with text feature	0.807	0.564

ISSN 2394 - 7780

The performance can be maintained same with a large number of datasets as there is the usage of preprocessing and filtering. However, the algorithm performs well with the large datasets and also the usage of incremental analysis i.e. comparing the rejected data again with the prototypes results in the classification of unknown malware as well.

VI. CONCLUSION AND FUTURE SCOPE

Vindictive exercises in the virtualized condition are winding up increasingly serious. The Internet is presented to vulnerabilities utilizing aggressors to get to the classified information. The essential and the static methodologies have flopped here because of the procedures utilized by the programmers and the absence of recognizing the new obscure mark of the malware. Among the few procedures utilized so far in the advancement of computerized malware investigation, the dynamic malware examination brought about better execution.

In this proposed strategy the extraction of malware conduct, recovering the best element, bunching to the related model just as allocating to the comparing class is accomplished which is valuable in the recognition of malware test in the virtualized condition. This work is for the most part worried to give better grouping and order of malware tests by delineating it as malignant or kindhearted. It has accomplished decreased rate of FPR and FNR when contrasted with the current methodologies. It tends to be utilized to defeat the issue of virtual machine openings and noxious exercises by a programmer. Since the virtual machines are associated with the host, it is verified at the hypervisor level, in this way guaranteeing the assurance of information will be at a high rate.

In future, the whole methodology can be robotized by incorporating the modules of the proposed framework with better machine learning ways to deal with have the effective grouping and arrangements of malware information.

REFERENCES

1. R. Islam, R. Tian, L. M. Batten, and S. Versteeg. Classification of malware based on integrated static and dynamic features. Journal of Network and Computer Applications. vol. 36, pp. 646-656, 2013.
2. M. Ahmadi and A. Sami. Malware detection by behavioral sequential patterns. Computer fraud and security, 2013.
3. Y. Park, D. S. Reeves, and M. Stamp. Deriving common malware behavior through graph clustering. in Computers and security (Elsevier), pp.419- 430, 2013.
4. M. Zolkipli and A. Jantan. Malware behavior analysis: Learning and understanding current malware threats. Second International Conference on Network Applications Protocols and Services (NETAPPS). pp. 218-221, Sept 2010.
5. M. Egele, T. Scholte, E. Kirda, and C. Kruegel. A survey on automated dynamic malware-analysis techniques and tools. ACM Comput. Surv. vol. 44, pp. 6:1-6:42, Mar. 2008.
6. A. Moser, C. Kruegel, and E. Kirda. Limits of static analysis for malware detection, in Computer Security Applications Conference, 2007. ACSAC 2007, pp. 421-430, Dec 2007
7. C. Liangboonprakong and O. Sornil. Classification of malware families based on n-grams sequential pattern features in 8th IEEE Conference on Industrial Electronics and Applications (ICIEA), 2013, pp. 777-782, June 2013.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

MALWARE ANALYSIS & SECURITY

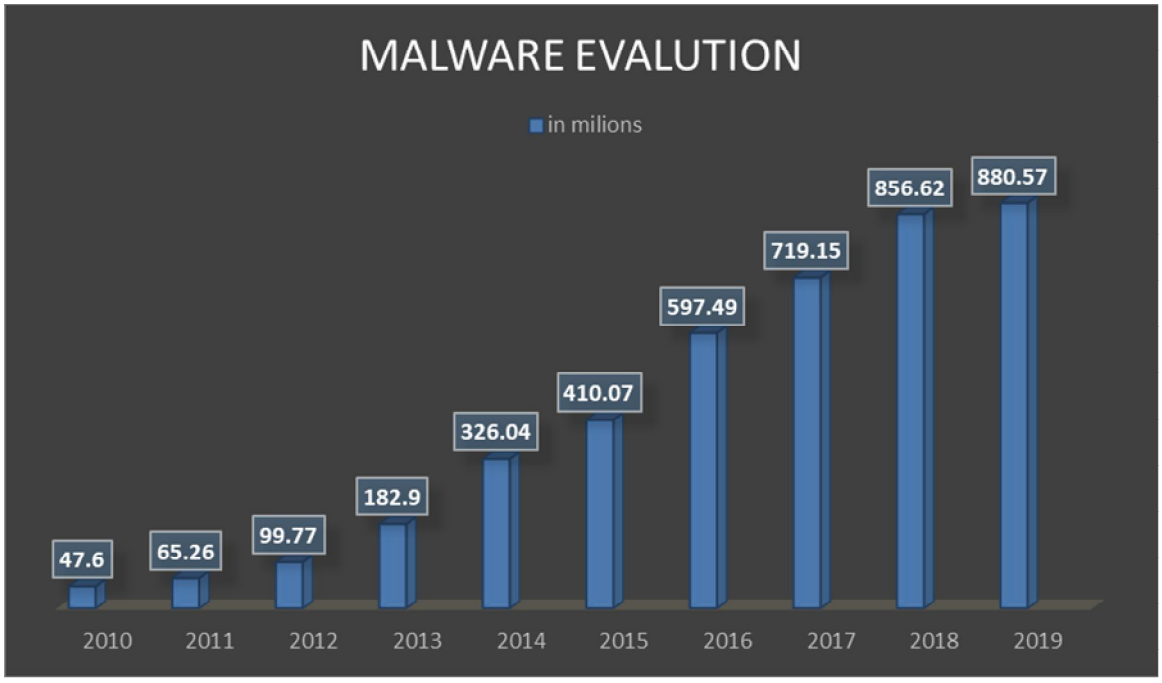
Ashwini Deshpande
Jaipur, Rajasthan

ABSTRACT
Malware standsgroup of maliciousssoftware productwith its main role to damagesyour system, network .Malware also harms and costs your organization as well personal assets. Malware has various types like virus, worms, Trojans ransomware adware, spywares, and keyloggers. Malwares are enters in your systems through system vulnerabilities like network loopholes, software misconfigurations open Wi-Fi network, unauthorized application downloading. Malware performs various kinds of functions like stealing user's data, performing activities like deleting altering modifying user's sensitive data. Virus is most common type of malware which are occurred most of time. Malware can be an executable code, script, active content and unauthorized network. Study of functionality, behavior and origin of malwares is named as malware analysis .Malware analysis techniques exist are static, dynamic, and threat analysis.

Keywords: Trojans, virus, malwares, spywares, worms, keyloggers

INTRODUCTION
Malware is malicious code which propagates over connected systems in network. This scenario is increasing day by day with progressive computing technology and communication network. Malware can be considered as entity in which new features can be easily added to enhance its dark side effects in the form of various attacks. These malwares can be dangerous with all their side effects on infected machines like disabling malware detectors or AV Scanners which installed for the security purposes. According to statistics, 70-80% of the malware comes from popular sites. Number of malware has grown rapidly. The rate of malware attacks and security solutions is not yet levelling. In fact, according to O'Farrell (2011) and Symantec Global Internet Security Threat Report Trends for 2010 (Symantec, 2010), attacks against Web browsers and malicious code variants installed by means of these attacks have increased. This paper describes different kinds of methodologies, detection and analysis techniques for handling threats in form of malwares for our presently working machines as found in relevant literature.

According to av-test it security institute the following stats represents last 10 year data related to increase number of malware count



Till March 18
Malwares and its types:-Malware stands for malicious software , designed to injury a computer system without the users informed consent **,**following data represents the summary of malwares release between 2000 to 2010

ISSN 2394 - 7780

Sr. no	Year	Malware type	Description
1	2000	ILOVEYOU	Spreading by way of an email sent with the seemingly benign subject line, "ILOVEYOU," the worm infected an estimated 50 million computers. Damages caused major corporations and government bodies, including portions of the Pentagon and British Parliament, to shut down their email servers. The worm spread globally and cost more than $5.5 billion in damages.
2	2001	Anna Kournikova Virus	Emails spread this nasty virus that purported to contain pictures of the very attractive female tennis player, but in fact hid the malicious malware.
3	2003	SQL Slammer Worm	One of the fastest spreading worms of all time, SQL Slammer infected nearly 75,000 computers in ten minutes. The worm had a major global effect, slowing Internet traffic worldwide via denial of service.
4	2004	Cabir Virus	Although this virus caused little if any damage, it is noteworthy because it is widely acknowledged as the first mobile phone virus.
5	2005	Koobface Virus	One of the first instances of malware to infect PCs and then propagate to social networking sites. If you rearrange the letters in "Koobface" you get "Facebook." The virus also targeted other social networks like MySpace and Twitter.
6	2008	Conficker Worm	A combination of the words "configure" and "ficker", this sophisticated worm caused some of the worst damage seen since Slammer appeared in 2003.

1.**Viruses** –A virus is a malicious program which replicates itself into other applications, files or even the boot sector. A virus then can do anything it is programmed to like stealing information, log keystrokes or even render a computer useless. The defining characteristic of a virus lies in the self-replication and insertion of malicious code into other programs without user consent. Just like most other malware a virus is designed for seeking profit

2.**Worms** - Worms are aptly named for their ability to "crawl" through networks. Worms replicate themselves however don't implant themselves in alternative programs as a virulent disease tends to try to. Worms move on a network affiliation seeking vulnerable machines to infect. For example, in 1988, the "Morris Worm" became thus widespread that it managed to slow the whole web.

3.**Trojans** - Trojan horses square measure usually unfold by some variety of social engineering, for instance, where a user is duped into executing an e-mail attachment disguised to be unsuspicious, (e.g., a routine type to be crammed in), or by drive-by transfer. Although their payload are some things, several fashionable forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer. While Trojan horses and backdoors don't seem to be simply detectable by themselves, computers could seem to run slower thanks to significant processor or network usage. Unlike pc viruses and worms, Trojan horses usually don't decide to inject themselves into alternative files or otherwise propagate themselves.

4.**Spyware** - Spyware's main function is to monitor what you are doing on your computer, on or off the internet, and send that information to a third party without your knowledge. In some cases, this data harvesting is used solely for marketing purposes. In other cases, the intent is more sinister. A larceny would possibly occur once associate cheat, posing as a client, directs a CPA to send a payment to an illegitimate recipient.

5.**Screen-locking ransom ware** - Lock-screens, or screen lockers is a type of "cyber police" ransom ware that blocks screens on Windows or Android devices with a false accusation in harvesting illegal content, attempting to scare the victims into paying up a fee. Jisut and SLocker impact Android devices more than other lock-screens, with Jisut making up nearly 60 percent of all Android ransom ware detections.

6.**Rootkits** - Once malicious software is installed on a system, it is essential that it stays concealed, to avoid detection. Software packages called rootkits enable this concealment, by modifying the host's operating system so that the malware is hidden from the user. Rootkits will stop a harmful method from being visible within the system's list of processes, or keep its files from being browse. Some types of harmful software contain routines to evade identification and/or removal tries, not simply to cover themselves.

7.**Backdoors** – A backdoor is a method of bypassing normal authentication procedures, usually over a connection to a network such as the Internet. Once a system has been compromised, one or additional backdoors is also put in so as to permit access within the future, invisibly to the user. The idea has typically been advised that pc makers preinstall backdoors on their systems to supply technical support for patrons, but this has never been reliably verified. Backdoors is also put in by Trojan horses, worms, implants, or alternative ways.

ISSN 2394 - 7780

How to secure system from malware attack:-following are guidelines for securing your computer from malware attack

- Upgrade your operating system and software' to latest version
- Be careful with unauthorized links and files email attachments
- Run antivirus software and scan regularly
- Backup your computers data
- Use strong and encrypted password
- Minimize downloads
- Use pop up add blocker
- Secure your network
- Think before clicking on any unauthorized link while surfing on browser
- Don't use open Wi-Fi network because it also contains malwares

MALWARE DETECTION TECHNIQUES

a. **Static analysis detection technique** - it's the procedure of analyzing software system while not execution it. During static analysis [Bergeron, J. et al] the application is break down by using reverse engineering tools and techniques, so as to re-build the source code and algorithm that the application has created. Static analysis are often done through program instrument, computer program and disassemble. Various static analysis techniques are as follows:

b. **Signature based detection technique** - This technique is also known as pattern matching or string or mask or fingerprinting technique. A signature could be a little bit of sequence injected within the computer programmed by malware writers, that unambiguously identifies a specific malware. To discover a malware within the code, the malware detector hunt for a antecedent such as signature within the code.

c. **Heuristic detection technique** - This technique is also known as proactive technique This technique is similar to signature based technique, with a difference that instead of searching for a particular signature within the code, the malware detector currently searches for the commands or directions that aren't gift within the computer programmed. The result's that, here it becomes simple to discover new variants of malware that had not nonetheless been discovered.

MALWARE ANALYSIS TOOLS

- Malware-Analyzer – Malware Analysis Too**l**
- Reverse-Engineering Malware Analysis Tool
- FireEye Malware Analysis Tool
- nyxbone android malware analysis tools
- REMnux Malware Analyis Tool
- Dependency Walker Malware Analysis Tool
- Sandbox Automated Malware Analysis
- netcat dynamic malware analysis tool
- download process monitor malware analysis tool
- filealyzer malware analysis tool for free

CONCLUSION

From above paper We have learnt Malware basics, malware analysis and techniques of analyzing malware. We have also learnt limitations of static malware analysis. After the discussion between static and malware analysis, Dynamic malware analysis is the best way to analyze malware samples. In this we have gone through the some tools for malware analysis. We also see current trends in malware and de-obfuscating malware.

ISSN 2394 - 7780

REFERENCES

- https://en.wikipedia.org/wiki/Trojan_horse_(computing)
- https://www.group-ib.com/digital-forensics.html
- https://www.av-test.org/en/statistics/malware/
- https://www.lastline.com/
- https://searchsecurity.techtarget.com/Understanding-encryption-and-cryptography-basics

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

STUDY AND ANALYSIS OF SECURITY FEATURES IN MALWARE

Ashwini Bhatkar
JVM's Mehta College, Airoli, Navi Mumbai

ABSTRACT
Today's world can be surely called as the world of computers. The rapidly growing importance of computer technology makes it a primary factor today. The advancements and changes that are brought up by the computer technology are leading us to a better future. But with this advancements, comes the concern of the security of the computer systems. Exactly here, my topic Malware Analysis comes into the picture. My article will drive you through the topics such as malware, its analysis and security. The purpose of this thesis is to identify the methods and tools used by anti-virus firms to protect Internet's users from the threats of malware. Understanding how the malware is built and how it is used by the attackers is becoming important for software engineers, system administrators, and IT security field specialist.

Keywords: Malicious, Software, Analysis, Network, Data, Damage, System, Spyware, Malware, Malicious, Virus, Worm Trojan, Process, Forensic, Antivirus, Threats, Security, Tool, Detect, Encrypting, Investigation, Analyzing, Attacker, Steal, Program, Functionality, Protection, Virtualization, Secure.

INTRODUCTION
Malware or Malicious Software is a kind of computer software that is intentionally designed to cause damage or destruction to computer system or network. Malware Analysis, therefore can be explained as - The study or process of analyzing or understanding the functions and working of this malicious software. Malware Analysis helps us to detect the malicious code which can differ in ways depending on their functionalities. These malware can be of various forms such as spyware, Trojan horses, viruses, worms, etc. Malware Analysis aims to detect the malicious code that can cause damage or try to steal or manipulate data on the system or network for potential or monitory benefits.

Different ways in which Malware Analysis can be done

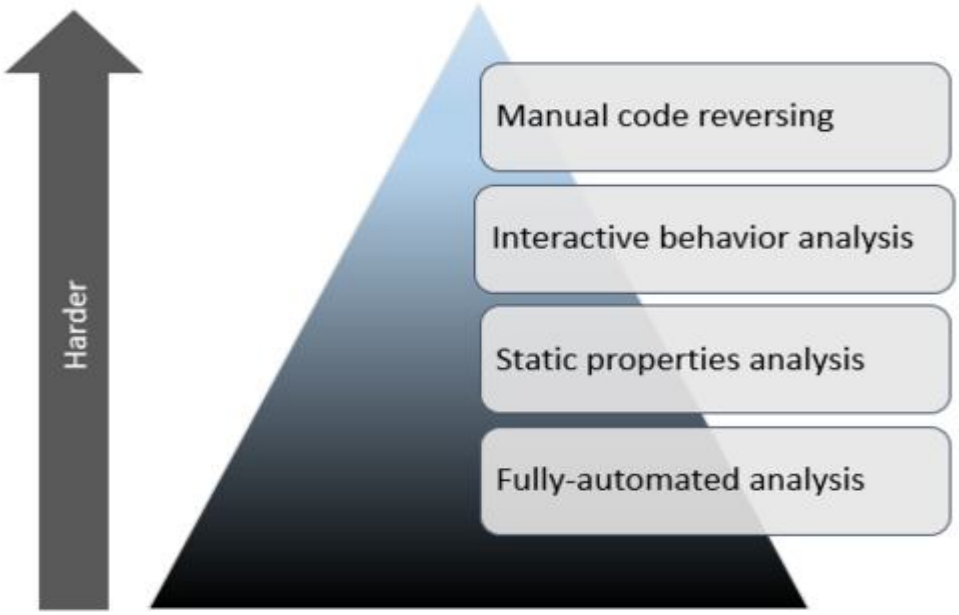
1. Computer Security Incident Management
When any system or network gets affected my any malware or if an organization feels that their network may have been affected by malware, then an event management team deployed by that organization will operate in this kind of situation. They will firstly try to determine any potentially malicious files are present in the system. If present they will try to determine its type and level of damage it can cause.

2. Malware Research
Researchers perform Malware Analysis to better understand the behavior of the malware. This gives detailed information about the malware and how it works. They try to determine the methods used for the creation of the malware which can thus be used to find out prevention methodologies and measures.

3. Bulk Malware Analysis
Bulk Malware Analysis is mostly carried out by the sellers of software products and solutions so that they can prevent their systems from any malware intrusions. This helps them to secure their products from malware attacks.

ISSN 2394 - 7780

Types of Malware Analysis



1. Manual Code Reversing
The logic or encrypted data behind the malware can be decrypted by reversing the code of malicious files.

2. Interactive Behavior Analysis
Observing the behavioral properties of the malicious code and determining the actions carried out b the code is another method. Checking if the code is trying to attach any host to our libraries etc can be done.

3. Static Properties Analysis
Analyzing the static properties such as hashes, embedded strings, embedded resources and header information.

4. Fully-Automated Analysis
Using automated analysis tools to detect malicious files or codes.

How to protect computer or system from malware?
So how do I protect my computer from malware?

The answer is – **1. Personal Vigilance**

2. Protective Tools
1. Personal Vigilance
The prime medium of malware transmission is through emails. A malware containing email looks exactly like a normal mail. This mail has on click events included so when we open such mails, the malicious code gets downloaded into our computer which causes potential damage to our computer. Being extra vigilant while accessing such mails can help.

2. Protective Tools
Our system or network can be protected by using a robust antivirus software package which will serve as a technological defense to our network. Well designed antivirus protection will help us ensure that our computer is malware free.

Types of Malicious Software
Malware is not a very common term to for majority of computer users. Instead few terms (types of malware) are well-known and widely used in media and press. The most popular are virus and spyware, due to a historical reason for the first one, while the latter one has infected most Internet users' computers.

1. Technically, the term **virus** is rarely used nowadays, because malware that uses the Internet to replicate itself is typically called a worm. However, media and most people still use the virus as a general term for any malware type. They replicate themselves inside the infected machine.

2. **Worms** are fundamentally similar to viruses but self-replicate themselves across computer networks such as the Internet and without direct human interaction. The self replication process happens silently at the background using different techniques. One effective method is by sending an email with an infected attachment or an infected website link to the user email contacts list.

ISSN 2394 - 7780

3. **Rootkits** are the newest type of malware and probably the most dangerous so far. They are designed to take control of the infected machine by the gaining administrator role in the operating system.

4. **Adware / Spyware** records information for the purposes of advertisements. They record a user's visited websites and purchased products online. This information is then sold to advertisement companies or used to display commercial advertisements related to the user shopping habits at the infected machine without the permission or willingness of the target user.

5. **Trojan horse** is an innocent file/program openly delivered through the front door when it in fact contains a malicious element hidden inside. It is very difficult for an ordinary computer user to identify the Trojan if it is embedded inside a program.

6. **Backdoor** creates an access channel that the intruder will use for spying or interacting with the victim's system. They can capture and transform key strokes (keyboard) to the hacker. Private information (passwords and credit card numbers) can be recorded before being encrypted by the website the user is purchasing from.

MALWARE FORENSICS

1. Basic Principles

Malware forensics is the process of investigating and analyzing malicious code to uncover its functionality and purposes, and to determine how the malware had infiltrated to a subject system. Many of the malware are stopped by anti-virus software, spyware removal tools and other similar tools but most of the anti-virus software fail to detect new malware. The reason is that they are built upon a signature-based detection method. This means that the anti-virus software compares the content of the suspected program to the stored signatures where each signature represents a code pattern or unique identification extracted from the original malware. However, polymorphism and metamorphism are techniques that thwart signature-based identification programs by randomly encoding or encrypting the program code in a way that maintains its original functionality.

2. Static and Dynamic Analysis

A **dynamic analysis** or behavioral analysis involves executing the malware and monitoring its behavior, system interaction, and the effects on the host system. Several monitoring tools are used to capture the malware activities and responses. These activities include the attempt to communicate with other machines, adding registry keys to automatically start the program when the operating system starts, adding files to system directories, downloading files from the Internet and opening or infecting (embedding itself) to other files.

Static analysis tools include program analyzers, disassemblers and debuggers. These tools are able to detect if the malware uses any of software protection techniques**.** Malware might start executing after period of time or when a special event occurs. Key logging feature might start only when the user browses online shop or visit a bank web site. It is important to discover how malware can escape detection by anti-virus programs, how they can bypass firewall and other security protections. Static analysis helps malware researches to reveal what a piece of malware is able to do and how to stop it. To be able to perform static analysis, malware researchers must possess a good knowledge of assembly language and the target operating system.

3. Virtual Environment

It is important to establish a secure environment before starting the analysis of a certain malware. The environment should not contain any important information, disconnected from the network (or the traffic is redirected to local host), and preferably contain fresh installation of the operating system. Virtualization products offer help for malware researchers. These products allow an unmodified operating system with all of its installed software to run in a special environment besides existing operating system.

CONCLUSION

In the good old days, digital investigators could easily explore, discover and analyze malicious code on computer systems due to the malware functionality which was easily observable; therefore little effort was required in performing in depth analysis of the code. Today, various forms of malware are proliferating, automatically spreading (worm behavior), providing remote control access (Trojan horse/backdoor behavior), and sometimes concealing their activities on the compromised host (rootkit behavior).Malware is like a tom and jerry game, as new malware analysis techniques are developed, malware authors respond with new techniques to thwart analysis. The increasing sophistication of malicious code and growing importance of malware analysis in digital investigation has driven advances in tools and techniques for performing autopsies and surgery on malware.

ISSN 2394 - 7780

REFERENCES

1. Malin CH, Casey E, Aquilina JM. Malware Forensics: Investigating and Analyzing Malicious Code. Syngress Publishing; 2008.
2. Intelligence Encyclopedia. Computer Virus. [online]. Answers.com. URL: http://www.answers.com/topic/computer-virus. Accessed 25 January 2009.
3. Eldad Eilam. Reversing: Secrets of Reverse Engineering. Wiley Publishing; 2005
4. Harris S, Harper A, Eagle C, Ness J. Gray Hat Hacking. 2nd ed. McGraw-Hill Osborne Media; 2007
5. Learning Malware Analysis, www.packt.com, By Monnappa K A.
6. Advanced Malware Analysis, PACKT Books - Packt Publishing, Evade malware using IDA Pro, OllyDbg, and WINDBG, Munir Njenga.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

CRYPTO CURRENCIES FORENSICS INVESTIGATION

Mustufa Nullwala
Jnan Vikas Mandal's Mehta Degree College, Navi Mumbai

ABSTRACT
Cryptocurrencies are the virtual currencies behind revolutionizing the trade markets by creating a peer to peer network for transactions. The concept of cryptocurrencies emerged during the end of the 20th century, various cryptographers played their role in bringing up this emerging technology to the most powerful digitized token as it is today. Cryptocurrency or digitized token is designed to work as a medium of exchange which uses strong cryptography in the parallel world of computer networks, forsecuring, analysing and verifying the financial transactions. The concepts of block chain are the heart of cryptocurrencies. This paper focuses on the concept of cryptocurrency, block chain and secured network, security trends and current challenges.

Keywords: Cyber Security, Cryptocurrency, Block Chain, Forensics

I. INTRODUCTION
Cryptocurrencies are more than a money digitized form, used for trading and financial purposes. These virtual currencies encourage the checkless, cashless society and is not under the control of any government or organisation. Instead of using a centralized system as most of the digital currency and central banking and Insurance Systems, it uses a decentralized network taking every transaction to a single platform. Cryptocurrencies came into existence in the real world of Internet after its pioneer Mr. Satoshi Nakamoto, pseudonymous developer in 2009 in the form of Bitcoin. It used SHA-256is a cryptographic hash function which is used for getting proof of work scheme. On daily basis, with the emergence of technology, 'n' number of cryptocurrencies are created. As per recent 2018-19, the most popular cryptocurrencies include, Bitcoin (BTC), Ethereum (ETH), Ripple (XRP), Bitcoin Cash (BCH), etc. as emerging future force of cryptocurrencies. Digital signatures play a major role in the transfer of assets between parties. It discourages double spending and thus uses the hash function for the same.

II. BLOCKCHAIN THE MYSTERY BEHIND CRYPTOCURRENCY EXPLAINED
Block Chain is parallel to Internet, but how? The answer is block chain are simple in terms of itsstructural point of view but complex in terms of itsalgorithmic and potential point of view. In the last century, the financial transactions were maintained in ledgers, a book or registry of all the records subjecting to it. If we consider blockchains to be ledger, then we can conclude that it basically is a record or log data of transactions. Further, if we call every real time transaction in a ledger as a node, then blockchain can be referred to as a Universal Ledger. Each of these nodes of transactions performed on a real time environment is called a block. Every block consists of data about transaction, hash of the block which is unique, a hash of a previous block and a variable time stamp.Then these blocks are added to a chain structure called block chain. For every new transaction that happens, a block of that is added to the chain. This block chain is protected by the best cryptography algorithm available and hence its very difficult to hack. Every block is connected to another block, if any hacker wants to change any of the transactional data in a block then he or she needs to change the entire chain, making it a highly secured network. Why is the Hash of previous transaction block needs to be stored in a block? These enables to trace back the transactions that have been occurred in the long run. When an event occurs, it triggers another event automatically. Smart contracts are the core logic in most block chains. Block Chains are built with Consensus, Security, Provenance and Trust factor as its deepest values. Distributed trust among the entities taking part in the transaction. The Proof of work slows down the creation of block as it always happens in a peer to peer network. Every entity is a peer to peer network has a copy of the block chain, whenever a new block is created, it is sent to all the entities and gets added to the block chain. Thus, the consistency of the transaction is maintained. Block chains have GDPR as its major constraints.

The Security key insights of a Block Chain includes –
- **Share the answers not the actual data**: It implies that as an end user, you never know how a hard code transaction was performed inside a block chain. It works in the way that users can broadcasts their questions to the database, and they will be answered accordingly.

-**Log everything on a block chain**: It helps for auditing, credibility, consistency and trace back purpose.

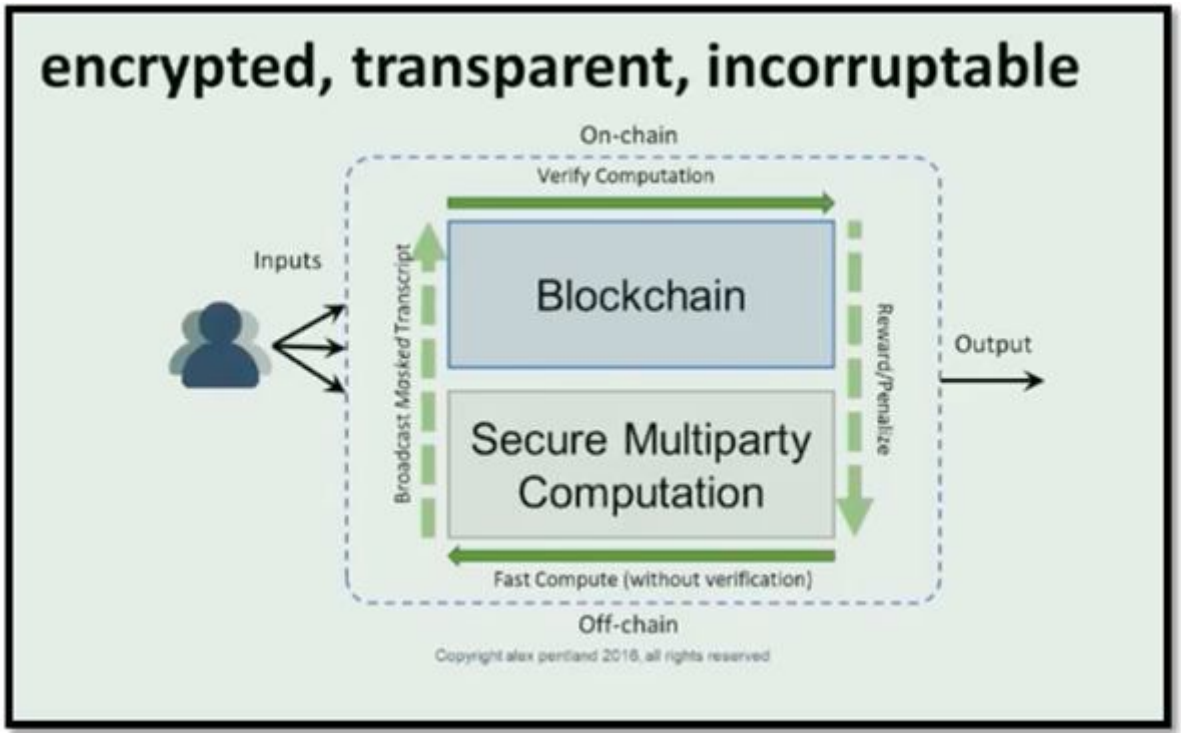
-**Transparent and incorruptible** – The data is highly secured and its almost impossible to hack a structure of a block chain. As the data that enters the block in an encrypted format and must to be processed in that form itself. That is, if a data is encrypted it is hard to break even for National Security.

ISSN 2394 - 7780

-Never decrypt the Data

Block Chain is far away from homomorphic computing i.e. the when we try to decrypt an encrypted result, the results match with the original data, such as converting from Plain text to Cyber text then back to Plain text. You can never get the same data on encrypting a block in a chain. It consists of keys to read it.

The processing architecture of a block chain by *Alex Pentland* is as below:

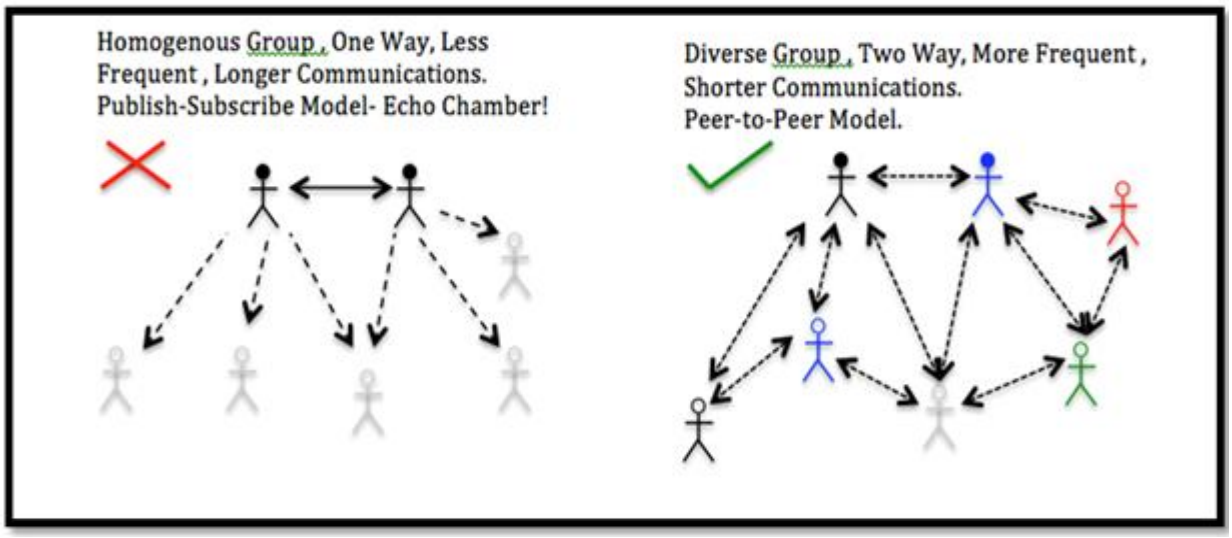


As the inputs are received, a broadcasting enables the On Chain verifications and identifications of the assets shared and blocks for the transactions are created and added to every chain in the peer network. Followed by a Certified Open Algorithm and then the result is shared.

Why Block Chain is most favoured?

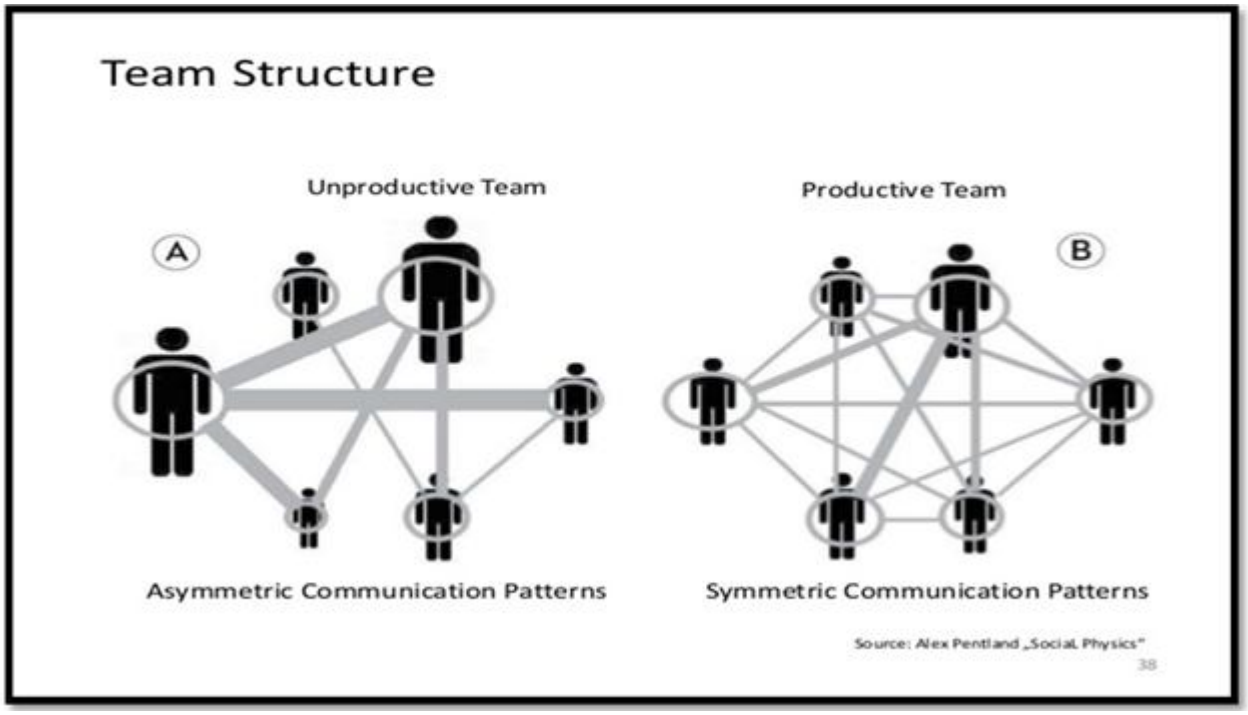
- It follows the GDPR Rules.
- Intrinsically better Security
- It provides better traceability for migrations.

The theory of social bridges (social physics) between the communities have a casual connection to their user behaviour. We can derive patterns on these user behaviours, without meeting them personally.



Social physics applied to hiring by Vinayak Joglekar

ISSN 2394 - 7780

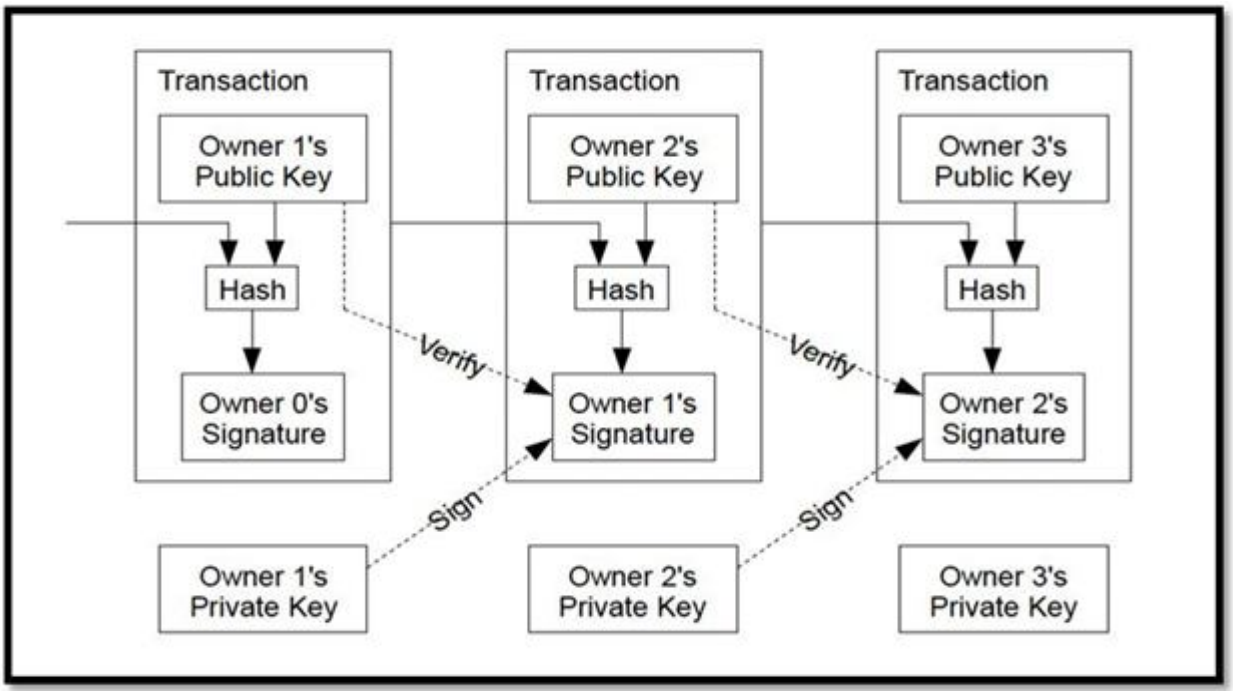


As social physics is applied to Hiring process by constructing the Communication patterns similarities and probabilities, the block chain understands the patterns of user behaviour.

Thus, a block chain can be used to solve trust dis intermediation, can be honest and peer to peer economy and allows a secured Multi party algorithm.

How does a transaction happen in a cryptocurrency?

For transferring the virtual currencies to the next owner, the user has to digitally sign a hash of the previous transaction (with a private key) and the public key of the next owner and adding these to the end of the currency. Below is the process architecture of bitcoin shared by Satoshi Nakamoto in his research paper, "Bitcoin: A Peer-to-Peer Electronic Cash System"



A payee can verify the signatures to verify the chain of ownership, but could not verify if one of the owners had double-spend the currency. The only feasible solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the currency / coin must be returned to the mint for issuing a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The

ISSN 2394 - 7780

major issue is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank. The CPUs with more cores and greater speed, multiple graphic systems, field-programmable gate arrays (FPGAs) and application-specific integrated circuits (ASICs) are some of the major requirements for the miners. What makes miners to provide their machines for processing the cryptocurrency? Whenever a new transaction is raised the public key of that transaction is shared and undergoes a verification. The Time Stamp Server takes the hash of the blocks which needs to be time stamped. The proof of work begins with scanning for a value that when hashed, the hash begins with a number of zero bits. In the time stamp network, the nonce are incremented in the block, until a hash with zero bits is found for the block.

III. CRYPTOCURRENCY IN FORENSICS

As mentioned earlier contexts, block chain consists of a built in highly secured and strong framework. How can the concepts of block chains can be applied in Cyber Security?

An answer to this is followed by using social physics in a research taken by ENDOR.coin

Case 1: Given a sample list of 50 ISIS Twitter accounts. Additional 75 known ISIS accounts, kept hidden ass test. We need to find the most ISIS accounts in Twitter.

The data provided for finding targets is very little. But we can derive patterns based upon the user behaviour of 50 ISIS Twitter accounts. On applying the concept of social physics, the team found a list of top 200 accounts which are most likely to be ISIS members. And it took about 2 hours for this sensitive information. In terms of accuracy, the team found 35 new ISIS accounts in top -50, 51 new ISIS accounts in top -100 and 72 new ISIS accounts in top -200.As the encrypted data uploaded in Cloud can be used without decrypting it. It has enabled us to a secured and consistency trade market.

In the recent year, ZCash a privacy owned cryptocurrency, had a certain error in the seminal cryptography paper that served as a foundation for a host of virtual clients. The paper had zero knowledge proofs, it can be referred as a cryptographic break through which revealed all the private details about ZCash and other currency projects. If any attacker had spotted this loophole, then it would have jeopardized billion-dollar business loss. Roughly it took about 8 months for the company to patch the security hole.

Satoshi Nakamoto had set bitcoins to a finite limit of 21 million bitcoins. Since there is no tracking of these virtual currencies, it would be difficult for the government body to identify the criminals.

Cipher Trace is one of the world's leading platform for bitcoins and cryptocurrencies analysis,tracing and forensics. These agencies help investigate money laundering, ransomware, drug trafficking, extortion, investment scams, dark market transactions, terrorist financing and fraudulent ICO. Since the data is encrypted, a real time forensics is required to enable the regulation of money, law enforcement, identification of fraudulent income and illicit activities among customers. The bitcoin fraud called as deanonymization is nothing but identification merging. The Forensics include investigation, analysis, deanonymizations, traceability over criminal activities using virtual currencies over the Internet. Hence the Counter Intelligence investigations to track the movements of money, continuous surveillance protocols over the crypto markets are being implemented.

Some major issues observed are

Stolen or Lost Cryptocurrencies – due to vulnerability in Private keys, spyware, hackers, viruses are prominent issues. Locke out addresses, Security 2FA, Phone SMS intercepts will be helpful.

Hidden Cash, assets and transactions – Illegal Purchases, dark web, hiding cash, cold wallets, hot wallets, hardware wallets, exchange vaults, fraud and extortion payments are the major crimes.

Tools for Forensics: Running a node, input clustering, change address identifying, exchange known addresses, etc.

About 95% of Cryptocurrencies are Spams according to the writer James Alctucher, Hacknoon, since most of these currencies never exist for a long time.

IV.CONCLUSION

Cryptocurrencies being virtual and decentralized. The inner platform made of block chain is secured, while the outerpart data needs to analyse for threats and frauds. A public ledger enables traceability, account numbers can be anonymous and are disposable, exchanges with fiat known information about block chain, public projects, publicized address are risky. Cryptocurrencies perform a irreversible transactions, they are anonymous and

ISSN 2394 - 7780

globally accessible. An inexperienced team, technical difficulties, hacking, unsecured platforms may lead to a bad experience.When money is invested in assets then it will be locked up for years, unless someone buys the equity or the company is acquired or goes public. No so with when investing in cryptocurrencies, where the investment is liquid.While it certainly needs some amount of experience before investing in cryptocurrency.

V. BIBLIOGRAPHY

1. https://odsc.thinkific.com/courses/take/blockchain-and-ai/lessons/5569444-blockchain-and-ai-or-future-data-systems-must-be-built-differently
2. https://www.csoonline.com/article/3279006/4-reasons-blockchain-could-improve-data-security.html
3. https://www.dummies.com/personal-finance/what-is-cryptocurrency/
4. https://thenextweb.com/hardfork/2019/03/14/gatecoin-cryptocurrency-exchange-dead/
5. https://cryptoslate.com/coinbase-custody-unveils-new-cold-storage-cryptocurrency-trades/
6. https://dailyhodl.com/2019/03/14/nasdaq-technology-powers-worlds-first-full-stack-cryptocurrency-ecosystem/
7. https://dci.mit.edu/
8. https://www.researchgate.net/publication/316656878_An_Analysis_of_Cryptocurrency_Bitcoin_and_the_Future
9. https://www.google.com/search?q=cryptocurrency+gartner+hype+cycle&source=lnms&sa=X&ved=0ahUKEwjO8sO_q4PhAhWEV30KHQnrBOgQ_AUICSgA&biw=1517&bih=694&dpr=0.9
10. http://randomwalker.info/publications/research-for-practice-cryptocurrencies.pdf
11. https://ciphertrace.com/forensics/
12. https://teeltechcanada.com/cyber-forensics/cryptocurrency-forensics/
13. http://liacfe.org/images/meeting/011818/2018_01_18_bitcoin_forensics___peter_theobald_w_fonts_w_handouts.pdf
14. https://www.entrepreneur.com/article/307585
15. https://bitcoin.org/bitcoin.pdf
16. https://file.scirp.org/Html/3-7201056_58098.htm
17. https://www.livemint.com/Money/nEAF8sZzgtImKrMYKDtuEJ/What-is-bitcoin-mining-How-to-get-started.html
18. https://medium.com/pillar-companies/machine-learning-for-encrypted-blockchains-sandy-pentland-mit-79c2d18eaf
19. https://oxfamblogs.org/fp2p/book-review-social-physics-how-social-networks-can-make-us-smarter/
20. https://www.google.com/search?biw=1517&bih=694&tbm=isch&sa=1&ei=YxGPXPrrNO_dz7sPkLudWA&q=social+physics&oq=social+physics&gs_l=img.3..0j0i24l9.55270.62228..62559...4.0..0.146.1892.5j13.....0....1..gws-wiz-img.....0..0i67j0i10j0i131j0i5i30j0i8i30.-bQEf1zKp8k#imgrc=PNfwiXu4W3rtnM:
21. https://vinayakjoglekar.wordpress.com/2014/05/16/social-physics-applied-to-hiring/

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

FILE STRUCTURE FORENSIC PLUS INVESTIGATION

Archana Ravindra Sanap
JVM's Mehta Degree College, Navi Mumbai

ABSTRACT
The Definitive Guide to filing structures Analysis: Key ideas plus active Techniques most digital proof is keep at intervals the PC filing structure, however filing structure work is the foremost technically difficult ideas for digital investigator as result of there exists very little documentation. Now, security skilled Brian Carrier has written the definitive reference for everybody who desires to grasp plus be able to testify regarding however filing structures analysis is performed. Carrier begins with an summary of investigation associate degree pc foundations then offers an authoritative, comprehensive, plus illustrated overview of contemporary space plus filing structures: Crucial information for hidden proof discovery, information rollbacky, validating your tools. Along a method, he describes structure of information, analyzes example disk pictures, delivers advanced investigation scenarios, plus uses today's most valuable open source filing structures analysis tools-including tools he personally developed Coverage includes conserving the digital crime scene plus, for "dead analysis" duplicating laborious disks distinguishing hidden knowledge on a disk's Host Protected space (HPA).

Keywords: FILING PROVISION TABLE Filing Structure, FILING PROVISION TABLE 32 Filing Structure, NETWORK FILE SYSTEM Filing Structure, EXT Filing Structures

INTRODUCTION
Filing structures may be a set of rules this decide however knowledge is keep plus arranged on the storage structure e.g., hard drive, flash drive, CD-ROM etc. Windows supports three well known formats FILING PROVISION TABLE32, exFILING PROVISION TABLE plus NETWORK FILE SYSTEM. All three formats have their own advantages plus disadvantages. Here, now discuss each of the filing structures, for maximum performance plus compatibility, it must be used

A filing structure during a pc is a manner during which filings are named plus rationally located for storing plus fetching. It may be thought of as an information or directory this contains the location of each single piece of knowledge on the various devices, like disc, Compact Disc, DVD. This information is prepared for filing this will be known as directory. This directory additionally holds headings plus filings.

Store plus fetching filings, filing structures uses all information, this contains a period, a filing is created; information changes, filing dimension, etc. They can additionally prohibit users to access a selected filing by victimization encoding or a watchword.

Filings are kept on a storage means in "segments". Idle segments may be used for storing knowledge, usually completed in sector clusters called as chunks. The filing structures identify the filing dimension plus position plus also the sectors this are obtainable for storage. If an erection for forming filings wouldn't happen, it'd not be doable to erase or retrieve filings, or to stay 2 filings with a similar name then all filings will exist in the common heading. Eg. It's as of headings, we will be able to name two completely different image filings with a similar name, as both exist in 2 dissimilar headings, then if 2 filing is within a similar manual, and it will not have the similar term.

Most of the applications want filing structures to work; thus each separator must have single. Package is also reliant on filing structures.

SOME GENERALLY RECYCLED FILING STRUCTURES
FILING PROVISION TABLE Filing structures
Filing Provision table will be filing structures used by working structures for tracing filings on a diskette. Because to separator, filings might be dispersed everywhere plus separated into units. Filing Provision Table structure keeps a path of all elements of filing. Filing Provision Table has existed as filing structures since the arrival of private computers.

KINDS
- Filing Name
- Filing provision Table structure in MS DOS allow filing terms of eight kinds one
- FILING PROVISION TABLE filing structures within Windows support large filing term including complete filing track existing as long as two hundred and fifty five kinds.

ISSN 2394 - 7780

- Filing term must start by alphabet plus numeric kinds.
- Filing term has any type excluding "/ \ = [], ^"". Filing terms will have over single amount plus areas. Kinds this come back once the last amount fully filing name are thought of because the filing addition.
- FILING PROVISION TABLE filing structures will not support filing plus limited safety. It means operators log into a pc regionally can gain whole entry to headings plus filings this dwell FILING PROVISION TABLE separators.
- It delivers firm access toward filings. The amount rest upon the dimensions of divider, filing dimensions, kind of filing plus count of filings into the folder. FILING PROVISION TABLE32 Filing structures

It is a new type will be the FILING PROVISION TABLE Filing structures plus might recycled onto a drives starting from five hundred and twelve MB and ending at two TB.

- It supports upto 2TB size
- Delivers a improved practise of diskette planetary
- Easy entry of filings into separators is minimum five hundred MB or maximum two GB in dimension.

The symbol lower shows separate layout in FILING PROVISION TABLE plus FILING PROVISION TABLE thirty two filing structures.

FAT File System

FAT 32 File System

NETWORK FILE SYSTEM Filing structures
The NETWORK FILE SYSTEM filing structures plus for plus spanking new Technology filing structures.

Features
- Naming.
- Filing name can be large as 255 kinds.
- Filing term has some type except this /\ " \:*
- They are not event delicate. It delivers heading plus filing security. This is completed by transient on NETWORK FILE SYSTEM authorization to filings plus folders. Safety workings at native moreover as network level. Every filing Associate in folder within the list will have an Access management List this features the operators, safety recognizer, plus an access rights this are decided to the operators. Filings plus separator dimensions are longer in NETWORK FILE SYSTEM. A NETWORK FILE SYSTEM separator is often of a size as massive as sixteen Exabyte's, but generally it is limited to 2TB.
- Filing dimension can range from 4GB to 64 GB.It delivers up to 50% filing compression
- It is a consistent plus rollbackable filing structure which makes use of business logs for updating filings plus folders automatically. It delivers bad-cluster mapping.

EXT Filing structures
Extended filing structures (EXT), Second Extended filing structures (EXT2) plus Third Extended filing structures (EXT3) are designed plus implemented on Linux. The EXT is Associate in recent filing structures this were utilized in pioneer UNIX structures. EXT2 is maybe one in all the foremost wide used UNIX filing structures. EXT three conjointly includes similar options as EXT a pair of, however conjointly includes journaling.

Features
- Supports filing kinds in Unix i.e. regular filings, device special filings, directories, symbolic links

ISSN 2394 - 7780

- Can control filing structures created on vast separators? Originally, here we are going to cite the foremost unremarkably used EXT2.
- Reserves about 5% of block for administrator usage, thus allowing the admins to rollback from situations of overfilled processes.

CONCLUSION

In order to stay a proof of each step of the research, file every procedural step.

Proof conferred while not correct documentation might not be acceptable in court.

These knowledge mustn't solely embrace the rollbacked filings plus knowledge, however conjointly the physical outline of the structure at the side of any encrypted or reconstructed knowledge. Forensic analysis of time-based information will facilitate analyst correlate distinct info rapidly plus to seek out remarkable time plus dates of actions associated with improper laptop usage, spoliation plus misappropriation.

REFERENCE

- Our computer forensic boot camp: https://www.infoseinstitute.com/courses/computer-forensics-boot-computer.
- Forensics: http://resources.infosecinstitute.com/category/computerforensics/introduction/.
- https://www.cyberforensic.com/courses/computer-forensics-boot-computer.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

CLOUD FORENSIC INVESTIGATION: NEW INVESTIGATION TREND

Shweta Pawar
Assistant Professor, M V Mandali's Colleges of Commerce & Science, Mogaveera Bhavan, MVM Educational Campus Road

ABSTRACT
The Cloud Computing is one of the most evolutionary technologies. Cloud environment include the service provider and customers of cloud services. Without distinct forensic capabilities, they are unable to ensure the robustness and suitability of their services to support investigations of any criminal activity. In this paper, the new area in forensic investigation, its challenges and opportunities are going to examine.

Keywords: Cloud Forensics, Cloud Computing, Digital Forensic Investigation

I. INTRODUCTION

Cloud computing is radically changing the way Information services were introduced long before. Cloud computing platform increases the scale of the computer systems in both hardware and software wise. The definition of digital forensics and cloud computing from NIST are:

Digital forensics is used for the identification, collection, examination, and analysis of data and preserving the reliability of the information and maintaining a strict chain of protection for the data. [1]

Cloud computing could be a model for enabling convenient, on-demand network access the configurable resources (e.g. network, servers, storage, various applications, and services) that can be speedily provisioned and free with minimum management effort or service supplier interaction. Cloud computing has 5main characteristics, i.e., on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. It has 3 service models, i.e., Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). And it has 4 deployment models, i.e., private cloud, community cloud, public cloud and hybrid cloud. [2]

The data is held and managed remotely via cloud software, platform or infrastructure by authenticating or authorized users. Despite many advantages, cloud computing involves greater exposure to various security threats and privacy breaches.

II. DIMENSIONS OF CLOUD FORENSIC

The default settings for cloud forensics are multiple jurisdictions and multi-tenancy, which create additional legal challenges. The interactions between Cloud Service Providers (CSP[1]) and Customers, by resource sharing and collaboration between International Law Enforcement agencies, are most important in cloud forensic investigation. In order to examine the domain of cloud forensics more comprehensively, it can be divided into three dimensions, the technical, organizational and legal dimensions.

A. Technical Dimension

The technical dimension encloses the procedure and tools that are needed to perform forensic investigation in the cloud computing environment. These include data collection, evidence segregation, virtualized environments and proactive measures.

Data collection is the process of identifying, collecting, cataloguing and obtaining the forensic data. The forensic data includes customer-side artifacts that conferred on customer's premises and provider-side artifacts that are located in the provider's infrastructure. To collect forensic database on the specific model of data in place, various procedures and tools are used. The collection method ought to preserve the integrity of information. It should not breach any law or any rules and regulations in the jurisdictions where data is collected, or compromise the confidentiality of other occupants that share the resources.

Another essential feature of cloud computing is resource management [3]. Multi-tenant environments reduce IT costs through resource sharing. However, the method of segregating evidence within the cloud needs compartmentalization [4].

[1] Cloud Service Providers (CSP) are those service providers which provides various services of Cloud such as IAAS, PAAS and SAAS.

ISSN 2394 - 7780

B. Organizational Dimension

A cloud forensic investigation includes at least two entities: the CSP and the cloud customer. However, the scope of the investigation can increase when a CSP outsources services to the other parties. Figure 1 show the various entities involved in a cloud forensic investigation.

Organizational policies or Service Level Agreement (SLA) facilitate communication and collaboration in forensic activities. In addition to enforcement, the chain of CSPs must communicate and collaborate with third parties and academia. Third parties will assist with auditing and compliance whereas academia will offer the technical experience that would enhance the potency and effectiveness of investigations.

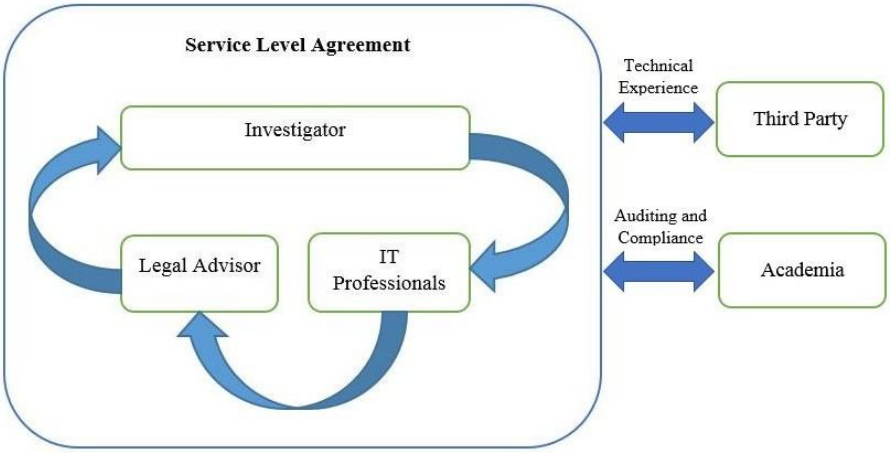


Fig-1: Entities in Cloud Forensic Investigation

To establish a cloud forensic process, each cloud entity must provide provider-customer collaboration and external assistance that fulfill the following roles:

- **Investigators**: Investigators examine allegations of misconduct and working with external law enforcement agencies. They must have enough experience to perform investigations of their own assets in addition as act with alternative parties in rhetorical investigations.
- **IT Professionals**: IT professionals include a system, network and security administrators, ethical hackers, cloud security architects, and technical and support staff. They provide skilled information in support of investigations, assist investigators in accessing crime scenes, and should perform data collection on behalf of investigators.
- **Legal Advisers**: Legal advisers are familiar with multi-jurisdictional and multi-tenancy issues in the cloud. They make sure that forensic activities don't violate rules and regulations, and maintain the confidentiality of different tenants that share the resources. SLAs must clarify the procedures that are followed in forensic investigations.

  Internal legal advisers should be involved in drafting the SLAs to cover all the jurisdictions in which a CSP operates. Internal legal advisers are also responsible for communicating and collaborating with external law enforcement agencies during the course of forensic investigations.

C. Legal Dimension

Traditional digital forensic professionals establish multi-jurisdictional and multi-tenancy challenges as prime legal considerations [5] [6]. Performing forensics in the cloud exacerbates these challenges. The legal dimension of cloud forensics needs the development of rules and agreements to make sure that forensic activities don't breach laws and rules within the jurisdictions wherever the information resides. Also, the confidentiality of alternative tenants that share a similar infrastructure ought to be preserved. SLAs define the terms of use between a CSP and its customers.

The following terms regarding forensic investigations should be included in SLAs:

(i) The services provided, techniques supported and access granted by the CSP to customers during forensic investigations;

(ii) Trust boundaries, roles and responsibilities between the CSP and customers concerning forensic investigations; and

ISSN 2394 - 7780

(iii) The method for conducting investigations in multi-jurisdictional environments while not violating the applicable laws, rules, and customer confidentiality and privacy policies.

III. CHALLENGES

Based on abovementioned dimensions of Cloud Forensic there may be following challenges can occur during the investigation:

A. Data Collection

In every combination of the cloud service model and deployment model, the cloud customer faces the challenge of decreased access to forensic data. Access to forensic data varies significantly based on the cloud model that's implemented [7].

Decreased access to forensic data means cloud customers typically have very little or no control or perhaps knowledge of the physical locations of their information. In fact, they'll solely be able to specify location at a high level of abstraction, typically as an object or container. CSPs advisedly hide information locations from customers to facilitate data movement and replication.

B. Evidence Segregation

In the cloud, different instances running on an individual physical machine are isolated from one another via virtualization. The neighbours of an instance have no more access to the instance than any other host on the Internet. Neighbours behave as if they are on separate hosts. Customer instances don't have any access to raw disk devices; instead, they access virtualized disks.

At the physical level, system audit logs of shared resources collect data from multiple tenants. Technologies used for provisioning and de-provisioning resources are perpetually being improved [4].

It is a challenge for CSPs and enforcement agencies to segregate resources throughout investigations without breaching the confidentiality of alternative tenants that share the infrastructure.

C. Virtualized Environment

Cloud computing provides information and computational redundancy by replicating and distributing resources. A hypervisor monitored and provisioned instances of servers. Hypervisors are main targets for cyber-attack, however, there's a lack of policies, procedures and techniques for forensic investigations of hypervisors.

Data mirroring over multiple machines in several jurisdictions and also the lack of transparent, real-time data concerning information locations introduces difficulties in forensic investigations. Investigators could unwittingly violate rules and regulations as a result of they do not have clear data concerning information storage jurisdictions [8].

D. Service Level Agreement

Current SLAs omit important terms regarding forensic investigations. This is because of low customer awareness, restricted CSP transparency and therefore the lack of international regulation. Most cloud customers are unaware of the problems that will arise in an exceedingly cloud forensic investigation and their significance.

IV. OPPORTUNITIES

Despite many challenges facing during Cloud Forensics, there are many opportunities that can support the forensic investigation.

A. Cost Effectiveness

Security and forensic services may be more cost-effective once enforced on a large scale. Cloud computing is engaging with small and medium enterprises as a result of it reduces IT costs. Enterprises that cannot afford dedicated internal or external forensic capabilities could also be ready to take advantage of low-cost cloud forensic services.

B. Robustness

Some technologies facilitate to improve the general hardiness of cloud forensics. IaaS offerings support on-demand cloning of virtual machines. As a result, within the event of a suspected security breach, a client will take an image of a live virtual machine for offline rhetorical analysis, which ends up in less downtime. Also, multiple image clones can speed up the analysis by simultaneously performing investigation tasks. This enhances the analysis of security incidents and will increase the likelihood of following attackers and patching weaknesses.

ISSN 2394 - 7780

C. Scalability

Cloud computing provides unlimited pay-per-use storage, permitting comprehensive logging without compromising performance. It additionally increases the potency of categorization, searching and query in globs. Cloud instances can be scaled as needed based on the logging load.

V. CONCLUSION

The traditional forensic process of investigation cannot applicable with cloud technology. The cloud exacerbates several technological, structure and legal challenges. Several of those challenges, like information replication, location transparency and multi-tenancy, are distinctive to cloud forensics. Opportunities and Challenges of cloud forensics were discussed in order to overcome the difficulties in the forensic investigation process in cloud computing. Nevertheless, cloud forensics brings unique opportunities which will considerably advance the effectiveness and speed of forensic investigations.

VI. REFERENCES

1. K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," August 2006, NIST SP800-86 Notes.
2. P. Melland T. Grance "Effectively and Securely Using the Cloud Computing Paradigm,"2009, NIST.
3. Keyun Ruan, Centre for Cybercrime Investigation, Prof. Joe Carthy, Centre for Cybercrime Investigation, Prof. Tahar Kechadi, Centre for Cybercrime Investigation, and Mark Crosbie, "Cloud forensics: An overview." [Online]. Available: https: //www .researchgate .net /profile /Tahar_Kechadi/publication/ 229021339_Cloud_ forensics_An_overview/links/02bfe50f55377829e3000000/Cloud-forensics-An-overview.pdf
4. https://www.infosecinstitute.com/career-profiles/computer-forensics-investigator/
5. R. Broadhurst, "Developments within the international enforcement of cyber crime," Policing: International Journal of Police methods and Management, vol. Vol 29(2), pp. 408–433, 2006. [Online]. Available: https://papers.ssrn.com/sol3/papers. cfm?abstract_id=2089650
6. S. Liles, M. Rogers, and M. Hoebich, "A Survey of the Legal Issues Facing Digital Forensic Experts," in IFIP International Conference on Digital Forensics, vol. Vol V. Digital Forensics 2009: Advances in Digital Forensics V, 2009,pp. 267–276.[Online]. Available: https:// link. springer.com /chapter /10.1007 /978-3-642-04155-6_20
7. "Amazon, AWS Security Center, Washington." [Online]. Available: https://aws.amazon.com/security/
8. "Cloud Computing Risk Assessment," Nov 2009. [Online]. Available: https://www.enisa.europa.eu/ publications/cloud- computing-risk-assessment
9. https://online.norwich.edu/academic-programs/resources/5-steps-for-conducting-computer-forensics-investigations
10. Cloud Security Alliance [CSA] 2009 Security Guidance for Critical Areas of Focus in Cloud Computing V2.1
11. https://www.7safe.com/digital-investigation-services/digital-forensics-investigations
12. https://www.csoonline.com/article/2120792/what-to-bring-on-a-computer-forensics-investigation.html
13. http://www.cloudforensicsresearch.org/publication/Survey_on_Cloud_Forensics_and_Critical_Criteria_for_Cloud_Forensic_Capability_6th_ADFSL.pdf
14. Birk D., "Technical Challenges of Forensic Investigations in Cloud Computing Environments", 2011: http://www.zurich.ibm.com/~cca/csc2011/submissions/birk.pdf
15. https://www.prodaft.com/resources/articles/why-cyber-intelligence-is-necessary/
16. https://cyberintelligence.my/
17. https://www.bankinfosecurity.com/blogs/cyber-intelligence-what-exactly-it-p-1061
18. https://www.businessnewsdaily.com/11141-cyber-threat-intelligence.html
19. Burke W., Baving R., "Cyber Forensics in the Cloud: Challenges and Best Practice", Sequirt CSi BV, 2011.
20. http://www.hackerhalted.com/Portals/3/Docs/Presentation%20Slides/Cyber-Forensic-in-The-Cloud-day3-Wayne-Burke.pdf

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

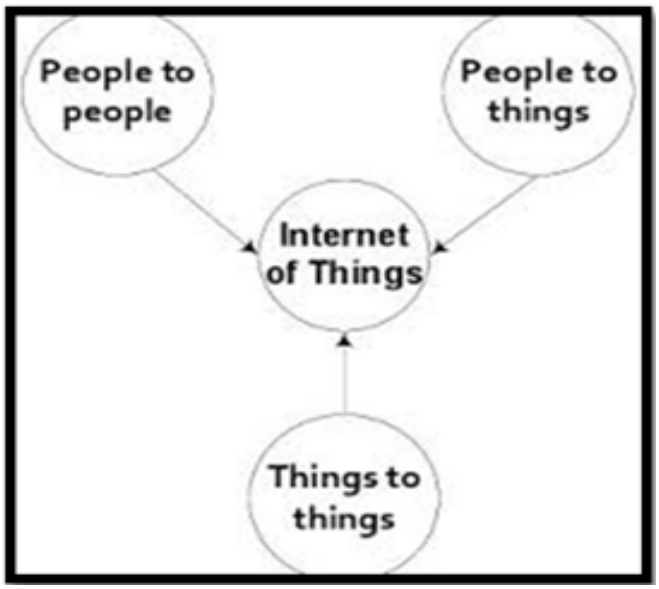
IOT AND DRONE FORENSICS INVESTIGATIONS

Priyadarshini Chettiar
Jnan Vikas Mandal's Mehta Degree College, Navi Mumbai

ABSTRACT
Internet of things is an interrelated network of computing devices, electronics, sensors, actuators, connectors and objects each provided with unique identifiers (UIDs) and with the ability to connect, interact and exchange data expanding its scope with the pace in the technologies. The collaborative study of Internet of things, Artificial Intelligence and Cloud based systems brings about the need of confirmatory secured and reliable systems. This work emphasis on various threats and events observed in IoT and drone forensics during investigations over years. Thus, rather than treating IoT as a conceptual model, we had tried to point out some of recent events and their consequences.

Keywords: Cyber Security, IoT terror, Drone forensics, resource protection, Vulnerable Systems, Cybercrime

I. INTRODUCTION
Internet of things is a superficial network of online embedded devices in our homes, workplaces and cities, that are constantly collecting, analysing and transmitting data. Some IoT devices, such as fitness bands or smartphones, are carried with us wherever we go. Others we interact with each other, such as domestic heating controls. Many are invisible or visible, operating silently to modulate traffic flows, industrial control systems, and much more.



-Edewede Oriwoh, an author of"Internet of things – the argument for Smart Forensics and investigations"

IoT is nothing more than a computer attached to the Things. As no computer is completely secured, neither any of the smart and virtual technologies can be secured. Thus, these objects form a massive distributed network with billions of entry points to be hacked. Due to lack of security in many cheap products it is relatively easy to be hacked. Even the devices with advanced security can be hacked, such as driverless cars are vulnerable, thus IoT technologies leads to some major security problems.

II. EFFECTS OF VULNERABILITY
Pacemakers getting hacked, air traffic control systems going down, and all out "cyber war" are just some of the worst-case scenarios. The exploitation of these vulnerabilities could lead to damage, injury and death. In 2015, the Ukrainian power grid was affected by a cyber-attack that left Kiev without electricity for several hours. In the same year, Sweden government leaks the personal details of nearly all the citizens. This was a huge knowledge breach within the Swedish Transport Agency (Transportstyrelsen) when the agency mishandled Associate in Nursing outsourcing trot out IBM, which led to the leak of the private data concerning each vehicle within the country, including those used by both police and military. All the sensitive data concerning about the voters, including fighter pilots of air force, members of the military's most secretive units, police suspects, people under the witness relocation programme, the load capability of all roads and bridges, and much more were exposed in this data breach.

ISSN 2394 - 7780

Reason behind the same was that the transport agency uploaded IBM's entire database with all the sensitive information onto the cloud servers and then emailed the entire database in messages to marketers that subscribe to it.

This outsourcing deal gave IBM employees outside Sweden access to the Swedish transport agency's systems while not undergoing correct security clearance checks.

Although the information breach happened in 2015, Swedish Secret Service discovered it in 2016.

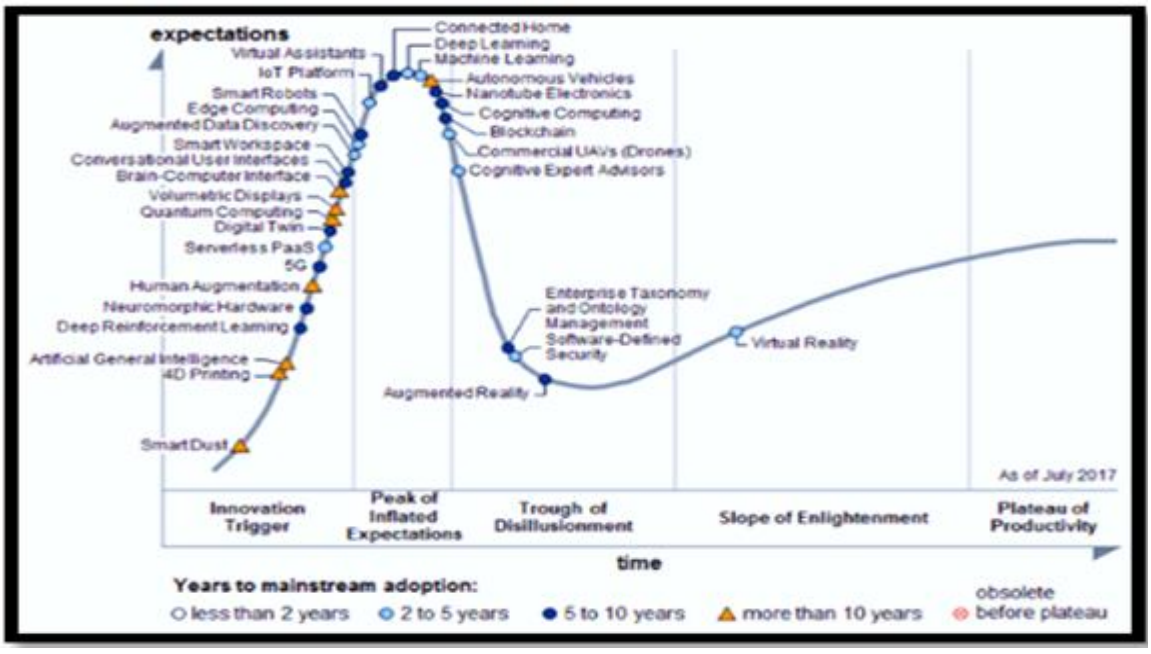
Recently, almost half a million Delhi citizen's Personal Data Exposed Online.

Bob Diachenko, a Cyber Security Consultant came across 4.1 GB-sized highly sensitive database online, named as "GNCTD", which consisted of information of 458,388 individuals from Delhi, which includes Aadhaar card numbers, qualification details, professional details and voter ID numbers. Reason behind the breach were the MongoDB instances found exposed to the Internet, as the administrators didn't follow the security checklist provided by the MongoDB maintainers. More recently in 2017, the UK's NHS faced issues for about weeks due to the malicious computer code (malware) WannaCry.

Airbus, the world's second largest manufacturers of commercial planes, after Boeing was hit by Cyber attack in March 2018. Now, again Airbus became a victim of data breach, some employees got data their exposed even after being in contact with regulatory authorities and data protection authorities pursuant to the European Union's new GDPR (General Data Protection Regulation) rules.

Data Breaches and Hackings are not only found in large scale industries and machineries but in small scale too. The BlueBorne attack, which enables hackers to take over Bluetooth enabled devices and unroll malwares, or may establish a "man-in-the middle" connection to gain access to device's data critical and networks without requiring any interaction from the victim. Turning on Bluetooth may turn your device vulnerable to such attacks, as BlueBorne attack may spread in the same way as the worm able WannaCry ransomware. Even the smartest of devices running Linux OS are vulnerable to such attacks. A BlueBorne Vulnerability Scanner was the most acceptable application to check whether the device was a victim of an attack or not. Security Researchers came up with zero-day vulnerabilities in Bluetooth Protocol which had impacted over 5.3 Billion devices – from Android to iOS, Windows, Linus to IoT devices –by only using a short-range Wireless Communication technology.

One major internet security company reported that IoT attacks which increased 800% in 2016-17. While the Hype Cycle for Emerging Technologies (Gartner, August 2015) says that IOT market will reach $3.04trillion and there will be 30 billion connected things by 2020 i.e. 5 per person on the earth.



The evergreen growth and demand of IoT devices, may forbid some of the rules of confidentiality, Integrity and availability. The National Security Agency (NSA) Strategic Intelligence had partnership with 80 Alliances over Major Global Corporations Supporting its missions, these include Telecommunications and Network Service Providers, Network Infrastructures, Hardware Platforms Desktops / servers, OS, Application Software, Security

ISSN 2394 - 7780

Hardware and Software and System Integrators. On failing to imbibe the proposals, these companies may lose their license to operate, thus your data is not safe anywhere.

III. WHEN STRUCTURE OF IoT CALLED UP IN FORENSICS

The structure of IoT includes Internet Cloud, IoT Servers that monitors the actions of the Big things (large and complex data models), small things(Simple data models) and the gateway. The Gateway Device Management manages the complex and dynamic data models, diagnose and repair, alarms and alerts, manages the configurations and security and provisioning. Based on messaging protocols and session-based protocol, the bottom line includes 4 major protocols i.e. MQTT, LWM2M, OMA-DM and TR-069. But the only end development controls available are set and get, yet powerful.

In broader aspect, IoT encourages the Machine to Machine Communications, RFID – Radio Frequency Identification, Context Aware computing and wearable ubiquitous computing. Forensics implies the usage of science and technologies for investigation and building of facts in criminal or civil courts of law. Digital forensics combines the laws of computing with the law of court for collecting and analysing data from computer systems, networks, wireless communications and storage devices. IoT Forensics – is an application of digital forensics in the IoT based Model.

IoT Security prevents IoT devices and networks from any malicious activity being performed on them. IoT Forensics focuses on the gathering the digital evidences for legal purposes from IoT devices, identifying the culprits and the victims. It includes the major steps of identification, preservation, analysis and presentation of every crime.

Identification answers to all the details about the site and its environment of crime, devices interaction, cryptographical principles, sensitivity of the data, stake holders if any, gather most of the evidences, jurisdiction, proprietary and their standards.

Preservation deals with the available tools for collecting and preserving the evidences, based on the necessity of keeping IoT as part of evidence without changing the status of evidences.

Analysis includes knowledge of all the branches of Science, Mechanics etc for reconstructing the crime scene in a test environment, with a common repository to store the data proving the accuracy of evidences with Court accepted tools and technologies. It includes analysing the device lifecycle and their interactions.

Presentation focuses on presenting the evidences with or without IoT devices taking into count, with major decisions often taken by IoT Forensics examiners, medical specialists etc. It involves a detailed study to come at a conclusion after carrying out the above steps.

IV. IoT WITHOUT INVOLVEMENT OF DRONE TECHNOLOGY IS INCOMPLETE

A drone is an Unmanned Aerial Vehicle (UAV) i.e. a pilotless aircraft, which can be controlled from a remote distance. Nowadays, drones are found being used in many cultural events adding up an extra light to it, the ending of Kumbh 2019 India was one of its spectators. Drones being easily affordable and accessible has gathered a great attention from the public. But this has also led to increase in crime rate. The aerial system structure of drones may include a camera to capture videos or images of targeted zone and are termed as drone camera. Its structure is relatable to flying quad copter with a camera, which can be monitored and controlled from a remote distance using any handheld device. Their task is to collect and store data in a centralized server. However, drones have got some restrictions too, the Federal Aviation Administration (FAA), a US body had set certain rules and regulations to fly drones i.e. a Certificate of Authorization is mandatory even when used for non- recreational purposes. Indian Drone rules permits the usage of Nano categorised drones while others need to register and acquire a Unique Identification Number(UIN) for getting authorized.

Drones being used for scientific purposes vary in system structure and components. The major system components of drones with camera are Imaging Sensors and Data Collectors, Antenna Tracking Systems, Detectors, Spectrometers, Spectrophotometers, Autopilot Navigation, UAV Engines, Ground Stations, Launch System and Auto landing Recovery. The camera is encapsulated with a Wireless router consisting of a wireless chipset which operates at 802.11 frequency set depending upon the specifications. The front and vertical HD camera are deployed for complete coverage, thus for collecting and transferring this data a high-power CPU is also one of the major requirement. Remote Devices and USB are the major storage mediums. Various types of sensors being in usage such as the image sensors, embedded inertial sensor (a combination of gyrometers and accelerometers), GPS systems and velocity sensors, their involvement is restricted to the scope of the purpose. The software components include an embedded OS and window sniffer for trafficking.

ISSN 2394 - 7780

Though drones were invented with the motto of being helpful in disastrous events, monitoring the environment, education and majorly for security surveillance services, they were the most encountered equipment used in crimes. Illegal usage of drones in war prone areas and for spying had created a havoc. There were some cases where the carrying capability of drones was exploited for performing illegitimate practices such as the transport of weapons, drugs in prisons and across country's boundaries.

A significant security threat was observed, when drones were used as deadly weapons in no-fly-zone areas of airspace, military base, power stations. But, in terms of Forensics these drones are helpful in collecting the information about the crime. When trying the recreation of the actions taken by the drone, recorded flight data is elucidated which includes information about timestamped latitude, altitude, speed, acceleration, battery level, GPS readings and other measurements collected via sensors. Drone Forensics is a division of Wireless Forensics and thus a sub division of Digital Forensics. Two popular drone systems are DJI Phantom 3 Professional and Parrot AR. Drone 2.0. both based on Linux OS, but still provides an unsecured access point. The applications of drones vary from vacuuming up ocean waste, delivering pizza, disease control, surveillance in military purposes, providing medicinal aids, crime scenes, preventing disaster, detection of intrusions, abnormalities in temperatures, animals and marine life conservation, agriculture, weather forecasting, waste management activities, Oil and gas inspection, Unmanned ground vehicle for mining, and the list goes on. Drone Forensics includes artefact- driven analysis on the UAVs and device platforms by identifying the potential suspects, analysing and auditing based on the flight data, server data and image forensics, extracting the data of the actual target specifications, all actions must be taken as per the guidelines for handling digital evidences.

V. CONCLUSION

A glimpse of events and threats observed in IoT Forensics and Drone Forensics have been discussed in this paper.

VI. BIBLIOGRAPHY

1. Artificial Intelligence: a Silver Bullet in Cyber Security? CPX 360 Keynote
2. https://www.youtube.com/watch?v=ggje-L0ViFM
3. https://www.dataforensics.org/drone-forensics/
4. https://www.militaryaerospace.com/articles/2018/03/terrorists-atomic-bombs-iot.html
5. http://theconversation.com/internet-of-things-when-objects-threaten-national-security-96962
6. https://www.richardvanhooijdonk.com/en/blog/all-the-surprising-and-scary-ways-you-and-your-systems-can-be-hacked/
7. https://ieeexplore.ieee.org/document/7323000
8. https://www.researchgate.net/publication/309479252_Internet_of_Things_Mobility_Forensics
9. https://computer.howstuffworks.com/computer-forensic1.htm
10. Drone Forensic Analysis Using Open Source Tools by M A Hannan Bin Azhar,Thomas Edward Allen Barton and Tasmina Islam
11. https://www.slideshare.net/KMSabidurRahman/iot-mobility-forensics
12. https://digitalforensic.jp/wp-content/uploads/2016/03/community-12-2015-07.pdf
13. https://thehackernews.com/
14. Internet of things – the argument for Smart Forensics by EdewedeOriwoh,
15. https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

DRONE FORENSICS INVESTIGATION: A SENSOR DEVICE

Pallavi Raut
M.Tech in Computer Science

ABSTRACT

This research paper provides basic idea that why and how widely drones (UAV) can be used in cyber law. The designs of an autonomous unmanned aerial vehicle (UAV) which is controlled by wireless technology through graphical user interface (GUI).

Drones are beginning to take off, and Drone code wants to take off with them. The organization designed to give resources and tools to developers announced powerful milestones that it are advancing its open-source platform for drones.

Controlling capabilities of drones and their easy way of accessibility to the generic have led to an increase in crimes committed using drones in recent years. So that the need for forensic analysis of drones captured from the crime scenes and the devices used for these drones is also supreme. Ease of availability and affordability of unmanned aerial vehicles (UAV) have led to an increase in its popularity amongst the public. The proliferation of UAVs has also augmented several security issues. These devices are used for illegal activities such as drug smuggling and privacy invasion. The purpose of this research paper is to analyze the basic architecture of a drone, and to propose a generic drone forensic model that would improve the digital investigation process. This paper also provides recommendations on how one should perform forensics on the various components of a drone such as camera and Wi-Fi and also a short note on sensor as a graphical user device.

Keywords: Digital forensics, Drone forensics, Open source tools,DGI Phantom. Framework.

INTRODUCTION

Drones, also known as unmanned aerial vehicles (UAV), are being amongst public due to their accessibility and affordability. It is not only helping in rapid growth of global commercial market of UAVs (Majendie & Chia, 2018; Moskwa, 2016) but also inevitably increasing drone crimes (Yeung, 2016). The carrying capabilities of drones over long distances (UAV, 2018) and their remote operation make drones ideally committed drone crime. This type of drone crime has detected around the world (Dinan, 2017; @ 2018 ADFSL Mikelionis, 2018), such as dropping weapons, phones, drugs into prisons or delivering drugs or the possibilities of drones being used in terror attacks is real. In some jails, drones have been spotted delivering cell phones and dropping other contraband over prison walls and arms in and out of a country bypassing borders. As well as smuggling, the camera mounted onto a drone, either as a static recording or a live streaming device, raises significant data privacy concerns for organizations and public. It also consists the ability of drones capturing pictures or videos of operations in designated no-fly-zone areas of airspace (CAA, 2015), such as, airports, military base and power stations, presents a significant security threat. Autonomous UAV mounted cameras are also being used for traditional crime such as burglary.

Unmanned Aerial Vehicles (UAVs) has become more ability to detect and prevent illegal usage of UAVs, It has the ability to find and show evidence of illegal drone usage when a case is brought in front of the court, it consider as a proof.

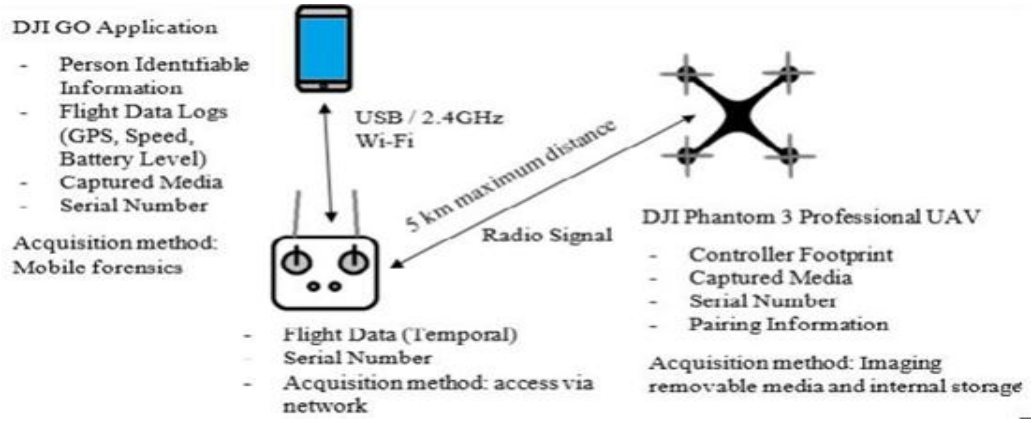
The framework is applied on DJI Phantom III,is a common commercial drones available in the market today. At the time of implementation of framework, we kept in mind the well-known forensic investigation principles such as preserving digital evidence, preserving chain of custody, avoiding adding data, extracting and documenting actions.

The signal generated by the sensor are processed in microprocessor which applies several cascading regulation loops, so that achieving the pilot control movements acts in combination with the corrections of the flight control system.

A piloting known as fly by wire is developed where the action do not directly on the control organs of the aircrafts but on the control algorithm that introduce the necessary corrections and compensation

Fig.DGI Phantom 3 Professional operation and potential artefacts.

ISSN 2394 - 7780



Drones As flight data such as GPS readings, altitude, speed, acceleration and battery levels were collected via various sensors present on the both the UAV systems.

1) DJI Phantom 3 Professional: An operational diagram of DJI with potential DJI GO Application Person Identifiable Information Flight Data Logs (GPS, Speed., Battery Level) Captured Media, extraction of Serial and parallel data.

The electronic control and communication system: The control system is responsible for the drone fly up, down; clockwise and anticlockwise rotation, for his reaction to the emerging forces and for stability. Most of the control systems are equipped with the same set of sensors with the difference in the speed of calculations and in algorithms used.

The control system consists of:

1. Flight controller, responsible for machine control capabilities,
2. Electronic Speed Control (ESC) –the unit responsible for engine rpm,
3. Supplying plate, separating the power supply for regulators turnovers and motors,
4. The transmission of telemetry data is allowed by Sim module
5. Proximity camera is an element of anti-collision system,
6. Customer PIN codes can be enter by numeric keypad

UAV Digital Forensics Investigation Framework

There is no standardized framework for digital forensics investigation of

UAVs. The proposed framework is applied on DJI Phantom III, one of the most popular commercial drones available in the market today. During the implementation, need to kept in mind the well-known forensic investigation principles such as preserving digital evidence, preserving chain of custody, avoiding adding data and documenting actions.

In order to disclose any evidence to the court and get it approved, a standardized, or at least acceptable, investigation framework should be used by the investigator. There are multiple kinds of UAVs available in the market and each company uses different hardware and firmware packages. For this reason, although it is difficult to create a single tool for investigating all UAVs, finding a generic investigation framework for all kinds of UAVs is a reasonable solution.

Here propose a seven-phased framework for the digital forensic investigation of UAV.

Table 1. Proposed Seven-Phased UAV Investigation Framework

UAV FORENSIC INVESTIGATION PHASES
1. Preparation
2. Scene Control
3. Customization Detection
4. Data Acquisition
5. Evidence Authentication
6. Evidence Examination
7. Presentation

ISSN 2394 - 7780

With the increased use of drones both by private, civilized and government agencies, it's essential for investigation department to craft effective law enforcement drone policy. Drones, also known unmanned aircraft systems (UAS), are aircraft that fly without a pilot on board. UAVs vary in size and capabilities from high-tech military drones all the way down to the remote-controlled toys many teens received for Christmas. Drones are fairly new technology, but they're gaining prominence. The military has been using UAVs for years in combat and surveillance operations. Many people still associate drones with military activity, but drones have several different commercial and recreational uses. Companies have begun using them to make deliveries. The digital forensic investigation of UAVs is crucial for providing Security, accessibility and accountability related to the use of these systems,

Now a day's photographers and videographers sometimes use them for overhead footage and photos. And many law enforcement agencies have started using them.

As part of our series on crucial policies for law enforcement, this will cover how civilian drone use affects your agency, how your department can prepare for the coming wave of drone technology, and how to craft effective policies around your state's drone laws.

Extraction of Forensic Data From Drones:
If drones used in crime do get captured, investigators will extract as much data from them as possible to help their cases. Now, the National Institute of Standards and Technology (NIST) has developed a website to help authorities glean "forensic images" from drones.

The forensic images contain all the binary coding that recovered from each model,

The images were created using industry standard data formats so that investigators can connect to them using forensic software tools and inspect their contents. Each model is having the image which also come with step-by-step instructions.

Investigators can be use the images for recovering data, including deleted files. Universities and forensic labs can use them for training, proficiency testing and research. And application developers can use the images to test their software.

There are many different kinds of drones available in the market, each potentially requiring unique approaches when it comes to data extraction.

The data from some drones can be retrieved while the drone is intact, Some drones require disassembly of the aircraft; other drones require complete disassembly down to the chips. the area of our research is identifying how to get the data of test devices so digital forensic practitioners have guidance when they receive devices as evidence.

There are many drone manufacturers and different models, there is no any single standard on the way these drones store digital data. The data can be stored in several different formats, though GPS coordinates can also be encoded in multiple ways. Due to the many variety of data formats and the potentially overwhelming amount of available evidence, manual extraction and examination of this evidence can be extremely time and labor efforts consuming, Hence drone forensics is still relatively new, very few tools exist for experts that allow the automation of these procedures.

FORENSIC TOOLS
Here are some freely available forensic tools work on local machines, on remote machine, to capture and check the volatile data on suspicion.

1. The SANS Investigative Forensic Toolkit (SIFT): SIFT forensic tool is based on is an Ubuntu Live CD which has all the tools user need to conduct an in-depth forensic or incident response investigation
2. CrowdStrike CrowdResponse Once user exported the data needed, afterword use CRconvert.exe to convert the data from XML to another file format like CSV or HTML.
3. Volatility: Response and malware analysis from Forensics framework for incident that allows user to extract digital facts from volatile memory (RAM) dumps.With the help of Volatility user can extract information about running processes, open network sockets and network connections, Dynamic Link Libraries(DLL's) loaded for each process, cached registry hives, process IDs, and more.
4. The Sleuth Kit (+Autopsy): In-depth analysis of various file systems can be performed by using the Sleuth Kit which is an open source digital forensics toolkit. Autopsy is essentially a GUI that sits on top of The

ISSN 2394 - 7780

Sleuth Kit. It provides features like Timeline Analysis, Hash Filtering, File System Analysis and Keyword Searching out of the box, with the ability to add other modules for extended functionality.

5. Oxygen Forensic Detective: Ability to extract digital evidence from the drone's internal storage or external SD card, parse and decode data, and present it to the investigator in a human-readable form.
6. FTK Imager: FTK Imager is a data preview and imaging tool that allows you to examine files and folders on local hard drives, network drives, CDs/DVDs, and review the content of forensic images which are stored in memory.
7. Linux 'dd':It comes with default on the majority of Linux distributions available like(e.g. Ubuntu, Fedora). This tool can be used for various digital forensic tasks such as forensically wiping a drive (zero-in and out a drive) and creating a raw image of a drive.
8. CAINE:CAINE (Computer Aided Investigative Environment) is Linux Live CD that contains a wealth of digital forensic tools. It includes the feature like a user-friendly GUI, semi-automated report creation and tools for Mobile Forensics, Network Forensics, Data Recovery and more.
9. ExifTool:ExifTool is a command-line application used to read, write or edit file metadata information. It has feature like fast, powerful and supports a large range of file formats (although image file types are its specialty). ExifTool can be used for analyzing the static properties of suspicious files in a host-based forensic investigation.
10. Free Hex Editor Neo:Free Hex Editor Neo is a basic hex editor that was designed to handle very large files.While a lot of the additional features are found in the commercial versions of Hex Editor Neo, This tool is useful for loading large files like database files or forensic images and performing actions such as manual data carving, low-level file editing, information gathering, or searching for hidden data.
11. Bulk Extractor: This computer forensics tool that scans a disk image, file, or directory of files and extracts information such as credit card numbers, domains, e-mail addresses, URLs, and ZIP files. The extracted information is output to a series of text files (which can be reviewed manually or analyzed using other forensics tools or scripts).
12. DEFT:It is another Linux Live CD which bundles some of the most popular free and open source computer forensic tools available. It aims to help with Incident Response, Cyber Intelligence and Computer Forensics scenarios. Amongst others, it contains tools for Mobile Forensics, Network Forensics, Data Recovery, and Hashing.
13. USB Historian: User can use USB information, primarily from the Windows registry, to give a list of all USB drives that were plugged into the machine. It displays information such as the name of the USB drive, the serial number, when it was mounted and by which user account.

INTERNATIONAL INTEREST

Due to drone forensic program is surveying users regarding their use of this data. It has responses from North America, South America, Europe, the Middle East, Asia, Africa, Australia, except Antarctica, Hence global issue being faced by law enforcement agencies around the planet. It also shows an impact on social media. People have misused a law or rule in a jurisdiction, the drone may be able to prove that. On the other hand, if drone operators are accused of misusing a law and rule and they did not do that.

The information which is same stored in the drone did not actually do what they are accused of. University of Guelph in Canada, has been using this forensic data to create artificial intelligence (AI) software to identify drones potentially affected by malware. The researchers amazed with the potential that all those data have in creation of AI agents that could provide active defense for drones and automatically detect those which are potentially compromised, The project gives an ideas for building forensically sound methods for drone investigation and, more specifically, identifying what implicit actions were taken and when those activities took place. At the same time, user can identify gaps or weaknesses that exist in extending current forensics practices to drone investigation. If any missing data that is supposed to be recorded and needed during an investigation, or changing the usual investigation process when dealing with drones. Globally the Law enforcement agencies and governments are using the scientific research completed to complete investigations, protect their citizens and make a difference in our world.

ISSN 2394 - 7780

CONCLUSION

Together efforts to establish a common platform and utilizing open-source best practices, possibly to build the foundation for a new era of drone applications that extend from the camera to the cloud. As per the study gives an idea for relevant Drone code is the highest growth rate for drones is in commercial opportunities across applications such as agriculture, energy, utilities, mining and construction, and the organization wants to help tackle the software and hardware barriers blocking the development and adoption of these critical apps. The organization announced the formation of three technical working groups designed to provide better standardization and airspace management; and hardware/software interfaces. In the research, its aimed that to create a framework for systematically detecting and classifying any criminal activity conducted with UAVs. Today increase in the usage of UAVs has also led to a dramatic in the illegal usage of these devices.

So, sensing UAVs equipped with sensors can be used as an aerial sensor network for environmental monitoring and disaster management. They can provide numerous datasets to support research teams, serving a broad range of applications such as drought monitoring, water quality monitoring, tree species, disease detection, etc.

Drones with sensors such as Thermal, LiDAR, Time-of-Flight and multispectral sensors are bringing major benefits to many sectors including Agriculture, Maintenance, Mining, Costructions,Environmental, Conservation, Search and Rescue, Crime Mapping, Information Technology, and the Rationality of Crime Control. Cybercrime investigation along with many others. The research gives an idea that our proposed framework contributes to digital forensics Investigators on the investigation of UAVs. In risk management, insurance companies can utilize UAVs to generate maps in order to have an overview of the damage for instance.

REFRENCES

- DJI. (2018). Phantom 3 Professional - Specs, FAQ, Tutorials, Downloads and DJI GO - DJI. Retrieved 23 March 2018, from https://www.dji.com/phantom-3-pro/info#specs
- Lum CW, Gauksheim K, Deseure C, Vagners J, McGeer T (2011) Assessing and estimating risk of operating unmanned aerial systems in populated areas. In Proceedings of the 11th AIAA Aviation Technology, Integration, and Operations (ATIO) Conference. Virginia Beach.
- Scheding S, Finn A (2010) Developments and challenges for autonomous unmanned vehicles: A compendium s.1. Springer Sci & Business 9.
- Zain M, Hussin AK, Ganraj D (2001) An ultralight helicopter for rice farmers. Universiti Teknologi MARA.
- Hejduk M (2015) The use of unmanned aerial vehicles - drones supply courier. Thesis Inzynierska. Wroclaw.
- Piotrowski P, Witkowski T, Piotrowski R (2015) Unmanned remote-controlled flying unit. Measurement Automation and Robotics 19: 49-55. 6. Bogusz P, Korkosz M, Wygonik P, Dudek M, Lis B (2015)
- "The standing Senate Committee on National Security and Defense", Evidence, April 2012. Unmanned Aerial Systems Circular (2011) International Civil Aviation Organization (CAO).Murrow HN, Eckstrom CV (1979) Drones for Aerodynamic and Structural Testing (DAST) - A Status Report 16: 521-526.
- W. Zhang, M. W. Mueller, and R. D'Andrea, "A controllable flying vehicle with a single moving part," in Proc. IEEE International Conference on Robotics and Automation (ICRA), May 2016
- AIAA Journal of Guidance, Control, and Dynamics. [Online]. Available: https://arc.aiaa.org/loi/jgcd [136] International Conference on Unmanned Aircraft Systems. [Online]. Available: http://www.icuas.com/ [137] DJI Phantom 3. [Online]. Available: http://www.dji.com/product/ phantom-4 [138]
- YUNEEC Typhoon H. [Online]. Available: https://www.yuneec.com/ en US/products/typhoon/h/ overview.html[139] Vicon. [Online].

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

AI IN CYBER FORENSICS AND INVESTIGATION

Sarita Sarang
Assistant Professor, Jnan Vikas Mandal's Mehta Degree College, Airoli, Navi Mumbai

ABSTRACT
Artificial intelligence is a branch of computer science which encourages the creation of intelligent machines. These intelligent machines can solve most problems in certain domains such as speech recognition, image search and processing, cyber security, computer vision, shopping predictions etc. This paper emphasizes on various applications and theory of ai accepted in the current and expected in the future generation of systems.

Keywords; cyber security, artificial intelligence, machine learning, ai for hackers, blockchain, cyber attacks

I. INTRODUCTION

Industrial Revolution had almost transformed from a Muscles working strategy to a Machines working strategy. While the revolution of Artificial Intelligence had introduced Machines with Brains. When AI was asked to explain in a Layman's language it is nothing but a strong team work of storage, computation and mathematics. AI consists of two major subdomains – the Symbolic Learning and the Machine Learning. Machine learning, being a back bone of AI Systems uses Mathematical and Statistical way of solving the problems related to data. Deep learning, a subdomain of Machine learning strengthens the usage of Convolutional NeuralNetworks which helps in Image processing, Object Recognition, etc. An artificial Neural network is a basically a framework of many different Machine Learning algorithms working together for processing the most complex data inputs. Implementation of Knowledge engineering for AI requires access to objects, categories, properties and their relationships with one another. Thus, a secured network framework is required while working on distributed systems.

II. INTRODUCING AI IN CYBER SECURITY

AI can be used in automating the detection of threats and combat without any human intervention. The main necessities of today's secured Cyber Network are Handling immense amount of security data, detecting threats in Cyber Stacks, accelerating the response times, continuing with the AI arms race and a common platform for human cyber security teams. The structure of AI includes a decision-making mechanism which is built using certain Machine Learning Algorithms. Most of the recent Systems are password protected and authentication detecting systems and hence vulnerable. Passwords are much easier to hack;thus your data is unsecured. While AI enables the use of certain technologies for the same to provide a more secured system, which includes biometric logins, thus it uses physical characteristics such as fingerprints, retina scans, etc for detection.

AI plays a leading role in Cyber Security and some of its major applications are as below:

Spam Filter Application: This application is basically an email filtering application for spams. The criteria for an email to be spam are anonymity, mass mailing and unsolicited emails. Thus, filtering and classification of emails based on these criteria must be done. A Naïve-Bayesian Classifier can be for the same. The steps for classifying and detecting spam mails starts with finding of words out of all possible traits and thus creating a variable of mutual information. The words are categorised, then Bayes theorem is applied to it which calculates the probability that an email is a spam or a false positive.

Network Intrusion Detection, Host based Intrusion Detection and Prevention Systems: A Network Intrusion implies an unauthorized activity on a computer network. Intrusion detection requires a defender to be aware of the most possible attacks. This will help in developing a most precise and robust network intrusion detection systems. A host-based intrusion is similar to the network-based intrusion, where the unauthorized activity is performed internally or externally via network packets. Intrusion Detection Systems thus are built with the capability to monitor, detect and analyse the activities of intrusion. If any malicious or policy violating activities are observed then, the details about the same are reported to the administrators or higher authorities using a Security information and Event Management System. The detection approach includes a signature, pattern identification, malware detection, anomaly-based detection. The scope of the Firewalls is limited to stop the outwardly intrusion and cannot signal the occurrence of intrusion inside the network. Thus, IDS is helpful in detection, prevention and a secured network.

Recently in the first weeks of March 2019, Citrix Systems Inc., a global technology provider confirmed being a victim of Intrusion. The breach has led to a loss of hundreds of millions of dollars and was notified to FBI. A data of about ten terabytes were stolen which were confidential to the company. Later it was found out that a

ISSN 2394 - 7780

spray attack was performed by the hacking committee. A spray attack is an automated attack pattern in which every possible password is attempted until the access is obtained. In addition to it, a multi-factor authentication tool was used for unauthorized access to the company's network via a Virtual Private Network (VPN) and Single Sign-On(SSO) resources. The most prevention methodology which any company must take are carrying a network segmentation, data loss prevention, IDS and IPS systems, validating the efficiency of the system controls, password policies, assessing and creating a demilitarized zone for screening packets before they reach the host. When using a Cloud based platform, using Cloud access security brokers will help in preventing spray attacks.

Fraud Detection: Phishing, a social engineering attack is a fraudulent attempt in stealing the user credentials, passwords, credit card details, etc. It is occurred when an attacker masquerades as a trusted entity and dupes the victim by opening an email, instant or text message, or in any electronic communication.Research by security company has found that 46 percent of UK organisations were compromised by phishing attacks between 2015 and 2018 — and that 54 percent had identified instances of employees replying to uninvited emails or clicking the links in them.With the use of Phishing emails, hackers try to attempt to lure victims to download malwares or to enter sensitive credentials into a phoney version of any banking or retailing website or any other fake login page. Any instances of password re-use can be easily identified by the hackers; thus, security professionals always suggest to adopt a multifactor authentication process. Some preventive measures from being a victim of phishing attacks are by reviewing the existing software and hardware configurations, password policies, encouraging credential protection, verification of threat intelligence in networks, verifying existing mail security system configuration,deep link inspection, multi-layer email security, false positives, web and document isolation using the isolation technique, Storage platforms Security checks, Reports and analytics tools using historic data for assessments.

Credit Breach Protection: In September of 2017, Equifaxthe company reported that hackers accessed the data of up to 143 million Americans, which included Social Security numbers, birthdates, addresses, credit card numbers and driver's license numbers. In the same year, in month of October additional 2.5million consumers were found to be victims of this attack according to Identify Theft Resource Centre. Anxiety filled the way, as this sensitive information can be sold in dark web for making money. Credit monitoring, getting a dark web scan for Social Security number, locking credit to prevent illegal activities, establishing online access through MySSA, using a two-factor authentication method, using a tax identity pin and by adding a fraud alert.

Botnet Detection: Denial of Service attacks, malware attacks, email spam campaigns, data theft and exploitation of Policies and vulnerabilities are the most prominent attacks which has caused the loss of millions of dollars of businesses. Mirai malware on Dyn.Inc is one such example, which led to the unavailability of the most popular websites such as Netflix, Twitter, PayPal, etc. A botnet created via a network of malware infected computer, each device in it is called a bot and enables a Third-Party Control. Bot herders recruits bot using virus, worms, etc. one a device is infected it is under the command and control of Bot herder Server and thus support hackers to perform criminal activities. Zeus Botnets, were the Trojan Horse that steals bank information using botnets and the attack was encouraged by 100s of cyber criminals as per FBI. In October 2010, FBI confirms a steal of over $70million dollars from bank accounts in United States. As botnets operates beyond user's knowledge it is difficult to trace them. Some symptoms indicating Botnets are IRC traffic (as botnets and bot masters, both make use IRC for communications) via Port no. 6667, Multiple machines on a single network making identical DNS requests via Port no. 1080, enabling SMTP traffic through spam using Port no. 25, click-fraud activities, high CPU usage, outbound messages and problems with Internet access etc. Network monitoring, Up-to-date Security Patches, Awareness, Anti Botnet Tools usage are some of the preventive measures against Botnet attack.

Secure User Authentication: Data Breach have been increased majorly on Third Party Companies. As a preventive measure we can use some software applications to analyse our Network data and spot the irregularities and log them. A user, asset and entity verification to be performed based on their behaviour patterns with the normal. Adding Security alerts, Strong Password measures, the type of network connection, the packets received will be helpful. Using physical characteristics of individuals as an authentication pattern will ensure a secured communication channel. Encrypting the data before sending and decrypting it before using will be helpful, but has got limitations too. In the man-in- the- middle scenarios, as harmful malicious files may have been shared, and trying to decrypt it will be dangerous and risky. Block Chains are definitely the most significant answer to this problem. A block chain is a chain of blocks each carrying an identification of the last block. Since all the blocks are linked with a chain, any changes performed on one chain, may significantly affect the other. Hence it would be difficult for a hacker to handle the situation. The algorithm of block chain is

ISSN 2394 - 7780

highly powerful and enables any transaction to be performed in an encrypted form itself. It works on trust and distributed systems.

Cyber Security Ratings: These are the ratings provided based on the Third- and Fourth-Party Risk Management Assessment, Alerts, Reporting and Intelligence. A dynamic measurement of an organization's cyber security performance is validated and verified. These ratings are calculated on scores using publicly available information to assess an organization's cyber risk. Internet traffic, botnets, malware, and cyber criminals across devices are assessed on a global scale that reveals links between an organization's networks and malicious activities if any. By analysing the connections made through their servers the threats and their events of occurrences for the IP Address are calculated. This will help the organization to learn how secured it is. But these ratings assessments should be followed and taken to overcome the loop holes.

Hacking Incident Forecasting: The use of AI and smart techs to overcome hacking is one of the best way. Awareness about the types of attacks, safe tools, preventive measures, network monitoring, up-to-date awareness about types of hacking incidents worldwide and trying to detect and analyse the current systems, strictly following the Cyber laws will be beneficial.

III.CONCLUSION

Organizations waste about $1.3 million per year responding to inaccurate and erroneous alerts as per the study by SANS Institute. Effective use of Machine Learning and AI Tools will help the organizations to overcome the major issues discussed in this paper. Behavioural User Analytics an Application of AI are treated as a Golden Standard Products for Cyber Security as per the research study. The study reveals that AI market is expected to grow from $21.46 Bn to $190.61Bn between 2018 and 2025. Insurance and Banking Companies are using AI to monitor the frauds. Shopping and Market Basket Analysis is possible using AI tools. Self Driving Cars, auto Pilot modes and smart home using sensors are expected to be most familiar victims of Cyber attacks hence a significant and robust use of AI algorithms would help to tackle this. Since AI is not limited for Security experts but also for hackers, upgrading with technologies and continuous learning, the future of AI depends on its purpose and usage.

IV. BIBLIOGRAPHY

1. https://odsc.thinkific.com/courses/take/blockchain-and-ai/lessons/5569444-blockchain-and-ai-or-future-data-systems-must-be-built-differently
2. https://opendatascience.com/an-open-framework-for-secure-and-private-ai/
3. https://www.techopedia.com/definition/190/artificial-intelligence-ai
4. https://www.youtube.com/watch?v=ggje-L0ViFM
5. https://en.wikipedia.org/wiki/Artificial_neural_network
6. http://houseofbots.com/news-detail/3703-1-10-plus-videos-to-learn-artificial-intelligence-machine-learning-and-data-science-for-beginners-must-watch
7. https://en.wikipedia.org/wiki/Intrusion_detection_system
8. https://searchcloudsecurity.techtarget.com/definition/cloud-access-security-brokers-CABs
9. https://searchsecurity.techtarget.com/tip/Nine-email-security-features-to-help-prevent-phishing-attacks
10. https://www.zdnet.com/article/half-of-organisations-have-fallen-victim-to-phishing-attacks-in-last-two-years/
11. https://www.creditkarma.com/insights/i/equifax-reveals-full-scope-breach/
12. https://www.veracode.com/security/botnet
13. https://www.aiaa.org/April-2018-Protocol/

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER FORENSICS AND INVESTIGATION

Sameer More and Purvesh Mokashi
JVM'S Mehta College, Navi Mumbai

INTRODUCTION

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

Forensic investigators typically follow a standard set of procedures: After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy.

Investigators use a variety of techniques and proprietary software forensic applications to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation.Computer forensics has become its own area of scientific expertise, with accompanying coursework and certification.

BASICS CYBER FORENSICSAND INVESTIGATION

The field of computer forensics is relatively young. In the time period of computing, courts thought-about proof from computers to be no totally different from the other reasonably proof. As computers became a lot of advanced and complex, opinion shifted -- the courts learned that laptop proof was straightforward to corrupt, destroy or modification. Investigators complete that there was a desire to develop specific tools and processes to look computers for proofwhile not moving the data itself. Detectives partnered with laptop scientists to debate the acceptable procedures and tools they'd ought to use to retrieve proof from a laptop. Gradually, they developed the procedures that currently structure the sphere of laptop forensics. Usually, detectives have to be compelled to secure a warrant to look a suspect's laptop for proof. The warrant should embody wherever detectives will search and what variety of proof they'll explore for. In different words, a detective can't just serve a warrant and look wherever he or she likes for anything suspicious.

In addition, the warrant's terms can't be too general. Most judges need detectives to be as specific as attainable once requesting a warrant. For this reason, it's important for detectives to research the suspect as much as possible before requesting a warrant. Consider this example: A detective secures a warrant to look a suspect's laptop computer. The detective arrives at the suspect's home and serves the warrant. While at the suspect's home, the detective sees a desktop PC. The detective cannot de jure search the computer as a result of it wasn't enclosed within the original warrant.

Every computer investigation is somewhat unique. Some investigations might only require a week to complete, but others could take months. Here are some factors that can impact the length of an investigation:

- The expertise of the detectives
- The number of computers being searched
- The amount of storage detectives must sort through (hard drives, CDs, DVDs and thumbdrives)
- Whether the suspect attempted to hide or delete information
- The presence of encrypted files or files that are protected by passwords

Timeline Forensics Analysis and Investigation Computer forensics needs applying technology to answer legal queries. Arranging events chronologically could be a great way of telling a transparent, compact story. As valuable as date- and time-based info typically is to a case, none of the leading forensic tools offer usable date and time oriented tools. Log2timeline is a superb tool for extracting date and time primarily based info from digital proof. In fact, the quantity of knowledge it extracts will overwhelm the examiner.

Most pc rhetorical timeline tools concentrate on either assortment or presentation of timeline information.

But few choices exist for storing the big quantity of information, much less managing it throughout the analysis process, through which a data set is reduced to its most representative and relevant set of facts. By organizing

ISSN 2394 - 7780

timeline information so it will either be viewed in outline or “drilled down” well, the sense of overwhelm that computer forensics examiners experience while analyzing the large information sets that accompany timeline analysis is reduced. This approach to organizing {the information|the info|the information} has evidenced effective in increasing the utility of alternative giant data sets, such as intrusion detection databases.

A device for log2timeline output Associate in Nursingd an Apache-MySQL-PHP net application square measuredelineated . What is required could be a timeline info that reduces overwhelm by summarizing information, will increasetargeted analysis by supporting filtering of the info set, and will increase understanding of the info by supporting automated and manual highlighting. Home improvement TV shows like square away that scale back litter focus initial on eliminating further stuff, then on organization of the items that stay. Since we don't have the option of eliminating evidence, let's focus on the evidence's organization. Tapestry is fabric woven from multiple lines together. In a similar manner, the log2timeline import script and info application are going to be wont to organize our timelines so we are able to higher see patterns. If Tapestry does a good enough job of organizing our data set, we can give it the reward for a job well done—more work. Where we might have used log2timeline and existing plugins to investigate one or many systems, we are able touse Tapestry to investigate atiny low subnet.

FILE SYSTEM FORENSICS AND INVESTIGATION

Most digital evidence is stored within the computer's file system, but understanding how file systems work is one of the most technically challenging concepts for a digital investigator because there exists little documentation. Now, security expert Brian Carrier has written the definitive reference for everyone who wants to understand and be able to testify about how file system analysis is performed.

Carrier begins with an overview of investigation and computer foundations and then gives an authoritative, comprehensive, and illustrated overview of contemporary volume and file systems: Crucial information for discovering hidden evidence, recovering deleted data, and validating your tools. Along the way, he describes data structures, analyzes example disk images, provides advanced investigation scenarios, and uses today's most valuable open source file system analysis tools—including tools he personally developed. Coverage includes

1. Preserving the digital crime scene and duplicating hard disks for "dead analysis"
2. Identifying hidden data on a disk's Host Protected Area (HPA)
3. Reading source data: Direct versus BIOS access, dead versus live acquisition, error handling, and more
4. Analyzing DOS, Apple, and GPT partitions; BSD disk labels; and Sun Volume Table of Contents using key concepts, data structures, and specific techniques
5. Analyzing the contents of multiple disk volumes, such as RAID and disk spanning
6. Analyzing FAT, NTFS, Ext2, Ext3, UFS1, and UFS2 file systems using key concepts, data structures, and specific techniques
7. Finding evidence: File metadata, recovery of deleted files, data hiding locations, and more
8. Using The Sleuth Kit (TSK), Autopsy Forensic Browser, and related open source tools

When it comes to file system analysis, no other book offers this much detail or expertise. Whether you're a digital forensics specialist, incident response team member, law enforcement officer, corporate security specialist, or auditor, this book will become an indispensable resource for forensic investigations, no matter what analysis tools you use.

DATA CATEGORIES

As we examine each of the different file system types in this part of the book, it will be useful to have a basic reference model so that the different file systems can be more easily compared. Having such a reference model also makes it easier to determine where your evidence may be located. For example, a reference model makes it easier to compare the difference between FAT and Ext3 file systems. For this basic model, we will use five categories: file system, content, metadata, file name, and application. All data in a file system belong to one of the categories based on the role they play in the file system. We will use these categories throughout this book when describing file systems, although some file systems, namely FAT, cannot be applied to this model as easily as others can. The tools in The Sleuth Kit (TSK) are based on these same categories. The file system category contains the general file system information. All file systems have a general structure to them, but each instance of a file system is unique because it has a unique size and can be tuned for performance. Data in the file system category may tell you where to find certain data structures and how big a data unit is. You can think of

ISSN 2394 - 7780

data in this category as a map for this specific file systemThe content category contains the data that comprise the actual content of a file, which is the reason we have file systems in the first place. Most of the data in a file system belong to this category, and it is typically organized into a collection of standard-sized containers. Each file system assigns a different name to the containers, such as clusters and blocks, and I will use the general term data units until we discuss specific file systems. The metadata category contains the data that describe a file; they are data that describe data. This category contains information, such as where the file content is stored, how big the file is, the times and dates when the file was last read from or written to, and access control information. Note that this category does not contain the content of the file, and it may not contain the name of the file. Examples of data structures in this category include FAT directory entries, NTFS Master File Table (MFT) entries, and UFS and Ext3 inode structures.

SOCIAL MEDIA FORENSICS AND INVESTIGATION

Mobile devices are increasingly utilized to access social media and instant messaging services, which allow users to communicate with others easily and quickly. However, the misuse of social media and instant messaging services facilitated conducting different cybercrimes such as cyber stalking, cyber bullying, slander spreading and sexual harassment. Therefore, mobile devices are an important evidentiary piece in digital investigation. In this chapter, we report the results of our investigation and analysis of social media and instant messaging services in Firefox OS. We examined three social media services (Facebook, Twitter and Google+) as well as three instant messaging services (Telegram, OpenWapp and Line). Our analysis may pave the way for future forensic investigators to trace and examine residual remnants of forensics value in FireFox OS.

In social media experiment, we were focusing the investigation for 2 social media applications and 3 social media mobile web. There were several forensic worth of evidence that we were trying to recover and trace. First, we have explored the residual artifacts generated by application and URL involved for mobile web. Second, we were trying find any ID name that able to be captured after we login into social media. Third, we have searched for any credential involving username and password after login process. Forth, we have traced back what activities that has been captured in the images. Lastly we have checked for the data remnant and left over after complete uninstallation of the application.

Investigative methods when collecting evidence from social media vary substantially from traditional digital forensic techniques creating new legal and procedural challenges.

Technology is rapidly changing the world. It has changed how we access and share information and how we communicate. Mobile devices and texting, free communication and file sharing solutions (think Skype and Dropbox), and social networks (such as Facebook, Twitter, and blogs) make it easier than ever for people to share information and express opinions.

As today’s digital world continues to evolve, so must the way we conduct cyber investigations. Sources of evidence are growing rapidly. For those who fail to keep up, collecting and authenticating evidence during a cyber investigation will prove to be a difficult task. For those with a clear understanding of how to leverage advances in technology and the wealth of information available online, the evidence collected during a cyber investigation can help create a solid case.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

A STUDY ON CYBER LAW'S AND CYBER CRIME W.R.T INFORMATION TECHNOLOGY

Shraddha Prasad Kokate and Dr. Pradhnya M Wankhade
Department of Information Technology, J. E. S College of Commerce, Science & Information Technology

ABSTARCT
The internet technology has been using by the few people for criminal activities like unauthorized access to other's network, scams etc. These criminal activities or the offense/crime related to the internet is termed as cyber crime. In order to stop or to punish the cyber criminals the term "Cyber Law" was introduced. We can define cyber law as it is the part of the legal systems that deals with the Internet, cyberspace, and with the legal issues. It covers a broad area, encompassing many subtopics as well as freedom of expressions, access to and utilization of the Internet, and online security or online privacy.We can define "Cyber Crime" as any malefactor or other offences where electronic communications or information systems, including any device or the Internet or both or more of them are involved.Cyber Crimes should be passed so the grey areas of the law can be removed.

Keywords: Cyber Law, Information Technology, The Information Technology Act of India, 2000 , Safety in Cyberspace, Cyber Crime.

INTRODUCTION

The invention of Computer has made the life of humans easier, it has been using for various purposes starting from the individual to large organizations across the globe. In simple term we can define computer as the machine that can stores and manipulate/process information or instruction that are instructed by the user. Most computer users are utilizing the computer for the erroneous purposes either for their personal benefits or for other's benefit since decades. This gave birth to "Cyber Crime". This had led to the engagement in activities which are illegal to the society. We can define Cyber Crime as the crimes committed using computers or computer network and are usually take place over the cyber space especially the Internet. Now comes the term "Cyber Law". It doesn't have a fixed definition, but in a simple term we can defined it as the law that governs the cyberspace. Cyber laws are the laws that govern cyber area. Cyber Crimes, digital and electronic signatures, data protections and privacies etc are comprehended by the Cyber Law. The UN's General Assembly recommended the first IT Act of India which was based on the "United Nations Model Law on Electronic Commerce" (UNCITRAL) Model.

CYBER LAW

In any field of human activity Success leads to crime that needs mechanisms to control it. The law is as stringent as its enforcement. Cyber law is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyber laws is a very technical field and that it does not have any bearing to most activities in Cyberspace. It is an endeavour to integrate the challenges presented by human action on the Internet with legacy system of laws applicable to the physical world. Cyber law plays a very important role in this new epoch of technology. It is important as it is concerned to almost all aspects of activities and transactions that take place either on the internet or other communication devices. Whether we are aware of it or not, but each action and each reaction in Cyberspace has some legal and Cyber legal views.

To aware the people about the cyber law awareness program is conducted with following points

- One should read the cyber law thoroughly.
- Basic knowledge of Internet and Internet's security.
- Read cyber crime's cases. By reading those cases one can be aware from such crimes.
- Trusted application from trusted site can be used for protection of one's sensitive information or data.
- Technology's impact on crime.

INFORMATION TECHNOLOGY

Information technology deals with information system, data storage, access, retrieval, analysis and intelligent decision making. Information technology refers to the creation, gathering, processing, storage, presentation and dissemination of information and also the processes and devices that enable all this to be done. The misuse of the technology has created the need of the enactment and implementation of the cyber laws. Many information technology (IT) professionals lacked awareness of an interest in the cyber crime. In many cases, law

ISSN 2394 - 7780

enforcement officers have lacked the tools needed to tackle the problem; old laws didn't quite fit the crimes being committed, new laws hadn't quite caught up to the reality of what was Information is a resource which has no value until it is extracted, processed and utilized. Information technology deals with information system, data storage, access, retrieval, analysis and intelligent decision making. Information technology refers to the creation, gathering, processing, storage, presentation and dissemination of information and also the processes and devices that enable all this to be done. Information technology stands firmly on hardware and software of a computer and telecommunication infrastructure. This is the only one side but today the challenges for the whole world like cyber crimes and more over cyber terrorism. The misuse of the technology has created the need of the enactment and implementation of the cyber laws. As the new millennium dawned, the computer has gained popularity in every aspect of our lives. This includes the use of computers by persons involved in the commission of crimes. Today, computers play a major role in almost every crime that is committed. Every crime that is committed is not necessarily a computer crime, but it does mean that law enforcement must become much more computer literate just to be able to keep up with the criminal element.

THE INFORMATION TECHNOLOGY ACT OF INDIA, 2000

The Information Technology Act, 2000 (also known as ITA-2000, or the IT Act) is an act of the Indian Parliament (no 21 of 2000), it was notified on 17th October 2000. It is the most important law in India that deals with the digital crimes or cyber crimes and electronic commerce.

Following are the sections under IT Act, 2000

1. Section 65- Temping with the computers source documents

Whoever intentionally or knowingly destroy, conceal or change any computer's source code that is used for a computer, computer program, and computer system or computer network.

Punishment:

Any person who involves in such crimes could be sentenced upto 3 years imprisonment or with a fine of Rs.2 lakhs or with both.

2. Section 66- Hacking with computer system, data alteration etc

Whoever with the purpose or intention to cause any loss, damage or to destroy, delete or to alter any information that resides in a public or any person's computer. Diminish its utility, values or affects it injuriously by any means, commits hacking.

Punishment:

Any person who involves in such crimes could be sentenced upto 3 years imprisonment, or with a fine that may extend upto 2 lakhs rupees, or both.

3. Section 66A- Sending offensive messages through any communication services

Any information or message sent through any communication services this is offensive or has threatening characters.

Any information that is not true or is not valid and is sent with the end goal of annoying, inconvenience, danger, insult, obstruction, injury, criminal intention, enmity, hatred or ill will.

Any electronic mail or email sent with the end goal of causing anger, difficulty or mislead or to deceive the address about the origin of the messages.

Punishment:

Any individual found to commit such crimes under this section could be sentenced upto 3years of imprisonment along with a fine.

4. Section 66B- Receiving stolen computer's resources or communication devices dishonestly

Receiving or retaining any stolen computer, computer's resources or any communication devices knowingly or having the reason to believe the same.

Punishment:

Any person who involves in such crimes could be sentenced either description for a term that may extend up to 3 years of imprisonment or with a fine of rupee 1 lakh or both.

5. Section 66C- Identify theft

Using of one's digital or electronic signature or one's password or any other unique identification of any person is a crime.

ISSN 2394 - 7780

Punishment:
Any person who involve in such crimes could be sentenced either with a description for a term which may extend up to 3 years of imprisonment along with a fine that may extend up to rupee 1 lakh.

6. Section 66D- Cheating by personaion by the use of computer's resources
Whoever tries to cheats someone by personating through any communication devices or computer's resources shall be sentenced either with a description for a term that may extend up to 3 years of imprisonment along with a fine that may extend up to rupee 1 lakh.

7. Section 66E- Privacy or violation
Whoever knowingly or with an intention of publishing, transmitting or capturing images of private areas or private parts of any individual without his/her consent, that violets the privacy of the individual shall be shall be sentenced to 3 years of imprisonment or with a fine not exceeding more than 2 lakhs rupees or both**.**

SECTION 67- TRANSMITTING OR PUBLISHING OBSCENE MATERIALS IN ELECTRONIC FORM
Whoever transmits or publishes or cause to publish any obscene materials in electronics form. Any material that is vulgar or appeal to be lubricious or if its effect is for instance to tends to corrupt any individual who are likely to have regard to all relevant circumstances to read or to see or to hear the matter that contained in it, shall be sentenced on the first convict with either description for a term that may extend up to five years of imprisonment along with a fine which may extend up to 1 lakh rupee and in the second or subsequent convict it can be sentenced either description for a term that may extend up to ten years along with a fine that may perhaps extend to two lakhs rupees.

SECTION 67A- TRANSMITTING OR PUBLISHING OF MATERIALS THAT CONTAINS SEXUALLY EXPLICIT CONTENTS, ACTS ETC IN ELECTRONICS FORM
Whoever transmits or publishes materials that contains sexually explicit contents or acts shall be sentences for either description for a term which may extend upto 5 years or imprisonment along with a fine that could extend to 10 lakhs rupees in the first convict. And in the event of the second convict criminal could be sentenced for either description for a term that could extend up to 7 years of imprisonment along with a fine that may extend up to 20 lakhs rupees.

SECTION 67B- TRANSMITTING OR PUBLISHING OF MATERIALS THAT DEPICTS CHILDREN IN SEXUALLY EXPLICIT ACT ETC IN ELECTRONICS FORM
Whoever transmits or publishes any materials that depict children in sexually explicit act or conduct in any electronics form shall be sentenced for either description for a term which may extend to 5 years of imprisonment with a fine that could extend to rupees 10 lakhs on the first conviction. And in the event of second conviction criminals could be sentenced for either description for a term that could extend to 7 years along with a fine that could extend to rupees 10 lakhs.

SECTION 69- POWER TO ISSUE DIRECTION FOR MONITOR, DECRYPTION OR INTERCEPTION OF ANY INFORMATION THROUGH COMPUTER'S RESOURCES
I. Where the Central government's or State government's authorized officers, as the case may be in this behalf, if fulfilled that it is required or expedient to do in the interest of the integrity or the sovereignty, the security defence of our country India, state's security, friendly relations with the foreign states for preventing any incident to the commission of any cognizable offences that is related to above or investigation of any offences that is subjected to the provision of sub-section (II). For reasons to be recorded writing, direct any agency of the appropriate government, by order, decrypt or monitor or cause to be intercept any information that is generated or received or transmitted or is stored in any computer's resources.

II. The safeguard and the procedure that is subjected to such decryption, monitoring or interception may carried out, shall be such as may be prescribed.

III. The intermediaries, the subscribers or any individual who is in the charge of the computer's resources shall call upon by any agencies referred to the sub-section (I), extends all services and technical assistances to:

a) Providing safe access or access to computer's resources receiving, transmitting, generating or to store such information or

b) Decrypting, intercepting or monitoring the information, as the case might be or

c) Providing information that is stored in computer.

ISSN 2394 - 7780

IV. The intermediaries, the subscribes or any individual who fails to help the agency referred in the sub-section (III), shall be sentenced for a term that could extend to 7 years of imprisonment and also could be legally responsible to fine.

SAFETY IN CYBERSPACE

The following point mention that how one can provide the security in cyber space:-

- If possible always use a strong password and enable 2 steps or Two-step authentication in the webmail. It is very important in order to make your webmail or your social media account secured.
- Guideline of strong password:
- Password should be of minimum eight characters.
- One or more than one of lower case letter, upper case letter, number, and symbol should be included.
- Replace the alike character.
- Example- instead of O we can use 0, instead of lower case l we can use I etc.
- Thing need to avoid while setting the password:
- Never use a simple password that can easily be decrypt
  Example- password
- Personal information should never set as a password.
- Repeating characters should be avoided.
  Example- aaaacc
- Using of same password in multiple sites should be avoided.

The two step authentication can be provided by considering following points:

- Never share your password to anyone.
- Never send or share any personal information like bank account number, ATM pin, password etc over an unencrypted connection including unencrypted mail. Websites that doesn't have the lock icon and https on the address bar of the browser are the unencrypted site. The "s" stands for secure and it indicates that the website is secure.
- Don't sign to any social networking site until and unless one is not old enough.
- Don't forget to update the operating system.
- Firewalls, anti- virus and anti-spyware software should be installed in ones PC and should be regularly updated.
- Visiting to un-trusted website or following a link send by an unknown or by an un-trusted site should be avoided.
- Don't respond to spam.
- Make sure while storing sensitive data in the cloud is encrypted.
- Try to avoid pop-ups: Pop-ups sometimes comes with malicious software. When we accept or follow the pop-ups a download is performed in the background and
- that downloaded file contains the malware or malicious software. This is called drive-by download. Ignore the pop-ups that offer site survey on ecommerce sites or similar things as they may contain the malicious code.

CYBER CRIME

We can describe "Cyber Crime" are the offences or crimes that takes place over electronic communications or information systems. These types of crimes are basically the illegal activities in which a computer and a network are involved. Due of the development of the internet, the volumes of the cybercrime activities are also increasing because when committing a crime there is no longer a need for the physical present of the criminal. The unusual characteristic of cybercrime is that the victim and the offender may never come into direct contact.

ISSN 2394 - 7780

Cybercriminals often opt to operate from countries with nonexistent or weak cybercrime laws in order to reduce the chances of detection and prosecution.

Cyber Crime can be classified into four major categories.

They are as follows:

a) Cyber Crime against individuals: Crimes that are committed by the cyber criminals against an individual or a person.
A few cyber crime against individuals are:

1] **Email spoofing**: This technique is a forgery of an email header. This means that the message appears to have received from someone or somewhere other than the genuine or actual source .

2] **Spamming**: Email spam which is otherwise called as junk email. It is unsought mass message sent through email.

3] **Cyber defamation**: Cyber defamation means the harm that is brought on the reputation of an individual in the eyes of other individual through the cyber space .

4] **IRC Crime (Internet Relay Chat)**: IRC servers allow the people around the world to come together under a single platform which is sometime called as rooms and they chat to each other.

b) Cyber Crime against property: These types of crimes includes vandalism of computers, Intellectual (Copyright, patented, trademark etc) Property Crimes Online threatening etc .property crime includes:

1] **Software piracy -** It can be describes as the copying of software unauthorizedly.

2] Copyright infringement - It can be described as the infringements of an individual or organization's copyright.

3] Trademark infringement- It can be described as the using of a service mark or trademark unauthorizedly

c) Cyber Crime against organization: Cyber Crimes against organization are as follows:

1] **DOS attack-** In this attack, the attacker floods the servers,

2] **Email bombing**: It is a type of Net Abuse, where huge numbers of emails are sent to an email address in order to overflow mailbox.

3] **Salami attack**: The other name of Salami attack is Salami slicing. In this attack, the attackers use an online database in order to seize the customer's information like bank details, credit card details etc

d) Cyber Crime against society: Cyber Crime against society includes:

1] **Forgery**: Forgery means making of false document, signature, currency, revenue stamp etc.

2] **Web jacking**: The term Web jacking has been derived from hi jacking

CONCLUSION

Cybercrime has become great threats to mankind. Protection against cybercrime is a vital part for social, cultural and security aspect of a country. Our main purpose of writing this paper is to spread the content of cyber crime among the common people. At the end of this paper" **A study on Cyber Law's and Cyber Crime w.r.t Information Technology".** we want to say cyber crimes can never be acknowledged. If anyone falls in the prey of cyber attack, please come forward and register a case in your nearest police station. If the criminals won't get punishment for their deed, they will never stop

REFERENCES

1. Cyber Crimes and Real World Society by Lalitha Sridhar.

2. Cyber Law and Information Technology by Talwanth Singh Addl.Distt. And Sessions Judge, Delhi

3. Information Technology Act, 2000

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER CRIME & CRIMINAL LAW

Chinmayi S. Vaidya
F. G. Naik College of Arts, Science (IT) and Commerce

ABSTRACT
Cybercrime is defined as a crime in which a computer is used as a tool to commit an offense .Cybercrimes are responsible for the interruption of normal computer functions.which may lead to fraud. This research paper covers the following topics of Cybercrimes :- the definition, why they occur, laws governing them, cybercrime prevention procedures.The number of people using internet is increasing day by day which has led to the rise in cybercrime.Lack of knowledge among people contributed to the growth in cybercrime .

Keywords: CyberCrime, Hacking, Internet, Cyber Laws, Breach

INTRODUCTION

With the advent of internet, a number of crimes related to the same have emerged. The space within which the internet operates is known as cyber space. The term cyberspace was originally coined by science fiction writer William Gibson.It is also called as "Hacking".

Internet is major source of Cyber Crime. This includes anything from downloading to stealing millions of dollars from online bank accounts. Cybercrime also includes other offenses, such as making viruses on other computers or stealing confidential information

Following are the examples of cybercrime.
1) Internet Fraud.

2) Spams.

3) Cyberbullying.

4) Gathering Information Illegally.

5) Identity Theft.

6) Phishing scams.

7) Hate Crimes.

Defining the Problem

We are duscussing about CyberCrimes.There are so many ways to define CyberCrime.Basic definition of CyberCrime is to steal or process information of an individual without their knowledge using computer and the internet.Some popular definitions are:

- **Webopedia**:-Cyber crime encompasses any criminal act dealing with computersand networks (called hacking)
  (https://www.webopedia.com/TERM/C/cyber_crime.html)
- **ResearchGate:-**Cybercrime is defined as crimes committed on the internet using the computer as either a tool or a targeted victim.

  (https://www.researchgate.net/publication/265350281_Cybercrime_definition)
- **SearchSecurity**Cybercrime is any criminal activity that involves a computer, networked device or a network.

  https://searchsecurity.techtarget.com/definition/cybercrime
- **BritaniccaCybercrime**, also called **computer crime**, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealingidentities, or violating privacy.

  https://www.britannica.com/topic/cybercrime

Laws of cybercrimes

In this section of this paper we'll discusses different Laws that governs cybercrime

ISSN 2394 - 7780

CYBER LAWS IN INDIA

1. **IT Act of India, 2000** The IT Act of India was passed by the Indian Government in May 2000.it contains the various cyber laws of the state. It is the law that deals with cybercrime and e-commerce. The Act was based on the United Nations Model Law on Electronic commerce. The Act aims to provide legal structure for all electronic transactions in India. Chapter IX of the Act states about the various penalties for cybercrime offences. The Act also talks about the compensation for the victims affected by cybercrime which does not exceed Rs. 100, 00,000. The Act talks about the various offences that can be classified as cybercrime.

2. **National Cyber Security Policy, 2013** This act was formalized by the Indian Government in 2013. It was taken as a step to counter cybercrime. The purpose of this document is to ensure a secure a safe cyberspace for the citizens of India. The policy states that education and training programmes are required for reducing the cybercrime rate. The policy aims to create 500,000 professionals within 2018 through advanced training and skill development programs.

3. Cyber Swachhta Kendra The Cyber Swachhta Kendra is an initiative taken up by the Government of India to create a secure cyberspace by detecting botnet infections and to enable cleaning and securing systems of users so as to prevent further infections. This policy is set up in accordance with the objectives of the 'National Cyber Security Policy.

Cyber Laws in United States

Federal Government Regulation

There are three main federal cybersecurity regulations –

– 1999 Gramm-Leach-Bliley Act

– 2000 Homeland Security Act, which included the Federal Information Security Management Act (FISMA)

Recent Federal Laws

Cybersecurity data Sharing Act (CISA) – Its objective is to enhance cybersecurity within the us through increased sharing of knowledge regarding cybersecurity threats, and for alternative functions.The law permits the sharing of web traffic data between the U.S.government and technology and manufacturing companies. The bill was introduced in the U.S.Senate on July ten, 2014, and passed within the Senate Oct twenty seven, 2015.

Federal Exchange information Breach Notification Act of 2015: This bill needs a insurance exchange to advise every individual whose personal info is thought to own been nonheritable or accessed as a results of a breach of security of any system maintained by the exchange as before long as potential however not later than sixty days when discovery of the breach.

PREVENTION:

How to protect yourself against cybercrime

1. Use a full-service internet security suite

Norton Security provides period protection against existing and rising viruses,worms,Trojan Horses i.e malware as well as ransomware and helps shield your personal and monetary info once you go surfing

2. Use strong passwords

Don't repeat your passwords on totally different sites, and alter your passwords often.

Make them complex. That means using a combination of at least 10 letters, numbers, and symbols.

3. Keep your software updated

It is very important to update your operating System to remove patches and loopholes.

Patching those exploits and flaws will create it less probably that you'll become a law-breaking target.

4. Manage your social media settings

Keep your personal and private information secure. Social media cybercriminals can get your information on a just one click.

5. Strengthen your home network

It's a good idea to use virtual private network. A VPN will encrypt all traffic.

If cybercriminals do manage to hack your communication line, they won't intercept anything but encrypted data.

It's an honest plan to use a VPN whenever you a public

ISSN 2394 - 7780

6. Keep up to date on major security breaches
find out what info the hackers accessed and alter your positive identification forthwith.

7. Know what to do if you become a victim
If you are a victim of a cybercrime, you immediately contact to the local police and, in some cases, the FBI and the Federal Trade Commission. If you think cybercriminals have stolen your identity. These are among the steps you should consider.

Contact the companies and banks where you know fraud occurred.

Place fraud alerts and get your credit reports.

Report identity theft to the FTC.

Try Other Relevant ToolsPlagiarism Checker Grammar Checker Spell Checker

FINDINGS

Findings on internet usage

94.25% respondents download various content from the internet, while only 5.8% do not download anything. 68.1% of the total respondents admitted that they downloaded movies, 85.3% of the total respondents download music, 66.25 downloaded various study material while only 39.2% downloaded general content such as Apks, books, software, games etc. 27.5% respondents download content very frequently. 43% respondents download quite often. 20.3% respondents download less frequently. 7.7% rarely download any content while only 1.4% never downloads anything.

FINDINGS ON CYBERCRIME AWARENESS AND SAFETY

25.1% respondents are very aware about cybercrime. 51.7% know about cybercrime. 21.7% don't know very well about cybercrime, while only 1.4% doesn't know anything about cybercrime.

Findings on awareness on anti cybercrime schemes by government Only 5.3% respondents are very well aware of the anti cybercrime schemes. 18.3% just know about it. 31.3% have heard about it. 30.8% don't know very well and have little information regarding it. 14.4% don't know about it. 53.4% of the total respondents know about the Information Technology Act, 2000. 48.1% of the total respondents know about the National Cyber Security policy, 2013. 18.8% of the total respondents know about the Cyber Swachhta Kendra.

Findings on trust on the existing Cybercrime laws Only 9% strongly agree that the cybercrime laws are strong enough to cybercriminals. 39.6% respondents agree that they are effective to control cybercriminals. 18.5% respondents disagree that the laws are effective while 6.3% strongly disagree that the laws are powerful enough to control and stop the cybercriminals. 26.6% respondents are on both sides, they are neutral. 15.8% strongly agree that the cybercrime can be completely eliminated in Kerala. 41.9% agree that the cybercrime can be eliminated in Kerala. However 14.4% disagree to it and 2.7% strongly disagree to the belief that the cybercrime can be eliminated in Kerala. The remaining 25.2% are neutral to this thought
(https://acadpubl.eu/hub/2018-119-16/1/130.pdf)

CONCLUSION

In Cybercrime internet is weapon to steal the information. Only remedy to the Cyber Crime is awareness among people.This basic awareness can help prevent potential cybercrimes against them.Training programs for youngsters helps a lot to reduce Cyber Crimes.The only possible step is to make people aware of their rights and duties and to make a law which is more strict.

REFERENCES

- (International Journal of Pure and Applied Mathematics Volume 119 No. 16 2018, 1353-1360 ISSN: 1314-3395 , page no-3,Sreehari A, K.J Abinanth, Sujith B, Unnikuttan P.S, Mrs.Jayashree)
- http://www.cameron.edu/search?cx=014940064196211141993%3Aottnfsmx9t0&cof=FORID%3A11&q=2_Hackers.docx
- Laws Relating to Cyber Crimes: Theories and Legal Aspects by Aqua Raza https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3066200
- https://techterms.com/definition/cybercrime
- https://acadpubl.eu/hub/2018-119-16/1/130.pdf
- https://www.researchgate.net/publication/322086317_CyberCrime_and_Security
- https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER THREAT FOR SMARTPHONE'S

Avanish Vishwakarma

ABSTRACT
In this world right now, Mobile devices or Smartphone's has become the most popular devices in recent past years. Mobile devices have the functionality not only of mobile phones but also some computers functionality such as data storage, an interaction between people i.e for communication purpose, or data processing. Mobile devices which are also used for multimedia , web surfing or web browsing, video call , Wi-Fi for internet connection and data transferring, Bluetooth which is used to connect car and also for wireless connection such as Headphones or speakers, General Packet Radio Services (GPRS) for 2G and 3G cellular networks used by previous 3G mobile phones. As the number of mobile user increases, the chances of susceptibility services are also increased. This results in an increase in attacks on personal data. In this paper, our goal is to educate the user about What is Mobile security? What are its consequences? What is the threat or risk to mobile data? What is the high level of attack? We have to target existing or previous technique and overcome it to protect mobile devices.

Keywords: Smartphone, Data Processing, General Purpose Radio Services (GPRS).

1. INTRODUCTION

In this introduction, we will understand about mobile security theory that is mostly used nowadays. Mobile security is an approach that gained a lot of importance ever since the first ever mobile Operating System(OS) i.e 'Symbian' was launched by Nokia in the year 1998. Symbian OS was continuing to achieve importance with enormous usage of Android OS.

Smartphone Security also known as Mobile Device Security has become more and more important in ubiquitous and mobile computing. Especially, concern with the privacy of the mobile device which is supposed to the assurance of personal, private information and business information that are now saved on smartphones. As the reliability of the mobile device increases every year, the idea of mobile device security become more important than ever.

Mobile computing is an expanding industry. The challenge has started when mobile devices replaced regular computers and laptops to do multitasking, social communicating, and business management through these tiny devices. Security had always been a consequence with computers, laptops or desktops. With the increasing number of mobile devices communication around the world, Cyber attacker or Hacker have drawn their eyes and targets on mobile devices.

In the world of wireless and mobile devices is expanding day-to-day, with many individuals relying entirely on their wireless devices in the organization and in the home. The rising use of mobile devices claims that organizations or an institute having more knowledge in securing and assuring this growing technology and resolve how to save their mobile devices.

2. WHAT IS A MOBILE DEVICE?

A mobile device or Smartphone is a computing or ubiquitous device which are compact in size that is small enough to hold and use with hand. Personal Device Assistant (PDA) and smartphones are two popular mobile devices. In most cases, the mobile device has an LCD or OLED display which provide a touch screen interface with onscreen buttons and keyboard on Smartphone's or with some older generation mobiles which have physical button and keyboard.

Mobile devices are a portable device such as tablets, phablets, laptop and etc. A mobile device may run on a mobile operating system such as Android, iOS, Windows. In the future or coming years, Fushia OS will be the new operating system for Smartphone's which is in a developing stage by Google. Major global manufacturer of mobile devices are Apple, Samsung, Xiaomi, Vivo, Oppo. Oneplus, Moto and etc.

3. WHAT IS MOBILE DEVICE SECURITY?

Mobile security is protection or preservation of the data on the portable mobile device such as Smartphone's, tablets, phablets, or laptop and networks connected to them. In this background, the main target of the mobile device on smartphones which are generally owned compared to other devices. In concern to the operating system of the mobile devices, the risk is made against the system and increasingly affects the user's and company's security. The risk or threat could be many types such as Malware(Trojan Horse, Ransomware,

ISSN 2394 - 7780

Worm), unauthorized access, device theft and etc. There could be the cyber attack of any type due to constantly increasing of portable devices which make the mobile security very important and very vulnerable as well.

4. THREATS AND RISK FOR MOBILE SECURITY

4.1 Application Cloning.

Android applications like Instagram, Pokémon GO which was not available in some of the countries which lead to hackers to develop the clone application with some change in code in the form of APK files in their server which can harm your device or stools your personal data from your mobile devices. Latest examples were Pokémon GO which was first released in form of APK files through some links, it leads the user to download the APK and install it on their devices. After installing it ask the device for permission and user blindly give access to its location, media files, contact and much more which become easier for hackers to have full access to your personal sensitive data, banking information and etc.

Further, Niantic which is American software based company known for its Augmented Reality games like Pokémon GO. The Niantic company later released the application to the trusted app store in some other countries preventing users to download APK files.

So it is safer to download any application from Google Play Store in Android or App Store in Apple rather than a third-party store.

4.2 Mobile Ransomware.

Mobile Ransomware is type malicious software program that affects mobile devices. A cybercriminal can use ransomware to steal the sensitive information or locking mobile devices and then demands for payment to return the users information or unlocking the mobile device. Ransomware was on the top in the list of Mobile Security and this year also it is too vulnerable.

The best way to escape this malicious program by downloading the application for a mobile device through a trusted app store and keep your system and application updated.

4.3 SMS bases Attack.

Nowadays, there are two-factor or two-way authentication via SMS which is recommended for safer Login. So after you enter the username and password we must submit the OTP(One Time Password) code sent via text to complete the Authentication. OTP(One Time Password) is code which is valid only for 1 login period or valid till specific period. Because of redirection to another webpage or interception, hackers can use SMS without needing the actual device.

SMS is not safe at some stage so there are other alternatives for two-factor authentications. The application like Google Authenticator is good options. Google Authenticator is a software token and uses 2-step Verification using TOTP(Time Based One Time Password) which generates six or eight digit code with the addition to username and password.

4.4 DATA LEAKAGE.

Data leakage is unintentional or intentional releasing of sensitive, private, and confidential information to untrusted user or environment. Data leakage also called as Data Breaching. In the previous year, there is a campaign started as "#Deletefacebook" due to in 2014, there is an application called "My Digital Life" developed by Alexander. So when there is any notification in facebook, the user clicks on that notification and granted all permission to any of the application which cause server of a third-party server to collect all the information about the user. The total count of 50+ Million user's data was leaked by Facebook. The founder of Facebook Mark Zuckerberg said himself about its data leaks. Nowadays, it said that "Data is the new Currency" i.e the big company sales your data to another company and get paid for user data.

The better way to protect your own data by seeing the permission ask by application and grant permission only when it is used.

4.5 Unsecured Wi-Fi

Today in the world of free wireless connection no one wants to burn or use their cellular network data. Nowadays people usually get free Wi-Fi or public Wi-Fi networks and connecting them at a coffee shop, Shopping Malls, Railways stations, Airports and etc to make use of free Wi-Fi.

While using public networks or unsecured Wi-Fi the hacker can monitor your usage and steals your data between the websites you visit via that public network and this attack is also known as Man In The Middle Attack. Using unsecured Wi-Fi connection an attacker can captures your accounts details like user ID and password, it can gain access to your computer and mobile device which can launch malware attack on your

ISSN 2394 - 7780

device or install Trojan Horse in you logged into and use it for bad purpose, Redirect you to malicious website or phishing webpage, where you might give your personal information.

Better to be safe while using unsecured Wi-Fi avoid accessing to log in your account for financial information social media account and online banking or online shopping and etc.

5. SOLUTION TO ENHANCED MOBILE SECURITY

5.1 Secure Mobile Device From Malware

The best way to protect your device against any of the threat and risk by don't open any suspicious link or emails which are in 'HTTP' format rather than 'https' and do not download any applications or any content from unreliable sources. We should have no problem at all if we don't do any this mentioned above also make sure that to install latest software update available for your device because it might feature a security patch for latest malware or ransomware out there.

5.2 Secure Mobile Device Data

The user has some sensitive and important data in their device thankfully android offer features to secure your data. First, you need to encrypt your device as it is not enabled to all of the devices. By encrypting your device, it will encrypt all account details, settings, downloaded applications, applications data, media files, and other files as well. Once your device encrypted your device data only decrypted by the PIN and Password set in your device.

5.3 Secure Mobile Device Users Privacy

While securing your device from malware and securing your data is important, securing your privacy is also very important. First lock your mobile device properly by using PIN, Password, Pattern, Fingerprint scanner, Iris Scanner, Face Unlock and other Biometric. Other than that you should create a separate account in your mobile device as Guest Account so that you can hand over your device to your friend without worrying about the privacy just by switching the account. You must also enable 2-step verification in a different account in any applications like Facebook, Instagram, Google, Snapchat and etc.

5.4 Secure Mobile Device From Application

The above mention techniques are to protect your device but there are some third-party applications from the trusted app store which can be used to protect your device. Applications like 'Privacy Guard', so if anyone trying to use or peep into your device, this application brings features to hide all the sensitive data and application. You should also use VPN application on unsecured Wi-Fi networks since anyone on open unsecured Wi-Fi network can try and get access to your data thus VPN application can access you log content and do lot more. Last but not the least, install an App Locker to your mobile device which can lock your application and local files with the PIN, Password.

6. CONCLUSION

All in all, smartphone and mobile devices provide satisfaction and increased efficiency in today's mobile industries. They are vast exposure to data and information that could not easily be exposed otherwise, with care and captiousness, all above threats and risk could be prevented, protected, managed or at least minimize. With increase advantage of using third party application, user review is always a better way to check the application authenticity.

7. REFERENCES

- https://www.researchgate.net/publication/309675787_Research_Paper_for_Mobile_Devices_Security
- Mobile devices Security Fall Quarter 2014-2015

  Name : Samaher ALJudaibi

  Instructor: Mr. Ellis Confer

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER LAWS AND CRIMES IN INTERNET TODAY

Pooja R. Dhumal
JVM's Mehta Degree College, Navi Mumbai

ABSTRACT

Today, law-breaking has caused heap of damages to people, organizations and even the govt. Cybercrime detection methods and classification methods have come up with varying levels of success for preventing and protecting data from such attacks.

Several laws and strategies are introduced so as to forestall law-breaking and therefore the penalties square measure ordered right down to the criminals.

This paper describes regarding the common square measure as wherever law breaking typically happens and therefore the differing kinds of cybercrimes that are committed these days. The paper conjointly shows the studies created on email connected crimes as email is that the most typical medium through that the cybercrimes occur.

*Keywords **:** financial crimes, cyber stalking, telecommunication frauds, e-mail related crimes, cyber law, email spoofing, email bombing.*

I. INTRODUCTION

The term crime is denoted as [1] associate unlawful act that is punishable by a state.

However, certain purposes have no statutory definition provided.

Crime is additionally referred to as as associate offense or a criminal offense.

It is harmful not solely to some individual however additionally to the community or the state.[2] Cybercrime has nothing to try to with the law implemented.

According to the authors in [3], cyber could be a prefix want to describe an individual, thing or idea as a part of the computer and information age. With the advancement of the web technologies just like the 2G and 3G, the worldwide village is effectively sharing and human action very important data(s) across the network. However, there are some United Nations agency are deliberately making an attempt to trace and extract the important and counseling lawlessly for his or her personal use or for the money action and plenty of additional.

II. CYBER CRIME

[7] Cybercrime encompasses a large vary of crimes together with stealing people's identity, fraud and monetary crimes, [2] erotica, mercantilism contraband things, downloading bootleg files etc

A. Financial Crimes

Financial crimes include credit card frauds, stealing money from on-line banks etc. The criminals of credit card fraud get information from their victims often by impersonating a Government official or people from financial organizations asking for their credit information. The victims fall prey to the current while not correct inquiries and provides away their mastercard data to those criminals.

B.Cyber Pornography

[8] Pornographic websites which allow downloading of pornographic movies, videos and pictures, on-line pornography magazines (photos, writings etc.), all come under this category.[5] The study created by the United Kingdom Home Affairs Committee Report on pc smut (House of Commons, 1994) says that "Computer pornography is a new horror" (House of Commons, 1994:5).

C. Drug Trafficking

[2] Drug traffickers contribute a significant a part of cybercrime to sell narcotics victimization the most recent technologies for encrypting mails.

Since there's no personal communication between the client and dealer, these exchanges are easier for intimidated folks to shop for banned medicine and even alternative things.

D. Cyber Terrorism

[7] Terrorism acts that square measure committed in computer network square measure known as cyber coercion.

ISSN 2394 - 7780

Cyber coercion could embody an easy broadcast of knowledge on the web regarding bomb attacks which can happen at a specific time within the future.

[2] Cyber terrorists square measure people that threaten and oblige a private, a company or perhaps a government by offensive them through computers and networks for his or her personal, political or

socialbenefits.

E. Online Gambling
[8] On-line gambling offered by thousands of websites that have their servers hosted abroad.

These websites square measure the one among the foremost necessary sites for cash launderers.

F. Cyber Stalking
[9] 'Stalking' as has been outlined in Oxford lexicon, suggests that "pursuing stealthily".

Cyber stalking is following associate degree individual's or organization's whereabouts on the net. This is primarily against the law wherever the individual is continually troubled by another individual example, causation constant mails to a person with unsuitable contents and threat messages.

G. E-mail, Spoofing and, Phishing, Scams
Cyber criminals often spoof e-mails of known and unknown individuals. [9] E-mail spoofing ba sically means sending an e-mail from a source while it appears to have been sent from another e-mail. E-mail spoofing is a very common cause of monetary damages.

[10] The act that tries to get important data like passwords, details of credit cards by dissimulation to be a trustworthy entity in associate degree electronic company is named phishing. Phishing e-mails are likely to contain hyperlinks to the sites containing malwares.

III.TYPES.OFCYBERCRIME
A. Theft in the Services of Telecommunication
[9] people associate degreed criminal organizations will gain access to the plugboards (PBX) [11] of an organization's switchboard and acquire the access to their dial-in or dial-out circuits. [10] larceny of telecommunication services has been one among the earliest varieties of cybercrime and is taken into account to be a violation.

The criminal is sometimes asked to pay a fine with a brief quantity of jail time.

B. Piracy of Telecommunication
[8] Digital technology today, has allowed the perfect reproduction of prints and dissemination of graphics, sound and other multimedia combinations.

This has been a crucial concern to the house owners of the copyrighted materials.

When the creators of a specific work don't seem to be ready to gain cash in on their own creations, it ends up in severe loss and a good impact on artistic

efforts generally.

C. Dissemination of Offensive Materials
[8] [10] These square measures the materials that square measure thought to be objectionable and exist within the computer network. Computer networks may also encourage be of use in furtherance-of extortion. [10] the kind of materials used, the placement of the criminal WHO is distributive the materials, andthe victim's location all definethe number of fines and penalties to be paid.

D. Laundering E-money and Evasion of Taxes
[8] For quite whereas, electronic funds transfers have been assisting in hiding and transportation of crimes. The origin of ill-gotten gains will greatly be concealed by the emerging technologies today. Taxation authorities might simply conceal those licitly derived financial gain. Central bank direction is going to be bypassed by the event of the informal banking establishments or the parallel banking systems.

E. Extortion
Terrorism and Electronic Vandalism [8] Unlike before, the western society of industries is relying upon a posh processing and also the telecommunications systems.

Hampering or damaging these systems will cause damaging consequences.

ISSN 2394 - 7780

[11] Vandalism in general can be considered as the denial of service attacks, bot-nets, or several other harmfulnetworkattacks.

F. Fraud in Sales and Investments

[8] The use and development of applications in digital technology becomes a lot of dishonest and is certain to increase because the electronic commerce becomes a lot of and a lot of rife. Cyberspace has currently availed tons of investment opportunities like bonds or stocks, sale and leaseback of machine machines, telephone lotteries etc.

[5] The nice and quick development in telecommunications permits new opportunities for electronic eavesdropping.

H. Fraud in Transfer of Electronic Funds

[8] Electronic transfer systems square measure proliferating, and the same goes with the risks that such type of transactions may be intercepted or diverted.

[13] there's little doubt that the E-fund transfer system has fulminant and wide acceptance globally.

IV. CRIMES ON THE INTERNET

The Cybercrime much doesn't ask the law and it's the idea that's created by the media to a bigger extend. In general term pc crime may be a crime that encompasses crimes like phishing, bank robbery, credit card frauds, child pornography, kidnapping of children by means of chat rooms, creation or the distribution of viruses so on.

A. E-mail related crimes

Electronic mail has speedily become the world's most most well-liked suggests that of communication. Across the globe, millions of e-mail messages are sent and received every day. E-mail, like every different suggests that of communication, is also being misused by criminals. It has become a robust tool for criminals thanks to the convenience, the speed of transfer and its relative anonymity.

1) E-mail Spoofing: it's found in [8] that Associate in Nursing e-mail that seems to originate from one supply whereas it's truly being sent from another supply is named e-mail spoofing. Email spoofing is usually committed by falsifying the e-mail address of the sender and or the name. to send an e-mail, one usually has to enter the following information's:

i. The e-mail address of the receiver.

ii. The e-mail addresses of the persons who will receive a copy

iii. a subject matter for the message, that may be a short title or a brief description of the message.

2) E-mail Defamation: Cyber defamation or cyber slander often proves to be very dangerous and even fatal for anyone with even a little knowledge of computers to become blackmailers often by threatening their victims through e-mails.

3) E-mail Bombing: [8] E-mails account (in case of Associate in Nursing individual) or servers (in case of a company) flaming thanks to an oversized quantity of emails received by a victim is called e-mail bombing. This can easily be done by subscribing the victim's e-mail address to a large number of mailing lists which are the special interests group created to share and exchange data and knowledge on a standard topic of with each other through the assistance of e-mails.

4) Spreading Malicious Codes: the foremost common and quickest ways that to unfold malicious codes square measure typically e-mails. With the assistance of email, a virus called The Love Bug, spread to millions of computers within the 36 hours of its release from the Philippines. Trojans, viruses and worms or different pc contaminations square measure typically banded with egreeting cards that square measure e-mailed to unsuspecting persons.

5) E-mail Frauds: Financial crimes are commonly committed through e-mail spoofing. It is turning into easier to assume Associate in Nursing identity similarly on hide one's own identity. The criminal is aware of o.k. that there's minimum likelihood of his being known.

6) Threats sent via e-mail: From [3], we find that the relative anonymity of e-mails offers technology savvy criminals a useful tool. Anyone with little knowledge of how to send an e-mail, can easily blackmail or threaten someone via e-mail without being identified.

ISSN 2394 - 7780

V. CYBER LAW

IT Act 2000 is the primary purpose of the Act it to provide legal action or recognition to electronic commerce and facilities filling of electronic records with that government this law is also called as ITA – 2000 or IT Act. It releases in 17th October 2000.

IT Act 2000 consist of the 94 section are segregated in 13 chapter. To provide legal recognition for transaction a transaction to legal recognizes going perform because of this IT Act is come & used. To facilities electronic filling of document with the government agencies. The Government agencies to legal electronic filing to perform legal aspect Because of this to came the IT Act 2000. To provide legal infrastructure as a framed for e-commerce in India. To amend the Indian penal code, the Indian evidence Act in 1872, the banker's book evidence Act in 1891 and the reverse bank of India Act in 1934. To provide the all the electronic record in legal framework.

VI. CONCLUSION

From this study created, it's been found that there are many ways and suggests that through that a personal will commit crimes on cyber house. Cybercrimes are associate offense and are punishable by law.

In section two, we've seen a quick discussion of the enlarging areas of cybercrimes.

In section three, we've seen the common sorts and areas wherever cybercrime happens terribly ofttimes.

We have conjointly mentioned the results of cybercrime that are inflicting tremendous monetary losses in several countries, particularly within the areas of sales and investments. Different fines and penalties are set down for this class of crime. Section four discusses concerning the various crimes on internet that are associated with Emails.

VII. REFERENCE

[1]. en.wikipedia.org/wiki/Crime

[2]. searchsoa.techtarget.com/definition/cyber

[3]. https://youtu.be/RjSF1oX6bcU

[4]. https://youtu.be/1vQhSm5_UqY

[5]. https://youtu.be/CcSCD6ft6PE

[6]. https://www.academia.edu/8387361/

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER LAW

Anjali R. Prajapati and Sonal S. Pophale

ABSTRACT
Cyber law is a term that refers to all legal and with its regulatory portion of World Wide Web and the Internet. Any feature of legal issues concerning to any activity of Neitizens and others in Cyberspace come within the ambit of Cyber law. Neitizens are internet users who utilize the networks from their home or workplace. Cybercrime is a new specialized domain in which online communication network medium is utilized with higher specification in identifying cyber criminals using Cyber laws. A lot of research is being conducted in terms of placing the relevant legal methodology for preventing and controlling the Cyber criminal activities. Just as a human mind is ingenious enough to get incited to commit a crime, it is necessary that effective legal activities and methodology to control and to prevent Cybercrimes by cyber laws techniques be channelized. Also it needs a strong security mechanism which includes Virtual Private Networks, Firewalls and Intrusion Detection Systems as well as various amendments of existing cyber laws and other cyber related laws to prevent the occurrence of Cybercrime in the cyberspace.

INTRODUCTION

The invention of Computer has made the life of humans easier and faster , it has been using for various purposes all over world , starting from the individual to large organizations across the globe. In simple term we can define computer as the machine that can stores data/information and manipulate /process information or instruction that are instructed by the user.

Most computer users are using the computer for the official purposes either for their personal benefits or for other's benefit . This gave birth to "Cyber Crime". This had led to the growth in activities which are illegal to the society. We can define Cyber Crime as the crimes committed using computers or computer network and are usually take place over the cyber space especially the Internet .

Now we will study the term "Cyber Law". It doesn't have a constant definition, but in a simple words we can define it as the law that governs / rules the cyberspace. Cyber laws are the laws that govern cyber area. Cyber Crimes, digital and electronic signatures, data protections and privacy etc are comprehended by the Cyber Law. The United Nations General Assembly recommended the first IT Act of India which was based on the "UNCITRAL" (United Nations Model Law on Electronic Commerce)

IPR IN CYBER WORLD

The people nowadays are so much busy in their virtual world rather than knowing that what the actual motive in the virtual world is and share their important information online without thinking twice or thrice that what might be the after effect of the data being uploaded by them and some people take advantage of such uploads and take it as a means to generate money. Hence the issue of I.P.R comes into the foray of Cyber Space. Now these questions might pop out from most of us that what exactly is I.P.R? So, I.P.R is nothing but Intellectual Property Rights, Intellectual property refers to creations of the intellect for which a monopoly is assigned to designated owners by the law. Intellectual property rights (IPRs) are the rights granted to the creators of IP, and include trademarks, copyright, patents, industrial design rights, and in some jurisdictions trade secrets. Artistic works including music and literature, as well as discoveries, inventions, words, phrases, symbols, and designs can all be protected as intellectual property. Likewise Cyber Space is a term which is being derived from a the Science Fiction movie by Mr. Fred Roderick in the year 1920, and the term actually describes the virtual world which is something different from the real world. And today this term is widely being used to describe the attachment that people have towards the internet services or can be simply put into the words of "Socialisation" and "Social Media", As of today the world has been facing a lot of surge in the Cyber Crime due to the only factor of Globalisation and in India it can be related to the government's L.P.G Policy i.e. (Liberalisation, Privatisation And Globalisation). Some of the recent incidents in Cyber Crime are as follows: Cyber Bullying, Cyber Stalking, Spamming, Ransom ware and various other Malware Attacks. Although these terms do not have anything in relation to I.P.R, basic thing which needs to be focussed is on violation of an individual's private right in the virtual world by any means and what remedy that victim might receive, and till now the I.T Act, 2000 or Information Technology Act, 2000 has been followed down all these years and as the time has drastically changed from where it all began, accordingly the act needs to go many further changes in order to adapt to the present case scenario and to applied further in any cases arising and to fix all the prevailing loop holes in the act. So in order to curb all these activities the government has to take some appropriate measures and our Legislature as well as our Judiciary needs to amend some policies to prevent those culprits from

ISSN 2394 - 7780

breaking the law. Cyber security denotes the technologies and procedures intended to safeguard computer networks and data from unlawful admittance of weaknesses and attacks transported through the internet by cyber delinquents. Intellectual property refers to creations of the human mind, for example; a story, a song, a painting, a design, a program etc. The facets of intellectual property that relates to cyberspace are covered by cyber law namely :

1) Copyright Law.
2) Trademark Law.
3) Semiconductor Law.
4) Patent Law.

Data protection and privacy laws aim to achieve a fair balance between the piracy rights of an individual and the interests of data controllers such as Banks, Hospitals, Electronic mail Service providers etc. The Indian Penal Code (I.P.C) (as amended by I.T Act) International Journal of Academic Research and Development 137 penalizes several cyber-crimes. These include forgery of electronic records, cyber frauds and destroying electronic evidence etc. The digital evidence is to be collected and proven in the Court of Law as per the provisions of the Indian Evidence Act (as amended by the I.T. Act 2000).

GDPR AND INDIAN LAW

At present, companies world over are in the process of assessing the impact that EU General Data Protection Regulations ("GDPR") will have on their businesses. High administrative fines in case of non-compliance with GDPR provisions are a driving force behind these concerns as they can lead to loss of business for various countries such as India.

India has had a peculiar economic structural transition. Economic Survey reveals a top down structure of economy with 66.1% contribution of services sector to GDP. Out of this, information technology – business process management (IT-BPM) sector "is expected to touch an estimated share of 9.5% of GDP and more than 45 per cent in total services exports in 2015-2016 as per NASSCOM. " Revenue contribution of Exports in IT-BPM is expected to touch 108 billion US dollars with a comparatively less domestic contribution of 22 billion dollar. "Major markets for IT software and services exports are the U.S. and the U.K. and Europe, accounting for about 90 per cent of total IT/ITeS exports".

According to NASSCOM estimates for 2014, UK and Continental Europe respectively accounted for 17.4% and 11.6% of India's IT/ITES services export. Given the criticality of IT–BMP services, India must do all it can to protect and promote business in this sector. To a large extent, future of business will depend on how well India responds to the changing regulatory changes unfolding globally. India will have to assess her preparedness and make convincing changes to retain the status as a dependable processing destination. This document gives a brief overview of data protection provisions of the Information Technology Act, 2000 followed by a comparative analysis of the key provisions of GDPR and Information Technology Act and the Rules notified under it.

HUMAN RIGHTS IN CYBER WORLD

The main focus of this paper is to enlighten not only the academicians but also the non tech savvy laymen to have firsthand information about latest electronic gadgets i.e. internet, cell phones, laptops, etc. and their linkage with human rights across the world. This paper acts like a litmus test to check the use and misuse of cyber space, the new technical name doing wonders in many a field. The internet has now become all encompassing; it touches the lives of every human being. We now a days, undermine the benefits of internet, however its anonymous nature allows miscreants to indulge in various cybercrimes. As is known well a kitchen knife can be used for cutting vegetables to prepare a good meal but at the same time, the same knife can also be misused to kill a person. Similarly, the cyberspace can also be used and misused. The only difference between a traditional crime and a cybercrime is that the cybercrime involves in a crime related to computers. As an example let us take Intellectual property in cyber space. Internet is one such a threat, which has captured the physical market place and has converted it into virtual market place. Therefore, it is the duty of the Intellectual Property Right (I.P.R) owner to invalidate and reduce such mala fide acts of criminals by taking proactive measures. Indeed, it is alarming to note a sea change in malfunctioning of cyber space. The recent malware named Uroburos/Snake, is an example of growing cyber espionage and cyber warfare. Stealing of sensitive information is the new trend. Digital signatures are mostly used for software distribution, financial transactions and in other cases where there is a risk of forgery. The Indian Parliament passed the Information Technology Act 2000 and amended in 2008 on the United Nations Commissions on International Trade Law

ISSN 2394 - 7780

(U.N.C.I.T.R.A.L) model Law. The law defines the offences in a detailed manner along with penalties for each category of offences. Thus cyber laws are the safe savior to combat cyber-crime. Human Rights in the digital age are being contested very openly today. The text of World Summit on the Information Society (W.S.I.S) (Convened on December 2003) Declaration of principles exposes a common vision of the information society, particularly with respect to Human Rights. This also examines the conflicts of law in civilians (mainly tort laws and laws on the protection of rights of the personality as well as intellectual property and criminal matters.

CYBER CRIMES AND CRIMINAL LAWS

HISTORY OF CYBER CRIME

The first Cyber Crime was recorded in the year 1820. The primeval type of computer has been in Japan, China and India since 3500 B.C, but Charles Babbage's analytical engine is considered as the time of present day computers /PC's. In the year 1820, in France a textile manufacturer named Joseph-Marie Jacquard created the loom. This device allowed a series of steps that was continual within the weaving of special fabrics or materials. This resulted in an exceeding concern among the Jacquard's workers that their livelihoods as well as their traditional employment were being threatened, and prefer to sabotage so as to discourage Jacquard so that the new technology cannot be utilized in the future.

EVOLUTION OF CYBER CRIME

The cyber crime is evolved from Morris Worm to the ransom ware. Many countries including India are working to stop such crimes or attacks, but these attacks are continuously changing and affecting our nation.

YEARS	TYPES OF ATTACKS
1997	Cyber crimes and viruses initiated, that includes Morris code worm and other.
2004	Malicious code, Torjan, Advanced worm etc.
2007	Identifying thief , Phishing etc.
2010	DNS Attack, Rise of BotNets, SQL attacks etc.
2013	Social Engineering, DOS Attack , BotNets, Malicious Emails, Ransom ware attack etc.
Present	Banking Malware, Keylogger, Bitcoin wallet, Phone hijacking, Android hack, Cyber warfare etc.

CONCLUSIONS

The rise and proliferation of newly developed technologies begin star to operate many cybercrimes in recent years. Cybercrime has become great threats to mankind. Protection against cybercrime is a vital part for social, cultural and security aspect of a country. The Government of India has enacted IT Act, 2000 to deal with cybercrimes. The Act further revise the IPC, 1860, the IEA (Indian Evidence Act), 1872, the Banker's Books Evidence Act 1891 and the Reserve Bank of India Act, 1934. Any part of the world cyber crime could be originated passing national boundaries over the internet creating both technical and legal complexities of investigating and prosecuting these crimes. The international harmonizing efforts, coordination and co-operation among various nations are required to take action towards the cybercrimes. Our main purpose of writing this paper is to spread the content of cyber crime among the common people. At the end of this paper "A brief study on Cyber Crime and Cyber Law's of India" we want to say cyber crimes can never be acknowledged. If anyone suffering by cyber attack, please come front and register a case in your nearest police station. If the criminals won't get punishment for their deed, they will never stop this crime at all.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

IPR IN CYBER WORLD

Smritigandha M. Bidkar
Assistant Professor, F G Naik College of Arts, Science [IT] & Commerce, Navi Mumbai

ABSTRACT
Intellectual Property Rights (IPR) is look after disparate issues related to Patent, Copyright, Trademark and protection of information in cyber world .TRIPS and WTO are two recognized organizations who are responsible for all happening on internet.With development and upgradation of computer network, use and services related to it have become important part of the every human. As we all know that it's positive as well as negative impact on human life is increased day by day. For this topic I have gone through the papers about IPR and related issues also about the topic issues on cyber space. Referred some information available on Wikipedia .Here we will discuss on disparate issues that concern to common man using the internet.

INTRODUCTION:

Nowadays, people are too much addicted to the social networking sites like facebook, whatsapp and instagram.Also they are busy in sharing information without thinking the impact of it. The people as well as many internet sites and channels are only interested on increasing their TRP without thinking about an impact. They are less sensitive while talking on different matters. They do not want to get in depth understanding of it. They just exaggerate news and increase their TRP and likes on social media. That's why now a days IPR is playing an important role in cyber world.

We know that IPR helps to protect the rights of creator in concern with patent, copyright,

Trademark, industrial design as well as artistic works. The cyber space is easily available source to place all these things and publish it. That's why issues related to Liberalization, Privatization and Globalization are on the top. The recent two/three incidence in our country will explain the above three factors. The addiction of social media and its impact on all the country people is increasing day today.

All these terms are not directly relate to Intellectual Property Rights but they point towards the violation of individual's private information and have a great impact on all the world

It will also change the nation's economic as well as social relationship with others.

That's why in order to control all these activities government has to take some appropriate action. They has find out Legislative and also Judiciary needs to make some amendment to prevent such things in present law.

Intellectual Property Protection:

By Thomas Jefferson's view creation or invention cannot be subject matter of property.

But in Intellectual Property Rights inventors or creators canpublish and distribute their invention or creation on the cyber world without hazel.They do not want to keep the information secrete.Anybody can go through it or refer it. Normally, IPR helps for the creativityand innovation in the field of computers . With the use of internet different software , hardware and other digital records had increased a much. Everything is available in the form of softcopy. The use of ecommerce and m-commerce application changed the life style of the people . From the last decade, the activities and operations are drastically changed from physical to virtual world.

This transition has a great impact on the social .economic and cultural life. According to social and economic theory , we should be able to identify the creative work with particular person and also benefit the creator by trademark law or copyright act .

IPR issues in India

The increasing and uncontrolled use of internet brings the different issues related to intellectual property right. Basically in India internet is easily accessible to all .With privatization there is no restriction over the use of it. Because of the privatization and competition in Internet Service Providers, internet is free or with less expense available to all. Also the smart phone network had changed the psychology of the people. People had become addict of this devices and services. As there is lots of changes in the network system. That's why communication become faster and easy as compared to the traditional way.

In India there is no control system as well as there is no observer to it. Even the government policies are not sufficient to look after all. This is become the main problem in concern with IPR.

ISSN 2394 - 7780

With the present Indian law publication on electronic media ,social media , communication through internet and different issues related to Internet Service Provider had not covered much . There is no punishment in these factors.

CONCLUSION

Government must keep logs of all data that are posted over the internet. Communication over internet must be scrutinized by authorized peoples. According to my research paper I will say that there must be a separate panel and guidelines for E-media where all the data is posted. I conclude by saying that even if internet is a best medium for communication , the use of it should be controlled and observed .

REFERENCES

- ArteeAggrawal , Trivedi : Usage Of Interner and Issues Vol I
- Prabhu ,Timmankondu ,Chellanpn : IPR and it's development in India
- VijaykumarChoube : IPR and it's protection in cyber space
- Intellectual Property Right :Wikipedia

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

AN ANALYSIS OF CYBER & TECHNOLOGY RELATED BANKING FRAUDS AND CRIMES

Sneha Anil Kumar and Purba Ganguly

ABSTRACT
The evolution of Information Technology has given birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyses etc. with the use of high technology. Due to increase in the number of netizens, misuse of technology in the cyberspace has given birth to cybercrimes at the domestic and international level as well. Although it is an irrefutable fact that the key factor which has led to enrichment of the banking sector is the advancement of technology in the digital world; this sector has also been susceptible to crimes in cyberspace. This article explores the concept of cybercrime while highlighting the specific types that makes the banking sector vulnerable. Further, it outlines the legal regime that governs such crimes in India as well as the lacunas that needs to be overcome. Keywords: Cyber-fraud, Cybercrime, Information technology Act, banking sector, Phishing, Hacking, Identity Theft.

INTRODUCTION
Information, Communication, and Technology (ICT), has been a major force for transformation and development in every sphere of human life. Technology is making our lives simpler yet simultaneously it comes with a bundle of complexities. The growing trend in the world today is the use of online transactions; digital data transfer; generation of electronic database; etc. to such a large extent that social, business, trade, and other activities, are carried out in the digital world entirely dependent on computers, internet and other tools of information technology. This effect is practically seen in banking, insurance, and financial organizations, who have now become the prime users of internet and online transactions. Technology is used by them to transfer cash, make payments, submit account information, conduct calculations, maintain databases, etc. However, ICT has brought with it unintended consequences in form of "cybercrimes" which in relation to the banking sector are crimes like ATM frauds, credit/debit card scams, phishing, identity theft, data theft, etc. The increase in frequency of such crimes has caused heavy loss of money to the customers every year.

WHAT ARE CYBER CRIMES
The world's 1st computer specific law was enacted in the year 1970 by the German State of Hesse was 'Data Protection Act 19703 for the purpose of protection of information stored, transferred, or utilised through computers. In India, the government enacted the Information Technology Act, 2000 (ITA) and the I.T. Amendment Act 2008 (ITAA) to provide for regulation, and penalties with respect of frauds committed to or by computers. However, the term 'cybercrime' is not defined in either of the acts, nor any other legislation in India.4 To define cybercrime we can say it is just a combination of crime and computer. In simple words, 'any offence or crime in which the computer is itself a target or used as an object of offence to commit some crime, is a cybercrime.5 Thus any criminal activity using the internet, cyber space, worldwide web or computers; right from downloading illegal files to siphoning off millions of rupees or dollars from bank accounts; fall within the purview of a cybercrime. Cybercrimes are not restricted to monetary gains but also include non-monetary offenses such as creating and distributing viruses on other computers or posting confidential business information on the Internet or cyber terrorism.

LAWS GOVERNING CYBER CRIME & FRAUDS IN THE BANKING SECTOR
Computerisation in banks began in India in the 80's with installation of Advanced Ledger Posting Machines (Separate PC for every counter/activity). In the 90's Total Branch Automation marked the beginning of a networked environment in the banks. A Local Area Network (LAN) under client-server architecture was created and records began to be maintained in electronic manner in hard-disks and external media like tapes for backup purposes. Ever since passing of the ITA and recognition being given to electronic records it become mandatory on the part of banks to maintain proper computerized system for electronic records. Further computerization has led to innovation and the provision of more facilities like internet banking, mobile banking, online transfers, credit card facilities, debit card facilities, etc., which can be accessed by the bank's customer, 24 hours of the day from any place in the country or world.

CYBER FRAUDS
Frauds may be committed either by the employees of the bank or outsiders. Sometimes frauds may be committed by outsiders with the connivance or negligence of the bank employees.6 The term "fraud" as such has not been defined in the Indian Penal Code (IPC) however it defines and prescribes punishment for various acts that may lead to commission of fraud.

ISSN 2394 - 7780

The Reserve Bank of India has classified frauds into the following categories for the purpose of uniformity of reporting by the banks to the RBI and in keeping with the provision of the IPC7:

(a) Misappropriation and criminal breach of trust.

(b) Forging of documents and instruments and manipulation of the books of accounts.

(c) Negligence and cash shortages.

(d) Cheating.

(e) Irregularities in extension of credit facilities against illegal gratification.

(f) Cases of frauds not covered above.

In Contractual terms fraud is defined in the Indian Contract Act under Sec 178 to mean and include any of the following acts committed by a party to a contract, or with his connivance, or by his agent, with intent to deceive another party, or to induce him to enter into the contract-

a) the suggestion, as a fact, of that which is not true, by one who does not believe it to be true;

b) the active concealment of a fact by one having knowledge or belief of the fact;

c) a promise made without any intention of performing it;

d) any other act fitted to deceive;

e) Any such act or omission as the law specially declares to be fraudulent.

This same concept of a dishonest act and behaviour by which one person gains or intends to gain advantage over another person can be associated with banking frauds. Banking frauds can be done traditionally for example misappropriation of funds by an employee; kite flying operations etc. or through modern means by taking advantage of the computerized system in place, and technology, known as cyber frauds.

CYBER CRIMES

1. Hacking

"Hacking in simple terms means unauthorised access made to a computer system, programs data and network resources.9 In the banking sector hacking is used as a means to gain unlawful entry into the banking sites or accounts of customer or to the electronic data store in banks and to tamper with the same. Hacking is not defined in the amended IT Act, 200010 but under Section 43(a) read with section 66 of ITAA 2008 and Section 379 & 406 of IPC a person or a hacker can be punished with imprisonment which may extend to 3years or fine which may be extended to five lakh rupees or both. According to section 77-B of the ITA, hacking offence is considered as a cognizable and bailable, but if section 379 of the IPC is also applied then the offence is cognizable, non-bailable and compoundable with the permission of the court.

Sanjay Kumar v State of Haryana11, in this case Sanjay Kumar was deputed by a software company to maintain the software system supplied by the company to the bank. He was also in charge of looking into systems of certain other banks. In connection to rendering such services the accused had access to the accounting systems and ledgers and various accounts held by the bank. While reconciling the accounts, certain discrepancies were pointed out by the bank officials, and in the investigation it was found that the accused petitioner manipulated entries by forging and fabricating the same from one account to another. He illegally and wrongfully withdrew rupees, 17, 67,409, from the bank. It was held that he committed wrong under section 420, 467, 468 and 471 along with commission of offences under section 65 and 66 of the IT Act. He was convicted and sentenced to three years' imprisonment, and had to pay 7000 rupees as fine.

2. Data Theft

According to ITA the crime of data theft under Section 43(b) is specified as "if any person without permission of the owner or any other person in charge of a computer, or computer system or network – downloads, copies or extracts any data, computer database or information from such computer system or network including information or data held or stored on any removable storage medium". Thus data theft is the unauthorised copying or removal of confidential information from a business or enterprise. It can take form of ID – related thefts or theft of company's customer records or proprietary information or intellectual property. S.43 (b) read with S.66 along with S 379, 405, and 420 of IPC is applicable to this offence. The penalty for such crime is imprisonment which may extend to 3 years and fine which may extend to 5 lakh rupees or both.

ISSN 2394 - 7780

3. Phishing/ Vishing

Phishing is the fraudulent process of attempting to acquire sensitive information such as user names, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication.12 They send out emails that appear to come from some legitimate website or as banking instructions. The email states that your information needs to be updated or validated and ask you to re-enter your username and password, after clicking a link in the e-mail. Some mails may ask you to enter even more information like your social security number, security pin number; credit card number etc. The fraudster then has access to the client's online financial balance available in the bank account. The major incidents are reported about ICICI, HDFC, UTI, and State bank of India. Many elderly customers who have just begun using online facilities of the financial institutions are falling prey to phishers. Under the ITA, section 66-D is applicable to this offence along with sections 379 and 420 of the IPC. The victim can file a complaint in the nearest Police Station where the above crime has been committed. This crime is punished with an imprisonment which may extend up to 3 years and fine which may extend to 5 lakh rupees or both.

Cyber security expert, Vijay Mukhi13 says, "The problem with the internet is that it doesn't recognize geographical boundaries. So, today most of the phishing attacks to a bank will never occur from the country itself. A person can launch a phishing attack on an Indian bank sitting in America and the spoofed page might be in Taiwan." The only way to curb it is by creating awareness and cooperation with banks and consumers.

In, State of Maharashtra v. Opara Chilezein Joseph and Ors,14 on Oct. 30 2013, a court in Panvel in Maharashtra convicted four Nigerian nationals for duping people across the country by sending them phishing emails and texts. They were asked to pay penalty of rupees 50,000 each because each of them had sent, e-mails and texts to people telling them, they had won a lottery.

4. Credit card & online banking frauds

When customers make online transactions using their credit or debit card and such electronic transactions are not secured, the credit card numbers can be stolen by the hackers who in turn misuse it to siphon funds from the cardholders account. The law applicable in this case is sections 43 (a), 43(b) and 43(g) read with section 66 and section 66D of the IT Act, and sections 420, 467, 468 of IPC. This crime is punished with an imprisonment which may extend up to 3 years and fine which may extend to 5 lakh rupees or both.15

Sanjay Dhande v. ICICI Bank and Vodafone,16 in this case IIT-Kanpur director was cheated of rupees 19 lakhs after his bank account, e-mail and SIM card was compromised. 18lakhs was awarded to him as compensation from Vodafone whom the court held has a bigger blame because the duplicate SIM card issued by them played a crucial role in this crime. ICICI had to pay rupees 6 lakhs because the bank had defaulted on multiple occasions and their omissions fall within section 43A of the IT Act.

5. ATM17 Frauds

ATM frauds are a type of fraud which occurs when an ATM is compromised by a skimming device, a card reader which can be disguised to look like a part of the machine. The card reader saves the users' card number and pin code, which is then replicated into a counterfeit copy for theft. Once the false cards are obtained either debit or credit cards, they are then used by criminals for their monetary benefits by withdrawing money from the victim’s bank account mala-fidely. Tamil Tiger Credit Card Scam: here, Sri Ramachandra Medical College police at Porur, Chennai, arrested G. Elango, a Tamil Tiger agent carrying a British passport, who illegally withdrew over Rs. 30 lakh from the ATM centres of a few nationalized banks and a private bank. The amount was then sent to the United Kingdom through unauthorized channels. Elango was caught red-handed while he was withdrawing money from the ATM machine using 28 different ATM cards.18

In Vidyawanti v. State bank of India and others,19 the National Consumer Commission observed a bank cannot escape its liability by claiming its security systems are fool proof. If there is a flaw or a loophole in the system, the bank would be liable to make good the loss caused to its customer. In this case Vidyawati and Mr. Sharma two customers of SBI bank utilised State Bank of Patiala (SBP)'s ATM machine which failed to dispense money owing to a technical fault. Later both received messages that 20000 rupees were debited from their accounts. The Commission concluded there was deficiency in service as the ATM was faulty, and held both SBI and SBP jointly responsible and liable.

6. Identity Theft

Identity theft is a term used to refer to a fraud committed that involves stealing money or getting other benefits by pretending to be someone else. It is the crime of obtaining the personal or financial information of another person for the sole purpose of assuming that person's name or identity in order to make transactions such as obtain loans, credit or purchases.20 In the United States and Canada, for example, many people have reported

ISSN 2394 - 7780

that unauthorized persons have taken funds out of their bank or financial accounts, or, in the worst cases, taken over their identities altogether, running up vast debts and committing crimes while using the victims' names. In many cases, a victim's losses may include not only out-of-pocket financial losses, but substantial additional financial costs associated with trying to restore his reputation in the community and correcting erroneous information for which the criminal is responsible.21

7. E-mail Fraud

Fraud whether financial, banking or social committed with the aid of email would be called email fraud. In today's world e-mail and websites are become a speedy, easy and preferred means of communication. Sometimes such fraud is made by some of the hacker or hacking organization send email to bank customers that "congratulation you have won such a huge amount to enchase it please share your bank details" and by such customer simply have to type credit card number in the link page for the information to be gathered by the fraudsters. Law applicable in this case is sections 66C and 66D of the IT Act, and Sections 415 and 420 of IPC.22

8. Denial of Service Attack

Denial of service attack involves flooding a computer with more requests than it can handle. This act causes the computer or web server to crash and results in authorised users being unable to access the service offered by that computer or website. Although this kind of stack does not usually result in theft of information or other security loss, it can cost the target person or company a great deal of time and money. A bank is yet to report this crime, but this crime has an impressive history of blocking out websites like Amazon, CNN, Yahoo, etc.23 The law applicable in this case would be section 43(f) read with section 66 of the IT Act.

CONCLUSION

The banking industry across the globe is facing a challenging situation which is the risk computerization has brought as a consequence. Technology driven approaches have been adopted for the management of risk. Due to the growth of IT, penetration of mobile networks in everyday life, the financial services have extended to masses. Technology has made sure that banking services reach masses as it made these services affordable and accessible. However, this has also increased the risk of becoming targets of cyber-attacks. Cyber criminals have developed advanced techniques to not only cause theft of finances and finances information but also to espionage businesses and access important business information which indirect impacts the banks finances.

The problem with cyber-crime is that it is not limited by territorial boundaries or geographical location. A person sitting at one end of the world may commit a crime at the opposite end of the world. The digital world is far more inter – connected, than our existence in the virtual world. Thus a remedy to this is not only the creation of laws but also the creation of specialised agencies to tackle only cyber-crimes, who will be experts in collecting forensic digital evidence, and they should be aware of the admissibility of such evidence as per the procedural laws of the State. Creating awareness of such crimes by the banks among its customers will also aid in curbing the same.

REFERENCE

1 LL.M, MH-SET, Working as Assistant Professor at M.K.E.S. College of law, Malad (West), Mumbai – 400064; e – mail id: sneha.cie@gmail.com

2 LL.M, MH-SET, working as Assistant Professor at M.K.E.S. College of law, Malad (West), Mumbai – 400064 Email.id: purba.chumki@gmail.com

3 Cyber Crimes and the Law; article available at, http://www.legalindia.com/cyber-crimes-and-the-law/

4 Cyber law & Cyber Crimes and the Information Technology Act 2000 with IT rules 2011; by Advocate Prashant Mali; 2nd edition 2015; page 1

5 Cyber laws in India; article available at, http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

6 Tannan's Banking Law and practices in India; 23rd edition – reprint 2012; page 1833

7 Banking Frauds, IPC & Fraud Prevention By Subash Agarwal

8 http://indiankanoon.org/doc/299780/ - section 17 Indian Contract Act 3

9 Cyber Crimes and Legal Measures by Dr. Manish Kumar Chaubey, 2013 print page 13

10 Types of Cyber Crimes & Cyber Law in India, Available at http://www.csiindia.org/c/ document_library /get_file uuid=047c826d-171c-49dc-b71b-4b434c5919b6,

ISSN 2394 - 7780

11 CRR No. 66 of 2013 decided on 10th January 2013

12 Cyber law & Cyber Crimes and the Information Technology Act 2000 with IT rules 2011; by Advocate Prashant Mali; 2nd edition 2015; page 34

13 http://www.cyberlawsindia.net/cases5.html

14 (C.R. No. 344/2012)

15 Cyber law & Cyber Crimes and the Information Technology Act 2000 with IT rules 2011; by Advocate Prashant Mali; 2nd edition 2015 at page 60

16 January 2015

17 Automated Teller Machine

18 http://www.cyberlawsindia.net/cases4.html

19 February 18 2015, Revision Petition No. 4868 of 2012; decision by national consumer forum; http://www.business-standard.com/article/pf/consumer-court-grants-relief-to-atm-fraud-victim-115040500695_1.html

20 Identity Theft Definition | investopedia http://www.investopedia.com /terms/i/identitytheft.asp#ixzz3t78c3eKJ

21 http://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

22 Cyber law & Cyber Crimes and the Information Technology Act 2000 with IT rules 2011; by Advocate Prashant Mali; 2nd edition 2015 at page 54

23 Ibid at page 95

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

AN INTRODUCTION OF SOCIAL NETWORKING PLATFORMS AND RELATED CRIMES

Rekha Madhukar Jagtap
Student, JVM's Mehta Degree College, Airoli

ABSTRACT
Mobile devices area unit progressively utilised to access social media and instant electronic communication services, which allow users to speak with others simply and quickly. However, the misuse of social media and instant transmission services speeded up conducting utterly completely different cybercrimes like cyber stalking, cyber bullying, slander spreading and harassment.

Therefore, mobile devices are a vital evidentiary piece in digital investigation For that there are different types of social networking platforms.

Keywords: Social Networking Platforms, social media crimes, Social Networking Applications & Mobile Devices, Digital forensics environment.

INTRODUCTION
Digital forensics, a branch of forensic science, deals with the investigation and recovery of digital information found in digital devices which are mostly found at crime/incident scenes. Early twenty-first century became the golden age of digital forensics because of the technological advances in today's world. Especially with convenient accessibility of smart devices, most data are now being stored and shared in digital forms such as pictures, diaries, calendars, videos, etc. Smart phones, tablets, computers, smart household devices. Moreover, wearable de-vices have already become part of our everyday life. The demand towards the usage of technological advances makes tremendous amount of data being stored and shared particularly in online social networks. This inevitable developments make any device a storage of potential evidence related to a crime or an incident.

Type of Social Networking Platforms
We generally understand what social electronic media is. But, what approximately don't know is that Facebook, Instagram, Twitter, Snapchat and WhatsApp are not the only mutual media platforms. The categorization of social media platforms is on the reality of its prime objective of manage Following are the different types of social networking platforms.

1. Social Networks
A social networking service (also social networking website, or SNS or social media) is an internet platform which individuals use to create soscial networks or social relations with people who share similar personal or career interests, activities, backgrounds or real-life connections. The social network is distributed across varied pc networks. The social networks are inherently pc networks, linking folks, organization, and information. Social networking services vary in format and also the variety of options. They can incorporate a spread of latest info and communication tools, in operation on desktops and on laptops, on mobile devices like pill computers and smartphones. They may feature digital photo/video/sharing and "web logging" diary entries on-line

Use: To associate with people and brands virtually.

Examples: Facebook, Twitter, WhatsApp, LinkedIn.

2. Media Sharing Networks
Media sharing sites permit you to transfer your photos, videos and audio to a web site which will be accessed from anyplace within the world. You can then share that media with the world or just a select group of friends. Many media sharing sites conjointly permit you to put media on alternative sites by 'embedding'.

Use: To search for and share photos, videos, live videos, and other forms of media online.

Examples: Instagram, Snapchat, YouTube

3. Discussion Forums
A program that permits members to carry discussions on-line.

The discussion is started by one member by posting a subject and different members reply.

This allows members of an equivalent cluster to share data and ideas.

ISSN 2394 - 7780

Use: is a platform to look, discuss, and exchange data, news, and opinions.

Examples: Reddit, Quora, Digg

4. Bookmarking and Content Curation Networks:-
"Bookmarking" is that the most casual action, it implies only the potential for interest, and mostly done for oneself.Curating requires both persistent and deep interest in the content, and adding an

unique value to the content you are curating.

Use: To explore, save, exchange, and discuss new and trending content and media.

Examples: Pinterest, Flipboard

5. Consumer Review Networks:-
A client review may be a review of a product or service created by a client WHO has purchased and used, or had expertise with, the merchandise or service.

Customer reviews square measure a type of client feedback on electronic commerce and on-line searching sites.

There are dedicated review sites, a number of that use client reviews in addition as or rather than skilled reviews. The reviews might themselves be hierarchic for quality or accuracy by alternative users.

Use: to go looking, review, and share opinions/information about brands, restaurants, products, services, travel destinations, etc.

Examples: Yelp, Zomato, TripAdvisor

6. Blogging and Publishing Networks:-
Blogging/publishing networks serve as a platform for publishing online content in a way that facilitates discovery, commenting and sharing.

Publishing platforms include ancient blogging platforms like Blogger and WordPress, microblogging platforms like Tumblr, and even interactive platforms such as Medium.

Use: To publish, explore, and treat content on-line.

Examples: WordPress, Tumblr, Medium

7. Sharing Economy Networks:-
It is also known as ‘collaborative economy network’. These networks alter folks to attach on-line for advertising, finding, sharing, trading, shopping for and commercialism of merchandise and services on-line.

Use: to seek out, advertise, share, and trade product and services on-line.

Examples: Airbnb, Uber, Task rabbit

8. Anonymous Social Networks:-
As the name itself states, such social networks alter users to share content anonymously.

Thus, miscreants are increasingly misusing such platforms for cyberbullying.

Use: To anonymously spy, vent, gossip, and typically bully.

Examples: Whisper, Ask.fm, After School

Types of social media crimes
1. Hacking:-Hacking typically refers to unauthorized intrusion into a laptop or a network. The person engaged in hacking activities is understood as a hacker. This hacker could alter system or safety features to accomplish a goal that differs from the initial purpose of the system. Hacking can even talk to non-malicious activities, sometimes involving uncommon or jury-rigged alterations to instrumentality or processes.

Social media hacking usually occurs when:

One does not log out from the account, especially when using a public computer.

Sharing of passwords with strangers either unintentionally, or as a result of social engineering.

Using easy to predict, or same passwords across multiple platforms.

Hacking of one’s login email ID.

ISSN 2394 - 7780

2. Photo Morphing:-
Photo morphing is that the use of piece of writing to alter associate degree image/shape into another while not a lot of issue. Available information shows that individuals share nearly three.2 billion images daily on social media platforms. The widespread accessibility of media on social networking platforms makes it a cakewalk for miscreants to transfer and misuse them.Miscreants morph the images of popular figures and upload them on adult websites or use them for blackmailing them for sexual or money favors.

3. Offer & Shopping Scams:-
Women ar sometimes illustrious to fall for such provide and searching scams on social networking platforms.

For example, a reprobate uses a searching provide to create a user click on a link. Once clicked, it prompts the user to forward it to twenty folks to avail the coupon. However, the user does not get any coupon, but the cybercriminal gets his/her personal information!

4.Dating Scams:-
In such scams, the fraudster connects with the victim employing a pretend name and film. Once they tie the victim, they move to a distinct platform for additional communication.Once they notice that the victim has fallen for them, they first send little gifts like flowers and cards, and later begin tight for emergency financial facilitate like recharging their phone to speak, booking flight tickets to fulfill, medical reasons etc. At times, fraudsters may additionally record video calls or screen, and later use them to blackmail the victim.

5. Cyberbullying
Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets.

Cyberbullying will occur through SMS, Text, and apps, or on-line in social media, forums, or recreation wherever individuals will read, participate in, or share content. Cyberbullying includes causation, posting, or sharing negative, harmful, false, or mean content concerning some other person. It will embrace sharing personal or non-public data concerning some other person inflicting embarrassment or humiliation. Some cyberbullying crosses the road into unlawful or criminal behavior. The most common places where cyberbullying occurs are:

- Social Media, such as Facebook, Instagram, Snapchat, and Twitter
- SMS (Short Message Service) additionally referred to as Text Message sent through devices
- Instant Message (via devices, email provider services, apps, and social media messaging features)
- Email

6. Link Baiting:
In such scams, the fraudster sends the victim a link that entices the victim to open it. On opening, it results in a faux landing page that prompts the victim to enter his/her account credentials. This provides the credentials to the cybercriminal who later uses it for illicit activities. Example: The victim gets a message: “Somebody simply place up these footage of you drunk at this wild party! Check ’em out here!” Immediately, the victim clicks on the fenced link, that results in his/her Twitter or Facebook login page. Once the victim enters his/her account details, the cybercriminal has the password and can take total control of the account.

Social Media Forensics or Social Network Forensics
Now that you just shrewdness perpetrators will use social networking platforms to work mayhem, square measure you considering AN exit? Well, allow us to enlighten you regarding digital forensics then! The increase in social media crimes has additionally resulted within the increasing importance of digital forensics for his or her investigation. Precisely called social media forensics or social network forensics, it focuses on retrieval of electronic proof from social networking activities. Such proof usually plays an important role within the conviction or final judgment of a suspect. Social media forensics involves the appliance of cyber investigation and digital analysis techniques for:

- Collecting data from social networking platforms like Facebook, Twitter, LinkedIn etc.
- Storing
- Analyzing, and

ISSN 2394 - 7780

- Preserving the knowledge for fighting a case within the court of law

Social Media Forensics is essentially regarding locating the supply of electronic proof. This is among assembling it in AN unhampered approach whereas yielding with all laws.

Social Networking Applications & Mobile Devices
Due to the increasing use of social applications on smartphones, they're the largest repertoire of proof for rhetorical investigators.Did you recognize that quite ninetieth of social media users use mobile devices to access social networking platforms?Thus, they store a great deal of potential info that social media forensics professionals will extract with the propertools.Furthermore, with the proper examination strategies and tools, such proof will give crucial leads in a very case.In fact, half Facebook users access Facebook through its mobile applications on their smartphones or tablets.Moreover, such users square measure double as active compared to those that use alternative devices (desktop, laptop) to access Facebook.Since a lot of users leverage social networking applications on their mobile devices, the likelihood of misuse is additionally quite high!Hence, a rhetorical analysis of the suspect's mobile device offers an excellent potential to help in his/her immurement or exoneration.

The Challenge for Social Media Investigations:-
Aside from what the Prime Minister David Cameron described as the social network's "social responsibility to act", the incident raises a number of questions concerning the increasingly important role that these social media channels play in cyber forensic investigations.

Facebook has a "social responsibility to act"
"Facebook and a number of different on-line platforms like Twitter, YouTube and WhatsApp Messenger are becoming primary means of communication and an everyday feature of our lives.

Their selection and practicality is ever-changing unrelentingly," explains Keith Cottenden, Director and Head of Investigations at CYFOR Digital Forensics."The prevalence of social media in our lives suggests that the sources of proof accessible to investigators square measure apace increasing. But with that expanding evidentiary environment come unique pitfalls and challenges different from what investigators have dealt with in traditional digital forensics, not least knowing how to access this information during a forensically sound manner which will produce a powerful case." The digital investigator needs a different way of thinking with social media investigations. Under normal circumstances Facebook, for example, allows an investigator the same level of access as any other user, i.e. a relatively unwelcome, uninvited guest associate degree attempt|attempting} to collect data on an account holder. Mr Cottenden says: "You can look at pictures, posts, likes etc. but you cannot control the hardware where the physical evidence exists, as with a traditional digital forensics investigation. To further complicate matters, content posted on social media and its associated meta-data is constantly changing, being edited or deleted at any given time; then there is the fact that identities in social media tend towards anonymity, add this to the sheer volume of data and you have an incredibly dynamic and complex set of variables to contend with."

DIGITAL FORENSICS ENVIRONMENT
The origin of Forensic can start from the practice of forensic medicine meaning "of or used in law courts" (Oxford Dictionary1999, p. 305). One of the classic examples of forensic tasks is identifying fingerprints. The term "Forensic" has become more familiar to the IT community and law enforcement, as the number of criminal activities using computer has increased (Reith, Carr, & Gunsch, 2002, p. 10). Thus, the new term 'Computer Forensics' has been introduced and more recently it is referred to as digital forensics. Recently, the term has subdivided into network forensics, Internet forensics, and Social Network Forensics.

Digital Forensics:
defines digital forensics as the application of computer investigation and analysis techniques to determine potential evidence.

Network Forensics:-
In network environments, data is transferred from one computer to another and this is when we need to use network forensic procedures when collecting evidence.

Social Network Forensics:-
Social network forensics came after the revolution of social networking sites but the term social network forensics does not have accepted definition. However, social network forensics will be a major focus of

ISSN 2394 - 7780

Digital Forensics in the future, and it will be a major part of today's and the future digital Landscape

Web Browser Forensics:-
The web browser is defined as the navigation and rendering tool for the Web (Berghel, 2008). Therefore, web browser forensic can be considered as a part of Internet forensics, which is focused on the web browser's history, cache, and cookie information in particular.

Digital Evidence:-
Digital proof is data AND knowledge useful to an investigation that's hold on, received, or transmitted by an electronic device. This proof is noninheritable once knowledge or electronic devices square measure confiscated and secured for examination.

CONCLUSION

We describe a forensic analysis of social networks and types of social networking platforms. Then how different types social media crimes occure and which Challenge take place for Social Media Investigations.

REFERENCES

- https://ifflab.org/application-of-social-media-forensics-to-investigate-social-media-crimes/
- https://core.ac.uk/download/pdf/56363107.pdf
- https://cyfor.co.uk/digital-forensics-and-social-media-investigations/
- https://arxiv.org/ftp/arxiv/papers/1706/1706.08062.pdf
- https://www.researchgate.net/publication/261306040_Forensic_analysis_of_social_networks_case_study

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER TERRORISM & CYBER WARFARE

Jayesh S. Patil
JVM Mehta College, Mumbai

ABSTRACT
Since the internet has born, the world has changed drastically by its advantages. The Internet has influenced almost every field. In this never changing world people are aware of the positive side of the internet but they are not aware of the negative side of it. Concepts like Cyber crime, cyber attacks and cyber terrorism is rarely known to the people. As the technology is rapidly growing day by day on the other hand there are many new ways evolving out for spreading crime. Hence there is a need of developing strong Cyber security systems and creating new laws for controlling cyber crimes and attacks.

In today's era Cyberspace has became an easy way for the terrorists to implement their illegal, terrorist activities in the public. Especially, young population is an easy target for them as they are not aware that terrorism can be done through cyber space. Terrorist groups use this way as it's much cheaper, because it only requires an investment in a computer and access to the Internet, it is not limited within area and the most important it is anonymous no one can find out who has done the attack . In recent years, the increasing problem that experts talk of in public is the "negative use of the internet", the "Dark net" or the "Deep Web". As the crime rate is in rise, there is need for cyber laws related to the applications of cyber space gather's great momentum. Considering the case of India, Information Technology Act is introduced in 2000 in order to deal with issues related to cyber space. There is need to stop the cyber terrorism and attacks before it becomes uncontrollable.

Keywords: Cyber terrorism, Cyber attacks, Cyber-crimes, Cyber security, Cyber laws, cyber risks, Youth, India

INTRODUCTION
Today we are living in an electronically connected world or we can say "online world". Our whole world is linked with internet. And we are advancing the human needs along with the internet in every field. Being connected to the world means we are up to date with what's going in the world. Nowadays almost all communication are done through the internet. Living in present world without referring to the past experiences is not possible. Knowing about the past is important for futuristic knowledge. Since from the Morris worm the first cyber attack till today the cyber crime has increased, matching with the speed of technology advancements. Hence to stop the cyber crime s and cyber attacks a strong security system has to be developed.

OBJECTIVE
Basically this paper gives a small idea about the rise of cyber terrorism and cyber attacks. And explains how the country's youth can be an easy target of the cyber terrorists.

1. To understand cyber terrorism
2. To understand the types of cyber attacks
3. To make youth aware of the impacts of the cyber crimes
4. To understand the steps towards cyber security
5. To understand the familiarity of youth with the cyber risks

Before understanding what actually cyber-crime is, we have to understand what the word 'cyber' means. The word cyber means computer or computer networks. It means anything related to the computer is categorized under the word cyber.

WHAT IS CYBER TERRORISM OR WARFARE?
Cyber terrorism is the new form of terrorism. In which the terrorists uses internet, electronic devices, technologies with the aim of doing illegal activities in the targeted area and spreading threat in the public.

Why do the terrorists rely on cyberspace and social networks?
The most common and obvious reason that terrorists uses cyberspace is that it is significantly cheaper, completely anonymous, and the variety and number of targets and potential victims are enormous and just "a click away" – there is no need to cross any distance. By using the Internet, because of its availability and distribution, it is easier to recruit and mobilize new supporters of terrorist ideas, to find information and facilities regardless of the part of the globe where they are physically located, it is easier to find sources of

ISSN 2394 - 7780

financing, to build connections for the implementation of joint actions, to exchange information and to educate new members for illegal activities. It is important to be aware of the effects of psychological warfare, because this way fear and panic can spread faster by the methods of disinformation, threats and setting the terrifying images of torture and executions.

DIFFERENT WAYS USED FOR CYBER ATTACK

Malware — Malware can be defined as the way through which the cyber terrorist of creates a software in such a way that it harms targeted computer network or server.

Phishing — Phishing is the way used by cyber terrorist to send corrupted e-mails which then after entering in the targets system starts harming the files.

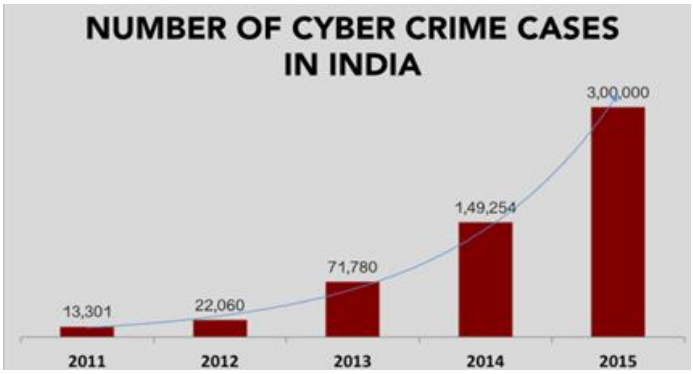
Service attacks - It is way through which the cyber terrorist breakdowns the website server by sending multiple requests.

Middle attacks -It is the method in which the cyber terrorists secretly interposes there man in the association who gave them the data information.

Crypto jacking —It is the attack by which others computer is used to generate crypto currency for the hacker.

SQL injection —It is the way through which the attacker injects an code in the system through which he drive the application.

Zero-day exploits — In this way the terrorist targets the system when the system is at the weak stage.



CYBER CRIMES AND CYBER ATTACKS IN INDIA

The cybercrime cases increased at the rate of 300%, which was registered under IT Act between the year 2011-2014. The number of registered cases related to cybercrime in the year 2015 reached 11.592. Basically the Sources of the cyber attacks in India are Nation, States, Cyber Criminal Organizations, Terrorists, Hackers / Hacktivists. In India most of the cyber attacks are done from inside side the country. India experience's most of the cyber attacks around the world. Indian law system has passed many laws in order to stop such major cyber attacks. Cyber attacks in India from within the country are majorly done with intentions of extorting money. For this India has passed the **IT Act law of 2000 (India).** This act is focused on information technology. This laws are made for Trojan attacks and cyber hackers. Some of the sections under this laws section(65,66,67,70,72,73)and IPC sections(503,499,463,420,383,500)

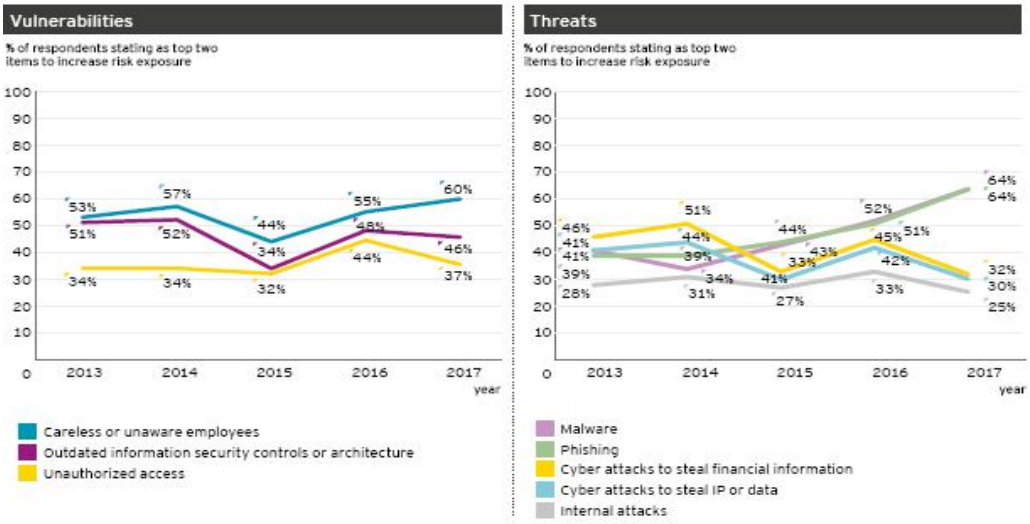
There many special acts made for specific crimes:

- The law against Online Sale of Arms Under Arms Act, was passed in the year 1959
- The law against Online Sale of Drugs Under Narcotic Drugs and Psychotropic Substances Act, was passed in the year 1985

ISSN 2394 - 7780

STEPS OF CYBER SECURITY

- **Network Security :** protecting the network from internal as well as form external attacks.
- **Malware Protection** :Creating and implementing relevant policies and anti-malware defence system .
- **Monitoring**: analyzing and monitoring all ICT system and networks
- **Incident Management:** Establishing an quick response management system.
- **User Education and Awareness**: Establishing user policies to aware user about cyber risks
- **Home and Mobile Working:** Developing mobile policy and training staff to protect in transit and at rest.
- **Secure Configuration**: maintaining configuration of all ICT systems
- **Removable Media Controls**: Producing policies related to all removable media devices in order to protect the systems from attacks
- **Managing User Privileges**: Creating user account managements system to keep an eye on the users privileges
- **Information Risk Management Regime**: establishing risk managements system and policies



YOUTH AWARENESS

India has largest youth population in the world. Hence it is important to aware the youth about the cyber risks. Youth is the nation's strength on which the nation's development depends. India's youth is using cyber on a large scale therefore they can be an easy target for terrorist groups. As India ranks 5th for being affected by cyber attacks and ranks 3rd in terms of the highest number of internet users in the world. The annual growth rate is 44% which has grown 6 times between 2012-2017. Hence there is an extreme need for developing new laws and making the youth aware about the cyber risks.

Different Kinds of Cyber Crime	Frequency	Percentage (%)
Credit Card Frauds	23	7.7
Cyber Bullying	5	1.6
Cyber Stalking	8	2.7
Cyber Terrorism	1	0.3
Defamation	2	0.7
Denial of Service	2	0.7
Don't Know	132	44
Hacking	103	34.3
Identity Theft	1	0.3
Morphing	3	1
Online Fraud	1	0.3
Phishing	15	5
Spam Mails	4	1.3
Total	300	100

ISSN 2394 - 7780

CONCLUSION

At last I would like to conclude my paper with the idea that the India and the world can be saved from cyber terrorism and cyber attacks by developing and building a strong security systems, laws. In the era of technology, terrorism can be seen as the terrorism done by war weapons (explosives, guns, etc.) used for the destruction of resources , or harming particular nation. But the cyber terrorism uses new weapons like malicious software, electromagnetic and microwave weapons for the destruction and modification of data in cyberspace. Because of the cyber terrorism phenomenon and its frequency, security agencies responsible for investigating terrorism, including cyber terrorism, must remain vigilant, which includes ensuring adequate funding for staffing, equipment, and training, encouraging citizens to be alert and to report any suspicious behavior. The possibility that the next generation of terrorists, who are now growing up in a digital world, where hacking tools are sure to become more powerful, more simple to use and much easier to access, would be able to see predict much more danger in future cyber terrorist acts is terrifying.

REFERENCE

- Techopedia. *(n.d.).* Retrieved December 2, 2017 from http://www.interpol.int/Crime-areas/Terrorism/Counter-Terrorism-Fusion-Centre
- The Use of the Internet for Terrorist Purposes. (2012). Retrieved February 02, 2017 from https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
- http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/Crime%20Statistics%20-%202016.pdf
- CyberSecurityConclaveAtVigyanBhavanDelhi_1%20(1).pdf
- VidaVilicFINAL.pdf http://www.iosrjournals.org/iosr-jhss/papers/Vol.%2022%20Issue4/Version-5/D2204052330.pdf
- https://www.ey.com/in/en/services/advisory/ey-global-information-security-survey-2016-2017-india-report

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER TERRORISM: A GLOBAL THREAT

Dhanraj Jadhav[1] and Dr. Swati Vitkar[2]
Assistant Professor[1], BSc (IT), Narsee Monjee College of Commerce & Economics, Vile Parle (West), Mumbai
Assistant Professor[2], BSc (IT), SIES (Nerul) College of Arts, Science and Commerce, Nerul, Navi Mumbai

ABSTRACT
In this research paper, we present a broad overview on the impact of cyber terror campaign which is a threat in front of the world. In today's world, the cyber terror campaign has turn out to be a hazard not just for few Asian countries but it has turn into a hazard to all communities across the world. In our paper, we have presented the existing laws and acts in few countries like US, UK, India, Canada and Australia. We have also considered the threat of cyber terror campaign from the Indian IT Act 2000 point of view. We have done a comparative analysis of these countries from the threat of cyber terrorism. Many cyber crimes always take place through such countries where the existing laws are not capable to control or prevent such crimes. Hence the need of the hour is that all countries should come forward and create or modify existing laws in such a way that the growth of such cyber terrorism activities could be prevented in near future and the countries which are supporting such activities should be banned for lifetime by international countries.

Keywords: Cyber-terrorism; Viruses; Worms; Trojan Horse; Hacking; Al-Qaeda;

I. INTRODUCTION

Cyber terror campaign is very debatable topic. While some researchers opt for narrow definition related to deployment by various terrorist groups of disruption attacks against daily functioning of the message delivery with an intention of creating an alarm, panic, or physical disruption, others prefer broader definition which relates cybercrime. There are various forms of cyber-attack by different terror groups which are mostly intentional with an intention to slow down the economy of the nation which are highly progressing. The more formal definition of cyber intimidation is the intentional use of computer and computer resources with public internet in order to cause destruction and harm for personal benefits. Modern day experienced cyber terrorist who are very skillful causes massive disruption to government systems, education system, hospital details and national security programs which creates a panic situation in the mindset of society, country etc. The main objective of such terrorist group may be political or ideological with the intention to cause a form of terror.

The world famous terrorist group, called Al-Qaeda, used internet to communicate with supporters worldwide and even to attract and recruit new members. Estonia in April 2007, got major disruption after some disputes regarding removal of World War II soviet statue.

International terrorist organization like ISIS or Al Qaeda has already created many such kind of cyber-attacks against many nations. Some of the commonly used computer crimes are online fraud and hacking attacks which are rising day by day.

The International Terrorist Groups like AL Qaeda or ISIS has already started using such kind of cyber-attacks against the existing informational infrastructure and Internet services in various developing nations across the globe. The use of online fraud and hacking attacks merely are examples of computer-related crimes that are committed by these international hacking groups on a very large scale increasing day by day. The financial damage caused by these cybercrime is having been reported to be enormous.Because of such potential threat, many such terrorist activities are actively involved in spreading its wings in many other countries which support such activities. Various local government bodies like FBI in US and NIA in India have taken proactive steps in spreading its wings and protect the integrity and harmony within its nation[2]. Because of the rapid growth of Internet, many terrorist'sorganizations not just use media as a tool to propagate its messages to the others but uses several IT and ICT tools to target the younger generation through various networking and social media interaction. This includes publication of various articles and pictures on WhatsApp, Facebook, Twitter, Instagram and other social media which is further supplemented by sending abusive audio and video links to support their actions of brutally killing innocent people. This results in pitching an emotional call for future supporters.

Al-Qaeda is the first terrorist organization to introduce first time cyber terrorist activity. They were the one who created the videos on the internet and urging people to join their organization. They were the first few terrorist group who urged people to join them and promoted the use of cyber-attacks against developed nations. They recruited most skilled and expert individuals worldwide who used to exploit computer and computer resources by using modern day programming paradigms. Some of these types of cyber-attacks are listed below a)

ISSN 2394 - 7780

Computer Virus: It is a self-triggered computer program which infects target programs by modifying their code structures. b) Computer worms: These are self-replicating block of code which is targeted to create the functional copies of itself and thereby eating up lots of memory space. c) Hacking: This kind of crimes are basically used by developing a strategy of using modern day technologies like packet sniffing, cracking of secure firewall, highly encrypted passwords etc. to get unauthorized access to the system. d) Denial of Service(DOS): The basic intention in such type attack is not to allowed the authorized parties to get full access on their own system. e) Cryptographic technique: Some international terrorist group have started to use the encryption mechanism so that their talks with their peers in instigating terrorist activity could not be heard by various governing agencies. f) Trojans: They are the computer program which are built in such a way that they pretend to do one thing and end up doing another thing. Out of these, the most widely used attack used in Public Key Infrastructure(PKI) is the use of computer worms and viruses. These attacks can be futher classified as follows: a) Physical Attack: This is the only attack which basically aims to destroy the Public Key Infrastructure. b) Syntactic Attack: This type of attack is aimed to modify the existing system by attaching with non-existing system with intention use a secret code which will make the existing system highly vulnerable. c) Semantic Attack: Such kind of attack is usually targeted to shatter the confidence of the individual by penetrating at the gateways of the network so that the security is breached without the knowledge of the genuine user.

II. CHALLENGES

The greatest challenge which resides with the international policing agencies is to how to restrains such cyber-attacks which not only aims to destroy the public and private PKI and their assets which create a panic and destroys them. We have enlisted some of these challenges as follows a) Every nation should ensure that there should be clear definition of the terrorist activity related to cyber violence is must. b) The loopholes in existing system should be fixed so that the cyber terrorist does not expose these kind of vulnerabilities in existing system for their own benefits. C) Vulnerability of existing laws allows these attackers to easily escape from harsh punishment hence we need to amend our existing laws in such a way that such types of crimes dealt with harsher punishment. Some nations existing legislations are not enough to stop such kind of malpractices and does not restrain terrorist activities propagating via Internet since most of their existing laws are confined to the physical boundaries of the nation. If the enforcement of conventional laws and prosecution of cyber offender are not proactive, this leads to repeated number of offences in cyber-crimes made by cross border terrorist organization like Jamatuddawa and Lashkar-e-Taiba.

III. EXISTING LAWS

1. Laws in United States[5]

After 9/11 attacks on twin tower in US, their perception towards terrorism and cyber terrorism has changed. We have presenting few existing laws currently active in US

a. **The Computer Fraud and Abuse Act (CFAA) [5],** 18 U.S.C. 1030, outlaws conduct that exploits the governmental or personal computer systems. It is the most widely used cyber security law. It protects federal computers, computers resources that are installed in the banking organizations, government organizations and the personal computers which are connected to the internet. It provides the necessary shielding for them in cases of cyber attack for corruptive or disruptive gains.

b. **The USA PATRIOT ACT [6]** This act was first implemented by the Government of United States as a counter response to the to the unfortunate attack that shook the entire world on 11th September 2001 in New York City. The full abbreviation for the Act stands for “Uniting and Strengthening America by Providing Appropriate Tools Required for Intercepting and Obstruct Terrorism Act of 2001". This Act was passed by the Federal American Congress Govt. on the date of the 26th October in 2001after the 9/11 incident took place in the US. This Act basically covers issues that were related to the terrorism and the terrorist activities, but have very little provision to address the issue of cyber terrorism like cyber threats and other cyber security concerns.

c. **The Cyber Security Research and Development Act (CSRDA) [7]** This has created a provision for the American Congress to provide funds for research and development over a period of five years in the area of computer security. The National Science Foundation and the National Institute of Standards and Technology will coordinate the use of the funds

2. Laws in United Kingdom [9]

Terrorism Act 2000[9]

The UK’s interpretation of Cyber Terrorism includes any individual or group with an intension of causing politically motivated cyber-attacks directly against Government of United Kingdom or its associates and

ISSN 2394 - 7780

protects the interest of its people against such kind of attack. The Sec. 1(2)(e) of this Act deals with intended cyber-attacks which are meant to seriously interfere with or to disrupt an electronic system and provides a shield to the victim. It includes the possible threats to their internet amenities, their governmental financial exchanges, their federal computer systems or the governmental controls of their national power. According to the UK government, they rate cyber-attacks in Tier-1 and considers it highest priority risk to their national security.

3. Laws in Canada

Canada defines the cyber terrorism in its own way by the **Anti-Terrorism Act 2001 ('ATA') [10].** It defines cyber terrorism as the act of causing massive disruption of essential services by using Internet facilities which results in conduct of harm to the federal government of Canada and its people. The laws say that anyone who commits an indictable offence for a group that is engaged in terrorist activities by means of cyber warfare against its nation, the maximum penalty is up to life imprisonment.

As per the ATA, 2011 it provides a maximum penalty of life imprisonment for anyone who commits an indictable offence for a group that is engaged in terrorist activities by means of the cyber warfare against Canada or its favouring countries.

4. Laws in Australia

According to the Federal Laws of Australia they have defined terrorism into the section 100.1 of their Federal Criminal Code Act 1995 ('Australian Criminal Code') made as per by the Security Legislation Amendment (Terrorism) Act 2002 (Cth) ('SLAT Act') [8]. The SLAT Act is their main legislation package of five government bills which was formed after the events of September, 2011 attacks occurred in the USA. As amended by the SLAT Act, the Australian Criminal Code provides a maximum penalty of life imprisonment for the 'terrorist acts' committed in any jurisdiction. As per SLAT Act the Terrorist act is defined as an action or threat of action where an action is performed or a threat is made with the intention of posing a threat to sovereignty of the government of the Commonwealth or a State, Territory of the Australian government, Foreign country, or of part of a State. The public Subsection (2) of this Act lists the possible harm requirements specifically related to the cyber terrorism that prohibits the acts of terrorism against the Federal electronic systems. It includes interference and disrupting, or destroying, an electronic information system or a governmental financial system.

5. Laws in India

Post November 2008 attacks in Mumbai, The Indian government has taken a number of counter measures to prevent the use of cyberspace for the terrorist-related activities. The Indian Parliament has passed amendments to its IT Act, with addition on emphasizing on the cyber terrorism and cyber-crime, in to the existing sections the IT Act and by addition of new sections, against these cyber threats. The Indian IT Act is defined as "an Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto. The act has various sections to deal with the activities that will set up Cyber terrorism."[11] The Sec. 66 of this IT Act deals with the not permitted hacking with a computer system and its resources. This section prevents unofficial access willingly to cause disruptive loss or damage to an individual, public or public property by means of unofficial access is punishable with an imprisonment up to 3 years in jail, or with imposing a fine of which may be extend uptoRs. 200000/- or with both.

IV. SUMMARY COMPARISONS

We have considered the existing laws in USA, UK, Canada, Australia and India in curbing the cyber terrorism threat and the following is the response on some critical parameters.

ISSN 2394 - 7780

Sr no	Particulars	USA	UK	CANADA	Australia	India
1	Laws Implemented	The Computer Fraud and Abuse Act (CFAA). The USA PATRIOT ACT . The Cyber Security -Research and Development Act (CSRDA).	Terrorism Act 2000[9].	Anti-Terrorism Act 2001 ('ATA') [10].	Federal Criminal Code Act 1995. The Security Legislation Amendment (Terrorism) Act 2002 ('SLAT Act').	IT ACT 2000
2	Judicial Implications Area	Within the Jurisdiction Range of USA	Inside & Outside UK, NATO as well.	Inside or outside Canada	Within the Jurisdiction Range of Australia	Within the Jurisdiction Range of India
3	Threats Covered	CFAA shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of fraud USA PATRIOT Act enables such computer allowing authorities from intercepting communications to and from a computer system trespasser. CSRDA provides funds for research and development in the area of computer security.	cyber-attacks that destroy electronic systems, interfere with national power and water supplies, cause major economic harm, physically injure civilians, or create a national public emergency	politically motivated cyber-attacks against 'services' and 'facilities'	politically motivated denial-of-service attacks	
4	Penalties	The penalty for attempting to damage protected computers through the use of viruses or other software mechanism was set to imprisonment for up to 10 years, while the penalty for unauthorized access and subsequent damage to a protected computer was increased to more than five imprisonment	Not Addressed	The Canadian provides a maximum penalty of life imprisonment for anyone who commits an indictable offence for the benefit of, at the direction of, or in association with a group that engages in terrorist activity.	a maximum penalty of life imprisonment to cyber attacks against nonessential infrastructure in Australia or any foreign country.	Cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.
5	National Security Policy	Yet to be needed.	Clearly Announced	Yet to be needed.	Yet to be needed.	Yet to be needed.
6	Provisions of Monitoring & Electronic Surveillance	Yes	Yes	Yes	Yes	Yes
7	National Nodal Agency.	Federal Beuro of Investigation (FBI), Central Investigation Agency (CIA)	Not Addressed	Not Addressed	Not Addressed	National Investigation Agency (NIA). CERT (Computer Emergency Response Team.
8	Implementation of Computer Emergency Team.	Yes	Yes	Yes	Yes	Yes

Figure-1: A Comprehensive Review of Cyber Terrorism in the Current Scenario Tabulated data

V. CONCLUSION

From the above study we conclude that as we are growing more dependent on the Internet for our daily life activities, we are also becoming more vulnerable to any disruptions caused in and through cyberspace. The cyberspace is becoming an important area for large number of terrorists to attack on crucial information infrastructure. The existing laws are inefficient to restrain the cyber crimes and There is a need of international cooperation of nations to crack down the efficiency on cyber crime, thereby ensuring a development of the internet cybercrime is not limited to states of boundaries, thus it requires a universal collaboration of nations to work together to reduce the ever growing threats and risk to a manageable level.

ISSN 2394 - 7780

VI. REFERENCES

1. Pub. In “Tcp_ip-protocol-suite”-4th-ed-b-forouzan-mcgraw-hill- 2010-bbs
2. Pub. In proceedings of “cyber terrorism-threats” , pp. 4–5, 2011.
3. Alex P. Schmidt, “Al-Qaeda’s “Single Narrative” and Attempts to Develop Counter Narratives: The State of Knowledge”, pub. in ICCT Research Paper, Netherlands, January 2014.
4. Pub. in “Common Cyber Attacks: Reducing The Impact” by GCHQ and Cert-UK, 2015.
5. Pub. in “Computer Fraud and Abuse Act” in Fraud and Related Activity in Connection with Computers Title 18 Sec. 1030.US Code, 1999.
6. Pub. in “The USA Patriot Act: Preserving Life and Liberty” pub. by Department of Justice, Federal Govt. of United States.
7. Pub. in “Federal Cybersecurity Research and Development Strategic Plan” by the National Science and Technology Council, US Govt., 2016.
8. Pub. in “Australia’s Cyber Security Strategy” by Govt. of Commonwealth of Australia, 2016.
9. Pub. in “Terrorism Act 2000” in Legislation passed by the UK Govt., 2000.
10. Pub. in “Canada’s Anti-terrorism Act: an unjustified limitation of freedom of information and privacy rights” by The House of Commons Subcommittee on Public Safety and National Security, Canadian Govt., 2005.
11. IT Act Notified with Gazette of Govt. of India, 2000.
12. PrashantVats,"A Comprehensive Review of Cyber Terrorism in the Current Scenario"

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

SECURITY ISSUES AND CHALLENGES IN WIRELESS SENSOR NETWORK

Janhavi Kshirsagar
Assistant Professor, Computer Science, JVM Mehta College, Navi Mumbai

ABSTRACT
Recently Wireless sensor networks (WSNs) have attracted a lot of interest over researchers from various fields. WSN has numerous applications, both indoor and outdoor. However, because of placement in remote areas and scattered nature the networks are vulnerable to multiple security intimidations which can affect their performance. The problem becomes more critical for the network deployed handling mission-critical applications like in a tactical battlefield. The nodes may also fail randomly when deployed in specific scenario. WSN permanently has resource constraints in the sensor nodes, hence the traditional security mechanisms with large overhead of computation and communication are infeasible. Therefore, design and implementation of WSNs with security aspects is a challenging task. This paper provides a comprehensive discussion on the state of the art in security technologies for WSNs. It provides types of possible attacks at different layers of the communication protocol stack in a typical WSN and presents their possible remedies.

Keywords: Sensor, Security, Attack, Challenge, routing

1 INTRODUCTION
The Wireless sensor networks (WSNs) is a network of hundreds or thousands of devices each capable of sensing, processing, and communicating various parameters. WSN has many applications in a variety of areas ranging from critical military surveillance applications to forest fire checking and building security nursing in the near future [1]. Here, a great number of tiny sensor nodes are positioned to monitor a big field, in which the operational conditions are harsh or may be hostile. However, the nodes in WSNs faces severe resource constraints because of limited processing power, storage and energy. Since these networks are usually positioned in remote places and left unattended, they must be equipped with security mechanisms. This will enable the WSN to defend against attacks such as node capture, physical tampering, snooping, denial of service, etc. Unfortunately, traditionally implemented security mechanisms having high overhead are not feasible for resource constrained sensor nodes. The investigators in WSN security have proposed various security schemes which can be optimized for these networks having resource constraints. A number of secure and efficient routing protocols [2, 3], secure data aggregation protocols [4, 5] etc. are proposed by researchers in WSN security.

In addition to traditional security issues like secure routing and secure data aggregation, security mechanisms deployed in WSNs also should involve collaborations among the nodes due to the decentralized nature of the networks and absence of any infrastructure. In real-world WSNs, the nodes cannot be assumed to be reliable. Researchers have therefore, focused on building a sensor trust model to solve the problems which are beyond the capabilities of traditional cryptographic mechanisms [6, 7]. Since in most cases, the sensor nodes are unattended and physically insecure, vulnerability to physical attack is an important issue in WSNs. A number of propositions exist in the literature for defense against physical attack on sensor nodes [8, 9].

In this chapter, we present a comprehensive overview of various security issues in WSNs.

2. CONSTRAINTS IN WIRELESS SENSOR NETWORKS:
A WSN consists of a large number of sensor nodes that are inherently resource-constrained devices. These nodes have limited processing capability, very low storage capacity, and constrained communication bandwidth. These constraints are due to limited energy and physical size of the sensor nodes. Due to these constraints, it is difficult to directly employ the conventional security mechanisms in WSNs. In order to optimize the conventional security algorithms for WSNs, it is necessary to be aware about the constraints of sensor nodes [10].

Some of the major constraints of a WSN are listed below.

Energy constraints: Energy is the biggest constraint for a WSN. In general, energy consumption in sensor nodes can be categorized in three parts: (i) energy for the sensor transducer, (ii) energy for communication among sensor nodes, and (iii) energy for microprocessor computation.

Memory limitations: A sensor is a tiny device with only a small amount of memory and storage space. Memory is a sensor node usually includes flash memory and RAM. Flash memory is used for storing downloaded application code and RAM is used for storing application programs, sensor data, and intermediate results of

ISSN 2394 - 7780

computations. There is usually not enough space to run complicated algorithms after loading the OS and application code. A common sensor type-

TelosB- has a 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage. The current security algorithms are therefore, infeasible in these sensors [11].

Unreliable communication and related latency: Unreliable communication is another serious threat to sensor security. Normally the packet-based routing of sensor networks is built on connectionless protocols and thus inherently unreliable. Packets may get damaged due to channel errors or may get dropped at highly congested nodes. Furthermore, the unreliable wireless communication channel may also lead to damaged or corrupted packets. Higher error rate also mandates robust error handling schemes to be implemented leading to higher overhead. In certain situation even if the channel is reliable, the communication may not be so. This is due to the broadcast nature of wireless communication, as the packets may collide in transit and may need retransmission [1].

The synchronization issues may sometimes be very critical in security as some security mechanisms may rely on critical event reports and cryptographic key distribution [12].

Unattended operation of networks: In most cases, the nodes in a WSN are deployed in remote regions and are left unattended. The likelihood that a sensor encounters a physical attack in such an environment is therefore, very high. Remote management of a WSN makes it virtually impossible to detect physical tampering. This makes security in WSNs a particularly difficult task.

3. SECURITY REQUIREMENTS IN WIRELESS SENSOR NETWORKS

The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehavior of nodes. The most important security requirements in WSN are;

Data confidentiality: The security mechanism should ensure that no message in the network is understood by anyone except intended recipient.

Data integrity: The mechanism should ensure that no message can be altered by an entity as it traverses from the sender to the recipient.

Availability: This requirements ensures that the services of a WSN should be available always even in presence of an internal or external attacks such as a denial of service attack (DoS).

Self-organization: Each node in a WSN should be self-organizing and self-healing. This feature of a WSN also poses a great challenge to security.

Secure localization: In many situations, it becomes necessary to accurately and automatically locate each sensor node in a WSN. For example, a WSN designed to locate faults requires accurate locations of sensor nodes to identify the faults.

Authentication: It ensures that the communicating node is the one that it claims to be. An adversary can not only modify data packets but also can change a packet stream by injecting fabricated packets.

4. SECURITY THREATS AND ISSUES IN WIRELESS SENSOR NETWORKS

WSNs are vulnerable to various types of attacks. These attacks can be broadly categorized as follows [13]:

• Attacks on secrecy and authentication: standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets.

• Attacks on network availability: attacks on availability are often referred to as

Denial-of-service (DoS) attacks. DoS attacks may target any layer of a sensor network.

• Stealthy attack against service integrity: in a stealthy attack, the goal of the attacker is to make the network accept a false data value. For example, an attacker compromises a sensor node and injects a false data value through that sensor node.

4.1 Attacks in Wireless Sensor Networks

Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Here we point out the major attacks in wireless sensor networks.

ISSN 2394 - 7780

4.1.1 Denial of Service (paper on security)
Denial of Service (DoS) [8] is produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy

a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

4.1.2 Physical layer attacks
The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption [1]. As with any radio-based medium there exists the possibility of jamming in WSNs. There are two broad categories of attack on WSNs in the physical layer: (i) jamming and (ii) tampering.

4.1.3 Link layer attacks
The link layer is responsible for multiplexing of data-streams, data frame detection, medium access control, and error control [1]. Attacks at this layer include purposefully created collisions, resource exhaustion, and unfairness in allocation. A collision occurs when two nodes attempt to transmit on the same frequency simultaneously [9].

4.1.4 Network layer attacks
The network layer of WSNs is vulnerable to the different types of attacks such as: (i) spoofed routing information, (ii) selective packet forwarding, (iii) sinkhole, (iv) Sybil, (v) wormhole, (vi) blackhole and grayhole, (vii) HELLO flood, (viii) Byzantine, (ix) information disclosure, (x) acknowledgment spoofing etc.

Spoofed routing information: the most direct attack against a routing protocol is to target the routing information in the network.

Selective forwarding: in a multi-hop network like a WSN, for message communication all the nodes need to forward messages accurately.

Sinkhole: In a sinkhole attack, an attacker makes a compromised node look more attractive to its neighbors by forging the routing information [9, 14, and 15]. The result is that the neighbor nodes choose the compromised node as the next-hop node to route their data through.

Sybil attack: it is an attack where one node presents more than one identity in a network. It was originally described as an attack intended to defeat the objective of redundancy mechanisms in distributed data storage systems in peer-to-peer networks [16].

Wormhole: a wormhole is low latency link between two portions of a network over which an attacker replays network messages [14]. This link may be established either by a single node forwarding messages between two adjacent but otherwise non-neighboring nodes or by a pair of nodes in different parts of the network communicating with each other.

HELLO flood: most of the protocols that use HELLO packets make the naïve assumption that receiving such a packet implies that the sender is within the radio range of the receiver.

Information disclosure: a compromised node may leak confidential or important information to unauthorized nodes in a network. Such information may include information regarding the network topology, geographic location of nodes, or optimal routes to authorized nodes in the network.

4.1.5 Transport layer attacks
The attacks that can be launched on the transport layer in a WSN are flooding attack and de-synchronization attack.

The possible DoS attacks and the corresponding countermeasures are listed in Table 1.

Table-1: Attacks on various layers of a WSN and their countermeasures

Layer	Attacks	Defense
Physical	Jamming	Spread-spectrum, priority messages, lower duty

ISSN 2394 - 7780

		cycle, region mapping, mode change
Link	Collision Exhaustion Unfairness	Error-correcting code Rate limitation Small frames
Network authentication,	Spoofed routing information & Selective forwarding Sinkhole Sybil Wormhole HELLO Flood Acknowledgment flooding	Egress filtering, Authentication, monitoring Redundancy probing Authentication, monitoring, redundancy Authentication, probing Authentication, packet leashes by using geographic and temporal info Authentication, verify the bi-directional link Authentication
Transport	Flooding De-synchronization	Client puzzles Authentication

Source: Y. Wang, G. Attebury, and B. Ramamurthy, IEEE Communications Surveys and Tutorials, Vol. 8, no. 2, pp. 2- 23, 2006.

4.2 Attacks on secrecy and authentication

There are different types of attacks under this category.

4.2.1 Node replication attack

In a node replication attack, an attacker attempts to add a node to an existing WSN by replication (i.e. copying) the node identifier of an already existing node in the network [17].

4.2.2 Attacks on privacy

Since WSNs are capable of automatic data collection through efficient and strategic deployment of sensors, these networks are also vulnerable to potential abuse of these vast data sources. Privacy preservation of sensitive data in a WSN is particularly difficult challenge [18].

5. SECURITY MECHANISMS FOR WIRELESS SENSOR NETWORKS

First, different cryptographic mechanisms for WSNs are presented. Both public key cryptography and symmetric key cryptographic techniques are discussed for WSN security. Various methods of defending against DoS attacks, secure broadcasting mechanisms and various secure routing mechanisms are also discussed. In addition, various mechanisms for defending the Sybil attack, node replication attack, traffic analysis attacks, and attacks on sensor privacy are also presented. Finally, intrusion detection mechanisms for WSNs, secure data aggregation mechanisms and various trust management schemes for WSN security are discussed.

5.1 Cryptography in WSNs

Selecting the most appropriate cryptographic method is vital in WSNs as all security services are ensured by cryptography. Cryptographic methods used in WSNs should meet the constraints of sensor nodes and be evaluated by code size, data size, processing time, and power consumption. Public key algorithms such as RSA and SHA. Symmetric key cryptographic mechanisms use a single shared key between the two communicating host which is used both for encryption and decryption. Five popular encryption schemes RC4, RC5, IDEA, SHA-1, and MD5 can be used.

5.2 Key management protocols

The area that has received maximum attention of the researchers in WSN security is key management. Key management is a core mechanism to ensure security in network services and applications in WSNs. The goal of key management is to establish the keys among the nodes in a secure and reliable manner. The key management protocols can be for the centralized key scheme, distributed key scheme, probabilistic key scheme and deterministic key scheme.

5.3 Defense against DoS attacks

Various types of DoS attacks in WSNs have been discussed in previous Section. In this section, defense mechanisms for each of those attacks are presented in detail.

ISSN 2394 - 7780

5.3.1 Defense mechanisms in the physical layer
Jamming attack may be defended by employing variations of spread-spectrum communication such as frequency hopping and code spreading. One approach for tolerance against jamming attack in a WSN is to identify the jammed part of the network and effectively avoid it by routing around.

5.3.2 Defense mechanisms in the link layer
A typical defense against collision attack is the use of error-correcting codes. A possible solution for energy exhaustion attack is to apply a rate limiting MAC admission control. A second technique is to use time-division multiplexing where each node is allotted a time slot in which it can transmit.

5.3.3 Defense mechanisms in the network layer
A countermeasure against spoofing and alteration is to append a message authentication code

(MAC) after the message. By adding a MAC to the message, the receivers can verify whether the messages have been spoofed or altered. To defend against replayed information, counters or time-stamps may be introduced in the messages. A possible defense against selective forwarding attack is using multiple paths to send data. A second defense is to detect the malicious node or assume it has failed and seek an alternative route.

5.4 Defense against attacks on routing protocols
Many routing protocols have been proposed for WSNs. These protocols can be divided into three broad categories according to the network structure: (i) Flat structure-based routing, (ii) hierarchical structure-based routing, and (iii) location-based routing.

5.5 Defense against Sybil attacks
Any defense mechanism against the Sybil attack must ensure that a framework must be in place in the network to validate that a particular identity is the only identity being held by a given physical node [15].

5.6 Defense against physical attacks
To protect against a possible physical attack, sensor nodes may be equipped with special hardware. The sensor nodes in a WSN may be protected against tampering by tamper-proofing the physical packages of the sensors. A mechanism that focus on building tamper-resistant hardware in order to make the memory contents on the sensor chip inaccessible to a potential external attacker is also proposed.

6. CONCLUSIONS
Although research efforts have been made on cryptography, key management, secure routing, secure data aggregation, and intrusion detection in WSNs, there are still some challenges to be addressed. First, the selection of the appropriate cryptographic methods depends on the processing capability of sensor nodes, indicating that there is no unified solution for all sensor networks. Instead, the security mechanisms are highly application-specific. Second, sensors are characterized by the constraints on energy, computation capability, memory, and communication bandwidth. The design of security services in WSNs must satisfy these constraints. Third, most of the current protocols assume that the sensor nodes and the base station are stationary. However, there may be situations, such as battlefield environments, where the base station and possibly the sensors need to be mobile. The mobility of sensor nodes has a great influence on sensor network topology and thus raises many issues in secure routing protocols.

REFERENCES
1. Akyildiz, F., W. Su, Y. Sankarasubramaniam, and E. Cayirci. August 2002. “A Survey on Sensor Networks.” IEEE Communications Magazine 40 (80): 102 – 114.
2. Deng, J., R. Han, and S. Mishra. November 2002. “INSENS: Intrusion-Tolerant Routing in Wireless Sensor Networks”, Technical Report CU-CS-939-02, Department of Computer Science, University of Colorado at Boulder, November 2002.
3. Tanachaiwiwat, S., P. Dave, R. Bhindwale, and A. Helmy. November 2003. “Routing on Trust and Isolating Compromised Sensors in Location-Aware Sensor Networks.” In Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (ACM SenSys’03), 324-325, Los Angeles, USA.
4. Estrin, D., R. Govindan, J. S. Heidemann, and S. Kumar. 1999. “Next Century Challenges: Scalable Coordination in Sensor Networks.” In Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom’99), 263-270, Seattle, Washington, USA, August 1999.

ISSN 2394 - 7780

5. Ye, F., L. H. Luo, and S. Lu. March 2004. “Statistical En-Route Filtering of Injected False Data in Sensor Networks.” In Proceedings of the 23rd IEEE Joint Annual Conference of Computer and Communication Societies (IEEE INFOCOM’04), vol 4, 2446-2457, Hong Kong, China.
6. Ganeriwal S., and M. Srivastava. 2004. “Reputation-Based Framework for High Integrity Sensor Networks.” In Proceedings of the 2nd ACM Workshop on Security on Ad Hoc and Sensor Networks (SASN’04), 66-77, Washington DC, USA.
7. Zhu, H., F. Bao, R. H. Deng, and K. Kim. September 2004. “Computing of Trust in Wireless Networks.” In Proceedings of 60th IEEE Vehicular Technology Conference, Los Angeles, California, USA.
8. Anderson, R., and M. Kuhn. November 1996. “Tamper Resistance- A Cautionary Note.” In Proceedings of the 2nd USENIX Workshop on Electronic Commerce (WOEC’96), 1-11, Oakland, California, USA
9. Wood A. D., and J.A. Stankovic. 2002. “Denial of Service in Sensor Networks.” IEEE Computer, 35 (10), 54-62.
10. Carman, D. W., P. S. Krus, and B. J. Matt. 2000. “Constraints and Approaches for Distributed Sensor Network Security.” Technical Report 00-010, NAI Labs, Network Associates Inc., Glenwood, MD, USA.
11. Perrig, A., R. Szewczyk, V. Wen, D. E. Culler, and J. D. Tygar. 2002. “SPINS: Security Protocols for Sensor Networks.” Wireless Networks, 8 (5): 521-534.
12. J.A. Stankovic, J. A. , T. Abdelzaher, C. Lu, L. Sha, and J. Hou. July 2003. “Real-Time Communication and Coordination in Embedded Sensor Networks.” In Proceedings of the IEEE, 91(7): 1000-1022.
13. Shi E., and A. Perrig. December 2004. “Designing Secure Sensor Networks.” Wireless Communication Magazine, 11 (6): 38-43.
14. Karlof C., and D. Wagner. May 2003. “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures.” In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, 113-127, Anchorage, Alaska, USA.
15. Newsome, J., E. Shi, D. Song, and A. Perrig. 2004. “The Sybil Attack in Sensor Networks: Analysis and Defenses.” In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, 1259-1268.
16. Douceur, J. March 2002. “The Sybil Attack.” In Proceedings of the 1st International Workshop on Peer-to-Peer Systems (IPTPS’02), 251-260, Cambridge Massachusetts, USA, Springer LNCS, Vol. 2429.
17. Parno, B., A. Perrig, and V. Gligor. May 2005. “Distributed Detection of Node Replication Attacks in Sensor Networks.” In Proceedings of the IEEE Symposium on Security and Privacy (S&P’05), 49-63, Oakland, California, USA.
18. Gruteser, M., G. Schelle, A. Jain, R. Han, and D. Grunwald. May 2003. “Privacy-Aware Location Sensor Networks.” In Proceedings of the 9th USENIX Workshop on Hot Topics in Operating Systems (HotOS IX), Vol 9, 28, Lihue, Hawaii, USA.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

HUMAN RIGHTS UNAWARENESS AND VIOLATION IN CYBERSPACE IN INDIA UNDER HUMAN RIGHTS IN CYBER WORLD

Satanuka Sinha
Assistant Professor, Pillai College of Arts, Commerce and Science, New Panvel

ABSTRACT
The paper focuses on the Human Rights in Cyber World and the lack of awareness regarding the violation of rights unknowingly in India. Cyberspace has been in boom recently in the youth as well as middle -aged age group. But due to lack of awareness about the cyber-crime which prevails the Indian youth and middle-aged group to use cyberspace freely, lot of law and order issues happen in the actual world due to the virtual world. The human rights violation like hatred messages are forwarded by the society without checking the accuracy of the messages. There are cases where due to rumours forwarded through social media, a person, or a family gets affected without checking the correctness of the information forwarded. Many people lost their lives due to the hatred message or rumours forwarded in the cyber world which violates the basic human rights of a common man in India. This paper will focus on what human rights are under cyberspace, which crimes a common person in India commits by forwarded message.

Keywords: cyberspace, cyber-crime, human rights.

INTRODUCTION:

The paper introduces and highlights the current condition in the cyber space, how the common man is trapped in the cyber world and forwards the messages using Social media without understanding the future consequences and in return unknowingly becomes part of the crime even though the intention of the person is good. This happens due to people blindly following the herd and forwarding the messages which can lead to creation of fear and disturbance in law and order along with the violation of human rights of a common man. Human rights can be explained in a simple way as the fundamental rights of a human being to live a life in a dignified manner.

LITERATURE SURVEY:

One of the important reasons of such cyber-crime human rights violation is due to the huge number of social media users which is based in various demographics of India. The huge number of internet users which was estimated at around 200 million in 2016 has gone up to about 500 million users in India in 2018 has users made its own benefits; however misuse of this technology has now proven to fuel rumours across the nation resulting in cybercrimes towards violation of human rights.

Factors that have contributed to the ever increasing number of users are ease of access to the internet and sharing content in multiple regional languages, availability of low cost smart phones with equally inexpensive data plans.

There has been numerous mob lynching and attacks in recent years due to the social media rumours which not just violated the basic dignity of individuals but also involving deaths in most of the cases.

It has been observed many a times when a national or state disaster takes place, the chances of rumours flooding through social media is commonly seen.

It is imperative that the content of social media travels almost at the speed of light. Thus, in some scenarios the governments were forced to shut down access to internet in order to stop any kind of social media related content to spread.

Though these efforts are somewhat effective in its own way, it comes with a downside as it involves taking down the access to internet. Thus there is a need for a more efficient way to address the issue. The Government has asked social media companies to take concrete steps to prevent misuse of their platforms.

Statistics of Violation of human rights in cyberspace:

According to the sources, there has been a 20% rise in cyber crime in the year 2016. Most of the cyber crime cases conviction rate is abysmally low. This data is about the crimes committed like cyber spoofing, theft of intellectual property, cyber stalking, money laundering through computer system using cyber space which is trackable but the rumours in the form of forwarded texts and pictures in social media becomes difficult for the cyber crime branch to track the source and to stop the spreading of the same among common man which creates an environment of hatred and riot-like situation. This becomes a human right violation for the common man to

ISSN 2394 - 7780

live in dignity and without fear. In such cases the conviction becomes lower than the cases of other cyber crime as it is difficult for the police to track down the actual culprit.

OBJECTIVE OF THE RESEARCH:

- To focus on the violation of human rights of common man.
- To understand how unknowingly common man becomes a part of cyber crime by forwarding social media rumours bringing law and order chaos.

RESEARCH METHODOLOGY:

The secondary data has been collected from news articles and various online magazines.
Formulation of hypotheses
Following hypothesis was taken into consideration.

The dimension taken here is does social media violates the human rights if used irresponsibly.

H0: The irresponsible use of social media has no significant effect on violation of human rights.

H1: The irresponsible use of social media has significant effect on violation of human rights.

DATA COLLECTION:

The primary data which has been collected through google forms consist of few questions mentioned below.

- How frequently the social media is used?
- How much Social Media is important in life?
- Do you check the history or genuine level of the messages you get ?
- Do you forward messages because of the hype created around it?
- Have you given a thought about how a message can violate someone's basic human rights?

It was concluded that most of the people due to emotional factor forward the fake messages thinking that it will help people without cross examining of the fact and are not aware that if social media used irresponsibly can lead to violation of human rights. Hence H1 hypotheses failed.

Human rights protection in Cyberspace:

It is high time that the Human Rights has to be protected in Cyberspace and has to be given equal importance just like the traditional human rights protection. This has to be done not just at national but also at an international level because it is not a problem in any particular country but it is prevailing throughout the world. Due to jurisdiction and the sensitive nature of the case, it becomes difficult to crack and sometimes it takes years to go into the depth of finding the source of the fake news. The government and cyber crime branch has taken many measures and IT Act 2000 is being introduced in India in order to give equal importance of cyber crime as a traditional crime.

CONCLUSION:

This focuses on the cyber hygiene and introduction of cyber law at school level in order to curb the problem of fake news and rumours to be spread especially during any National disaster. The students should sense the importance at an early age in education that how a social media rumour can affect the human rights in the form of living life with dignity and not considering them as kidnappers in order to avoid mob lynching by the people.

REFERENCES

- https://timesofindia.indiatimes.com
- https://www.news18.com
- https://www.statista.com/
- https://www.livemint.com/
- www.quora.com
- www.washingtonpost.com

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER LAW – "REVIEW OF IPR IN CYBER WORLD"

Ashwini Amit Gangal
JVM's Mehta College of Arts, Science and Commerce, Navi Mumbai

ABSTRACT
Computers are an essential part of our life. A sufficiently great percentage of today's transactions and processes take place using the computer and Internet. People have readily chosen Internet technology and trusted it while using it avoiding the limitations and threats to the system security. With the advance of technology, crimes started emerging. Different types of cyber-attacks from various sources may adversely affect computers, software, a network, an industry, or the Internet itself. Thus companies and their products aim to take help of legal and computer forensics. Digital forensics deals with computer-based facts to determine who, what, where, when, and how crimes are being committed. Computer and network forensics has evolved to assure proper presentation of cybercrime, serving data into court. Forensic tools and techniques are an integral part of criminal investigations used to investigate suspect systems, gathering and preserving proofs, reconstructing the event, and assessing the current state of an event. In this paper we focus on two aspects; first, various types of crimes in the cyber space and various sources of cyber-attacks, and second, investigation processes for various cyber-attacks with the assistance of digital rhetorical tools. This paper acts as a litmus test to ascertain the employment and misuse of cyberspace. The only difference between a traditional crime and a cybercrime is that the cybercrime involves in a crime related to computers.

Keywords: Cyber-crime, Cyber space, Digital forensic, Intellectual Property Rights

INTRODUCTION
Intellectual property rights are ruled by WIPO, the world property Organization. WIPO uses global policy and protects IPR across borders. Intellectual property rights are the legal rights that cover the special rights given to individuals who are the holders and creators of a work, and have created something with their creativity. The creator gets exclusive rights against any misuse of work without his/her prior information. However, the rights are granted for a restricted amount of your time to keep up equilibrium.

The following list of activities that are lined by the property rights are ordered down by the World Intellectual Property Organization (WIPO) −

- Industrial designs.
- Scientific findings.
- Protection against unfair competition.
- Trademarks, commercial names.
- All other rights resulting from intellectual activity in the industrial, scientific, literary, or artistic fields.

TYPES OF INTELLECTUAL PROPERTY RIGHTS
Intellectual Property Rights will be further classified into the subsequent classes −

- Copyright : The exclusive legal right given to creator for fixed number of years, to print, publish etc.
- Patent : A government authority conferring a right for a set period.
- Design Rights : It gives us exclusive right for the appearance of that particular product.
- Trademarks : A symbol/word legally registered by use as representing a company or product.
- Database rights : It protects investment in obtaining, verifying and presenting the contents of database.
- Performers rights : It is a right to perform music in public.

ADVANTAGES OF INTELLECTUAL PROPERTY RIGHTS
Intellectual property rights are advantageous in the following ways −

- Provides exclusive rights to the creators or inventors.
- Encourages individuals to distribute and share information and data instead of keeping it confidential.

ISSN 2394 - 7780

- Provides legal defence and offers the creators the incentive of their work.
- Helps in social and financial development.

INTELLECTUAL PROPERTY IN CYBER SPACE

Every new invention within the field of technology experiences a spread of threats. Internet is one such threat, which has captured the physical marketplace and have converted it into a virtual marketplace.

To safeguard the business interest, it is vital to create an effective property management and protection mechanism keeping in mind the considerable amount of business and commerce taking place in the Cyber Space. Today it's vital for each business to develop a good and cooperative IP management mechanism and protection strategy. The ever-looming threats in the cybernetic world can thus be monitored and confined. Various approaches and legislations have been designed by the law-makers to up the ante in delivering a secure configuration against such cyber-threats. However it's the duty of the intellectual property right (IPR) owner to invalidate and cut back such mala fide acts of criminals by taking proactive measures.

To design and implement a secure cyberspace, some stringent strategies have been put in place.

This chapter explains the foremost methods utilized to make sure cybersecurity, which include the following −

- Creating a Secure Cyber Ecosystem
- Creating an Assurance Framework
- Encouraging Open Standards
- Strengthening the Regulatory Framework
- Creating Mechanisms for IT Security
- Securing E-governance Services
- Protecting Critical Information Infrastructure

A strong cyber-ecosystem has 3 dependent structures − Automation, Interoperability, and Authentication.

- Automation − It eases the implementation of advanced security measures, enhances the swiftness, and optimizes the decision-making processes.
- Interoperability − It toughens the collaborative actions, improves awareness, and accelerates the learning procedure. There are three types of interoperability –
- Semantic (i.e., shared lexicon based on common understanding)
- Technical
- Policy − Important in assimilating different contributors into an inclusive cyber-defence structure.
- Authentication − It improves the identification and verification technologies that work in order to provide –
- Security
- Affordability
- Ease of use and administration
- Scalability
- Interoperability

COMPARISON OF ATTACKS

The following table shows the Comparison of Attack classes against Desired Cyber system Capabilities –

ISSN 2394 - 7780

Categories of Cyber Attack								
Desired Cyber Ecosystem Capabilities	Attrition	Malware	Hacking	Social Tactics	Improper Usage (Insider)	Physical Action; Loss or Theft	Multiple Component	Other
Automation	x	x	x	x	x	x	x	x
Authentication	x	x	x	x		x	x	x
Interoperability	x	x	x	x			x	
Automated Defense Identification, Selection, and Assessment	x	x	x	x	x	x	x	x
Build Security In	x	x	x	x		x	x	x
Business Rules-Based Behavior Monitoring	x	x	x	x	x	x	x	x
General Awareness and Education	x	x	x	x	x	x	x	x
Moving Target	x	x	x	x			x	x
Privacy	x	x	x	x	x	x	x	x
Risk-Based Data Management	x	x	x	x	x	x	x	x
Situational Awareness	x	x	x	x	x	x	x	x
Tailored Trustworthy Spaces	x	x	x	x			x	x

TYPES OF ATTACKS

The following table describes the attack categories −

Attack Category	Description of Attack
Attrition	Methods used to damage networks and systems. It includes the following − • distributed denial of service attacks • impair or deny access to a service or application • resource depletion attacks
Malware	Any malicious software used to interrupt normal computer operation and harm information assets without the owner's consent. Any execution from a removable device can enhance the threat of a malware.
Hacking	An attempt to intentionally exploit weaknesses to get unethical access, usually conducted remotely. It may include − • data-leakage attacks • injection attacks and abuse of functionality • spoofing • time-state attacks • buffer and data structure attacks • resource manipulation • stolen credentials usage • backdoors • dictionary attacks on passwords • exploitation of authentication
Social Tactics	Using social tactics such as deception and manipulation to acquire access to data, systems or controls. It includes − • pre-texting (forged surveys)

ISSN 2394 - 7780

	• inciting phishing • retrieving of information through conversation
Improper Usage (Insider Threat)	Misuse of rights to data and controls by an individual in an organization that would violate the organization's policies. It includes − • installation of unauthorized software • removal of sensitive data
Physical Action/Loss or Theft of Equipment	Human-Driven attacks such as − • stolen identity tokens and credit cards • fiddling with or replacing card readers and point of sale terminals • interfering with sensors • theft of a computing device used by the organization, such as a laptop
Multiple Component	Single attach techniques which contains several advanced attack techniques and components.
Other	Attacks such as − • supply chain attacks • network investigation

CYBERSTALKING

Cyberstalking is use of the web and email to "stalk" another individual. The crime of stalking has existed for decades; stalking refers to recurrent harassment of somebody wherever the stalker acts in a very threatening behaviour toward the victim. Threatening behaviours embody following the victim, showing at the victim's place of labour or close to his or her home, then making eye contact so the victim knows someone is following, and feat threatening messages on paper or the phone. Stalking leaves its victims afraid of bodily damage or death.

Intellectual property pirates use the pc to steal immense amounts of proprietary material and cause severe injury to the victimised firms. Internet pirates target the net shoppers WHO rummage around for discounted, however legitimate, products. They do therefore by emails and web advertisements that appear to be the important issue. Not simply people, however firms, academic establishments, and even government agencies are tricked by information processing pirates into shopping for taken merchandise.

Intellectual property pirates additionally return from several foreign countries like China, Asian country, Vietnam (Southeast Asia), and Russia. International IP law is practically non-existent. While offline IP violations can be investigated by the traditional law enforcement tactics such as using undercover agents, cyber IP criminals operate only in cyberspace and can disappear in seconds. Cyber Crimes area unit on the increase in India and this poses a challenge for law manufacturers and enforcement agencies because of the greatness and reach of the cyber house.

CONCLUSION

Intellectual property rights are monopoly rights that grant their holders the temporary privilege for the exclusive exploitation of the income rights from cultural expressions and inventions. There must be good reasons for a society to grant such privileges to some of its individuals, and therefore the proponents of these rights have provided all the widely accepted justifications to defend.

To argue for the abolition of intellectual property rights we have to challenge all the justifications. Therefore we have discussed whether a creator or inventor can be considered as the owner of an expression or an innovation because he is the individual who created or invented something.

We have seen that 2 elements are sometimes mentioned as justifications for such individual possession.

There are several smart reasons to question the justifications for intellectual property rights and so it's time to begin the political discussion regarding the ending of those rights to

create a world during which belongings is common property.

REFERENCES

1. "Intellectual Property Rights" by Neeraj Pandey and Khushdeep Dharni

ISSN 2394 - 7780

2. "Intellectual Property Rights In India" by V K Ahuja
3. https://superioressaypapers.com/write-research-paper-intellectual-property-rights/
4. https://hbswk.hbs.edu/Pages/browse.aspx?HBSTopic=Intellectual%20Property
5. https://www.southcentre.int/wp-content/uploads/2016/07/RP69_IP-and-Access-to-Science_EN.pdf
6. https://www.theguardian.com/law/intellectual-property

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER TERRORISM, CYBER WARFARE AND ITS SECURITY MEASURES

Gaurav Sanjay Ghadge
Jnan Vikas Mandal's Mehta Degree College, Navi Mumbai

ABSTRACT
This Study Discusses The Problems Of Terrorism In Cyberspace And Examines The Real Truth Of The Perceptions Of This Problem That Have Formed In Recent Years. Timeline Of Preceding Cyber Terrorism, Why They Use Cyber Terrorism And What Internet Offers To Terrorist And Also We Are Going To See Some Cyber Warfare Over All World And Some Points On How To Over Come On It.

Keywords: Cyber Terrorism, Cyber Warfare, Internet, Government, solutions

INTRODUCTION
- The act of terrorism is one amongst the foremost regarding and necessary areas of security for all national states.
- As mentioned by Garrison (2003), act of terrorism encompasses a history of over 2000 years, qualitative analysisback to forty eight AD whereby the somebody resistance cluster Sicarii-Zealots allotted attacks against Romans.
- by teams of people with explicit motivations, willing to cause hurt to innocent civilians to push their cause.
- Aims and methodology this study aims to deal with the growing concern of cyber act of terrorism.

CYBER TERRORISM
- Through internet tools to slow down or shut down critical structure of orgs.
- Orgs such as transport, government actions etc
- Or to force and terrorize a government or civilian population."
- The intimidation of public enterprise through the use of great (high) technology or deleting censorious structural data or information.
- terrorist programs intended to damage vital computer systems
- The term was invented in the 1980s by Barry Collin, a senior research fellow(man) at the organization for Security and Intelligence in California, who in 1997 was accredited for creation of the term "Cyberterrorism", shows terrorist act because the convergence of IP and terrorism.

WHAT CYBER TERRORISM IS NOT!
- You can tell as Cyber terrorism is a part of information warfare, but information warfare is not cyber terrorism.
- None of the three, however, are similar with cyber terrorism
- IW, EW, and IO encompass the use of coding, jammers, high-altitude aerial reconnaissance, electronic surveillance, electronically acquired insight, and secret writing.
- IW, EW, and IO stands for (Information warfare), (electronic warfare), (information operation)
- Cyber terrorists may use these same tools.
- The important, however, is not the technological tools they use but the context and target.

TIMELINE OF PRECEDING EVENTS AND SOME HISTORICAL FACTS
- Early 1970s-Early starting of the internet during the days of the Cold War, when the U.S. Division of Defense wanted to reduce the subjection of its communication networks to nuclear attack.
- Late 1980s- Net opened up to mercantile (commercial) users.
- Mid 1990s thenetwork (Internet) connected more than 18,000 private, public, and national networks. With increasing amount along with 3.2 million multitude (host) computers and as many as 60 million users spread across the globe.

ISSN 2394 - 7780

HISTORICAL FACTS

- One of the first visibled cyber-terrorist attacks was in 1996 when a computer hacker reportedly associated with the White Supremacist movement shortly disabled a Massachusetts web net service provider (ISP) and harm the part of the ISP's track keeping system.
- The ISP had tried to stop the hacker from sending out globally racist messages under the ISP's name.
- The hacker loggedoff with the threat, "you have yet to see true electronic terrorism.
- Since 1996, attacks have pursued with high increasing severity.

WHY CYBER TERRORISM? AND COUNTRIES WITH MOST HACKS AND TERRORISM

- low cost able than other methods.
- higher difficulty level to get caught.
- Can be done from anyplace
- Can be done from any where
- Can harm more people

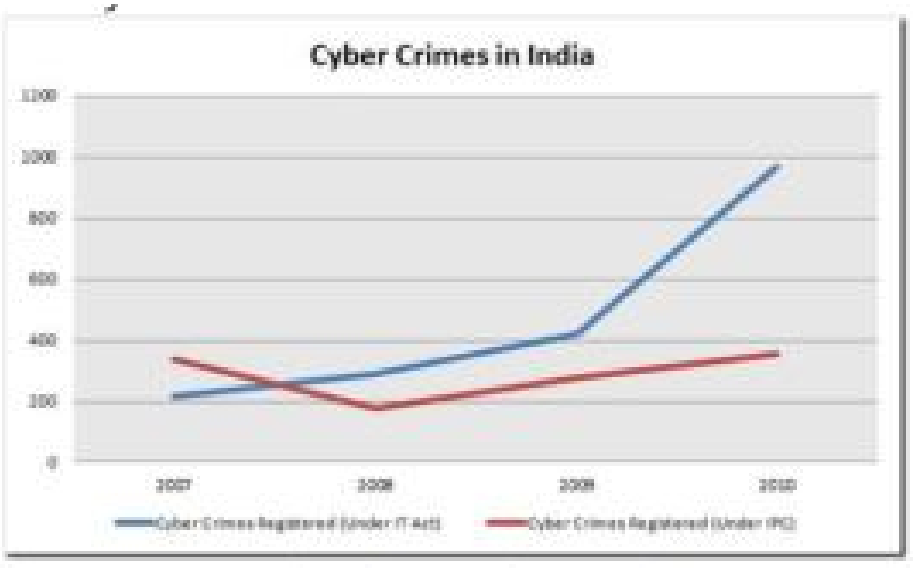
COUNTRIES WITH MOST CYBER HACKS AND TERRORISM

1. China = 41 %(of the world's attack traffic)
2. United States = 10%
2. Turkey = 4.7%
4. Russia = 4.3%
5. Taiwan = 3.7 %
6. brazil = 3.3%
7. Romania = 2.8%
8. India = 2.3%
9. Italy = 1.6%

MORE STATISTICS IN TERM OF INDIA

Even as web net population in India has extended a crossed 100 million, cyber-crimes are increasing. There are huge types of cyber-crimes: Phishing attacks, Identity Theft, Website hacks, creating Trojans (viruses) all amount to cyber crimes. The reasons for cyber-crimes are differ as well. Some do it out of hate(loathe), some out of greediness while some do it just for kicks! At same time some cyber attacks (if it can be known for constructive certainty feedback as well!

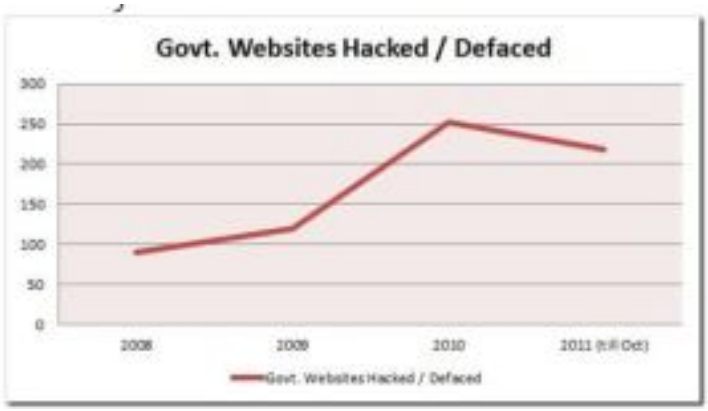
One of the main aims of attacks world over are administration websites – They not only furnish big coverage to attacker, but also furnish with very high sensitivity &secretively with government data. Govt. of India today published the number of cyber-attacks it is proof As per numbers released by National Crime Records Bureau, Cyber Crime cases registered under IT Act more than twice, from 420 to 966 amid(between) year 2009 and 2010.



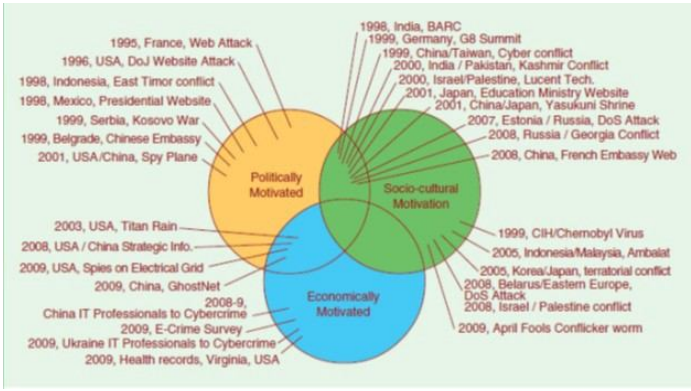
We have covered about three instances where high-profile Government websites were hacked and vandalize. However, the actual amount of Government Websites that were hacked are quite high.

ISSN 2394 - 7780

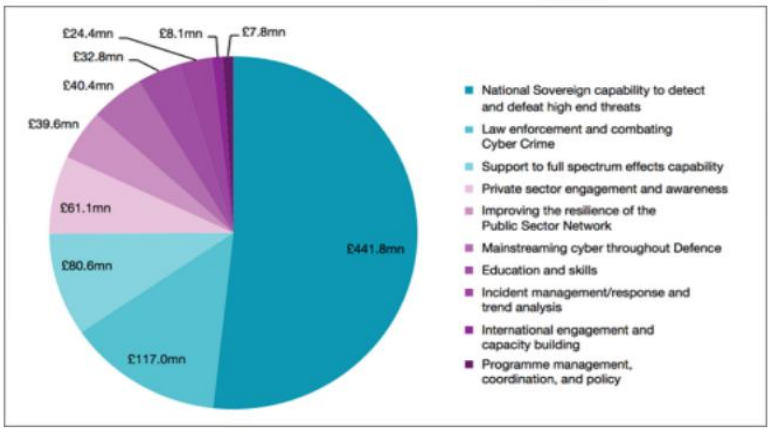
A total number of (90, 119, 252 and 219) administrating websites traced by the Indian intelligence Computer Emergence Response Team were hacked and vandalize by various hacking clan in the year 2008, to Jan–Oct 2011 respectively.



- ***The distribution of cyber-attack over social, cultural, political and economical motivation:***



- ***Five year spending review of the government program to improve the National Cyber Security Strategy The distribution of cyber-attacks across cultural, social, economic and political motivations:***



Some Cyber terrorist organizations all over the world and some banned organizations in India

Today the amount exceeds more than 40 terrorist orgs that maintain websites and use distinguished languages.

Their websites provide with inform about the organization.

Some of their purposes are to change public opinion, weak down public support for a governing regime, and even take them low.

FROM THE MIDDLE EAST

- The Unix Security Guards (pro Islamic group)
- The Popular Front for the Liberation of Palestine
- The Anti-India Crew

ISSN 2394 - 7780

FROM EUROPE

- The Irish Republican Army
- The Basque ETA movement.

SOME BANNED ORGANIZATIONS INDIA

The cabinet Ministry of Home Affairs of India has prohibited a number of orgs that have been denounce as terrorist orgs under the illegal occupation (Prevention) Act.

- Akhil Bharat Nepali EktaSamaj (ABNES)
- Al-Badr (Jammu and Kashmir)
- All Tripura Tiger Force
- Al-Qaeda
- Al-Umar-Mujahedeen
- BabbarKhalsaInternational
- Communist Party of India (Maoist) all its evolution and forepart oforganizations.
- Communist Party of India (Marxist-Leninist) -- People's Warfare, All its evolution and forepart oforganizations.
- DeendarAnjuman
- Dukhtaran-E-Millat (DEM)
- Garo National Liberation Army (GNLA), all its evolution and forepart of organizations.

WHAT INTERNET OFFERS TO TERRORIST

- Easy access
- Minimum regulation, censorship, or any type of administration control
- Potentially large audience spread throughout the world;
- Anonymity
- Fast movement of information.
- Low-cost maintenance of a webpage.
- A multimedia environment (the ability to combine text, graphics, audio, and so forth);
- The capacity to shape coverage in the conventional mass media, which hugely use the internet as a source for stories.

CYBER WARFARE

What does Cyber warfare mean?

- Cyber warfare is any indirectwar initiated as a politically inspired attack on an enemy's computer and information systems. executed via the Internet, these attacks weaken economical and organizational systems by stealing or altering arranged data to erode networks, websites and services.
- Cyber warfare is also called as cyber war.

CYBER WARFARE INVOLVES THE FOLLOWING ATTACK METHODS:

vandalize: Army and economical computer systems are at endangered for the disruption of normal operations and apparatus, such as communications, fuel, energy and transportation base.

spying and/or security violation: These unlawful damaging methods are used to low down networks, software, computers or the web net to steal or capture arranged information from rival orgs or individuals for defense, political or economic gain.

- **WANNACRY(CYBER CONFLICT)**

The WannaCryransom ware attack was a worldwide cyber-attack by the WannaCry ransomware cryptoworm, which targets computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bit coin cryptocurrency.

ISSN 2394 - 7780

Researchers have identified some similarities in the WannaCry code and tools used by State hackers in previous attacks. Although, they have cautioned that it is too early to definitively attribute the attack to a state actor

Case Code	**Wannacry**
Status Quo States	**150 Countries**
Non Status Quo States	**-**
Region	**World**
Conflict type	**Interstate(involving twoor more states)**
Motive	**Sabotage(destroying machinery)**
Phase(year)	**Jan 16, 2017-may 14, 2017**

WannaCry: Case Detail

WannaCry: Regions simultaneously affected by the malware:

One of the defenseresponses:
Experts instantly advised targeted and affected users against paying the ransom payment due to no reports of people getting their data back after ransome payment and as high income would motivate more of such campaigns. As of 14 June 2017, after the attack had subsided, a total of 327 payments totaling US$130,634.77 had been transferred.

How To Overcome And Protect Yourself From It

overcome cyber crimes

1. Use a full-service internet security suite
2. Use strong passwords
3. Keep your software updated
4. Manage your social media settings
5. Strengthen your home network
6. Talk to your derived one's about the internet
7. Keep up to date on vital security violation
8. Take estimate to help secureyou against identity thieving
9. Know that identity theft can happen anywhere
11. Know what to do if you become a casualty.

how to overcome cyber conflict and cyber attack

1) Identify the Threats
2) Beware of Cybercrimes

ISSN 2394 - 7780

3) Keep an Eye on Employees
4) Use Two-Factor Authentication
5) Conduct Audits on a Regular Basis
6) Ensure a Strong Sign-Off Policy
7) Protect the Important Data
8) Carry Out Risk Assessments
9) Insure Your Company Against Cybercrime
10) Have In-Depth Knowledge About Risk Factors

CONCLUSION

Change is inevitable and therefore the dilemmas that advancement in technology poses cannot be avoided. The reality is that the criminals have modified their strategies and have started hoping on the advanced technology, and to subsume them the society, the legal, and therefore the enforcement authorities, the non-public companies and organizations will get to modification their mechanism to combat it. Additional such consultants should not solely be knowledgeable however should even be given necessary technical hardware's and computer code in order that they will expeditiously fight the cyber criminals. Thus, necessary facilities should be established in varied components of the country in order that crime within the virtual world may be controlled'.

The legal systems round the globe are, with each passing year, attempting to implement new measures to combat cyber act of terrorism. However, with a lot of innovative ways that of operating within the cyber area, a lot of loopholes is shaped which can get to be crammed in by the countries by amending the procedures and the laws in effect to tackle cyber act of terrorism.

REFERENCE

1. Crime in India: 2011-Compendium (2012), National Crime Records
2. Bureau, Ministry of Home Affairs, Government of India, New Delhi, India.
3. Cyber Law & Information Technology (2011) by Talan Singh,
4. Additional District & Sessions Judge, New Delhi, India.
5. Introduction to Indian Cyber Law (2008) by Rohus Nagpal, Asian School of Cyber Laws, Pune, India
6. Cyber Crime (2003) by R.K. Suri and T.N. Chhabra, Pentagon Press, New Delhi, India.
7. RohasNagpal (2002): "Defining Cyber Terrorism". In the ICFAI Journal of Cyber Law, Vol. 1, No. 1 (November) 75 at p.77
8. ICFAI Journal of Cyber Law (2002).
9. Indian Penal Code (1860).
10. YogeshBarua& Denzyl P.Dayal (2001): Cyber Crimes, New Delhi: Dominant Publishers & Distributors, pg3
11. http://en.wikipedia.org/wiki/Computer_crime
12. https://cybercrimelawyer.wordpress.com/category/66cpunishmentfor-identity-theft/
13. http://ncrb.nic.in/
14. www.economictimes.indiatimes.com/
15. Bureau, Ministry of Home Affairs, Government of India, New Delhi, India.
16. Teachers and friends .

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

USER PERCEPTION ON MOBILE DEVICE SECURITY AWARENESS WITH SPECIAL REFERENCE TO THANE DISTRICT (MUMBAI)

Divya J. Gautam
Asstiant Professor, JVM Mehta College, Navi Mumbai

ABSTRACT
Mobile computing is an increasing industry. The challenge has started when mobile device replaced traditional devices like computers and laptops to do multi tasking work also for social communication and business management through these cellular devices. With so many applications available consumer are often confused and unable to manage theses device security which requires extra knowledge. This paper presents the findings of a survey into the opinions of user regarding mobile security, their level of awareness towards threats and need for security. For conducting the research questionnaire was made and data was collected from 90 respondents.

Keywords: Mobile Security; Awareness; Privacy; Authentication.

INTRODUCTION
Mobile device are available everywhere and they are accompanying us in every step of life, no matters where we are ,it is simply connecting us to the world by calls SMS and internet. People are familiar in using electronic facilities like M-commerce, Banking through mobile creates threat of social issues like information security, privacy violation hacking and many others. supported by internet connection mobile device work like minicomputers and people use it for formal and informal use. Now a days mobile phones have become a focus of attack especially the smart phones. The virus writers and hackers are easily able to misuse the data available in the phone. The average cost pf a corporate data breach is $4million .in 2018 Enterprise Mobility Exchange Poll,28% of user identifies fake Wi-Fi network as the biggest threat to mobile Device, with malware infection coming in at 27% malicious mobile apps at 25% and phising attacks at 20%.mobile security is the protection of portable devices as Smartphone. They are targeted by Cyber attackers more than before this is mobile device vulnerability.

OBJECTIVE
1. To study the user knowledge on mobile device security.
2. To create the awareness among user about the threats and securities related to the mobile device.

THREAT AND SECURITY RISK
Mobile security is at the top of most of the consumer's worry list. The more realistic mobile security hazards lie in some easily overlooked areas, all of which are only expected to become more pressing as we make way through 2019.

1 .Insecure Data Storage
Having mobile phone as a way of communication and run daily task, these information include password, location study personal data

2. Weak server side control in third party applications
Each application should have the security to prevent unauthorised access to the server or the application database

3. Poor authorization and authentication
The lack of these two factors may easily lead to corruption. While the use of proper authentication will help to identify unauthorised code, user or software to be recognized and blocked.

4. Password protection
Some device does not have a tight password security software, user does not use lock on their device or app and if they use it remains simple not hard to predict and hacker could easily assume it.

5. Wireless transmission is not secured or encrypted
Portable device can be connected to both public and private network. Public network usually are not encrypted and therefore data transmitted through it can be exposed and disclosed to the mass.

ISSN 2394 - 7780

6. Malware attacks

Malware a malicious software could do a severe harm to mobile device. Start from SMS text message, spam, spam ads, fake phone calls, on the user cost calls and transaction, fraud transaction to controlling the whole device or shut it down. It could result into:

- Denial of service attacks
- Unauthorised access
- Masquerade
- Eavesdropping
- Alteration

RESEARCH METHODOLOGY:

To identify the user's perception and knowledge and also to create awareness on mobile device security among the user,a questionnaire was prepared and distributed to respondents. The questionnaire was prepared by used both open and closed ended set of questions. The respondents were clearly intimated about the study to fill the questionnaire. The quota sampling method was used to select the respondents. Both primary and secondary data collection method was used.It was distributed to 100 people out of whom only 90 responses were collected due to improper understanding and filling of data. The area of data collection was Thane (Mumbai).

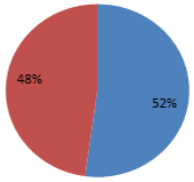
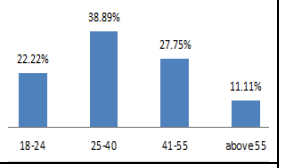
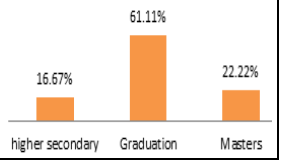
Questions asked to 80 people		Frequency	%	Diagrammatic representation
1.Gender • Female • Male	Male	47	52.22	
	Female	43	47.78	
2.Age	18-24	20	22.22	
	25-40	35	38.89	
	41-55	25	27.78	
	Above 55	10	11.11	
3.Education	Higher secondary	15	16.67	
	Graduation	55	61.11	
	Masters	20	22.22	

Table 1: Distribution of respondents by Gender, Age and Usagage

ANALYSIS AND INTERPRETATION OF DATA

In second step of data collection the question were asked on mobile device security, virus, user's knowledge and awareness on security measure.

1. Reason to use subscription

It was noticed that 70% of the user prefer post paid services and only 30% use pre paid subscription. It was necessary to consider the subscription because with the post paid services the international messages and calls are sent which generate virus and also lead to huge amount of bill amount.

2. Reason to use current device

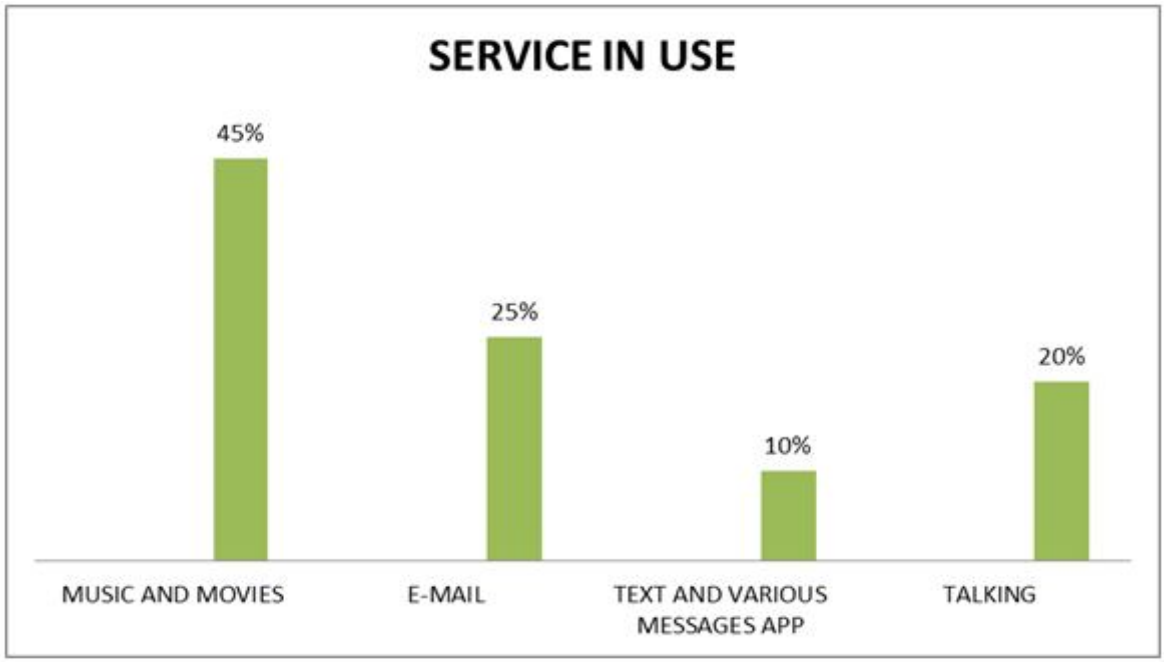
User buy the device by seeing its price, camera, brand name and other security feature.30% of the user buy on brand name, 35% on the basis of price 15% on the basic of camera quality and only 20% consider device security as one of the basic factor of purchasing the device.

3. Service in use

It was noted that majority of respondents are using downloading of music and movies. Since user don't read the notification coming in dialogue they welcome the virus in their device, improper use leads to vulnerability, following graph shows the detail use of various services.

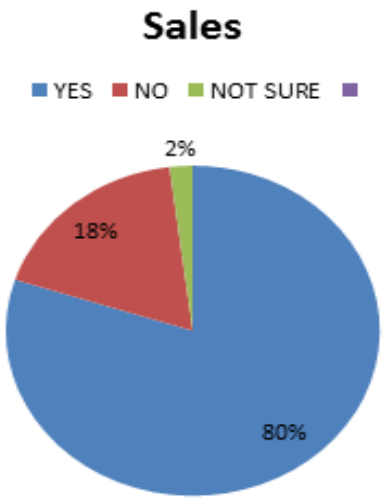
ISSN 2394 - 7780

GRAPH



4. Virus and Basic Awareness Measurement

When asked from the respondent whether they notice that their device is not working properly which may be probably due to virus infected the device,70% answered "yes "they noticed and further out of this 58% user agreed that they lost the valuable data. respondents also observed that data from the mobile device got deleted without deleting it.The above data supports that the awareness about the anti-virus software is the need and around 80% of the respondent agreed that they should install anti –virus software to protect their mobile device.the figure below shows respondents' opinion about the need for security of device.



5. Update and privacy

Most of the respondent was not interested in updating the device as survey said 40% of them choosing this option, only 7% of them are considered to be very much interested in updating the device.

Figure

When privacy related questions were asked like do they like accessing social network like face book or instagram via their phone,59% responded with "yes". this is to be considered as user save auto login information and they do not use PIN protection for authentication. Also respondents' answered to the question of saving auto log in information in their device near about 70% of them said "No" and 20% said "Yes "rest were not sure. Its good that percentage of respondent saying yes is less.

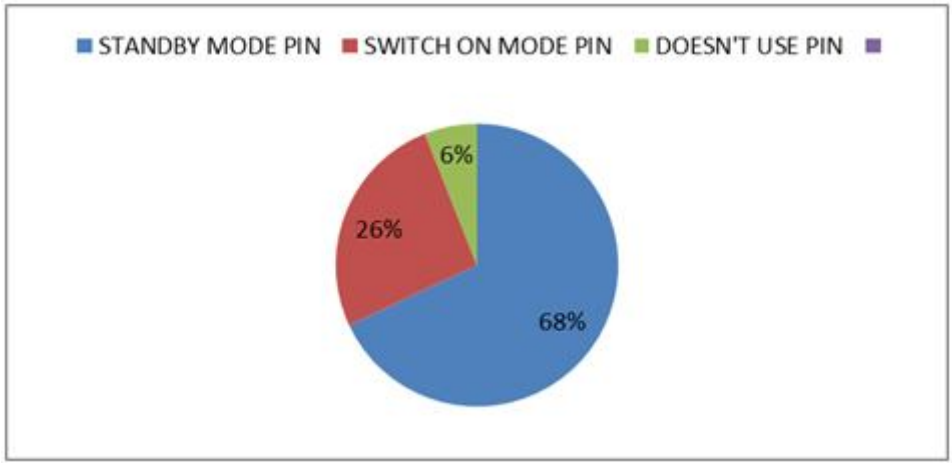
The third question was asked about submitting the credit card information to shop via their mobile device while 55% of people trust on submitting which is risky due to weak mobile browsing encryption.

ISSN 2394 - 7780

The final question which is of a great concern when asked to the respondents whether they save their bank account or credit card number in unencrypted form in their device ; 48% said “yes” .Now this is high percentage as it might be used by hackers to hack the account its very easy form them to get confidential details of your bank account with unencrypted password or details.

6. Awareness

In this section of survey awareness regarding PIN protection was analysed.68% of them use PIN for switch on mode, 26%use standby mode pin and 6% doesn’t use pin in their device. It was further continued to change in pin details,70% of those who use pin doesn’t change the pin in a year. The figure below explains how the respondent gives importance to pin change.



7. Attitude

Respondent’s Attitude Towards Current and Future Security

QUESTION	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Should mobile phone security increase?	8%	10%	2%	56%	24
Do you agree paying more for to get more security in your mobile phone?	36%	30%	17%	13%	4%

From the above details it can be seen that 56 % of respondent strongly agree with the phone security enhancement but it was also observed that only few of them i.e 13 % are agreed to pay more for higher security level in mobile device.

FINDINGS

It was found that half of the respondents have experienced some symptoms of infection in device like no responding of device or unusual action. Few of them have lost data without deleting them. The user who have faced problem agree to that data is valuable and want to protect it but they doesn’t have knowledge of security measure like Anti-Virus software. The internet usage is increasing day-by-day on device like mobile. People get easily get connected to access point around them via Wi-Fi this raise more risk while ordinary mobile browsing. Down loading free music, movies, themes etc also leads to infection of virus in mobile device.

User privacy is at risk which leads to privacy vulnerabilities this include auto login, social network application, E-mail Mobile banking and saving bank account number. Researcher result recoded that most of the user do not use PIN protection which increase risk. Most of the respondent agree that mobile security features must be enhanced so that user will be able to use mobile device with higher level of trust which will lead to qualitative digitalization.

CONCLUSION

It can be concluded from the whole research that mobile security awareness for user is relatively critical. The increased use of mobile for different services increased the need for higher security which is a major issue.

The objective of this study is to enhance the awareness of mobile device security among the user can be achieved by providing guidelines which can be presented to the consumer or enforced in organise workshop can be conducted on cyber crime which will give knowledge about the hacker and virus to the user.

ISSN 2394 - 7780

REFERENCES

1. Rayed and saleem(2013).users' perception of mobile phone security:A survey study in the kingdom ofsaudi Arabia.
2. Ahmed sabeeh (2011)user' perception on mobile device security awareness in Malaysia.international conference on internet technology and secured transaction.
3. Tao zhang 1,pei-luen Patrick rau 2,Jia zhou 2.consumer perception of mobile phone attributes(2010).
4. Kazi wahiduzzaman.Consumers' perception to mobile banking
5. Leavitt,N.(2005)will proposed standard maje mobile phones more secure?
6. Aite.Global consumer survey trust and security perceptions
7. Samia and ompraksah (2003).consumer perception and attitude towards mobile communication in international journal of mobile communication.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

DATABASE SECURITY AND PROTECTION METHODS AGAINST ATTACKS

Anuradha Chaukate
Research Scholar, Pune University, Pune

ABSTRACT
Day by day, preparation of the data becomes very fast and is kept at place called database. This data is processed easily and efficiently. In Database management system different operations like manipulation and maintenance are performed. It is important to secure the data for organization. If data has been protected from any database attack then it will be a secure data. Some security models have been developed for securing database and these databases are dealing with different issues. It is very difficult for securing database for selecting an appropriate model. In this paper I have made discussion on some of the attack and methods for avoiding it. To protect a database and maintain the security is very complicated task for companies.

Keywords: Threats, Attacks, Securit, Database, DBMS, Security

1. INTRODUCTION

we can define database as a collected work of processed data which is gathered on the system. Legitimate users are allowed to use saved data and analyze fast. It is may have a set of views, tables and queries. Within database, the stored data are organized which support the process that requires information storing and retrieval. To interact with database by using user interface we have database management system. As per many IT experts, many peoples from industries doesn't know which tables and columns has sensitive data as they might have handling any other application. Though we have complete knowledge of the database, it will be very hard to protect our data. Hence we can say that database security means securing data against any internal or external attack. It involves different types of controls regarding to administrative, technical and physical control. Protecting confidential data stored in database comes under database security. There are many layers of security in database as system administrator, database administrator, security officer, developers and employee and security can be broken at any of these levels only.

2. DATABASES THREATS

Now a days technologie are being developed so different kind of attacks are existing for the databases. Firstly we will discuss about the existing attacks on databases and then will focus on techniques to secure our databases.

2.1 Excessive privileges

in this technique the authorized user may misuse the privilege for unauthorized task. Misuse of privileges may comes as Excessive privilege abuse, unused privilege abuse and legitimate privilege abuse. This type is more dangerous as authorized user are making misuse of data and creates more risk. These authorized peoples may be company employee or ex-company employee

Countermeasures

1. It can be stop by providing proper audit trail.
2. By using access control policy do not grant unnecessary privileges to all users

2.2 SQL Injection

in most of the cases the data supplied by user as an input is used to dynamically build sql statements and it directly affects the databases. In SQL injection the original intent of any application is manipulated by the attacker and supplied to database directly. We can divide SQL Injection in two ways as-

SQL Injection and NOSQL Injection

Countermeasures

1. Try for implementing MVC architecture
2. Instead of direct queries make use of stored procedure.

2.3 Malware

Different types of malwares, spear phishing emails can be used to penetrate organization and steal data. Without knowing of malware attack the legitimate user becomes a medium for these groups to access network and data of organization

ISSN 2394 - 7780

Countermeasures
To avoid malware we have to enable firewall protection and install antivirus.

2.4 Weak audit trail
organization having weak database audit mechanism will increase risk in all levels. Most of this audit mechanism are unaware of the end user as all activities are associated with the users account name. Visibility, reporting and forensic analysis are vulnerable as there is no proper link to specific user. And finally with knowing or unknowingly the legitimate user with administrative access to database can turn off native database auditing to hide his fraudulent activities.

Countermeasures
1. Always offer granular data collection and use network based audit appliances.

2.5 Weak Authentication
In this attackers can assume the identity of legitimate database users. In this a specific attack includes brute force attack, social engineering attack etc.

2.6 Unmanaged Sensitive Data
Many times the company employees may forget the passwords for old backup databases. This may contain any sensitive information. In such case this will exposed to threats if specific controls and privileges are not implemented properly Counter measures of unmanaged Sensitive Data

1. The sensitive data in the database must be encrypted.
2. Controls and permissions to the databases must be required to implement.

2.7 Denial Of Service
it is a general type of attack which contains denial of access to network application or data to intend user.

Countermeasures-
1.Apply a network Intrusion Detection System (IDS) as it can automatically detect and respond to SYN attacks.

3. CONTROL METHODS FOR DATABASE THREATS
To protect and remove the threats every organization should have certain security policy which must be implemented. In this policy the authentication is important because if it is proper then the threats will be minimum. Following are some methods by which we can secure our database.

3.1 Access control
It is basic fundamental services which any database should have. It is used to protect the data from unauthorized read and write operations. This policy ensure that all communication to the database and other system objects must follow this policy. Controlling includes file permission, program permission and data rights.

3.2 User Identification /Authentication
in this technique it is required that you should identify your users and this identification must be done prior to their privileges and access rights determination by you. It is very basic method since it ensures the security of identification process of definite set of peoples who access the data. This identification helps to secure the sensitive data and protect it from being modified by unauthorized user. Attacker can take different approaches like bypass privilege escalation, Default Password, authentication, Password Guessing by brute force and rainbow attack .

3.3 Accountability and auditing
it is used to monitor and record actions related to configured database. It is also used to maintain an audit trail for user action performed in system. It is used to ensure the physical integrity of the data so that database is handled through auditing and for keeping the records.

3.4 Encryption
in this the information is converted into a cipher text so that nobody can read it except those people who has it's key for cipher text. This cipher or encoded text is called as encrypted data.

4. CONCLUSION
Finally summarizing all this, access protection starts with user who can access data and what type of data attackers want to access. The topics discussed here gives the information of different threats and it's security

ISSN 2394 - 7780

issues of databases. This paper focused on threats and its possible counter measures that can be possible to secure data in databases.

REFERENCES

[1] IMRAN, Dr Irfan Hyder, Security Issues in Database, Second International Conference on Future Information Technology and Management Engineering, 2009.

[2] Mr. Saurabh Kulkarni, Dr. Siddhaling Urolagin, Review of Attacks on Databases and Database Security Techniques, Facility International Journal of Engineering Technology and Database Security Techniques Research, Volume 2, Issue 11, November-2012.

[3] Shelly Rohilla, Pradeep Kumar Mittal, Database Security: Threats and Challenges, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

DATABASE SECURITY USING BLOCK CHAIN

Bhagyashri Kulkarni
JVM's Mehta Degree College, Navi Mumbai

ABSTRACT
Blockchain has wide ability to put everything in order issues, which has decentralized development. Cryptography confirms record in a blockchain development and each trade is appended to before trade or record, those trades are affirmed by computations on the centers. Blockchains give straightforwardness, ability to screen the trades at whatever point to individuals. Through contract we can make secure trade which helps unsettling influence from outcast. Ethereum is a stage that runs contracts. This encourages engineers to make markets to move assets as per directions given long previously. Blockchain enables exchanges to be safely put away and checked without the need of any brought together expert. The primary highlights of blockchain are Decentralization, Immutability, Transaction and quicker approval and so on.

INTRODUCTION
The 21st century is about development. With the extending prerequisite for improvement in our for a long time lives, people are accessible to enduring new advances. Advances like extended reality and IoT that have gotten pace inside the earlier decade and starting at now there's a crisp out of the plastic new development to the pack for instance Blockchain Technology.

The dynamic advancement influencing absolutely exceptional undertakings wonderfully were introduced inside the business segments with its horribly first current application Bitcoin.

Bitcoin is nothing in any case a sort of cutting edge money (cryptographic cash) which might be utilized in the spot of paper money for business and the development behind the accomplishment of advanced monetary standards is known as Blockchain. There's a standard idea among people who Bitcoin and Blockchain are one and along these lines the equal, regardless, that isn't the circumstance. Making computerized monetary forms is one in all of the usages of Blockchain advancement and next to Bitcoin, there are varied applications that are being made on the reason of the blockchain development.

BLOCKCHAIN
In the most effortless terms, Blockchain may be described as an information structure that holds esteem based records and making certain security, straightforwardness, and decentralization. You can also consider it as a course of action or records keep inside the sorts of obstructs that area unit obliged by no single master. A blockchain could be an appropriated record that everybody can use the framework. At the point when data is keep on a blockchain, it is unfathomably difficult to change or alter it. Each social occasion action on a blockchain is confirmed with an automated imprint that shows its acceptability. On account of crafted by encoding and modernized imprints, the data set away on the blockchain is cautiously planned and can't be changed. Blockchain advancement enables all the framework individuals to achieve AN assention, normally known as accord. Every one of the information keep on a blockchain is recorded cautiously and features an average history that is open for all the framework individuals. Thusly, the possible results of any misleading development or duplication of trades is cleared out without the need of an outcast cooperation. In order to know blockchain higher, consider a model where you are looking for a decision to send some money to your partner who lives in a substitute zone. A general credibility that you essentially will as a general rule use may be a bank or by methods for a portion trade application like PayPal or Paytm. This option incorporates untouchables so as to procedure the social occasion movement by virtue of that an additional measure of your cash is subtracted as trading charge. Also, in cases like these, you can't guarantee the security of your cash since it is potential that a developer may irritate the framework and take your cash. In both the cases, the customer perseveres. This is the spot Blockchain comes in. As opposed to using a bank for trading cash, if we use a blockchain in such cases, the methodology ends up being significantly less requesting and secure. There is no extra cost required as the advantages are explicitly arranged by you along these lines, clearing out the necessity for an untouchable. What's more, every one of the information and records kept on the blockchain are open and decentralized. Since the data isn't keep in a single recognize, there's no chances of corruption of the data by any developer.

WORKING OF BLOCKCHAIN
A blockchain could be a chain of hinders that contain data or information. In the year 2009, the primary effective use of the Blockchain innovation came. He made the essential computerized digital money alluded to as Bitcoin using Blockchain innovation. How about we see how a blockchain really functions. Each square in an

ISSN 2394 - 7780

exceedingly blockchain organize stores a few information related to the hash of its past square. A hash could be an unmistakable numerical code that has a place with a specific square. In the event that the information inside the square is changed, the hash of the square will go be liable to alteration as well. The structure of squares through unmistakable hash keys is the thing that makes blockchain secure. While exchanges occur on a blockchain, there are hubs on the system that approve these exchanges. In Bitcoin blockchain, these hubs utilize the idea of verification of-work so as to process and approve exchanges on the system. All together for a gathering activity to be substantial, each square should look for exhortation from the hash of its first square. The gathering activity can happen exclusively and giving the hash is right. On the off chance that a programmer endeavors to assault the system and adjust information of a particular square, the hash shut to the square likewise will get changed.

BLOCKCHAIN FEATURES

The accompanying choices make the progressive innovation of blockchain emerge:

DECENTRALIZED

Blockchains are decentralized in nature suggesting that no single individual or social event holds the pro of the general framework. While everyone inside the framework has the copy of the appropriated record with them, nobody will change it on his or her own. This specific segment of blockchain gifts straightforwardness and security however offering ability to the customers.

DISTRIBUTED NETWORK

With crafted by Blockchain, the participation between 2 parties through a mutual model is absolutely drilled while not the need of any pariah. Blockchain uses P2P tradition that enables all the framework individuals to pass on a standardized copy of trades. For example, if you should need to outline any trades from one a bit of the globe to an other, blockchain help you to do this free from any other individual inside a few minutes. Extra charges won't be deducted in the trade.

IMMUTABLE

The changelessness property of a blockchain suggests the built up truth that any information once formed on the blockchain can't be modified. To grasp steadiness, consider causing email as accomplice degree show. When you send accomplice degree email to a heap of individuals, you can't take it back. In order to seek out the way around, you'll must be compelled to raise all of the recipients to eradicate your email that is truly dull. This is the way by which immutability works. At the point when the information has been dealt with, it can't be balanced or changed. Change in one hash can cause modification all around the following hashes. It is incredibly hard for someone to change all of the hashes as it requires a lot of computational ability to do thusly. From this time forward, the data set away in a blockchain is non-unprotected to adjustments or software engineer attacks as a result of immutability.

TAMPER-PROOF

With the property of perpetual nature introduced in blockchains, it winds up less requesting to recognize adjusting of any data. Blockchains are unit thought of fixed as any change in even one single square are much of the time recognized effectively. There zone unit 2 key ways that of police work change of state particularly, hashes and squares. As addressed previously, each hash business related with a square is uncommon. You can think of it as sort of an extraordinary finger impression of a square. Any alteration inside the information can cause a change inside the hash work. The hash limit of one square is joined to next square. If the software engineer reveals any enhancements, he/she should change hashes of the impressive number of squares which are incredibly troublesome.

TYPES OF BLOCKCHAIN

In spite of the fact that Blockchain has developed to numerous dimensions since origin, there are two general classifications in which blockchains can be ordered significantly for example Open and Private blockchains.

Public Blockchain-This record is permissionless and can be gotten to by everyone. Anyone with the passage to the web is met all requirements to download, trade and access it. What's more, one can even check the general history of the blockchain close by any trades through it. Open blockchains now and again repay their framework individuals for acting the mining method and keeping up the permanency of the record. An instance of the open blockchain is that the Bitcoin Blockchain. Open blockchains license the systems worldwide to exchange information straightforwardly and securely.However, a comprehensible impairment of this sort of blockchain is that it is undermined if the principles around it are not run completely. Also, the principles chose and associated toward the start have for all intents and purposes zero degree of alteration inside the later stages.

ISSN 2394 - 7780

Private Blockchain-In resistance to the open blockchain, private blockchain is the one which are shared just among the trusted in individuals. The general organization of the framework is inside the hands of the owners. Likewise, the principles of an individual blockchain is balanced by different elements of assents, introduction, extent of people, endorsement, etc. Private blockchains will run severally or is consolidated with choice blockchains too. These are regularly used by endeavors and affiliations. Thusly, the proportion of trust required among the individuals is higher in private blockchains.

CONCLUSION

Other than these couple of points of reference, the dynamic advancement of Blockchain holds a high capacity of usages in various elective endeavors and fragments. Blockchain may be another name inside the universe of advancements at any rate it's unequivocally the one to last. For sure, even inside the starting time frames, the development has expanded tremendous pervasiveness starting with their outright first utilization of computerized types of cash. More zones of uses are being found and attempted over the long haul. At the point when the development is gotten and recognized on a world measurement, it will revamp the way in which we live nowadays.

REFERENCE

1. https://blockgeeks.com/guides/what-is-blockchain-technology
2. http://www.computerweekly.com/feature/Blockchain-and-the-promiseof-cooperative-cloud-storage.
3. https://www.computerworld.com/article/3233187/mobile-wireless/fintech-builds-on-blockchain-forinternational-mobile-payments.html.
4. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=CHJ12351USEN.
5. https://en.bitcoin.it/wiki/Proof_of_work.
6. https://en.bitcoin.it/wiki/Proof_of_Stake.
7. https://en.wikipedia.org/wiki/Proof-of-space.
8. https://en.wikipedia.org/wiki/NEM_(cryptocurrency)#Proofof-importance.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

MOBILE DEVICE SECURITY

Sunita B. Rai
Assistant Professor, Department of Computer Science, G. N. Khalsa College, Matunga (E), Mumbai

ABSTRACT
Long years back, it was only a dream to have a device that could go wherever you are moving and connect you to anywhere and anytime you want in the world. It was only a dream to have GB/TB hard drive that could fit into the palm. With the exponential increase in mobile industry over the past couple decades; it has created a great demand for the devices along with great dependence on their capabilities. There is a range of mobile devices among which can be found laptops, tablets, smart phones, and personal music players. All these provide a way for doing personal and business work. Practically they are offering same capabilities as desktop workstations as well as come to be powerful in terms of processing, storage and installing numerous applications. Today's mobile devices handle information such as contacts, banking details, GPS location, and e-mail etc. Because of the dependency on mobile devices for everything from personal to banking information, their security is crucial. With the advancement in technology, there has also arisen a new type of criminal known as cracker, hacker, or cyber criminal. Based on increasing the range of mobile application within variety of platforms, security is regarded as on the most valuable and considerable debate in terms of issues, trustees, reliabilities and accuracy. This paper aims to introduce a security on mobile devices and providing knowledge of threats to the users and enterprises. This paper also introduces some background on mobile technologies and then describes different types of mobile malware.

Keywords: Mobile Security, attacks, cyber, threats

I. INTRODUCTION
Mobile devices and smart phones enable access to information and services anywhere, anytime for personal and corporate use. Small, portable, always on, allowing Internet access and a range of mobile applications, these computing devices have become indispensable to many people. However, their small size and the increasing amount of data accessed by and stored on these devices makes them susceptible to loss or theft. In addition to threats such as malware, viruses, worms etc. mobile devices are more prone to physical attacks. Mobile device security deals with the protection of information stored on devices and system itself. Mobile device security aim is to provide security triad (Confidentiality, Integrity and Availability).

As mobile devices provide the range of services, thus are having challenges like security and privacy. Since for performing most of the operations the Internet is used, so it is necessary to ensure security and safety of information. For security (authentication) some mechanisms like PIN, pattern, finger prints unlock, face unlock can be used. But these methods are not so secured because of different types of attacks such as brute force, dictionary etc.

Critically, a lot of Viruses, Trojans, Worms, Spyware, Adware and Malware have been developed which can come with different applications and look safe. Some reliable applications like different mail services and social sites collect user's information without user's knowledge which is again a threat in security. Due to emerging enormous numbers of mobile platforms security requirement is one of the emergent areas.

II. MOBILE TECHNOLOGIES
A. Wireless Telecommunication Technologies:
Transmission of information over a distance without help of wires, cables or any other forms of electrical conductors is called wireless communication. The transmitted distance can be anywhere between a few meters (for example, a television's remote control) and thousands of kilometres (for example, radio communication). The most important wireless technologies are GSM, GPRS, EDGE and UMTS.

1) GSM: Global System for Mobile communications (GSM)
GSM is a digital mobile network that is used by mobile phone users in Europe and other parts of the world. The GSM network consists of four parts: the mobile device, the base station subsystem (BSS), the network switching subsystem (NSS) and the operation and support subsystem (OSS). These components perform different functions, such as forwarding calls, sending SMS, sending mails, authenticating, storing caller account information via SIM cards, teleconferencing service, digital fax.

ISSN 2394 - 7780

2) GPRS and EDGE
They are developed to improve performances of GSM network enabling user to access high data rates with lower access time. General Packet Radio Service (GPRS) uses packet switching to enable the exchange of data between users. Enhanced Data rates for GSM Evolution (EDGE) standard was developed to improve the features offered by GPRS by providing higher reliability and transmission rate.

3) UMTS: The Universal Mobile Telecommunications System
It represents the third-generation (3G) on cellular system transmission rate up to 2Mbps. Provide services such as conversational, streaming, interactive and background.

B. Networking Technologies
With the popularity of mobile devices Wireless Local Area Network (WLAN) has become very popular. It allows exchange of data between large and small information system. Different standard are available for regulating communication in WLAN.

1) Bluetooth
Bluetooth is a standard that describes how mobile devices and other devices can easily communicate with each other using a short-range wireless connection. There are three different classes of Bluetooth devices according to the power consumption and range of communication. Bluetooth technology has simplified task such as taking printouts from Bluetooth enabled printer, connecting keyboard or mouse.

2) Wireless LAN IEEE 802.11
Wireless LANs are those LAN that use high frequency radio waves instead of cables for connecting the devices in LAN. Users connected via WLANs can move around within the area of network coverage. It is based on standard IEEE 802.11 or Wi-Fi. Main advantage of using it is that devices may be added or removed from the network at a greater ease. Also setup and installation is easier and less costly.

III. MOBILE DEVICE SECURITY PRINCIPLE

Mobile device security deals with the protection of the information and system stored on mobile devices. Its aim is to provide the devices from unauthorized access, use, modification, disruption or destruction. Confidentiality, Availability and Integrity (CIA) are three main requirements that each system should have to secure the data and provide the appropriate security. Confidentiality ensures that an information system is accessed by only an authorized person. User Id's and passwords, access control lists (ACL) and policy based security are some of the methods through which confidentiality can be achieved. Integrity ensures that data can be modified only by authorized. Hashing algorithms are key mechanism in providing integrity. In order for any system to be of use it has to provide available information as on when it is required, this is called principle of availability. Hardware maintenance, software patching/upgrading ensures availability. When the information of a system is confidential, integral, and available, it can be considered as secure system

Control mechanisms are devised to control security aspects. Logical or technical controls are used to inspect and control the access to the information. Examples are: access control lists (ACL), passwords, data encryption, network intrusion detection systems (NIDS), authentication servers, biometrics, cryptography, Virtual Private Network and host and network based firewalls.

In order to make mobile devices completely secure it needs to be physically secured by the user. Physically securing mobile devices is different than physically securing non-mobile devices. Maintaining the security of a device that is designed to constantly move is more difficult.

V. THREATS ON MOBILE DEVICES

A threat is something that may or may not happen, but has the potential to damage your information or system. Mobile devices face a range of threats. They can be intentional or unintentional.

Table I. Sources of Mobile Threats

Sources of Threats	Description
Cyber Criminals	An individual who commits cybercrimes, by making use of the mobile either as a tool or as a target or as both. They attack mobile devices for monetary gain. They gain access to mobile devices using spam, phishing or malware and commit attack such as identity theft, online fraud and so on.
Hackers	Hackers use mobile devices to demonstrate their skills and to gain prestige in the hacker community.
Terrorists	Terrorists may seek to destroy infrastructures such as mobile networks, to threaten

ISSN 2394 - 7780

	national security, weaken the economy, or damage public morale and confidence.
Foreign Intelligence Services	They may attack mobile devices as part of their information-gathering and espionage activities. They develop programs, that could disrupt the supply chain, mobile communications, and economic infrastructure

VI. ATTACKS ON MOBILE DEVICES

Common mobile attacks are described as follows:

1. Malware: Malware, or malicious software, is a program or file that is harmful to a system user.Malware includes viruses, worms, Trojan horses and spyware. It can do perform various activities such as stealing, decrypting sensitive data, altering core computing functions and monitoring users' activity without user consent. Malwares includes Viruses, worms, Trojans, Rootkit, Spyware, Botnets, Ransomware.
2. Phishing: It obtains sensitive information by disguising as a trustworthy entity in an electronic communication.
3. Unauthorized location tracking: Location tracking allows registered mobile to be known and monitored. Location can be misused for various reasons.
4. Unauthorized location tracking: Location tracking allows registered mobile to be known and monitored. Location can be misused for various reasons.
5. Theft/loss: Because of small size mobile devices can be easily stolen or lost. If mobile devices are lost or stolen information stored on them can be misused.
6. Keystroke logging: Records key typing on mobile devices in order to get sensitive information.
7. Network exploits: With special tools, attackers can trace users on a Wi-Fi network and can use those credentials to impersonate a user online.
8. Browser exploits: Visiting certain web pages or accessing hyperlinks can trigger browser exploits that install malware or perform other malicious activities on a mobile device.

VII. SECURITY SOLUTIONS FOR MOBILE DEVICES

Following are some existing mechanism that can be used to prevent attacks on mobile:

1. Install firewall: Firewall monitors incoming and outgoing traffic and filters based on specific rules.
2. Enable user authentication: Settings for password or PIN can be done for checking credentials of users.
3. Enable two-factor authentication for sensitive transactions: Two factor authentication incorporate minimum two factors, something that user have or something that user knows.
4. Enable encryption for data stored on device or memory card: Encryption converts data into unreadable format. Data stored on mobile or file could be protected using inbuilt capability of mobile devices or by using any other tools.
5. Monitor and control devices: Mobile devices can be monitored for controlling inappropriate use of data and for preventing applications being installed.
6. Use of Digital Signatures: Digital Signature can be used for signing email digitally which guarantees data integrity.
7. Implement a virtual private network (VPN): VPN allows encrypted connection over inter from a device to internet. VPN helps to ensure that data is safely transmitted.
8. Enable and analyze device log: Log files can be maintained for detecting and reviewing malicious activities.

VIII. CONCLUSION

With rapid enhancement in mobile devices, the number of threats and attacks are also increasing tremendously. Different from desktop system security solution for mobile devices vary in many aspects like storage, power, computation capability, availability of storage, network and many more. In this paper I have tried to discuss different mobile technologies, principles on which security works also platforms for mobile devices and threats or possible attacks on them. Security controls for mobile devices are never going to be common but certain guidelines can be followed to prevent or control them.

ISSN 2394 - 7780

REFERENCES

1. Mobile Application Security Platforms Survey, International Journal of Computer Applications (0975 – 8887).
2. A. Agrawal and A. Patidar, "Smart Authentication for Smart Phones," Citeseer, vol. 5 (4), pp. 4839–4843, 2014.
3. Delac, G. Silic, M. and Krolo, J. (2011), Emerging Security Threats for Mobile Platforms' MIPRO 2011, May 23-27, 2011, Opatija, Croatia
4. A Survey on Security for Mobile Devices, Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra.
5. A Survey on different Attacks on Mobile Devices and its Security, International Journal of Application or Innovation in Engineering & Management.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

TO STUDY THE CYBER SECURITY AND SOLUTIONS

Manjushree Yewale
KES's Pratibha Commerce and Computer Studies, Chinchwad, Pune

ABSTRACT
Cyber security over internet is the protection of internet-connected systems, including hardware, software and data. Computer security or information technology security is the protection of computer systems from theft or damage hardware, software or electronic data, or unauthorized access. Cyber security is the practice of protecting systems, networks, and programs from digital attacks. Cyber securities are one of the most curial things of electronic commerce. Cyber stores or E-commerce transaction face greater e-transaction security risks due to insufficient internet safety from cybercriminals, Not only is hacking a huge risk for all online merchants, but accepting a fraudulent payment also comes at the cost of having to refund the charges. However, using the right tools will minimize the threat of fraud and in still trust within user cyber protocol base. The most prevalent cyber security threats include phishing attacks, hacking, and IP spoofing, sniffing, denial of service, credit card fraud, data errors or unprotected online services. Security solution is an essential part of any transaction that takes place over the internet. Major security solutions are Digital Signature, Digital certificates, Digital envelopes, SSL certificates. This paper presents study of cyber security issues of e-commerce and provides possible solution for them. This paper work also makes the Internet or cyber safer for everyone.

Keyword-:B2B, Digital certificate, Digital signature, Spoofing, sniffing, SSL, SSH

INTRODUCTION
In today's internet world, everyone beneficial from advanced cyber defence programs. At an individual level, cyber-security attack can result in everything from identity theft, to extortion attempts, to the loss of confidential data like family photos etc. Securing these and other organizations is essential to keeping our society functioning. Cyber security refers to a set of techniques or protocols used to protect the integrity of cyber networks, programs, records or data from attackers, make damage or unauthorized access from hacker's. Cyber security is providing the tools, procedures of protecting systems, networks, and programs from cyber-attacks. It makes **protection** of various internet assets from unauthorized access. Cyber securities provide reveal new vulnerabilities, educate the internet users on the importance of cyber security, and provide open source tools and education. The increasing use of the Internet improving the deploy technology to protect the cyber. The Extension of the basic technologies to defence multicast communications is possible and can be expected to be implementing as multicast becomes more widespread in all over world. Cyber-attacks are usually task at modifying, accessing, corrupt, interrupting or destroying sensitive information. Implementing effective cyber security is challenge today because there are more devices than user, so attackers are also becoming more innovative and advance in Technology. Every users of internet is essential to give training the computer security tools which embedded to protect from cyber-attacks. Cyber security is the process of protection of cyber assets from unauthorized retrieves, apply, modify or destroy.

There are six dimensions of cyber security must be Implementing during internet using Applications

1. Integrity: It provides prevention against unauthorized attacker's to data modification.
2. No repudiation: It prevention against any one group party or individual from deny on an agreement after the fact deal.
3. Authenticity: identify the authentication of data resource
4. Confidentiality: protection against unauthorized data interpretation or disclosure
5. Privacy: provision of data access control and discover
6. Availability: prevention against data delays or removal

METHODOLOGY
Today Internet user uses E-Commerce and E-Media to transaction purpose. It is a methodology of modern business, which addresses the need of business development, increase quality, to reduce cost and while increasing the speed of delivery. Today world make a global communication and refers the paperless exchange of business information using the following are the key areas

ISSN 2394 - 7780

Electronic Data Interchange

- Electronic Mail
- Electronic Cash
- Electronic Fund Transfer (EFT)
- Some others Network-based technologies
- Credit Card system

Main Types of cyber security threats

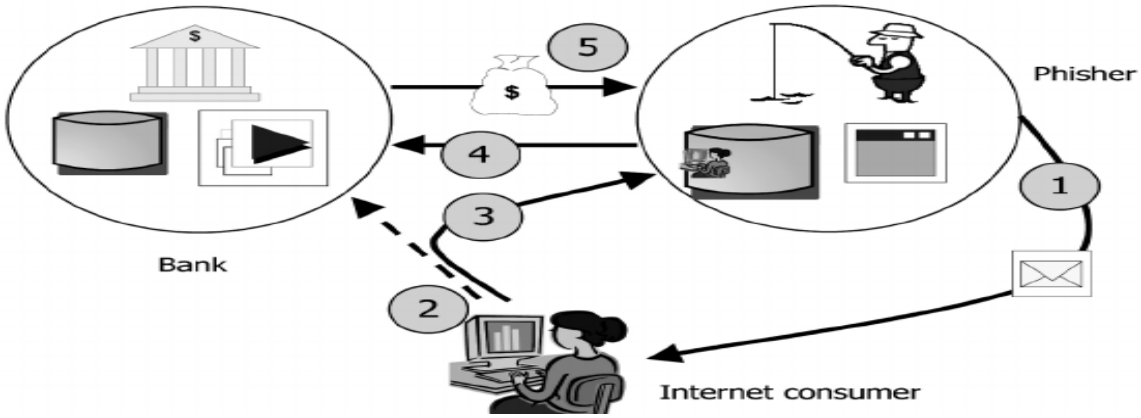
Any security needs set of protocols that safely guide cyber application and transactions. Security requirements protect companies, business agencies, organization from threats like credit card fraud, or they risk and customer cyber rules trust, due to the inability to guarantee safe credit card system processing.

1) Phishing attacks

Phishing attacks target users such as login information like user name, password, and account no, credentials and credit card numbers. Using social engineering, an attacker will pose as an entity to deceive a victim into opening an email, text message or instant message.

2) Social engineering

Phishing is one of the types of social engineering attack often used to steal user information, including login credentials and credit card numbers. The recipient or user is then tracked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a malware attack or the hacking of sensitive information.



3) CYBER THREAT

Threats are anyone with the capability, technology, opportunity, and intent to do any unwanted harm. Potential threats can be foreign or domestic, internal or external, state-sponsored or element. There are no of various types of cyber threats. Some are accidental, some are purposeful, and some of them are due to human errors. The most security threats are under social engineering is phishing attacks, money thefts, data misuse, hacking, credit card frauds and unsafe services.

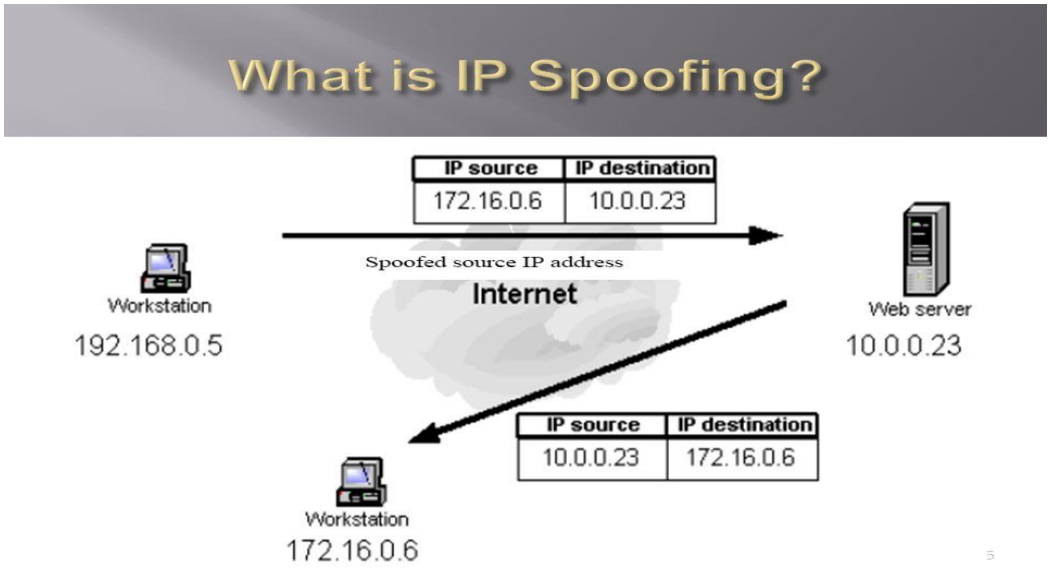
4) Malicious code threats

These code threats typically involve viruses, malware, worms, and Trojan horses. Viruses are external threats and can corrupt the files on the website if they find way in the internal network. Viruses can be very dangerous as they destroy the computer systems completely and can damage the normal working of the computer and its application. A virus always needs a host or users as they cannot spread by themselves. Worms are different and serious than viruses. It places itself directly through the internet. It can infect millions of computers in a matter of just few hours or second.

5) IP Spoofing

IP spoofing refers to IP address connection hijacking through a fake Internet Protocol (IP) address. IP spoofing is the action of masking or hiding a computer IP address so that it looks like it is authentic. During this masking or hiding process, the fake IP address or duplicate IP address sends to with a malicious code message with an IP address that appears to be authentic and trusted or valid. In IP spoofing, IP headers are masked or duplicated through a form of Transmission Control Protocol in which spoofing discover and then manipulate or modify or access vital information contained in the IP header such as IP address and source and destination content information in details.

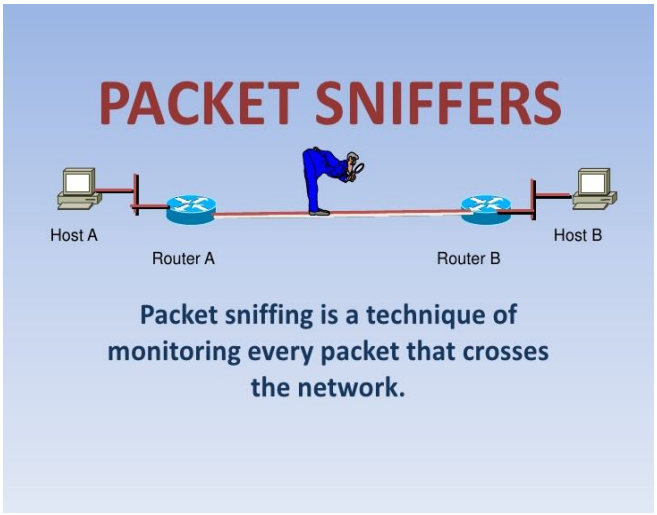
ISSN 2394 - 7780



Spoofing is when a malicious code party or hackers impersonates another device or user on a network in order to launch attacks against network hosts, steal data, hack information, spread malware or bypasses the access controls.

6) Sniffing Attack

Sniffing attacker is in context of internet or cyber network security, corresponds to theft or interception or analysing detail of data by capturing the network traffic using a sniffer. This is an application aimed at only read or capturing network data information or status of traffic. When data is transmitted across networks and data packets are not encrypted or not secure over transmission channel.

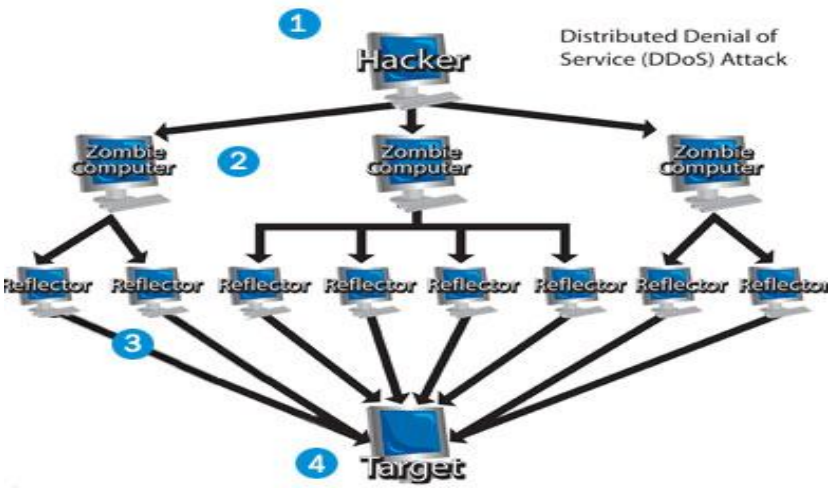


This is a process of monitoring and capturing or viewing all data packets passing through given network channel. Sniffers are used by network system administrator to monitor or analysing and troubleshoot network traffic. Attackers use sniffers to capture or read data packets containing sensitive information such as password, user name, account information etc. Sniffers can be any app, protocol, hardware or software installed in the system. The network or server will not be able to find or detect the return address of the attacker when sending the authentication, causing the server to wait or unavailable before closing the connection of network. When the server closes the connection, the attacker sends more authentication messages or information with invalid return addresses. Hence, the process of authentication and server wait will begin again and again, keeping the network or server busy or server not found. Denials of services attack are designed to make a machine or network resource unavailable to its users.

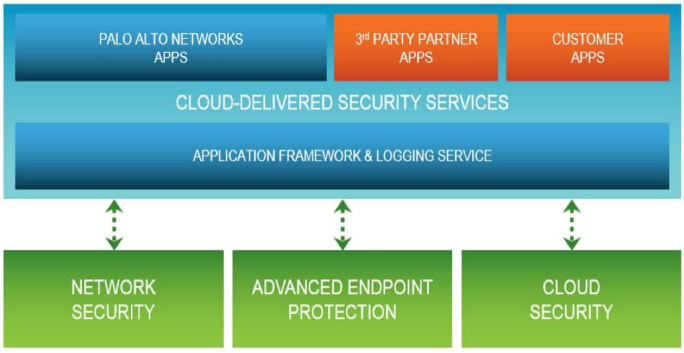
6) Distributed Denial of Service

Denial attacks are the most common forms of cyber-attack, with the number of global distributed denials of service attacks increasing to Cyber networking. Denial of service refers to a cyber-attack resulting in victims being unable to access systems or receive the information and network resources because of that disrupting internet services.

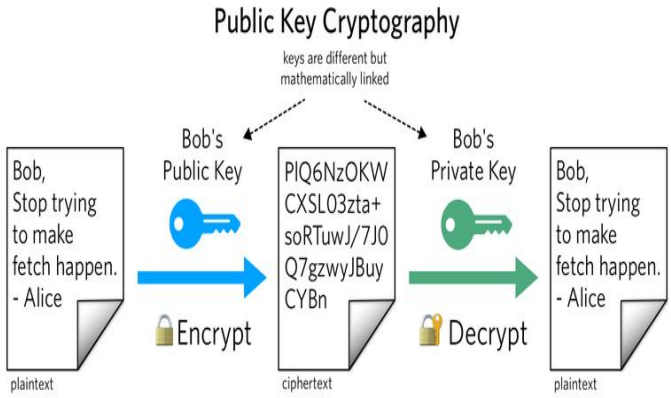
ISSN 2394 - 7780



Measures to ensure Security issues solutions



Encryption under cyber Cryptography is the process of encrypting data into an unreadable format, known as cipher text. It uses to protect data, payment information or account information or emails, only those who possess a secure key can decrypt the messages into plain text. Encryption is the practice of encoding data to ensure the data can be securely relayed over the internet. It acts as one of the most effective methods in mitigating ecommerce security risks to protected data integrity and confidentiality.



Digital signature with digital certificate is most important role in security. Computer User needs a digital certificate to digitally sign a document with encryption. If the user create and use a self-signed digital certificate the recipients of user documents will not be able to verify the authenticity of user digital signature at all. They will have to manually trust user self-signed verified and validated certificate.

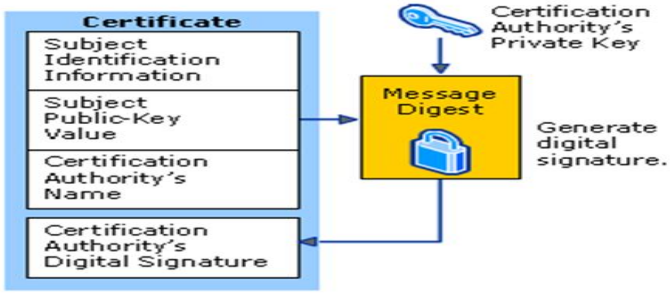
Digital certificate

A digital certificate, also known as a public key or asymmetric certificate, is used to cryptographically link ownership of a public key with the entity that owns it.

For digital certificate, host send a request which includes user distinguished name, user certificated number, user public key, and user signature. Domain name is a unique identifier for user or every host for which

ISSN 2394 - 7780

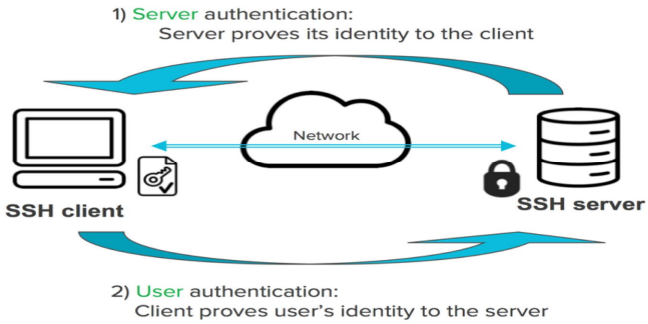
applying for a certificate. The CA (certificate authority) checks user valid signature using user public key and performs some level of verification of user identity. After verification, the CA sends user a signed digital certificate that contains user distinguished name, user server name, user public key, and the signature of the certificate authority or verification. User stores this signed certificate in user key database as record storage.



SSL certificate

Shell security certificates use data files to secure a cryptographic key protect to a company's file. Shell SSL certificate is installed on a network server, it uses specific protocols and algorithms to facilitate a secure connection from the server to browsers' certificates authenticate the identity of user business and secure or protect the data in transit during after the checkout points. This keeps user organization and user customers protected from having financial or important information compromised by hackers or attackers.

Internet service provider (ISP) provides internet over server uses shell SSL which provides a secure channel over an unsecured network in client-server architecture, connecting client application with server protection. The protocol specification differentiated between two versions types, referred to asSSH1and SSH2. Shell is generally used to access various operating systems and network.



CONCLUSION

This paper studies the issues and solutions over of professional and security attackers and defence in cyber or internet system. Current technology allow for security be less than recovering data from victim of an attack. There is a need of controlling, monitoring, auditing and take action to attain highest level of security. The paper provides all possible solutions and need to know security threat using multiple keys it will help in increasing security. This paper also comes to know security threats, there counter measure as well as awareness between user and website. The risk of identity thefts or attackers, market place, and privacy issues will always exists. Cyber Security comes in picture in many daily activities, although sometimes it can be difficult to distinguish between a security attack and an ordinary human or technological breakdown.

REFERENCES

[1]. https://www.bigcommerce.com/ecommerce-answers/why-online-security-so-important/

[2]. https://www.tutorialspoint.com/e_commerce/e_commerce_security.htm

[3]. https://www.techgenyz.com/2017/04/05/e-commerce-major-threats-e-commerce

[4]. https://www.cl.cam.ac.uk/~jac22/books/mm/book/node352.html

[5]. https://www.academia.edu/37862618/Protocols_and_standards_for_E-commerce

[6]. https://www.tutorialspoint.com/e_commerce/e_commerce_quick_guide.htm

[7]. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[8]. https://www.paloaltonetworks.com/cyberpedia/what-is-cyber-security

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

SECURITY ASPECTS IN MOBILE DEVICES

Monica V. Parad
F. G. Naik College, Navi Mumbai

ABSTRACT

Malware, conjointly called malicious code affects the user's ADPS or mobile devices by exploiting the system's vulnerabilities. It is the key threat to the protection of data within the pc systems. Some of the categories of malware that are most typically used are viruses, worms, Trojans, etc. Nowadays, there's a widespread use of malware that permits malware author to urge sensitive info like bank details, contact info, which is a serious threat in the world. Most of the malwares are unfold through web attributable to its frequent use which might destroy massive info in any system. Malwares from their early designs which were just for propagation have now developed into more advanced form, stealing sensitive and private information. Hence, this work focuses on analyzing the malware in an exceedingly restricted surroundings and the way info will be preserved. So, in different to handle the negative effects of malicious code, we tend to mentioned a number of the malware analysis ways that was wont to analyze the code in an efficient manner and helped us to control them. Various malware detection as well as malware propagation techniques were conjointly highlighted. This work was all over by examining malware mitigation methods which might facilitate USA shield our system's info.

Keywords: Malware Analysis, Mitigation, Malware Analysis ways and Techniques, Malware Software, and tools etc.

I. INTRODUCTION

One of the foremost dangerous phenomenons we tend to are observant nowadays on the web is that the unexampled spreading of malware, a program written with malicious intents. Malware (Andreas, M. et al) may be a general term used for programs having malicious code snip which can cause a significant threat to any user. Malware analysis is that the study or method of determinant the practicality, origin and potential impact of a given malware sample like an outbreak, worm, trojan horse, rootkit, or backdoor. Malware or malicious code is any pc code supposed to hurt the host software or to steal sensitive knowledge from users, organizations or companies. Malware could embrace code that gathers user info while not permission. Malware may be a malicious code that propagates over the network (Uppal, D. et al, Mehra, V. et al, &Verma, V. et al). It will be thought-about because the one to that new options will be simply additional to boost its attack. It can even be powerful therefore on take full management of infected host and network association disabling all the firewalls and put in hymenopteran viruses. The problem is cumulating with the use of internet as most of the web pages have been infected with various types of malware downloads which are delivered by just opening the web page. According to statistics by Google, seventieth of the malware comes from standard sites. According to Osterman analysis survey, eleven million malware variants were discovered by 2008 and ninetieth of the malware comes from hidden downloads, pointers in trusty and standard websites. These threats delivered in many various variant modes often referred to as amalgamated threats that contain multiple elements like fishing tries, spams, viruses, worms and Trojan. Malware is often wont to steal info that may be without delay monetized, like login credentials, mastercard and checking account numbers, and property like pc code, financial algorithms, and trade secrets. Although many cybercriminal groups square measure trafficking in commodities shared by multiple trade sectors, like mastercard numbers, there square measure some things whereby one company is clearly the target of one opponent, whether it be an organized crime syndicate, nation-state, or a single operative. Everyday vital vulnerabilities are according on a good form of in operation systems and applications, and malicious activities perpetrated through Internet are quickly becoming the number one security problem, which ranges between massive scale social engineering attacks and exploiting vital vulnerabilities. Recent refined attacks use polymorphism and even geologic process mixed with cryptographically robust algorithms and self-updating practicality that makes analysis and defense more and more troublesome. Nowadays a quick and reliable mechanism to mitigate, pick out and generate vaccines for such attacks is significant for the successful .

II. TYPES OF MALWARES AFFECTING SYSTEMS:

Most popular categories of malwares are viruses, worms, Trojans, ransomwares, adware and spywares. They are known for the manner in which they are spread, rather than any specific types of behaviour.

1.Viruses - A computer virus can be thought of as a program that takes shelter on the host system and start infecting the system by inserting them into another programs or files, and that typically performs a harmful

ISSN 2394 - 7780

action (such as destroying data). An example of this can be a alphabetic character infection, a technique, usually used to multiply malware, that inserts extra data or executable code into PE files

2.Worms - Worms are aptly named for their ability to "crawl" through networks. Worms multiplies themselves however don't implant themselves in alternative programs as a virulent disease tends to try to. Worms move on a network affiliation seeking vulnerable machines to infect. For example, in 1988, the “Morris Worm” became thus widespread that it managed to slow the whole web.

3.Trojans - A bug could be a harmful program that misrepresents itself to masquerade as an everyday, benign program or utility so as to steer a victim to put in it. A bug typically carries a hidden damaging operate that's activated once the appliance is started. The term springs from the traditional Greek story of the bug accustomed invade town of Troy by hiding. Trojan horses square measure usually unfold by some variety of social engineering, for instance, where a user is duped into executing an e-mail attachment disguised to be unsuspicious, (e.g., a routine type to be crammed in), or by drive-by transfer. Although their payload are some things, several fashionable forms act as a backdoor, contacting a controller which can then have illegal access to the infected system. While Trojan horses and backdoors don't seem to be simply detectable by themselves, computers could seem to run slower thanks to significant processor or network usage. Unlike pc viruses and worms, Trojan horses usually don't decide to inject themselves into alternative files or otherwise propagate themselves.

4. Spyware - Spyware’s main function is to monitor what activities you are performing on your computer either you are connected to network or not, and send that information to a third party without your knowledge. In some cases, this data harvesting is used solely for marketing purposes. In other cases, the intent is more sinister. A larceny would possibly occur once associate cheat, posing as a client, directs a CPA to send a payment to an illegitimate recipient.

5.Screen-locking ransom ware - Lock-screens, or screen lockers is a type of “cyber police” ransom ware that blocks screens on Windows or Android devices with a false accusation in harvesting illegal content, attempting to scare the victims into paying up a fee. Jisut and SLocker impact Android devices more than other lock-screens, with Jisut making up nearly 60 percent of all Android ransom ware detections.

6.Rootkits - Once malicious software is installed on a system, it is essential that it stays concealed, to avoid detection. Software packages called rootkits enable this concealment, by modifying the host's operating system so that the malware is hidden from the user. Rootkits will stop a harmful method from being visible within the system's list of processes, or keep its files from being browse. Some types of harmful software contain routines to evade identification and/or removal tries, not simply to cover themselves. An early example of this behaviour is recorded within the Jargon File tale of a try of programs infesting a Xerox CP-V sharing system: every ghost-job would notice the fact that the opposite had been killed, and would start a new copy of the recently stopped program within a few milliseconds. The only thanks to kill each ghosts was to kill them at the same time (very difficult) or to deliberately crash the system.

7.Backdoors – A backdoor is a method of allowing normal authentication procedures, usually over a connection to a network such as the Internet. Once a system generated, one or additional backdoors it also put in so as to permit access within the future, invisibly to the user. The idea has typically been advised that pc makers preinstall backdoors on their systems to supply technical support for patrons, but this has never been reliably verified. It was reportable in 2014 that United States government agencies had been entertaining computers purchased by those thought-about "targets" to secret workshops wherever software package or hardware allowing remote access by the agency was put in, considered to be among the most productive operations to obtain access to networks around the world. Backdoors is also put in by Trojan horses, worms, implants, or alternative ways.

III. MALWARE DETECTION TECHNIQUES

There are techniques utilized in detection malware activities within the system.

a. Static analysis detection technique - it's the procedure of analyzing software system while not execution it. During static analysis [Bergeron, J. et al] the application is break down by using reverse engineering tools and techniques, so as to re-build the source code and algorithm that the application has created. Static analysis are often done through program instrument, computer program and disassemble. Various static analysis techniques are as follows:

b. Signature based detection technique - This technique is also known as pattern matching or string or mask or fingerprinting technique. A signature could be a little bit of sequence injected within the computer programmed

ISSN 2394 - 7780

by malware writers, that unambiguously identifies a specific malware. To discover a malware within the code, the malware detector hunt for a antecedent such as signature within the code.

c. Heuristic detection technique - This technique is also known as proactive technique This technique is similar to signature based technique, with a difference that instead of searching for a particular signature within the code, the malware detector currently searches for the commands or directions that aren't gift within the computer programmed. The result's that, here it becomes simple to discover new variants of malware that had not nonetheless been discovered

IV. CONCLUSION

Day to day malware is being unfolded via network like conflagration. However, conserving data and records during a system involves making certain they continue to be accessible, usable and free from malware attacks. Information and records can deteriorate over time, whether or not they're paper, photographic, digital or audiovisual if they cannot be preserved from possible malware attacks. In this work, we had survey a study regarding varied kinds of malware, malware propagation techniques and categories of malicious software. Although, the speed hazards of malware are increasing at Associate in nursing forbidding rate, this paper provides a thorough study of tools for analyzing malware with different techniques. Hence, the necessity for data preservation in extremely very important and in demand.

V. REFERENCES

- https://www.kaspersky.co.in/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it
- https://us.norton.com/internetsecurity-malware.html
- Andreas, M. Christopher Kruegel, and EnginKirda. (2007). Exploring Multiple Execution Paths for
- https://www.kaspersky.co.in/resource-center/preemptive-safety/malware-remover-vs-antivirus-software
- Malware Analysis. In Proceeding of the IEEESymposium on Security and Privacy, Oakland, California, USA, pages 231.
- Anderson, B., Storlie, C. and Lane, T. (2012). Improving Malware Classification: Bridging the Static/Dynamic Gap.
- https://www.getsafeonline.org/online-safety-and-security/anti-malware/

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

MOBILE DEVICE SECURITY

Madhuri D. Gabhane
Rayat Shikshan Santha's K.B.P. College, Vashi, Navi Mumbai

ABSTRACT:
Smartphone becomes the foremost typical and standard mobile device in recent years. It combines the practicality of mobile and personal organiser. Besides, it provides several computer's practicality, such as processing, communication, data storage and etc.

It additionally provides several computer's service, such as web browser, portable media player, video call, GPS, Wi-Fi and etc. This paper informs about the feature and security issues.

This paper contains depth description of security models of modern mobile operating system like Android and iOS Phone. These security models are cornerstones of security on current platforms. Despite of different approaches of security they have a lot in common. This paper also contains the most discussed security problem of nowadays, Malware. Description of malicious software is from Application-based view. However, modern operating system has strong protection against viruses and other types of infection through its security model, the weakest point of mobile devices are still users. These users usually install additional software into their devices. This paper focuses on Android and iOS malware infection and provides a few protection methods against this type security threat.

INTRODUCTION

1.1 What is mobile equipment?

Mobile equipment is a tiny, transportable machine that permits user to input data through touchscreen or tiny keyboard.Comparing with conventional computer, mobile device is easily carried out but provides much computer functionality, such as processing, communication, storage etc. PDA and smartphone are among the most popular mobile gadgets. Smartphone combines working of mobile phone and PDA.

This paper mainly focuses on analysis of security issues on smartphone. Smartphone usually provides many computer's services, such as web browser, video or audio player, video call, GPS, Wi-Fi, and etc. The top two successful smartphone brands are Google Android, Apple iPhone. The following sections will analyze and compare feature and security issue of these two kinds of smartphone.

1.2 What is Mobile Security?

Mobile security is that the protection of transportable devices like, smartphones, tablets or laptops. Threats may be malware, unauthorized access , device theft etc. This increase in cyber attacks, make the mobile security very important and very vulnerable as well.

1.3 Mobile Security Vulnerability:

Smartphones and mobile devices are exposed to a higher number of threats than other devices like laptops. Also, they're targeted by Cyber attackers quite before. This is mobile devices vulnerability..

First, Mobile devices were used for daily social media interaction and for associated business tasks.It contains a huge amount of personal information that could be easily misused.

In today's business world, the cloud system is dominating organization's technology. BYOD (Bring your own device) is taken into account one amongst several challenges for mobile security.

ISSN 2394 - 7780

Second, their movability, which allow the user to connect to various networks in or outside safe or secured network parameters mostly all the time.

Third, the rise of usage of third party apps and malicious software system square measure one amongst the foremost common ways in which to attack a mobile device.

Threats and security Risks for mobile devices

a) Insecure Data Storage

b) Weak Transport layer protection

c) Poor authorization and authentication

d) Sensitive info may be leaked and disclosed to be exposed or misused

e) Password protection is unavailable

f) Wireless transmission isn't secured or encrypted

g) Malware attacks:

(1) Denial of service attacks

(2) Unauthorized access

(3) Masquerade

Solutions to enhance mobile security

For organizations, they will increase mobile security by unifying the design of the network system.They can combine wireless network, wired network and VPNs into one centralized, Highly secured, encrypted infrastructure.

It will additionally facilitate them notice threat quicker than if it absolutely was localized. They can perform performance test using ethical hackers. In addition, Transport layer should be encrypted with a PKI(Public Key infrastructure) to make sure the authentication and authorization is performed. Workshop, and training programs are necessarily for employees to help increase such security. Users ought to use watchword protection to unlock the device watchword oftentimes, and it will avoid duplication of password. Moreover, users ought to install anti malware, Anti spam and on device personal firewall to minimize the device vulnerability.

A mobile security solution will protect devices against malicious code embedded in apps.

With Mobile defense, you can detect malicious apps that have withstood app store vetting and have been published in public app stores. You can even find apps that has added malicious capabilities through updates and background downloads.

Smartphone Security

This section illustrates the feature and security issue of two kinds of popular smartphone in the market: Android, iPhone.

ISSN 2394 - 7780

Android vs. iOS: The threat level

Apple's operating system is a closed system. Apple doesn't unharness its ASCII text file to app developers, and therefore the house owners of iPhones and iPads cannot modify the code on their phones themselves. This makes it tougher for hackers to search out vulnerabilities on IOS-powered devices.

Android devices unit of measurement the opposite, looking forward to a ASCII code, which means that the house owners of those devices will tinker with their phone's and tablet's in operation systems.

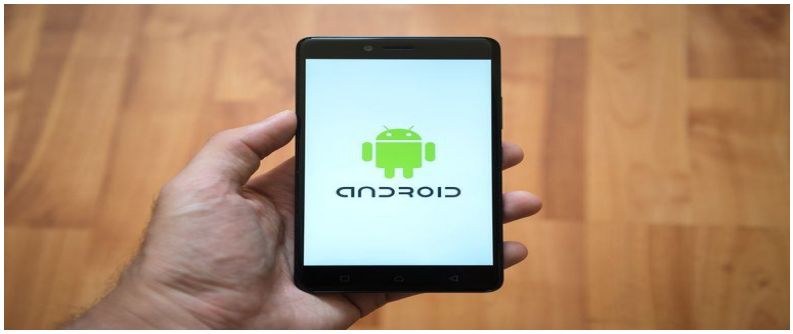
Android is more often targeted by hackers, too, because the operating system powers so many mobile devices today. The global quality of the automaton software package makes it a additional engaging target for cybercriminals. Android devices, then, are more at risk of the malware and viruses that these criminals unleash. While iOS may be considered more secure, it's not impossible for cybercriminals to hit iPhones or iPads.

1. Google Android:

The first part will introduce the history of the mobile operating system and main features of the smartphone. The second part will analyze security issues of this sort of smartphone.

1.1 Features:

Android is a famous operating system for mobile device. Its name is from the first developing company, Android Inc.



Android Smartphone (source: [Shutterstock])

The most attractive part of Google Android is that Google releases most of source code. Google allows the companies within Open Handset Alliance freely install this operating system. Google Android has became the best selling mobile device platform.

Besides that, third-party application developers can use Java, C, or C++ to develop their applications. Google provides online software store whose named is Market. Users can search and download third party applications from this application. Here are 10 options distinctive to Android's OS.

1) Near Field Communication (NFC)

2) Alternate Keyboards

3) Infrared Transmission

4) No-Touch Control

5) Automation

6) Wireless App Downloads

ISSN 2394 - 7780

7) Storage and Battery Swap

9) Widgets

10) Custom ROMs

1.2 Security Issues:
Android also provides application security through "sandbox" which isolates applications from each other. Without permission, one application can not access to other application's data or private information in the mobile device.

Since Android is an open platform operating system, it provides more freedom to the users to install their desire applications. However, it causes the system easier to be attacked at the same time. There are some types of security issues as below.

The second type of security issue is that malicious applications can steal users' private data.This may cause a serious damage to users, especially when the device stores lots of confidential information. Although these sorts of malwares shows up occasionally, Google removes them quickly.

The third type of security issue is Root Trojans.Android default setup is to disable of access root, however several users prefer to root their mobile device.

This increases the potential of being attack. Some malwares can steal users' confidential information or even remotely control the users' device. Whenever Google finds out these bad applications, it will remove them quickly. But still, this kind of Trojan does not stop, so it is better for users to ensure root safety by themselves.Here are some tips for users to improve the level of security for their Android phones.

First, the foremost straightforwardmethodology is to line watchword of the device.Before inputting correct the password, attackers can not access stored information. Fingerprint lock is the most secure method. Since some user may concern about leakage of their biometric information, setting up a password still can well protect the device.

Second, user should not change root Android device. Some users want to download applications from unofficial third-party application store, so they choose to root their Android device. This is a dangerous call, as a result of it'll take away several restrictions and security protections from default setting Third, although Google Android Market does not ensure that all their applications are free of malwares, Google will remove that application from Market and remotely remove them from devices if many users report a same malicious application. So downloading applications from official Android Market ensures higher degree of security. Fourth, there are some anti-virus applications available on the Market.

Installing one amongst in style anti-virus will facilitate users scan dangerous applications and enhance the protection. Fifth, user should ensure the wireless connection is secured and turn off Wi-Fi when they do not use it. Only connecting to familiar wireless network is also a good method to protect the security of device.

2. IPHONE:

iphone (source: [Shutterstock])

ISSN 2394 - 7780

2.1 Features:

1. Web browsing/ Email/ ipod/ video playback/ Apps/ Camera
2. iPhone Home Screen
3. iPhone Controls (Home Button, Volume Button, Ringer Button , Dock Connector.
4. iPhone with iTunes (Activation, Sync, Restore and Reset)

2.2 Security issues : If an iPhone is lost or purloined, even if it's locked, it's possible for a hacker to obtain sensitive data. The iPhone is additionally vulnerable to remote code injection attacks and to hackers intercepting wireless signals.

Viruses, worms and Trojan horses may also access secure resources for the needs of disrupting services, causing damage or extracting confidential information. Given the quickly growing range of enterprise iPhones, it has no choice but to confront these security challenges head on. Wi-Fi security measures, virtual private networks (VPNs) and Exchange ActiveSync are just some of the tools and strategies that can help abate the security risks that come with iPhones.

IT should take each step potential to guard the information keep on users' iPhones. That means encrypting transmitted knowledge, using digital certificates for authentication and enforcing strong passcode-lock rules. Beyond knowledge protection, mobile device management (MDM) is at the center of effectively incorporating iPhones into the enterprise.

Apple'siOS

More tight controls: It's tougher for developers to induce apps into the App Store.That's because the review process is more stringent.Because of this, it's less seemingly for a malicious app to sneak into Apple's store.

Less flexibility: Apple doesn't permit the house owners of its devices to switch its iOS software package or custom ROMs to be loaded on their devices.That makes the system safer since Apple controls the whole expertise.This doesn't stop some house owners from "jailbreaking" their Apple mobile devices, modifying their source code.Jailbreaking opens new capabilities on the devices — like dynamic digital-assistant Siri's voice, for instance.

A less tempting target: Because the iOS operating system powers fewer mobile devices, hackers don't target the system as often.This makes sense that the Hackers and cybercriminals will guarantee a lot of victims if they focus a lot of of their attacks on the a lot of well-liked robot software package.

APPLICATIONS

- Secure your network connections on the back end
- Put identification, authentication, and authorization measures in place
- Have a solid API security strategy in place
- Test your app software—then test again
- Build a strong security framework
- Creates caution against using BYOD policy
- Protects our devices

CONCLUSION

We focused solely on mobile security. Our mission is to secure mobile devices and apps and defend the those that use them. The mobile app testing, device observance, forensics gave us with a singular set of mobile security information. We printed this report back to share a number of that information and therefore the ensuing insights with the general public. We also aim to help enterprises manage and secure the mobile devices and apps that connect with their corporate assets each day: Mobile security needs a special approach not targeted on malware. Leaky apps that store or transmit sensitive personal and company information in associate insecure manner area unit of so much bigger concern at this time in time. Even legitimate apps while not by design malicious practicality that area unit downloaded from official app marketplaces will embody high risk security problems.

ISSN 2394 - 7780

- Mobile security needs distinctive and remediating security problems in device OSs and configurations, the apps put in on those devices, and therefore the network connections those devices create on a daily basis.

REFERENCES

- https://www.upwork.com/hiring/mobile/mobile-application-security/
- https://searchmobilecomputing.techtarget.com/tip/Enterprise-iPhone-security-issues-and-how-to-address-them
- https://books.nowsecure.com/mobile-security-report/en/conclusion.html
- https://us.norton.com/internetsecurity-mobile-android-vs-ios-which-is-more-secure.html
- https://www.gazelle.com/thehorn/2014/02/10/the-android-operating-system-10-unique-features/
- https://www.lifewire.com/apple-iphone-basics-features-1999727
- https://www.proofpoint.com/us/visibility-mobile-defense

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

NEED OF CYBER SECURITY IN TODAY'S MODERN AGE

Yogita Y. Sawant
Assistant Professor, JVM's Mehta College, Navi Mumbai

ABSTRACT

In today's highly advanced technological world internet has become the fourth most important necessity after food, clothing and shelter. Google, Facebook, Instagram and Twitter have become an important platform to post information about our lives. All our important information and transactions are stored in computers or expressed through internet which can easily be accessible to anyone at anytime. We all have become so much technologically addicted and virtually driven that we completely ignore the darkest part of this cyber world and i.e. cyber crime. The rate of cyber attacks are increasing day by day and as the world is having cyber war it has become necessity to understand cyber crimes and protect our information and ourselves from such crimes. And that's where cyber security comes in the picture. This paper mainly focuses on the need of cyber security in today's modern age.

Keywords: Technological, Information Cyber Security, Cyber Crime

OBJECTIVES OF THE STUDY

The objectives of this study are -

1. To understand the importance of cyber security in today's world.
2. To focus on increasing number of cyber crimes and the ways to deal with it through cyber security.

RESEARCH METHODOLOGY

The research is mainly based on the secondary data. The secondary data has been collected from various reference books, research papers, articles and websites.

INTRODUCTION

The innovations of computers have changed our lives in such a way that the virtual life has become as important as real life. With internet facilities available at cheaper rate and anywhere in the world it's difficult for people to resist themselves from using it. Whether it be communicating with friends, paying bills, reading news, playing games or managing our bank accounts everything is internet based and at the tip of our fingers. But what we forget here is that the more we use internet and social media as a tool to reveal our information the more we give chance to others to invade our privacy and steal all our information without our knowledge. If we are not careful about the information shared on internet, our identity can easily be stolen or our finances drained.

Cyber related crimes are increasing day by day across the world. Hacking and viruses are the most common methods used to steal important personal information. Understanding cyber-crime has become need of an hour to understand how criminals are using the Internet to commit various crimes and what can be done to prevent these crimes from happening. That's where Cyber security plays an important role.

CYBER CRIME

The role of cyber security will not be clear unless we understand the darkest side of this cyber world and i.e. cyber crime.

"Cybercrime is any illegal activity that is performed on the Internet or any network-based device. These crimes include identity cyber theft, viruses, cyber hacking, cyber stalking and phishing."

TYPES OF CYBER CRIME

Hacking

It is the skill which can be used to have unauthorized access to someone's digital device such as computer, laptop or phone.

Identity Theft

Identity theft occurs when an individual's personal information such as bank account information, social security numbers, and addresses are stolen by hackers. The hacker will then use this information to steal money from victim's account.

ISSN 2394 - 7780

Viruses
Computer viruses are pieces of code that are usually attached to downloadable files. These viruses infect important information and can lead to deletion or corruption of important system files. These viruses may also allow personal information and files to be accessed by another user.

Cyber Stalking
Cyber stalking is a crime that occurs when a person is being stalked, harassed or threatened by another person using social media, email etc. Threats are often received by the victim as a strategy to get the victim to reply which makes the victim suffer from anxiety and fear.

Malicious Software
These are soft wares or programs which are made with an intention to disrupt a network or to steal sensitive information or gain access to data.

Ransomware
It is a crime where a victim's computer is infected via phishing attacks or any other exploitative means. After successful infection, the ransomware commonly encrypts the victim's data. It then demands a huge sum of money in exchange for the return of their data. But there's also no guarantee that the victims will ever get their data back

Phishing
Phishing is a crime where malicious mails are sent to the victim to gain access to victim's financial or personal information accounts. The victim, if not cautious, will enter their personal information on a site that will mimic the website used for personal information. Users are even tricked into emails claiming they need to change their password or update their billing information, giving criminals access.

IMPORTANCE OF CYBER SECURITY

Ever since computers have become inevitable part of our life the need for cyber security has accelerated. In this digital world all our daily activities are depended on the internet and this allows for predators to attack, hack, damage and steal our personal and government information. Cyber security is thus designed to secure our computers and data from these attempts and to ultimately have safe networks and computers.

"Cyber security or information technology security is the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide."

NEED FOR CYBER SECURITY

1. The rising cost of breaches
Cyber Security is important because without any knowledge or awareness of the issue we are waiting to be attacked. It may not happen today, but eventually we can be victimized and be breached. We will have to deal with the consequences and wait to find solution over it. These cyber attacks can be extremely expensive for businesses or for our personal life. It can also damage one's reputation.

Suffering a cyber attack can cause customers to lose trust in a business and having a reputation for poor security can also lead to a failure to win new contracts. So as rightly said prevention is better than cure one should have complete cyber security while dealing with their data rather than repenting later.

2. Increasing numbers of sophisticated hackers
It is impossible today to have a business without using internet,websites,social media tools or any other platforms.Almost every business has a website or webpage which provides an exposure to criminals to enter into internal networks. Hackers have a lot to gain from successful data breaches, and there are endless examples of well-funded and coordinated cyber-attacks against some of the largest companies in the India, USA and UK. Ironically, even Deloitte, the world's largest cyber security consultant, could not secure itself from a cyber attack .

With highly sophisticated attacks now common individual and businesses need to assume that they will be breached at some point or other in the lifetime and should implement controls that help them to detect and respond to malicious activity before it causes damage and disrupt their software.

3. Widely available hacking tools
The wide availability of hacking tools and programmes on the internet is also creating more threat from less skilled individuals as they are using it to make easy money. The monetary benefit aspect of cybercrime has

ISSN 2394 - 7780

made it easy for anyone to obtain the resources they need to launch damaging attacks, such as ransomware and cryptomining.

4. A proliferation of IoT devices

In this era of smart world all our smart devices are connected to the internet. These are known as Internet of Things or IoT devices. These devices simplify and speed up our tasks, and even offer greater levels of control and accessibility. But there proliferation, however, presents a problem.

If not managed properly, each IoT device that is connected to the internet could provide cyber criminals a chance to damage or steal one's data. With use of IoT devices leading to wide range of threats, it is wise to conduct regular security assessments to help identify and address risks presented by these assets.

5. Tighter regulations

It is not just criminal attacks that is motivating us to invest in cyber security but the introduction of regulations by the government that is forcing organisations to take security more seriously than ever, to implement appropriate technical measures to protect data, plus detect, investigate and report breaches or face heavy fines.

CONCLUSION

The increasing number of cyber-attacks all over the world is creating the need for updated, advanced and much stronger cyber security. Computer networks will forever be the target of criminals, and it can be argued that the danger of cyber-security breaches will only increase in the future as networks continue to expand. Having proper preventive measures and specialist assistance is essential to minimize and control damage, and recover from a cyber breach and its consequences.

Finally, to protect ourselves from cyber-crimes we have to be aware of what information to put on the Internet and to be aware that there is no privacy in this internet based advanced world and so the information can be seen at any time by any person in the world. There are cyber crime and cyber security departments whom one can report about any cyber-attacks.

REFERENCES

- Dr. Ahmad Farroq, 'Cyber Law in India (Law on Internet).' New Era Law Publications, Delhi, 2011
- Goutam, R. K. (2015). *Importance of Cyber Security*. International Journal of Computer Applications, 111(7) doi:10.5120/19550-1250
- Prasad, R.S., 'Cyber Crime: An Introduction.' ed.-P', The ICFAI University Press, Hyderabad, 2004.
- Williams, B. K. Sawyer, S. C. (2015) *Using Information Technology*. New York, New York: McGraw-Hill Education

WEBLIOGRAPHY

- https://www.forbes.com/sites/larrymagid/2014/10/01/why-cyber-security-matters-to-everyone/#1e699d771fd0
- https://www.bbc.co.uk/news/uk-36239805
- https://www.whitecase.com/publications/insight/cyber-risk-why-cyber-security-important
- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

ISSUES IN DATABASE SECURITY

Nitin N. Kawle and Vinay D. Jadhav
JVM'S Mehta Degree College, Navi Mumbai

ABSTRACT

Security is one among the key issues for any direction system. developing an honest information and providing security management for the information has perpetually been an enormous issues. In today's world information is generated at a speed and final destination of such information such information is information. information is hold on in data for simple and economical due to manage these info.

All the operations of knowledge manipulation and maintenance or done practice management system during this paper we've mentioned a number of the attacks and managements which will be potential with its counter measures and its control ways which will be potential. securing data is extremely vital approach for the planning of specific and directive based data security wants. as complexity of information can increase we tend to could tend to possess additional complicated security problems with information.

Information is that the foremost expensive quality in todays world as a result of it's utilized in day to day life from one individual to huge organizations. to create the retrieval associate degreed maintenance {of info of data of knowledge} straightforward and economical it's hold on in an extremely information databases area unit a favourite target for attackers or hackers. because the amount of knowledge collected maintained and shared electronically expands therefore will the necessity to grasp information security. I even have discuss during thistopics of what's information or information.

INTRODUCTION OF SECURITY

Within the straightforward words security means safety and protection. in different terms security suggests that the protection of information networks and computing power. the protection of data of knowledge of information security or information security is that the most vital 3 main factors:

1. Hacking tools that will be found very just by every one just by googling which they're endless.
2. Technology with the end-users has increased quickly within these years like net information measure and pc process speeds.
3. Access to hacking info manuals. potential losses thanks to security attacks:- the potential losses during this computer network area unit several although you're employing a single pcin your area. here it'll be listing some examples that have associate degree on the spot impact on you and on others:

Losing you information if your pc has been hacked or infected there's an enormous probability that every one your hold on information may well be taken by the aggressor. dangerous usage of your laptop resources this implies that your network or laptop can get into overload thus you cannot access your services or in associate degree extremely worst case situation it area unit typically utilised by the hacker to attack another machine or network. name loss merely assume if your facebook account or business email has been owned by a social engineering attack and it sends fake data to your friends business partners. you may need time to realize back your name. fraud this can be a case wherever your identity is picture name cognomen address and mastercard and might be used for against the law like creating false identity documents.

WHY IS NEEDED SECURITY OF INFORMATION

It'll topics discuss varied controls of security of information. That can handle the code applications or systems and any organization to protected of secure information which will provided. information security strives to insure that alone several users perform approved activities at approved times. information security is constructed upon a framework 3constructs: confidentiality integrity and convenience.

WHY IT'S REQUIRED

Once pc applications were developed to handle monetary and private information the $64000 would like for security came into the image. we'd like security to:

1. To shield our information files and folders.
2. To shield our resources.
3. To shield e-commerce group action info user id positive identification pin etc.

ISSN 2394 - 7780

4. To shield our IP addresses.

5. To shield my e-mails.

INFORMATION SECURITY COVERS ASPECTS AND COMPONENTS

1. Information hold on in information

2. Information server

3. DBMS

4. Different information work flow applications.

THERE AREA UNIT TWO TYPES OF SECURITY CONTROLS AS FOLLOW

MANAGEMENT CONTROLS

The safety controls that specialise in the management of risk and therefore the management of knowledge system security operational controls:- the safety controls that area unit primarily enforced and dead by folks.

TECHNICAL CONTROLS

The safety controls that area unit primarily enforced and dead by the system through the systems hardware code or computer code.

WHAT'S INFORMATION SECURITY

Information is nothing however info and information is assortment of information. Database security issues the use of a broad vary of information security controls to defend databases.

Information security could be a specialist topic of pc security info security and risk management. as a general rule if your company collected any sort of information concerning customers or different community it's hold on a information elsewhere. this information is also personal or sensitive and might be subject to stricted privacy term and condition.

As an example client has your facet give with you email address communication address and mobile variety once they purchases. but if this information will access while not authorization sold to 3rd party or otherwise victimized you'll be subject to strictly legal proceeding from the folks. whose privacy has been compromised. in traditional type information security is any sort of security accustomed shield databases and therefore the info they contain from compromised. However hold on information are often protected embody

1. Code is employed to insure that third party or hackers cant gain access to the information through virus hacking or any method.

2. Physical control:- associate degree example of a physical element of information security may be the constant monitor information by company personnel to permit them. the establish any potential weakness.

3. Body control:- this refers to things just like the use of positive identification proscribing the access of bound peoples.

PRINCIPLES OF INFORMATION SECURITY

Once managing thoughts of security model of security is needful. whereas relating to information security comes in varied forms that reckoning on roles and purpose. the key categories area unit areas of interest threats impact and loss what is more as a result of the actions involved in addressing them.

Security risks square measure to be seen in terms of the loss of assets these assets include:

Hardware software data quality credibility availability business benefit types of information or database security control

- **Access control:-** it access control determines who should be able to access what. for instance the employees within an organization may be able to see the data record in the database but be may not be permitted to update. whereas an administrator may be able to view as well as update or modify the contain because of the authority that he has. it also helps in defining the user rights and maintenance of the activity log
- **Authentication:-** authentication mechanism help establish proof of identities. the authentication method ensures that the origin of associate piece ofemail or document is properly known.

3. Auditing:- database auditing involves perceptive a information therefore on remember of the actions of information users .database auditing is used to track database access anduser activity. auditing is wont to

ISSN 2394 - 7780

determine united nations agency accessed information objects what actions were performed and what data was changed.

4. Encryption:- the process of coding plain text messages into cipher text messages is named as cryptography. in associate cryptography theme the meant info or message referred to as plain text is encrypted using an encryption algorithm a cipher generating cipher text that can be read only if decrypted. the process of converting cipher text to plain text by the receiver is called decoding or decryption.

5. Integrity controls:- data integrity is that the maintenance of and therefore the assurance of the accuracy and consistency of information over its entire life-cycle. Dataintegrity is the opposite of data corruption .stability performance re-usability and maintainability this features responsibility of the database to ensure data integrity as well as the consistency model for the data storage and retrieval.

6.Flow management distributed systems embrace plenty of knowledge result one website to a different and additionally inside a site.

flow management prevents information from being transferred in such how that it is accessed by unauthorized agents. a flow policy lists out the channels through that info will flow. it additionally defines security categories for information further as transactions.

COMPUTER MISUSE OF SECURITY
Hacking offence

Simple unauthorized access –there should be access to only users who are related to that organization or firm not to others users who not belongs to that organization

Unauthorized access-with intent to commit an offence security of data must be there so that an unauthorized person is not allow to access that information.

Unauthorized modification- there should be permission given to access to that users who are eligible to handle that information with privacy related.

Incorrect data modification:- it is a loss of integrity. incorrect results in database the use of incorrect information may result inaccuracies erroneous decisions which in turn can lead to financial losses but also to a loss ofconfidence

SECURITY PLAN RELATED TO DATABASE

- Identify the user community.
- Gather the database information.
- Determine the types of user account establish
- DBA authorities and procedures.
- Establish policies for managing making deleting auditing user accounts.
- Establish the user identification method.
- Define security incidents and reporting procedure.
- Assess the sensitivity of specific data objects.
- Establish standards and enforcement procedures as well as back-up and recovery plans of course.

WHY IS DATABASE SECURITY IMPORTANT

Database security is more than important because sufficient database secure prevent data bring lost or compromised for the company both in terms of finances and reputation.

Database security helps

- company block attacks
- prevent malware
- loss of corruption data

SECURITY IN MICROSOFT OFFICE ACCESS DBMS

In microsoft office access the sql grant and revoke statements are not available. so in microsoft office access securing a database is very important which can be secured by setting a password for opening a database. a

ISSN 2394 - 7780

password can be set when opening a database from the option of tools security menu .thus only users who key in the correct password could open the database. if the unauthorized user try to access it will not allow to proceed to login if the user is using correct password then only system will be allow toopen the database so that user will access and modify as per their needs .ifuser is entering correct password then only the database will be open after that only all the objects in the database will be accessed.

CONCLUSION

The need to secure pc systems is well understood associated securing information should be a part of an overall pc security arrange. database security is turning into associate more and more vital topic and students got to develop core understandings during this space. modification of data the concepts related to database security are multifaceted. this makes it difficult to show the fabric once information security is enclosed as only one element of a bigger course.however this is often however most students square measure exposed to the subject. this paper suggested a set of sub-topics in a database security course component and introduced a set of interactive software modules mapped to each sub-topic presented. To summarize access protection begins with who can access data and what type of data attackers want to access.

There is plenty of scope to enhance the techniques used for information security.

According to the survey eighty four firms feel that information security is adequate. 73% of firms that predict information attach can increasing day by day. 48% of attackers are authorized users.

48% of users have done misuse of their privileges.

according to the survey this paper focused on threats and its possible counter measures that can be possible to secure data in databases

REFERENCES

[1] Mr.SaurabhKulkarni, Dr.Siddhaling Urolagin, Review of Attacks on Databases and Database Security Techniques, Facility International Journal of Engineering Technology and Database Security Techniques Research, Volume 2, Issue 11, November-2012.

[2] Sohail IMRAN, DrIrfanHyder, Security Issues in Database, Second International Conference on Future Information Technology and Management Engineering, 2009.

[3] Emil BURTESCU, Database Security- Attacks and Control Methods, Journal of Applied Quantitative Methods, Volume 4, Issue 4, 2009.

[4] JipingXiong, LifengXuan, Jian Zhao and Tao Huang, Web and Database Security, Zhejiang Normal University.

[5] Shelly Rohilla, Pradeep Kumar Mittal, Database Security: Threats and Challenges, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER SECURITY

Sayli Rajaram, Kadam and Mansi Ajit Madhavi

ABSTRACT

Cybersecurity plays an important role in the field of information technology Securing the information have become one of the biggest challenges in the present day. Whenever we think about cyber security the first thing that comes to our mind is 'cyber crimes' which are increasing immensely day by day. Various Governments and companies are taking many measures in order to prevent these cybercrimes. Besides the various measures, cybersecurity is still a very big concern to many. This article mainly focuses on the challenges faced by cybersecurity on the latest technologies. It also focuses on the latest about cybersecurity techniques, ethics and the trends changing the face of cybersecurity.

INTRODUCTION

Today's man is able to send and receive any form of data and information may be an e-mail or an audio or video just by clicking a button. But did ever think how securely his data id is being to be transmitted or sent to the other person safely without any leakage of information? Today the Internet is the rapidly growing infrastructure in everyday life. In today's technical environment many latest technologies are changing the face of mankind. But due to these emerging technologies, we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are increasing day by day. Nowadays more than 60 per cent of total commercial transactions are done online, so this field requires a high quality of security for transmission and best transactions. Hence cybersecurity has become the latest issue. The scope of cybersecurity is not just limited to securing the information and data in the IT industry but also to the various other fields like cyberspace etc. Even the latest technologies like cloud computing, mobile computing, E-commerce, Net banking, E-Auctions etc also need a high level of security. Since these technologies hold some important information and data regarding a person their security has become a must thing. Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer and protecting Internet users has become integral to the development ofnew services as well as to the governmentalpolicy.

CYBERSECURITY

Privacy and security of the data will and always be top security measures that any of the organization takes care of. We are presently living in a world where all the information and data is maintained in a digital form. Social networking sites or social media provide a space where the users feel safe as they interact with their friends and family. In the case of home users, cyber-criminals would continue to target social media sites to steal personal data. Not only social networking but also during the bank transactions a person must take all the required security measures.

Cyber Security Incidents reported to Cyber999 in Malaysia from January–June 2012 and 2013 clearly exhibits cybersecurity threats. As crime is increasing, the security measures are also rapidly increasing. According to the survey of U.S. technology and healthcare executives nationwide, Silicon Valley Bank founded that companies believe cyber attacks are a serious threat to both their data and their business continuity.

ISSN 2394 - 7780

- 98 per cent of the companies are maintaining or increasing their cyber security resources and of those, half are increasing resources devoted to the online attacks this year.
- The majority of the companies are preparing for when, not if, cyber attacks occur.
- Only one-third per cent are completely confident in the security of their information and data and even less confident about the security measures of their business partner.

There will be new attacks on the Android operating system based devices, but it will not be on a massive scale. The fact tablets share the same operating system as the smartphones mean they will be soon targeted by the same malware as those platforms. The number of malware specimens for the Macs would continue to grow, though much less than in the case of PCs. Windows 8 will allow users to develop applications virtually for any device (PCs, tablets and smartphones) running Windows 8, so it will be possible to develop malicious applications like those for Android and hence these are some of the predicted trends running in cybersecurity.

WIRELESS SECURITY

Wireless network security is the process of designing, implementing and ensuring the security on a wireless computer network. It is a subset of the network security that adds protection for a wireless computer network. Wireless network security is also known as 'wireless security'.

Wireless network security primarily protects a wireless network from an unauthorized and malicious access attempt. Typically, wireless network security is delivered through wireless devices such as wireless router or switch that encrypts and secures all the wireless communication by default. Even if the wireless network security is compromised, the hackers are not able to view the content of the traffic or packet in transit. Moreover, wireless intrusion detection and prevention systems

also, enable the protection of a wireless network by alerting the wireless network administrator in the case of a security breach.

Some of the common algorithms and standards to ensure the wireless network security are Wired Equivalent Policy which is also known "WEP" and Wireless Protected Access is known as "WPA".

DATABASE SECURITY

As the general rule now, if your company collects any information about customers, suppliers, or the wider community, it is stored on the database somewhere. This information may be sensitive and private and can be subject to the strict privacy agreements including those referred to the above content. For instance, your customers may provide you with an email address, postal address, and phone number when they purchase something from you. However, if this data is accessed without authority, sold to third parties, or otherwise misused, you could be subject to strict legal action from the people whose privacy has been compromised. Basically, database security is any form of security used to protect databases and the information they contain from compromise. Examples of how stored data can be protected include:

- Software – software is used to ensure that people can't gain access to the database through viruses, hacking, or any similar process.
- Physical controls – an example of a physical component of database security could be the constant monitoring of the database by company personnel to allow them to identify any potential weaknesses and/or compromises.

MALWARE ANALYSIS & SECURITY

The term malware is a short form of malicious software, as the name suggests malware are intended to harm computers and computer users by stealing information, corrupting files and by just doing mischievous activities to annoy users. Malware is widely and rapidly spreading, it is suggested, there is a massive increase in the security incidents of computers. Development of networks is hindered by malware. Malware targets the applications that run over the internet. As almost all fields of life use the internet to improve its quality of service increase the need to detect and deactivate malware as early as possible so that the negative results created by this malware can be avoided. The malware that has propagation ability is the most dangerous one because there is no central control so defending them is not an easy task.

A Study on Malware and Malware Detection Techniques 21 threat to computer security. Malware creators are always come with new ideas. They develop malware in such a way that they changed themselves from time to time so that they cannot be detected easily. Malware writers always try to write programs that cannot be easily

ISSN 2394 - 7780

detectable, with the passage of type they made improvement in the techniques that are used to hide or morphed the malicious code successfully.

MOBILE DEVICE SECURITY

The growth in wireless technology and in the improvement of mobile device usage has been increased in the mobile market. The growth in the creation and even in the maintenance and security of secure identities for the mobile devices had created challenges and tackles for each and everyone, society and businesses particularly in the mobile added value services such as mobile banking, mobile check-in, mobile ticket and the government security services. Below are the few prominent challenges with mobile devices because of threats and vulnerabilities.

CYBERSECURITY TECHNIQUES

Access control and password security The concept of user name and password has been a fundamental way of protecting our information. This may be one of the first measures of cybersecurity.

The documents that we receive must always be authenticated be before downloading that is it trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the antivirus software present in the devices. Thus a good antivirus software is also essential to protect the devices from viruses. 6.3 Malware scanners- This is the software that usually scans all the files and documents present in the system for the malicious code and harmful viruses like Viruses, worms, and Trojan horses are examples of malicious software that are always grouped together and referred to as malware. 6.4 Firewalls- A firewall is the software program or the piece of hardware that helps screen out hackers, viruses, and the worms that try to reach your computer over the Internet. All the messages entering or passing out, the internet pass through the firewall present, which examines each of the messages and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware. 6.5 Anti-virus software Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as antiviruses and worms. Most of the antivirus programs include an auto-update feature that enables the program to download the profiles of new viruses so that it can check for the new viruses as soon as they are discovered. Antivirus software is a must and basic necessity for every system.

CONCLUSION

Cybersecurity is a vast topic that is becoming more essential because the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cybercrime continues to diverge down different paths with each New Year that passes and so does the security of the information. The latest and disruptive technologies, along with the new cyber tools and threats that come to light each day, are challenging organizations with not only how do they secure their infrastructure, but how they require the new platforms and intelligence to do so. There is no perfect solution for cybercrimes but we should try our level best to minimize them in order to have a safe and secure future in cyberspace.

REFERENCES

1. A Sophos Article, eight trends changing network security by James Lyne.

2. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole

3. Computer Security Practices in Non-Profit Organisations – A Net Action Report by Audrie Krause.

4. A Look back on Cyber Security 2012 by Luis corrals – Panda Labs.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

SECURITY APPROACHES APPLICABLE FOR MOBILE DEVICES

Sanjivani Nalkar
Computer Science-Department

ABSTRACT
It is very difficult to manage our daily work without mobile devices as they provide us to access huge variety of services. Presently the uses of mobile devices has significantly increased as it offers connectivity feature like Wi-Fi, GSM, Bluetooth and GPRS. Due to this connectivity feature vulnerabilities exploiting these mobile devices has also increased. Therefore smartphones becomes the perfect goal for malware writer. Due to increase in vulnerabilities and then performing attacks increased the urge in finding the security solutions researched by researcher. As we are very much aware that making research in this field in depth is immature and unexplored, hence my aim is to provide an overview of research on these mobile device's security solutions. Within this paper I have discuss the survey made within year 2004-2016, by focusing on high level attacks made on user applications. With existing solution on problems I aimed to suggest the different approaches for protecting the mobile devices.

Keywords: Mobile Security, Wi-Fi, GSM, GPRS

INTRODUCTION
Existing mobile devices gives lots of the capabilities of conventional personal computers and hence offers a wide selection for connectivity choices like Wi-Fi, GSM, Bluetooth, GPRS, UMTS and HSPA. Hence it results as a perfect goal for an attacks. Earlier days, smartphones are packaged with standardized operating system which results in a single vulnerability to attack many types of devices by breaking security. But recently many operating systems are introduced for smartphones like android, symbian, windows mobile and iphone OS. Though the global sales of smartphone will increased then also it will be less as compared to PC malwares. For example, many peoples downloads and installed different applications for their smartphones which results in increase of malicious code installation. After this peoples are using their smartphones for performing sensitive operations such as online banking and shopping, so the this generate gain for attacker. With this intention attackers focuses on smartphones platform and the cases of mobile OS vulnerability has been increased. By having survey on such types of cases researchers also started to work on smartphones security. To get the knowledge of current security issues related with smartphones I review attacks, vulnerability, attacks and different solutions to protect smartphones.

MOBILE DEVICE TECHNOLOGIES
Here I want to focus on some information on wireless and networking mobile device technologies which results in the interest of using smartphone.

A. Wirless Communication Technologies
The most useful technology in are GSM,GPRS,EDGE and UMTS.

i) GSM: it is known as Global System for Mobile communications (GSM). It is a most famous technique used in Europe. It belongs to second generation(2G) wireless telephones technology. It is developed in 1990 by Group Special Mobile called CEPT(Conf´erence Europ´eenne des administrations des Postes et des T´el´ecommunications), created a cellular networks where mobile phones communicates with one another by using data transmission, email, digital fax, short message services(SMS), call forwarding teleconferencing etc.

ii) GPRS and EDGE: General Packet Radio Service(GPRS)referred as 2.5 generation was developed to improve GSM network's performance so that user can get higher data rate within lower access time compared to old GSM standard. GPRS is based on packet switching technique to exchange the data between users. Afterwards many multimedia applications like Wireless Application Protocol (WAP) and Multimedia Messaging Services(MMS) are introduced. In 2000, the GPRS features were improved by supporting higher transmission rate and reliability and called it as Enhanced Data rate for GSM Evolution(EDGE).

iii) UMTS: In 2002, a standard has been introduce, which represent a third generation(3G) on cellular system and is known as the Universal Mobile Telecommunication System(UMTS). In this circuit and packet switching connections are used parallel.

ISSN 2394 - 7780

B. Networking Technologies

Within few years, the popularity of Laptop computers has been increased due to easy installation. Due to this Wireless Local Area Network(WLAN) also became popular and this enables the devices to connect by wirless distribution methods and allow user to move within local coverage premises without losing their connectivity. Out of different stands which regulates communication in WLAN, Bluetooth is most popular. Bluetooth technique was developed in 1999, by Special Interest Group(SIG). In this technique user can exchange data within small area with short radio transmission wavelength. It is a technology which creates Personal Area Network with high level of security. It also provide some more features as lower power consumption, small production cost, shorter range communication.

MOBILE MALWARE

This section explains overview of mobile malwares. Malwares are kind of annoying software or code, intrusive or hostile (Backdoor, Trojan, rootkit) developed to use the devices without owner's permission. They can also be distributed as malicious attachment or a link in an infected website send as a spam. Depending on the features, Malware can be categories as

- virus;
- worm;
- Trojan;
- rootkits;
- botnet.

A virus is a small code which replicates itself these replication can infect other programs, boot sectors or files.

A worm is also a small code and also creates it's own copies. It transfers from one device to other without users interventions.

A Trojan is also a malware and provides same functionality and does the maximum damage.

A Rootkits is a malware which performs it's task by infecting the OS. It disables firewalls, anti viruses and installs Trojan in system. Botnets are a set of devices which are infected by viruses and allows an attacker to control these devices remotely.

ATTACKS ON MOBILE DEVICES

In this section we discussed different attacks performed on mobile devices.

- Wireless;
- Break-in;
- Infrastructure-based;
- Worm-based;
- Botnet;
- User-based.

1) Wireless Attacks: There are many attacks which can be performed on mobile devices and can target the personal and sensitive information. The most common attack is eavesdropping on wireless transmission to get the confidential information. Malware usually exploits Bluetooth as a medium for fast propagation.
2) Break-in Attacks: this technique allows attacker to gain control on the targeted machine by using buffer overflow or format string vulnerability. These are used to launch a further attack.
3) Infrastructure-based Attacks: the damage performed by this attack is huge as services provided to mobile devices are based on infrastructure such as calling/receiving a calls, SMS and e-Mails Since the services provided.
4) Worm-Based Attacks : the main based characteristics of worms are based on

- Transmission channel - In this type transmission channels like internet, Bluetooth, memory cards, MMS messages are targeted to perform an attack.
- Spreading parameters- In this type a warms can be spread out by single click and can infect any mobile devices located in any part of the world with confirm chance of success.

ISSN 2394 - 7780

- User mobility models- this type focus on provisioning and capacity, devices and communication patterns, topologies, services. The important for this is it required internet connectivity for spreading of mobile worms.

5) Botnets: after making the mobile devices relatively isolate from internet so there is need to protect them from botnets. As networks are integrated with internet the threat on internet transfers from mobile networks consist of botnets asmobile devices can turned into botclients easily.

6) User as an Attack Vector: it contains each exploits which is not technical in nature. Many mobile malwares are not based on technical vulnerability but a trick by which user override the technical security.

SECURITY SOLUTIONS FOR MOBILE DEVICES

This section has discussed existing mechanisms which are developed to protect mobile devices from different threats.

A. Intrusion Detection Systems

Here we discuss the state of art of different models and tools that implement Intrusion Detection System's(IDS's).

IDS is based on two approaches as

a.Prevention based approaches- it works on digital signature, cryptography, hash function.

b. Detection based approaches- it works as a first line of defense by identifying different malicious attacks.

Further again two types of detections as

a. Anomaly based- it compares the "normal" behavior with "real" one.

b. Signature based- it is based on well known pattern of an attack.

B. Trusted Mobile

Trusted Computing Group(TCG) prepared a specification called Trusted Platform Module(TPM) and Core Root Of Trust Measurement(CRTM) used to measure, store and report.

CONCLUSIONS

With the rapid use of mobile devices with lots of features, sensors and many connections which results in increase in mobile malware. There are certain differences between applying malware prevention solution to PC and smartphones as they belongs to different environments.

Here I have discussed the recent situations of mobile malwares.

In this work, first of all we have discussed the current. Then we focusing on how an attack is carried out and what is attackers goal is. Finally, with the help of existing techniques based on intrusion detection and trusted mobile platforms we done the review on current security solutions.

REFERENCES

[1] M. Kotadia, "Major smartphone worm by 2007," Gartner Study, June 2005.

[2] Gartner Research, "Gartner Says Worldwide Mobile Phone Sales Grew 35 Percent in Third Quarter 2010; Smartphone Sales Increased 96 Percent," 2010. [Online]. Available: http://www.gartner.com/it/page.jsp?id=1466313

[3] IMS Research, "GlobalSmartphones Sales Will Top 420 Million Devices in 2011, Taking 28 Percent of all Handsets, According to IMS Research," July 2011. [Online]. Available: http://imsresearch.com/press-release/Global Smartphones Sales Will Top 420 Million

[4] Q. Yan, Y. Li, T. Li, and R. Deng, "Insights into Malware: Detection and Prevention on Mobile Phones," in Security Technology, D. ´Slzak, T.-h. Kim, W.-C. Fang, and K. P. Arnett, Eds. Springer Berlin Heidelberg, 2009, vol. 58, ch. 30, pp. 242–249.

[5] S. Coorporation, "Symantec Internet Security Threat Report Volume XVI," Whitepaper, vol. 16, Apr 2011.

[6] Kasperksy Lab, "Popular Porn Sites Distribute a New Trojan Targeting Android Smartphones," 2010. [Online]. Available: http://www.kaspersky.com/news?id=207576175

ISSN 2394 - 7780

[7] C. Papathanasiou and N. J. Percoco, “This is not the droid you’re looking for...” in DEFCON 18, July 2010.

[8] J. Bickford, R. O’Hare, A. Baliga, V. Ganapathy, and L. Iftode, “Rootkits on smart phones: attacks, implications and opportunities,” in Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications, ser. HotMobile ’10. New York, NY, USA: ACM, 2010, pp. 49–54.

[9] D. Damopoulos, G. Kambourakis, and S. Gritzalis, “iSAM: An iPhone Stealth Airborne Malware,” in Future Challenges in Security and Privacy for Academia and Industry, ser. IFIP Advances in Information and Communication Technology, J. Camenisch, S. Fischer-H¨ubner, Y. Murayama, A. Portmann, and C. Rieder, Eds. Springer Boston, 2011, vol. 354, ch. 2, pp. 17–28.

[10] A. Gostev, “Mobile malware evolution: An overview,” Kaspersky Labs Report on Mobile Viruses, 2006.

[11] M. Hypponen, “Malware Goes Mobile,” Scientific American, vol. 295, no. 5, pp. 46–53, 2006.

[12] G. Lawton, “Is It Finally Time to Worry about Mobile Malware?” Computer, vol. 41, pp. 12–14, May 2008.

[13] M. Hypponen, “Mobile Security Review September 2010,” F-Secure Labs, HelsinkiFinland, Tech. Rep., September 2010.

[14] A.-D. Schmidt and S. Albayrak, “Malicious Software for Smartphones,” Technische Universit¨at Berlin - DAI-Labor, Tech. Rep. TUBDAI 02/08-01, February 2008, http://www.dai-labor.de.

[15] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, “Survey of Mobile Malware in the Wild,” 2011. [Online]. Available: http://www.eecs.berkeley.edu/∼afelt/malware.html

[16] N. Leavitt, “Mobile Phones: The Next Frontier for Hackers?” Computer, vol. 38, pp. 20–23, April 2005.

[17] F-Secure, “Liberty (Palm),” Aug 2000. [Online]. Available: http: //www.f-secure.com/v-descs/lib palm.shtml

[18] “Bluetooth-Worm:SymbOS/Cabir,” Jun 2004. [Online]. Available: http://www.f-secure.com/v-descs/ cabir.shtml

[19] McAfee Labs, “Mobile Security Report 2009,” 2009. [Online]. Available: http://www.mcafee. com/us/resources/reports/rp-mobile-security-2009.pdf

[20] S. T¨oyssy and M. Helenius, “About malicious software in smartphones,” Journal in Computer Virology, vol. 2, no. 2, pp. 109–119, 2006.

[21] S. Viveros, “The economic impact of malicious code in wireless mobile networks,” in 3G Mobile Communication Technologies, 2003. 3G 2003. 4th International Conference on (Conf. Publ. No. 494), Jun 2003, pp. 1–6.

[22] K. Dunham, Mobile malware attacks and defense. Syngress, 2008.

[23] N. Leavitt, “Malicious Code Moves to Mobile Devices,” Computer, vol. 33, pp. 16–19, December 2000.

[24] McAfee Labs, “2011 Threats Predictions,” 2010. [Online]. Available: http://www.mcafee.com/ us/resources/reports/rp-threat-predictions-2011.pdf

[25] D. Barroso, “ZeuS Mitmo: Man-in-the-mobile,” Semptember 2010. [Online]. Available: http:// securityblog.s21sec.com/2010/09/zeus-mitmo-man-in- mobile-i.html

[26] A. Gostev, “Kaspersky Security Bulletin. Malware Evolution 2010,” Feb 2011. [Online]. Available: http://www.securelist.com/en/analysis/204792161/Kas- persky Security Bulletin Malware Evolution 2010

[27] Cisco, “Cisco 2010 Annual Security Report,” Jan 2011. [Online]. Available: http://www.cisco.com/ en/US/prod/collateral/ vpndevc/security annual report 2010.pdf

[28] PandaLabs, “Annual Report,” 2011. [Online]. Available: http://press.pandasecurity.com/wp-content/uploads/2010/ 05/PandaLabs-Annual-Report-2010.pdf

[29] Google Mobile Blog, “An Update on Android Market Security,” March 2011. [Online]. Available: http://googlemobile.blogspot.com/2011/03/update-on-an- droid-market-security.html

[30] Sophos, “Security Threat Report,” 2010. [Online].Available: http://www.sophos.com/sophos/docs/eng/ papers/sophos-security-threat-report-jan-2010-wpna.pdf

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

SECURITY MEASURES IN MOBILE DEVICES

Tanvi Bhatkar
JVM's Mehta College, Airoli, Navi Mumbai

ABSTRACT
When we first started using mobile phones, we make calls, send texts and not much else. Smartphones and tablets can do much more things, but to do this we need to store and use lot of information about us. This information can be absolutely misused by attackers and hackers, so we should be aware of how to provide security to our mobile devices so as to protect our data. Our smartphone's doesn't only contain private data but often times it may also contain confidential data about our business or sometimes even we might be connected to our organization by means of mobile devices. So we need to think about privacy and security of mobile devices as they can be easily accessed by unauthorized user or person.

Keywords: Mobile Device, Security, Risk, Private, Sensitive, Confidential, Password, Hacker, Attack, Share, Smartphone, Tablet, Threat, Software, Browser, Data, Information, Organization, Individual, Unauthorized, Application, Client, Mechanism, Lost, Stolen, Network, Protect.

INTRODUCTION
Now-a-days, digitization is on full swing. In every aspect of transactions taking place worldwide, we have started relying on portable devices for speedy transactions. Mobile device security can be thought of measures which can be used to authenticate the user and methods or practices used for protecting personal data. Also, providing privacy measures in the event of accidental loss of portable devices. Providing security measures to devices is now becoming a major concern as increasing trends with smart devices results in increasing number of cyber crimes. Additionally, a range of third-party mobile device security solutions are providing a further layer of protection for mobile devices.

Why Mobile Device Security is necessary?
Hackers want information such as

-Usernames

-Passwords

-Payment Details

-Personal Information

They then use this information to buy and sell on the dark web or to use it themselves. Businesses hackers to gain access to competitor information and records of third parties.

Mobile banking is very flexible in today's digital age with many banks offering impressive apps for conducting financial transactions remotely using mobile devices such as smartphone or tablet. The ability to deposit a cheque, to pay for merchandise or to transfer money to a friend are reasons why people choose to use online banking. However, it is important to have a unthreatened connection before logging into a mobile banking app or else a user might risk his personal data being compromised. Risks associated with mobile banking other than phishing , viruses and Trojans include hacking. However, one needs to be careful and not to share your net banking password. Also do not access your banking passwords from a wifi spot and ensure that you do not use easy passwords. This can be extremely dangerous and full of risks.

Mobile Threats: They can be possibly defined as something that can affect or cause damage to mobile devices in some or the other way to gain potential or monetary benefits.We can divide mobile threats into categories: application-based threats, web based threats, network based threats and physical threats.

TYPES OF MOBILE THREATS
Application-based threats: - These are threats that occurs due to downloading applications that are intended to lead to some kind of fraudulent actions which includes viruses, spywares and vulnerable applications. Malware is a malicious program that is intended to cause direct or indirect damage or harm to laptops, tablets, smartphones and other portable devices while spyware is a software that is designed to gather data or information from our device so as to make use of that data to perform some illegal activities. Vulnerable applications are those which can exploit whole device to stop smoothly running services, get access to data and steal that data with fraud or wrong intentions.

ISSN 2394 - 7780

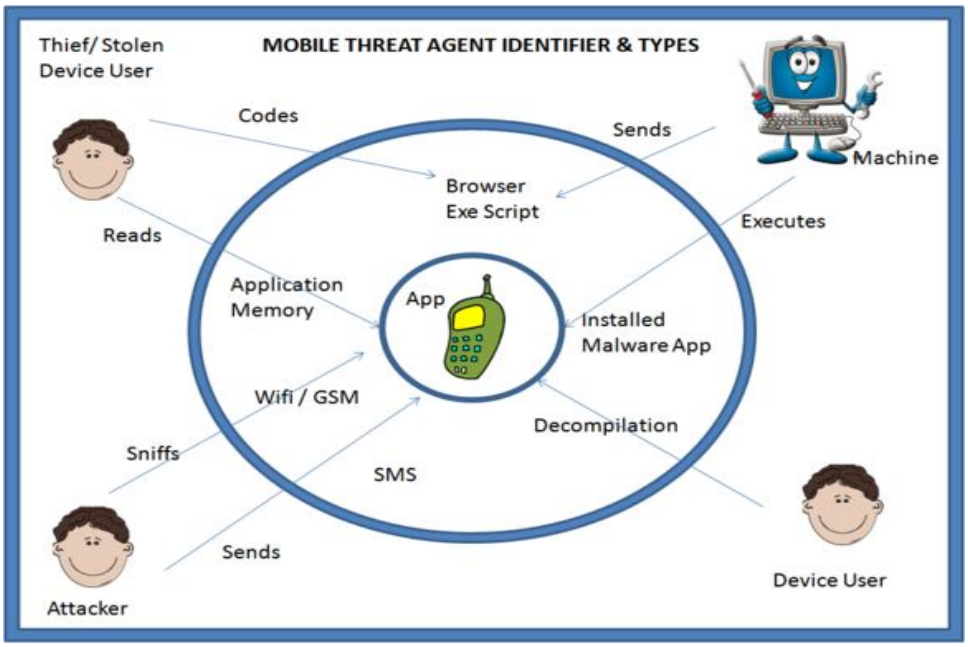
Web-based threats:-They are caused as our mobile devices are continuously connected to Internet and web-based services. Phishing Scams are text messages, emails, texts that comes with fraudulent links that leads you to website which is designed to get your personal data and passwords in a tricky way. Drive-By-Download is concerned with many things, each concerning with unintended download of software or app on your device. Browser exploits are vulnerabilities in your mobile browser or software package launched by the browser like a Flash player, PDF reader, or image viewer.

Network related threats:-Mobile devices support cellular networks and local wireless networks (WiFi, Bluetooth) which leads to network related threats.Network exploits can install malware on your phone without your knowledge.Wi-Fi Sniffing intercepts unencrypted data which is traveling through the air between the device and the WiFi access point without any safety measures.

Physical threats :-Physical security of mobile devices is also an important consideration as it leads to physical threats. Mobile Devices that are lost, bagged or robbed with fraud intentions leads to most common mobile threats. The mobile device is valuable not only because the hardware itself can be re-sold in the black market, but more importantly because of the personal and organizational information it may contain.

MOBILE DEVICE RISKS

From a security perspective, the risks and potential effects of deploying and supporting mobile devices as a company tool should be understood.



Trusted Clients: Mobile devices often have elevated levels of trust due to inherently strong client identification mechanisms and thus owners may bypass device restrictions through a method known as “jailbreaking”. Once users jailbreaks their phones, they can remove any policy requirements on the phone, install unapproved applications and potentially be exposed to additional security threats.

Network Architecture: The network strategy to provide mobile device data access presents the security risks. In addition, it can create unexpected vulnerabilities in the security of the implementation.

Policy Implementation: Compared to laptops, mobile devices typically contain stronger client-side controls that may withdraw the focus of safety measures away from infrastructure to device. However, an attacker can easily bypass incorrect, insufficient or weakly implemented controls and allow a malicious user to attack the internal network.

Stolen or Lost Devices: A fundamental problem of mobile devices is physical access control as these devices are on the move with the owner. As the device on the move is more likely to be lost or stolen and subsequently used by a malicious attacker.

BEST PRACTICES AND REQUIREMENTS FOR MOBILE DEVICE SECURITY

Enable full disk encryption

Encryption is a technique to protect our data or information by converting it into encoded format so as to prevent it from unauthorized access. Ensure full disk encryption to your device.

ISSN 2394 - 7780

Back up your data frequently
Backing up your data frequently can lead to less harmful scenarios to data loss.

Choose a strong password
Hackers most commonly break into victim's device by guessing passwords and knowing victims internet habits. Commonly used passwords and reusing similar passwords across many online accounts enable mobile intruders gain access to victim's device or system easily. Strong passwords effectively protects data from unauthorized access thus decreasing the financial frauds and identity thefts.

Never share your password with anyone
Sharing of password with other person makes your personal and professional data vulnerable to security threats. Best practice is not to share your username and password which helps prevent unauthorized use of funds or resources.

Verify apps before installing
Verifying an app ensures that safety check is performed on the app and it is good to go on your device. It warns you about suspicious files and folders that violates our Unwanted Software Policy.

Install an anti-malware app
Anti-Malware can be thought of any software that can be used to identify, detect and protect from suspected programs in your device.

Keep your operating system up-to-date
Updating your operating system regularly provides stronger security and the ability to work with newer programs.With outdated operating systems, cyber-crime becomes a possibility and system will no longer receive security updates. To prevent this best practice is to update your operating system to the latest version.

Promptly report a lost or bagged device
Once device is reported as robbed or bagged, it's important to report it immediately. Ensure you revisit your security policies to prevent any events that will damage your reputation.

Disable features and applications that you don't use
Unnecessary features and applications from your devices not only occupies space but also slow down the activity of your device. Delete all data that you do not need so as to increase life of your device.

Limit who can access your mobile device
Access to your mobile devices should be limited by passcode lock and PIN to protect your data.

CONCLUSION

As mobile technology companies continue to innovate over the coming years, organizations using these technologies will need to continuously assess the security implications of adopting these advancements. A consistent and agile multi-perspective mobile security risk assessment methodology will enable evaluation of the risk exposure in these systems. We need to train developers for safe and secure coding practices for mobile device platforms and create an encrypted password-protected sandbox for sensitive data also enforce device-side technical policies.

REFERENCES

1. [MobileDevice] "Mobile Device", http://en.wikipedia.org/wiki/Mobile_device, Description: an introduction of mobile device in wiki webpage.
2. Mobile Security: A Pocket Guide by Steven Furnell Publisher: IT Governance Publishing Release Date: July 2009
3. Daniel , K. Foiling the Cracker: A Survey of, and Improvements to, Password Security, Proceedings of the 2nd USENIX UNIX Security Workshop, pp.5-14, August 1990.
4. "AndroidSecurityTips",http://www.cio.com/article/675129/Android_Security_Six_Tips_to_Protect_Your_Google_Phone?page=3&taxonomyId=3061, Description: a webpage to introduce six tips to protect Google Android smartphone.
5. "Google and Apple to Tighten Security in Mobile Devices following Vulnerability Tipoffs - Tech2." Tech2. Tech2.com, 19 Sept. 2014. Web. 26 Sept. 2014.

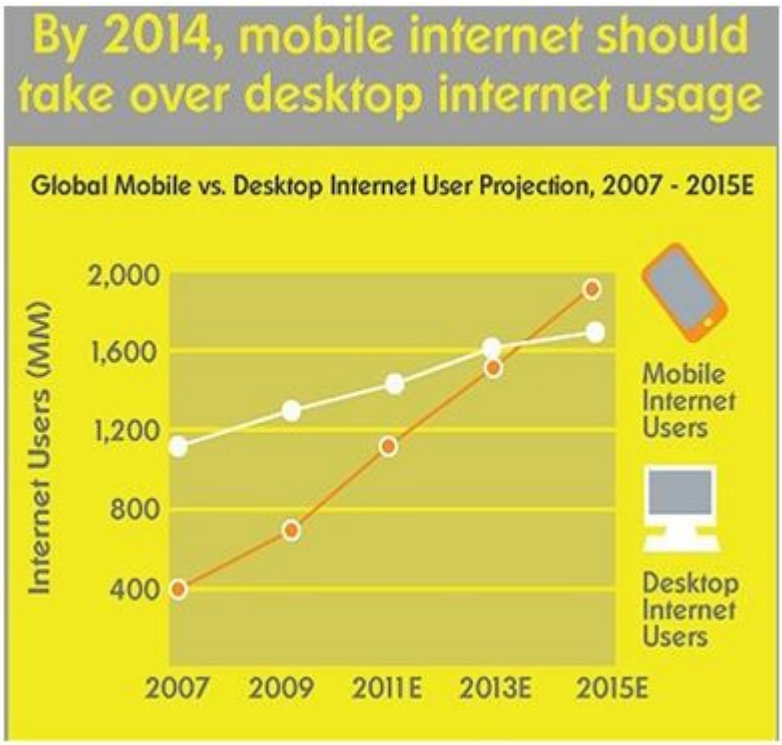
International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

USAGE OF SMART PHONES AND ITS SECURITY ISSUES IN TODAY'S WORLD

Rajshree N. Pisal
JVM's Mehata Degree College, Navi Mumbai

ABSTRACT
Nowadays the mobile device industry has increased rapidly. We can make use of mobile device for our personal as well as professional work. Mobile device stores our valuable information. Today's mobile equipments handle data like contacts, banking details, GPS location, corporate e-mail etc. To keep the mobile devices safe, specific preventive measures are needed and we can maintain its privacy by safeguarding its passwords and locks because all our works mainly depends on these devices.

INTRODUCTION
Smartphone gives lots of knowledge on traditional personal computers (PCs) also offers various selection of connectivity options, such as IEEE 802.11, Bluetooth, GSM(Global System for Mobile), GPRS(General Packet Radio Services), UMTS(Universal Mobile Telecommunications System) HSPA(High Speed Packet Access) etc. These computing equipment has capability of advanced information processing, Net browsing etc. Smart phones are of significant importance in today's world. The capabilities of this smart phones have increased dramatically in short period. This exsisting tools have made technology very important part of the everyday life for most people.

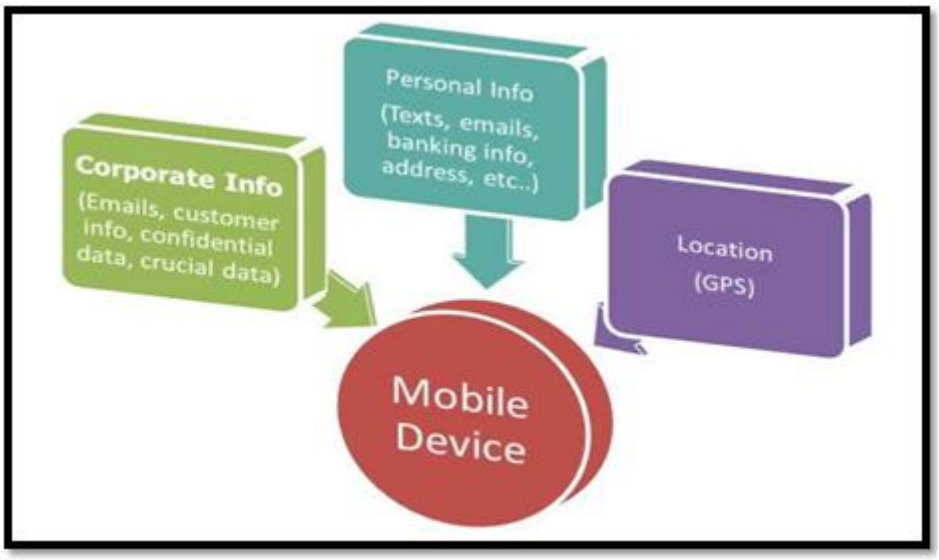


Above diagram gives details about how important mobiles are becoming in regards to internet usage. It shows an increase in internet browsing of about 300 percent between 2007 and 2012 and projects surpassing quantity of browsing in comparison with desktop usage in the year 2015. It is very important for companies and public in general due to the amount of browsing over unprotected networks. Most of the smart phones contains valuable organizations data along with personal data, if a breach occurs companies and users can end up losing huge data, to avoid it aware of the protection methods.

People are still doubtful to use it because of its privacy issue. It is mandatory to suggest a reliable method to secure these technology against diverse attacks one way is to use Biometrics technology.

NEED OF SMARTPHONES SECURITY
The risk involved with smart phones is based on the users reliance on them because it contains private info. Many smart phones face different challenges :-example constant GPS location. Devices that handle the personal messaging, personal and business e-mailing, net banking, and even the location of individual at all times need to be safeguard.

ISSN 2394 - 7780



PRINCIPLES

It deals round the safety of system and info present on mobile. Task of maintaining the privacy comes with great responsibility. CIA compose the main requirements for smart phone protection and handling various data.

Confidentiality deals specifically with keeping info on a device from being disclosed into threatened hands. Example:- protecting data of a credit card. A secure mobile system ensures the privacy of data while being transferred without loss of valuable data.

Integrity – It focuses on the information that should not be modified without modification being detected by system which ensures that all data is accessed by authorized user is trustworthy and therefore usable. A secure system typically provides message integrity along with data confidentiality.

Moreover, when the system's data is confidential, integral and available then we can say that system is secured. There are different control factors that affect the privacy of device. Examples include: passwords, ACL's, data encryption etc. The smart phones should be fully protected, it also needs to be physically secured.

EXISTING SOLUTIONS

There are various basic measures that an organization and users of a mobile device may take to safeguard the devices. Some measures are as follow:

1. Make the device identifiable if lost.

2. Make a note of the IMEI (International Mobile Equipment Identity)

3. The user or company could consider a policy for the mobile, of which there are two primary types. In the case of smart phones or network connected tablets, the owner can purchase insurance from the network carrier and the equipment itself would be replaced but not the info.

4. A mobile security solution will protect devices against malicious code embedded in apps.

With mobile defence, you can detect malicious apps that have withstood app store vetting and have been published in public app stores. You can even find apps that have added malicious capabilities through updates and background downloads.

PREVENTIVE MEASURES

Malicious attacks can be done on mobile devices, through the internet's connection via Wi-Fi. Many times we make use of the connection which is free to use but we don't take care about the privacy. Many times we do not understand that data which we are sending and receiving through that network like email, messages etc.

Two essential things to be done by users while contacting these networks is to make sure we are not stealing the service but to know where it's coming from. Many Wi-Fi enabled systems have mechanisms which allows us to know if the network is encrypted or if it is just an ad-hoc connection. Typically open public networks appears to be free pose a threat to gain private details from the individuals. It is not mandatory to always have a hacker who'll steal user's identity, it might be a company that would like to acquire people's browsing habits or survey people's interest on a particular product.

ISSN 2394 - 7780

CONCLUSION

In recent years the world of mobile electronics has marked our culture also set pace for technological development. These equipments reshaped our societies thinking in terms of speed of data, instant gratification, mobility, and operability. The newly founded markets of smart phones and tablets are shaping our approach to mobile computing step by step.

We focused solely on mobile security. Our mission is to secure mobile devices and apps and defend from those that use them. The mobile app testing, device observance, forensics gave us with a singular set of mobile security information.

Therefore, everyone should be aware of the threats they face, existing types of safeguards to make a balanced decision on which of the ways to implement for every specific situation. Whether it is simple passwords, simple or complicated encryption, people or organizations need to be aware that certain preventive measure needs to be implemented for every situation. Lastly, we are waiting for upcoming changes such as biometric implementation. This proves an interesting topic to both those who are interested in futuristic electronics and field of information security . Future will be marked by innovations that not only does what we want to do, but also recognizes what it should do by itself and does it. Since relying on human's for the protection of info will be a risky option but in future due to increase in usage, technology like Siri that implements automatic actions to help the user is a significant addition to smart phone security. The progress in technology that are currently being seen are bringing industries one step closer to that reality.

REFERENCES

- http://www.law.cornell.edu/uscode/44/3542.html
- http://www.periphman.com/degaussing/tape-degaussing/degaussing-erasing.shtml
- www.bcs.org/server.php?show=ConWebDoc.2774
- www.checkpoint.com/press/pointsec/2006/06-08.html
- www.globalsecuritymag.com
- http://www.books24x7.com.libproxy.library.wmich.edu/marc.asp?bookid=34445
- https://www.computerworld.com/article/3233187/mobile-wireless/fintech-builds-on-blockchain-forinternational-mobile-payments.html
- Mobile Security: A pocket guide by Christidis, M. Devetsikiotis.
- Authentication of users on mobile telephones – A survey of attitudes and practices by L. Mearian FinTech
- Authentication Framework Evaluation by S. Ahamad and M. Nair, B. Varghese

Figures Sources

- Figure 1. Mobile Device Usage.
- Figure 2. Information Input to Mobile Devices.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER SECURITY WITH WIRELESS SECURITY

Karishma S. Bhosale
University of Mumbai

ABSTRACT
This paper is about the spreading the awareness of Cyber Security with the evolving hacking events around us, we can see the news regarding organizations being hacked around the world It is the duty of an organization to make their customers aware about basic security precautions for a safe browsing experience. Cyber Security refers to protecting our devices, processes, infrastructure and assets of the organization from cyber-attacks, data theft, breaches, unauthorized access so that we can have safe browsing and no danger or fear from Cyber Attacks.

Keyword: Cyber Security, Cyber Attacks, Cyber Defence and Wireless Security.

INTRODUCTION
Cyber Security is defined as the state or process where we can protect and recover network, device, and programs from any type of Cyber Attack.

The Term Cyber Security refers to the technologies and processes designed to defend laptop systems, software, networks and user knowledge from unauthorized access conjointly from threats distributed over the Internet with the help of Cyber Criminals, Terrorist Groups, and Hackers and many more. Cyber Security is all regarding protective your devices and network from unauthorized access or modification. The Internet is not only the way where communicate or learn, but it is also a medium through which people do business with the help of internet and use of their intelligence.

Cyber Security aims to protect the computers, networks, and software programs from such Cyber Attacks. Most of these digital attacks when they hack computer or phone or laptop are aimed at accessing, altering, or deleting or capturing or retrieving sensitive information and which further can lead to extorting money from victims or interrupting normal business operations with extorting huge amount of money. A Cyber Security system has multiple ways of protecting our data or confidential information spread or receive across computers, networks, and programs.

But a robust Cyber Security system depends not solely on Cyber Defence technology, however conjointly on folks creating sensible Cyber Defence selection. Cyber Security refers to the practice of ensuring the integrity, confidentiality, and availability (ICA) of information. Cyber Security now has developed the way of introducing of evolving set of tools, risk management approaches, various technology, training and best practice designed to protect networks, devices, programs and data from attacks or unauthorized access.

Cyber Security is Associate in nursing umbrella term that encompasses differing types of Security.
1) ***Application security:*** This constitutes the measures and counter measures meant to tackle threats and vulnerabilities that arise in the development stage of an application such as design application, development, deployment, maintenance, upgrade, etc.

Some of the techniques used are input parameter validation, session management used mainly when internet connection is ON, user authentication and authorization, etc.

2) ***Information security:*** This refers to the protection of information and data from theft, unauthorized access, breaches in order to uphold user security and prevent identity theft.

3) ***Disaster Recovery:*** This involves coming up with and strategizing to alter organizations to get over Cyber Security/ IT disasters.

This includes risk assessment, analysis, prioritizing and establish disaster response and recovery mechanisms in place.

This enables various organizations to recover faster from disasters that can cause to loss and find the way to minimize loss.

4) ***Network security:*** This constitutes monitoring and preventing authorized access and exploitation of internal networks of an organization.

By investing each hardware and code technology, Network Security ensures that internal networks are safe, reliable and usable and have less fear of Cyber Attacks.

ISSN 2394 - 7780

Antivirus and anti-spyware software, VPN, IPS, Firewall, etc. are used to prevent cyber-threats facing the organization.

5) ***Website security:*** This is used to prevent and protect websites from Cyber Security risks on the internet.

Holistic web site security programs that are style to hide the website's info, applications, source codes and files and help protecting confidential information.

There has a steady rise in the number of data breaches on websites in the past few years resulting in identity thefts, downtime, and financial loss can impact to organization or industrial loss of reputation etc.

The main reason for this has been the misunderstanding among web site homeowners that their web site is protected by web site hosting supplier.

Thus, leaving them vulnerable to Cyber Attacks.

Some of the necessary techniques and tools used for web site security are web site scanning and malware removal, website application firewall, application security testing, etc.

6) ***End to End Security:*** This enables organizations to protect their servers, workstation, computers and mobile devices from remote and local cyber-attacks. Since devices on a network are connected, it creates entry points for threats and vulnerabilities that can lead to Cyber Security. End to End security secures the network by blocking attempts made to access and enable these entry points. File integrity monitoring, antivirus and anti-malware software, etc. are major techniques used.

Common types of security
Network Security protect network traffic by controlling incoming and outgoing connection to prevent threats from entering or spreading or causing on damage on the network.

1) ***Knowledge Loss hindrance*** (DLP) protects knowledge by that specialize in the situation, classification and monitoring of information at rest, in use and in motion .Cloud Security provides protection for data used in cloud-based services and applications.

2) ***Intrusion Detection Systems*** (IDS) or Intrusion Prevention Systems (IPS) work to identify potentially hostile cyber activity.

3) ***Identity and Access Management*** (IAM) use authentication services to limit and track worker access to safeguard internal systems from malicious entities. Encryption is that the method of cryptography knowledge to render it unintelligible, and is often used during data transfer to prevent theft in transit.

4) ***Antivirus/anti-malware*** solutions scan computer systems for known threats. Modern solutions are even ready to discover antecedent unknown threats supported their behaviour.

Importance: The infamous Cyber Attacks such as the Golden Eye and Want to cry attacks have crippled several organizations and forced many to shut down their operations. In the wake of these sophisticated Cyber Attacks and security breaches, Cyber Security has taken the spotlight among organizations of all sizes. Cyber threats continue to evolve.

Not solely have we tend to seen a rise in Cyber Attacks on Many of years have come, there will be even more advanced Cyber Attacks using new technologies, victims, and intentions and more inventions of new Technology. There will be a tricky having risen in the availability of Ransomware-as-a-Service and Malware-as-a-Service on the dark website or internet explorer. It will allow anyone to learn and get the technical knowledge and easily and quickly initiate a Cyber Attack.

Cyber Attack in the past, now there is a much greater awareness about Cyber Attack and the need for better Cyber Security measure among organizations of all types. This will serve as a motivation for cybercriminals to up their game by staging new and more sophisticated attacks in the future. Wide-ranging security vulnerabilities, faster and more sophisticated Cyber Attacks are all making it extremely difficult for security experts to prevent those threats. Thus, there should be a proper Cyber Security plan in place to prevent Cyber Attacks from causing any damage.

Wireless security: Wireless network or Wi-Fi, the moment you hear these words you realize how convenient your life has become. Wireless Internet Connection has made it easy for anyone to use the Internet at any device ranging from Laptops, Smartphones, and Tablets, etc. from anywhere in the house without managing tons of cable bundles.

ISSN 2394 - 7780

One important thing to consider here that wireless network does not end at your home or office's wall; it is possible that the signals of your wireless network are extended to other neighbouring homes or offices.

Wireless has become the communications medium of choice for many people. However, this is meaningless without a good, solid understanding of effective Cyber Security and knowing how to protect information whether it's at home or at work. Consider these tips and best practices for developing a robust wireless security system to protect sensitive information. So it was not a rocket science to understand how many risks are involved if you do not have a secure wireless network, now in this part of the article we are going to discuss the ways you can secure wireless network.

This is the first and one of the most important steps towards securing a wireless network. Encryption of the wireless network simply means that you should not just leave your network without any password for anyone to connect. There is usually three kind of security WEP, WPA, WPA2. WEP is generally the default password that comes printed on the router and is the easiest way to break.

Though WPA2 is more secure, these days WPA is compatible with more client devices. We suggest that you keep a strong password which is at least 8 characters long. Usually, an alphanumeric password is preferable, and if your router settings allow a space, it is even better because these passwords are difficult to guess. I suggest "Do Not" use your phone number or your pet's name as your wireless network's password because since most people use them, these are very easy to guess.

Every router comes with a lot of important default settings. Moreover, since the manufacturer sets these settings, these are available to everyone. Keeping these settings sure makes the setup process easy but at the same time vulnerable to a breach. If you are serious to secure wireless network, you need to consider changing these default settings.

The most important default settings that you should consider changing are:
Make sure that once you change these settings, you also remember them because in future to access your router's settings you have to use both these new credentials. As the wireless network password, these should be difficult to guess too. Usually, routers allow you to access their settings/interface only from a connected device. However, some of them allow access even from remote systems. We highly recommend you to keep these settings disabled all the time because cyber criminals can use this to access your router's setting without even connecting a device. To make this change, access the web interface and search for **"Remote access"** or **"Remote Administration".**

Updating Router's firmware is a good move towards a secure wireless network. Firmware updates usually carry patches for known bug fixes and security updates. Router's firmware, like every other software, contains flaws and can be exploited by the cyber criminals and hackers. Most of the times routers do not have an auto update feature, so you have to update the firmware manually. Sometimes updating the firmware can cause a router reset so in that case we recommend you to take a backup of all your settings beforehand.

Many routers come with a firewall that can be enabled from the router's settings. If it is available, we suggest you enable this feature, as it shall help add an additional layer of security. The wireless network is cool, and we cannot imagine a life without it. We use internet day in day out but keep your device connected to some wire while using it is unimaginable. With all the cool features or qualities there is a dark side to it too. We should take all the possible measures to secure wireless network because leaving it unprotected may have consequences.

CONCLUSION
Network professionals usually state that a network administrator should never assume his or her network is completely safe. That is a good and healthy attitude. You should always be aware of strange occurrences in network traffic (peaks, most importantly). Inspecting your network logs may reveal suspicious traffic or logon attempts.

1) WEP or Preferably WPA or AES Encryption
2) MAC Filtering
3) SSID Broadcast disabled
4) Strong Router Password

ISSN 2394 - 7780

REFERENCES

1) Yooseph S Heyer LJ, Kruglyak S. Exploring Exp-ression Data: Identification and Analysis of Coe-xpressed Genes. Genome Research,.
2) Mathioudakis and N. Koudas. Twitter monitor: Trend detection over the twitter stream pages.
3) Business Intelligence from Twitter for the Television on Media: a case study Vignesh T.S, Praveen Kumar.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

SECURITY TECHNIQUE TO SECURE WIRELESS NETWORK

Kajal M. Singh
JVM'S Mehta Degree College Airoli

ABSTRACT
This articles briefly describes the important security protection methods like Wired Equivalent Privacy & WI-FI Protected Access and it focus on comparison between Bluetooth and Wifi for security purpose and also discussed about various attacks in wireless security networks and defenses against the attacks and various security weaknesses . Many laptop computers have wireless cards pre-installed .The ability to enter a wireless network has nice edges . However, wireless networking has many security issues . Hackers have found wireless networks comparatively straightforward to interrupt into, and even use wireless technology to crack into wired network . As a result, it's extremely necessary that enterprises outline effective wireless security policies that guard against unauthorized access to big resources.

Keywords: Wireless Security, Bluetooth Vs Wifi , security weakness , Attacks , Defenses.

INTRODUCTION
An increasing variety of government agencies, businesses, and residential users area unit mistreatment, or considering using, wireless technologies in their environments.Wireless security is that the prevention of unauthorized access or injury to computers or information victimisation wireless networks. The most common kinds of wireless security square measure Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). Many laptop computers have wireless cards pre-installed.

The ability to enter a network whereas mobile has nice advantages.

However, wireless networking is liable to some security problems.

Hackers have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks .Wireless Intrusion Prevention Systems (WIPS) or Wireless Intrusion Detection Systems (WIDS) area unit usually wont to enforce wireless security policies . Wireless networks are vulnerable for attacks like: Eavesdropping, Masquerading, Denial of service , Man-in-the-middle attack, Attacks at wireless clients.

Why people invest in wireless security systems and ditch landline-based ones
you can arm and disarm system easily from wireless device. you can receive notification. communication get provision on cellphones. Advantage of wireless domain is there is no wire to cut. You are there without actually being there.

WIRELESS NETWORK PROTECTION METHOD
• WEP (Wired Equivalent Privacy)
WEP could be a wireless security protocol that provides knowledge privacy and uses a shared key, to cipher traffic before its transmission . RC4 cryptography formula could be a stream cipher used by WEP for encryption.WEP doesn't work well wherever high levels of security square measure needed. Authentication, access management and virtual non-public networks ought to be used wherever high levels of security square measure needed.WEP is easy to implement as you only have to configure the secret writing key on the APs and your purchasers.

It could provide basic security for WLAN applications.WEP is tough to manage as a result of it provides no mechanism to vary the shared secret.(If change required then all APs and clients must be simultaneously changed). For providing WLAN security, WEP is inadequate.(You have to be compelled to use it along side another technology).If the aggressor has management of the shared key he will access the network additionally to rewrite the messages.

The solution is to distribute separate keys throughout the system, one for authentication and one for secret writing.

• WPA (WI-FI Protected Access)
WPA was developed by the Wi-Fi Alliance to provide more sophisticated data encryption and better user authentication than Wired Equivalent Privacy (WEP), the original Wi-Fi security standard. The two encryption methods which can be used with WPA are: Temporal Key Integrity Protocol (TKIP) &

ISSN 2394 - 7780

Advanced Encryption System (AES). WPA provides better security than what WEP does.WPA uses a singular secret writing key for each packet that's transmitted. Some wireless network hardware does not support WPA. WEP on the other hand is generally supported.

Best Practices for Securing Wireless Networks
If possible, place the wireless network in a wireless demilitarized zone (WDMZ). A router or firewall should isolate the private corporate network from the WDMZ. DHCP should not be used in the WDMZ. Use extended subnet mask to limit the amount of hosts. If potential, purchase an AP that enables you to minimize the wireless zone's size through modification of the power output.

APs ought to be placed within the center of a building not close to windows.

It is suggested that you just don't use DHCP for wireless shoppers.

You should undoubtedly not use DHCP if SSID broadcasts square measure allowed.

Bluetooth vs. Wi-Fi IEEE 802.11 in Networking
Bluetooth and Wi-Fi are both methods that provide wireless communication, but the difference between the two mainly stems from what they are designed to do and how they are used.The main distinction is that Bluetooth is primarily wont to connect devices while not victimization cables, while Wi-Fi provides high-speed access to the internet.

Wi-Fi uses the same radio frequencies as Bluetooth, but with higher power, resulting in a faster connection and better range from the base station.

Wi-Fi is meant as a replacement for cabling for general native space network access in work areas.Bluetooth may be a replacement for cabling in a very type of in person carried applications in any ambiance and may conjointly support mounted location applications like good energy practicality in the home (thermostats, etc.).Bluetooth and Wi-Fi have several applications: putting in networks, printing, or transferring files.

Security weakness
Wireless networks ar extraordinarily vulnerable to interference thus radio signals, radiation and the other similar sort of interference might cause a wireless network to malfunction.

Wireless networks can be accessed by any pc inside vary of the network's signal thus info transmitted through the network (including encrypted information) could also be intercepted by unauthorized users.

• A **Denial-of-Service (DoS)** attack is an attack meant to shut down a machine or network, making it inaccessible to its intended users.

There are two general ways of DoS attacks: flooding services or blinking services. Flood attacks occur once the system receives an excessive amount of traffic for the server to buffer, inflicting them to bog down and eventually stop.

• **Bluejacking** is the practice of sending messages between mobile users using a Bluetooth wireless connection . People victimisation Bluetooth-enabled mobile phones and PDAs will send messages, including pictures, to any other user within a 10-meter or so range. Because such communications do not involve the carrier, they're freed from charge, which can contribute to their attractiveness.

Attacks in Wireless Security Network
Sensor nodes themselves ar points of attack for the Wireless device Networks.

If device nodes square measure compromised, the attackers square measure able to grasp all the confidential info keep on them and will launch a range of malicious actions against the network through these compromised nodes.

- **Physical Attack**

Another name for Physical Attack is node capture.In this sort of attack, attackers gain full control over some sensor nodes through direct physical access.Physical attacks have significant impacts on routing and access management mechanisms of WSN. For example, obtaining key info hold on sensing element node's memory offers offender the chance of unrestricted access to WSN.

- **Attacks at Different Layers**

Physical layer is answerable for actual knowledge transmission and reception, frequency choice, carrier frequency generation, signal operate and encoding.

ISSN 2394 - 7780

- **Jamming:** In physical layer, jamming is a common attack that can be easily done by adversaries by only knowing the wireless transmission frequency used in the WSN

Network layer is answerable for routing messages from one to a different node that area unit neighbors or could also be multi hops away.

- **Selective Forwarding**: Selective forwarding is an attack where compromised or malicious node just drops packets of its interest and selectively forwards packets to minimize the suspicion to the neighbor nodes
- **Sybil Attack:** In Sybil attack,a malicious or subverted node forges the identities of more than one node or fabricates identity.

The data link layer is answerable for the multiplexing of knowledge streams , knowledge frame detection , medium access and error management. This layer is liable to knowledge collision once over one sender tries to send knowledge on one transmission.

- **DoS Attack by Collision Generation**
- **Sinkhole Attack** : In sinkhole attack, a compromised node attracts a large number of traffic of surrounding neighbors by spoofing or replaying an advertisement of high quality route to the base station
- **Wormhole Attack** : Wormhole is a critical attack, where the attacker receives packets at one point in the network , tunnels them through a less latency link than the network links to a diffent purpose within the network and replay packets there regionally
- **Hello Flood Attack** : In Hello flood attack , the attacker broadcasts hello message with a very powerful radio transmission to the network to convince all nodes to choose the attacker to route their messages.
- **Desynchronization attack** : In desynchronization attack, an attacker repeatedly forges messages to one or both end points of an active connection with fake sequence number or control flag. Thus attackers desynchronise the tip points in order that detector nodes convey messages and waste their energy

In application layer, data is collected and manages. Here, sensor nodes can be subverted to reveal its information including disclosure of cryptographic keys hence compromising the whole sensor network. If a node is compromised, detection and exclusion of that node from the sensor network is a probable solution. LEAP can verify whether a node has been compromised or not and can revoke compromised nodes with efficient re keying mechanism.

In Transport layer finish to finish connections area unit managed.

- **Flooding Attack**: Adversary sends many connection establishment request to the victim node to exhaust its resources causing the Flooding attack.One answer against this attack is to limit the amount of connections that a node will build

Wireless Security Network Defenses

WSN needs effective, energy and resource efficient key management scheme for providing confidentiality, integrity and authentication security services. Secure routing is another essential requirement for protecting WSN against external and insider attack.

- **Cryptography:** Cryptography is essential for ensuring security services. Public key cryptography such as Diffie-Hellman key agreement protocol or RSA signature is not suitable for WSN because of its limitation in memory, computation and power. For example , to perform a single security operation RSA executes thousands or even millions of multiplication instructions

o Hierarchical Key Management

- **Key Distribution / Management:** sometimes sensor nodes are just air dropped in enemies' arena. In such situations , sensor nodes organize themselves to form a wireless network. Key pre-distribution is a key management scheme where before deployment each sensor node is provided with some keys and after reaching the target position the sensor nodes builds up a secure network among them supported those keys.

CONCLUSION

We have given an overview of the security techniques .Next to this we have discussed the various attacks on different layers and defenses and explained about various protection methods.

ISSN 2394 - 7780

REFERENCES

- https://www.democratandchronicle.com/videos/news/2018/08/02/why-people-invest-wireless-security-systems-and-ditch-landline-based-ones/878946002/
- https://www.esat.kuleuven.be/cosic/publications/article-503.pdf?ref=Guzels.TV
- https://www.diffen.com/difference/Bluetooth_vs_Wifi
- https://pdfs.semanticscholar.org/6bdd/597202ab52036e3e2ca656782ef504989fab.pdf
- https://opus.govst.edu/cgi/viewcontent.cgi?article=1054&context=capstones

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

A BRIEF STUDY ON MOBILE DEVICE SECURITY

Deepali Gupta
University of Mumbai

ABSTRACT
This article is about security threats to mobile devices. The growing quality of wireless technology could have finally attracted enough hackers to form the potential for serious security threats a reality. The world of computers and communications, the additional wide a technology is used; the additional doubtless it's to become the target of hackers. Such is that the case with mobile technology, notably smartphones, that have exploded in quality in recent years. Many users download mobile applications with little regard to whether they're secure, providing a ready way for hackers to attack the device.

Keywords:Mobile security, smartphones, malware, spyware, phishing.

INTRODUCTION
In the world of computers and communications, the more widely a technology is used, the more likely it is to become the target of hackers. Such is that the case with mobile technology, particularly smartphones, which have exploded in popularity in recent years. According to market analysis firm ABI Research, 370 million smartphones were in use globally last year. Many users download mobile applications with little regard to whether they're secure, providing a ready way for hackers to attack the devices. Smartphones usually connect with the web, still to PCs for computer code updates or media synchronization, providing convenient attack vectors. Device makers and wireless-service providers have long focused on communications and other services, with security remaining an afterthought. Referring to the two most popular smartphone platforms, Ed Moyle, senior analyst with research firm Security Curve, said, "Security is currently enjoying catch-up with the speedy adoption of Android and iPhone, each of that area unit arduous for enterprises to manage. Thus, after years of warnings concerning mobile security, there finally seems to be a reason to stress. In fact, the quantity and kinds of mobile threats-including viruses, spyware, malicious downloadable applications, phishing, and spam- have spiked in recent months.

All smartphones, as computers, area unit most well-liked targets of attacks. These attacks exploit weaknesses inherent in smartphones that can come from the communication mode—like Short Message Service (SMS, aka text messaging), Multimedia Messaging Service (MMS), Wi-Fi, Bluetooth and GSM, the de facto global standard for mobile communications. There also are exploits that concentrate on computer code vulnerabilities within the browser or software system.

And some malicious computer code depends on the weak information of a median user.

Security countermeasures area unit being developed and applied to smartphones, from security in several layers of computer code to the dissemination of knowledge to finish users.

There area unit sensible practices to be determined the least bit levels, from style to use, through the event of operative systems, software layers, and downloadable apps.

CHALLENGES OF SMARTPHONE MOBILE SECURITY
1. Threats
A smartphone user is exposed to varied threats once they use their phone. In just the last two-quarters of 2012, the amount of distinctive mobile threats grew by 261%, in line with ABI analysis.

These threats will disrupt the operation of the smartphone, and transmit or modify user data. So applications should guarantee privacy and integrity of the knowledge they handle. In addition, then certain apps may themselves be malware, their functions and activities ought be restricted (for example, proscribing the apps from accessing location data via GPS, blocking access to the user's report volume, stopping the transmission of data on the network, sending SMS messages that are billed to the user, etc.)

2. Consequences
When a smartphone is infected by AN assaulter, the assaulter will try many things:

The offender can manipulate the smartphone as a zombie machine, that is to say, a machine with which the attacker can communicate and send commands which will be used to send unsolicited messages (spam) via sms or email;

ISSN 2394 - 7780

The assaulter will simply force the smartphone to make phone calls. But the invader also can use this technique to decision paid services, resulting in a charge to the owner of the smartphone. It is conjointly terribly dangerous as a result of the smartphone may decision emergency services and therefore disrupt those services.

3. Social Networking

As smartphone use has mature, so has mobile social networking.

Malicious links on social networks will effectively unfold malware. Participants tend to trust such networks and are thus willing to click on links that are on "friends'" social networking sites, even though-unknown to the victim-a hacker may have placed them there, said M86's Antsis.

4. Bluetooth

Bluetooth enables direct communication, including the sharing of content, between mobile devices.

Wireless devices can broadcast their presence and allow unsolicited connections and even the transmission of executable if users don't configure their Bluetooth operations appropriately.

5. Wi-Fi

Hackers can intercept communications between smartphones and Wi-Fi hotspots. The fundamental vulnerability is hotspot architecture with no encryption to protect transmitted data. "If a user connects to [such] a hotspot for the first time, the end-to-end connection between the user's device and the hotspot provider is not secured, so the [hacker] can intercept and manage The user's traffic, aforementioned Carnegie Andrew William mellon University technology prof St. Patrick Tague. In this state of affairs, the hacker gets between the user and therefore the hotspot supplier and hijacks the session via a man-in-the-middle attack.

6. Malicious Applications

In some cases, hackers have uploaded malicious programs or games to third-party smartphone-application marketplaces-such as those for Apple's iPhone and Google's Android devices-or have otherwise made them available on the Internet.

7. Password cracking

In 2010, man of science from the University of Pennsylvania investigated the likelihood of cracking a device's positive identification through a smudge attack (literally imaging the finger smudges on the screen to make out the user's password). The researchers were able to make out the device positive identification up to sixty eight of the time below bound conditions. Outsiders might perform over-the-shoulder on victims, such as watching specific keystrokes or pattern gestures, to unlock device password or passcode.

8. Malicious software (malware)

As smartphones are a permanent purpose of access to the web (mostly on), they can be compromised as easily as computers with malware. A malware may be a worm that aims to damage the system within which it resides. Trojans, worms and viruses are all considered malware. A Trojan may be a program that's on the smartphone and permits external users to attach discreetly. A worm may be a program that reproduces on multiple computers across a network. A virus is malicious package designed to unfold to different computers by inserting itself into legitimate programs and running programs in parallel. However, it should be aforementioned that the malware are so much less various and vital to smartphones as they're to computers.

Traditional Security Approaches

Mobile communications can use the same types of security-sincluding antivirus and firewall products-v-as fixed communications. Most of those merchandise work very similar to their laptop counterparts. For example, mobile antivirus products scan files and compare them against a database of known mobile malware code signatures. Noted Mocana's Stammberger, this approach is compure-intensive and "eats batteries for lunch."

Mobile security software is also more likely to use the cloud to offload some of the processing typically associated with PC-based products, said Chris Perret, CEO of security vendor Nukona.

Countermeasures

The security mechanisms in situ to counter the threats delineated higher than ar bestowed during this section. They are divided into completely different classes, as all don't act at an equivalent level, and that they vary from the management of security by the OS to the behavioral education of the user. The threats prevented by the varied measures don't seem to be an equivalent looking on the case. Considering the 2 cases mentioned higher than, within the initial case one would shield the system from corruption by associate application, and within the second case the installation of suspicious software would be prevented.

ISSN 2394 - 7780

Security in operating systems
The first layer of security in a smartphone is the operating system (OS). Beyond eager to handle the same old roles of associate OS (e.g. resource management, programing processes) on the device, it must also establish the protocols for introducing external applications and data without introducing risk.

Security software
Above the OS security, there is a layer of security software. This layer consists of individual elements to strengthen numerous vulnerabilities: stop malware, intrusions, the identification of a user as a human, and user authentication. It contains package elements that have learned from their expertise with laptop security; but, on smartphones, this software must deal with greater constraints.

Resource monitoring in the smartphone:
When associate application passes the varied security barriers, it will take the actions that it absolutely was designed. When such activities are activated, the movement of a malicious application can be sometimes detected if one monitors the various resources used on the phone.

Depending on the goals of the malware, the consequences of infection are not always the same; all malicious applications are not intended to harm the devices on which they are deployed.

The following sections describe alternative ways to observe suspicious activity.

- **Battery**

Some malware is aimed toward exhausting the energy resources of the phone. Monitoring the energy consumption of the phone is the simplest way to find bound malware applications.

- **Memory usage**

Memory usage is inherent in any application. However, if one finds that a considerable proportion of memory is employed by associate application, it may be flagged as suspicious.

User awareness
Malicious behavior is permitted by the carelessness of the user. Smartphone users were found to ignore security messages throughout application installation, especially during application selection, checking application reputation, reviews and security and agreement messages. From simply not leaving the device while not a positive identification, to precise control of permissions granted to applications added to the smartphone, the user has a large responsibility in the cycle of security. This precaution is particularly vital if the user is associate worker of a corporation that stores business information on the device. Detailed below are some precautions that a user will fancy manage security on a smartphone.

Next Generation of mobile security
A secure kernel which will run in parallel with a fully featured Rich OS, on the same processor core. It will embody drivers for the made OS ("normal world") to speak with the secure kernel ("secure world").The trusty infrastructure might embody interfaces just like the show or data input device to regions of PCI-E address house and recollections.

CONCLUSION

Mobile security needs a special approach not centered on malware. Leaky apps that store or transmit sensitive personal and company information in associate insecure manner are of so much larger concern at now in time. Even legitimate apps while not deliberately malicious practicality that is downloaded from official app marketplaces will embody high risk security problems. Mobile security needs distinguishing and remediating security problems in device OSs and configurations, the apps installed on those devices, and the network connections those devices make each day.

REFERENCES

- *Bishop, Matt (2004). Introduction to Computer Security. Addison Wesley Professional.* ISBN 978-0-321-24744-5.
- *Rogers, David (2013). Mobile Security: A Guide for Users. Copper Horse Solutions Limited. ISBN 978-1-291-53309-5.*
- *Becher, Michael (2009). Security of Smartphones at the Dawn of Their omnipresence (PDF) (Dissertation). Mannheim University.*
- *Bilton, Nick (26 July 2010).* "Hackers With Enigmatic Motives Vex Companies". *The New York Times. p. 5.*
- *Cai, Fangda; Chen, Hao; Wu, Yuanyi; Zhang, Yuan (2015).* AppCracker: Widespread Vulnerabilities in Userand Session Authentication in Mobile Apps (PDF) *(Dissertation). University of California, Davis.*

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

NETWORK SECURITY

Prashant Khot
JVM's Mehta Degree College, Navi Mumbai

ABSTRACT
Security may be a basic part within the computing and networking technology. The computer network technology is developing apace, and also the development of web technology is added quickly, individuals additional tuned in to the importance of the network security. After analyzing and quantifying the network information security parts' confidentiality, integrity and availability, this paper describes the network security confidentiality vector, network security integrity vector and network security availability vector. There are different forms of attacks that may be once sent across the network. In this paper, we are attempting to check most forms of attacks together with varied different forms of security mechanism that may be applied consistently with the requirement and architecture of the network.

Keyword: Network Security, attacks

INTRODUCTION
Network Security management is totally different for all types and is important because of the growing use of web. A home or little workplace might solely need basic security whereas giant businesses might need high maintenance and advanced package and hardware to forestall malicious attacks from hacking and spamming.

"New Threats Demand New Strategies" as the network is the door to your organization for both legitimate users and would-be attackers. For years, IT professionals have engineered barriers to forestall any unauthorized entry that might compromise the organization's network. And this network security is vital for each network planning, building, and operating that consists of strong security policies. The Network Security is continuously evolving, due to traffic growth, usage trends and the ever changing threat landscape. An effective network security arrange is developed with the understanding of security problems, potential attackers, needed level of security, and factors that make a network vulnerable to attack. The steps involved in understanding the composition of a secure network, internet or otherwise, is followed through this research endeavour. Typical security presently exists on the computers connected to the network. Security protocols generally typicallyseem as a part of one layer of the OSI network reference model. Current work is being performed in employing a bedded approach to secure network style. We have given the Trend small security approach that is predicated on most then single layer of security. This security approach ends up in an and efficient style that circumvents several common security issues.

TYPES OF ATTACKS
Here, we are presenting some basic class attacks which cause for slow network performance that can be,uncontrolled traffic, viruses etc.

1. Passive Attack
A Passive attack monitors unencrypted traffic and appears for clear-text passwords and sensitive information which will be utilized in alternative sorts of attacks. The watching and listening of the communication by unauthorized attacker's area unit refers to as passive attack. It includes traffic analysis, watching of unprotected communications, decrypting debile encrypted traffic, and capturing authentication information like passwords. Passive interception of network operations allows adversaries to visualize approaching actions. Passive attacks or data files to Associate in Nursing offender while not the consent or knowledge of the user.

2. Active Attack
In an active attack, the attacker tries to bypass or break into secured systems in the on-going communication. This can be done through concealing, viruses, worms, or Trojan horses. Active attacks embodies to bypass or break protection options, to introduce malicious code, and to steal or modify information. The unauthorized attackers monitor, listens to and modifies the info stream within the communicating square measure called active attack. These attacks square measures which are mounted against a network backbone, exploit info in transit, electronically penetrate an enclave, or attack an authorized remote user during an attempt to connect to an enclave. Active attacks end in the revelation or dissemination of knowledge files, DoS, or modification of knowledge.

ISSN 2394 - 7780

A. Modification
When malicious node performs some modification within the routing route, in order that sender sends the message through the long route.

B. Distributed Attack
A distributed attack needs that the human introduce code, like a worm or back-door program, to a —trusted part or software package which will later be distributed to many different corporations and users Distribution attacks specialize in the malicious modification of hardware or software package at the mill or throughout distribution. These attacks introduce malicious code like a back door to a product to realize unauthorized access to info or to a system perform later.

C. Business executive Attack
Business Executive Attack in step with a Cyber Security Watch survey insider were found to be the cause in 21% of security breaches, and an additional 21% could have been due to the actions of insiders. More than half of the respondents to a different recent survey it's tougher these days to observe and stop corporate executive attacks than it had been in 2011, and 53% were increasing their security budgets in response to corporate executive threats. While a big range of breaches are caused by malicious or dissatisfied workers - or former workers - several are caused by well that means workers United Nations agency that are merely attempting to do their job. BYOD programs and file sharing and collaboration services like Dropbox mean that it'll be more durable than ever to stay company information beneath company management within the face of these well-meaning but irresponsible employees.

Here we are presenting some basic class of attacks which can be a cause for slow network performance, uncontrolled traffic, viruses etc. Attacks to network from malicious nodes. Attacks can be categories in two: 505 Mohan V. Pawar and J. Anuradha / Procedia Computer Science 48 (2015) 503 – 506 "Passive" when a network intruder intercepts data traveling through the network, and "Active" in which an intruder initiates commands to disrupt the network's normal operation.

3. Insider Attack
A business executive attack involves somebody from the within, like associate authorize worker, assaultive the network business executive attacks can be malicious or no malicious. A business executive attack may be a malicious attack perpetrated on a network or PC system by a person with authorized system access. Insiders that perform attacks (insider's attacks) have a definite advantage over external attackers because of they need authentications to system access and conjointly is also at home with network architecture and system policies and procedures. In addition, there could also be less security against insiders (that perform attack) because of several organizations specialize in protection from external attacks and can't specialize in business executive attackers. A business executive attack is additionally referred to as associate degree business executive threat.

4. Hijack attack
In a Hijack attack, a hacker takes over a session between you and another individual and disconnects the other individual from the communication. You still believe that you are talking to theoriginal party but may send some private information to the hacker by accident.

5. Phishing Attack
A phishing attack is fashionable at this point. During this attack, the hacker creates to pretend computing machine (to communicate with the people) that appears specifically sort of a fashionable site such as the SBBJ bank, Paytm or PayPal. Phishing is a part of the attack is that the hacker then sends associate e-mail message trying to trick the user into clicking a link that results in the pretend website. When the user tries to check in with their Personal info and account info, the hacker records the username and arcanum and so tries that info on the important website. When you access net on its time you get some message which says for clicking on a selected link associate then evoke your email id and parole once you entered your id parole then it's mechanically save your data and so use it on your behalf.

6. Close-in Attack
A close-in attack involves somebody trying to urge physically near to network parts, data, and systems so as to be told additional a few networks. Close-in attacks accommodates regular people attaining shut physical proximity to networks, systems, or facilities for the aim of modifying, gathering, or denying access to data. One fashionable style of move on attack is social engineering. In a social engineering attack, the wrongdoer compromises the network or system through social interaction with someone, through Associate in Nursing e-mail message or phone. Various tricks are employed by the individual to

ISSN 2394 - 7780

revealing data regarding the safety of company. The information that the victim reveals to the hacker would presumably be utilized in an ulterior attack to achieve unauthorized access to a system or network.

ADVANCE ATTACKS

7. Black hole attack

Black hole region attack is one among the advance offensive that wrongdoer uses the routing protocol to advertise itself as having the most effective path to the node whose packets it wants to intercept. A hacker uses the flooding primarily based protocol for listing the request for a route from the leader, then hacker produce a reply message he has the shortest path to the receiver. As this message from the hacker reached to the leader before the reply from the receiver node, then leader will contemplate that, it's the shortest path to the receiver. So that a malicious fake route is create.

9. Rushing attack

In rushing attack, when sender sends packet to the receiver, then attacker alters the packet and forward to receiver. Attacker performs duplicate sends the duplicate to the receiver once more. Receiver assumes that packets come back from sender therefore the receiver becomes busy endlessly.

10. Replay attack

It this attack, a malicious node could repeat the info or delayed the info. This can be done by conceiver United Nations agency intercept the info and convey it. At that point, AN assailant AN intercept the positive identification.

11. Byzantine attack

A collection of intermediate node works between the sender and receiver and perform some changes like making routing loops, sending packet through non-optimal path or selectively dropping packet, that end in disruption or degradation of routing services.

12. Location revelation attack

Malicious node collects the knowledge concerning the node and concerning the route by computing and observation the traffic. So malicious node could perform a lot of attack on the network.

CONCLUSION

Security may be a terribly troublesome but an important topic. Everyone includes a totally different plan relating to security' policies, and what levels of risk are acceptable. The key for building a secure network is to outline what security means to you want of the time and use. Once that has been outlined, everything that goes on with the network can be evaluated with respect to that policy. It's important to create systems and networks in such how that the user isn't constantly reminded of the safety system around him. However, Users World Health Organization notice security policies and systems too restrictive can notice ways in which around them. There square measure completely different forms of attacks on the safety policies and conjointly growing with the advancement and therefore the growing use of web. In this paper, we tend to try to check these completely different forms of attacks that penetrates our system. As the threats square measure increasing, so for secure use of our systems and internet there are various security policies are also developing. In this paper we've got to mention several the safety policies which will be used principally by range of users and a few new advance qualities that matches to the today's additional penetrating environments like Trend small security mechanism, use of massive information qualities in providing security, etc. Security is everybody's business, and solely with everyone's co-operation, AN intelligent policy, and consistent practices, will it be achievable.

REFERENCES

1. https://www.ijcsmc.com/docs/papers/May2015/V4I5201599a46.pdf
2. https://www.researchgate.net/publication/277723629_Network_Security_and_Types_of_Attacks_in_Network
3. https://www.researchgate.net/publication/316782131_Different_Type_Network_Security_Threats_and_Solutions_A_Review
4. https://www.researchgate.net/publication/267691532_MODERN_NETWORK_SECURITY_ISSUES_AND_CHALLENGES

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

IMPLICATIONS OF SOCIAL MEDIA ON DATA SECURITY IN THE AGE OF INTERNET

Nrupura R. Dixit
Assistant Professor, Department of Information Technology and Computer Science, Laxman Devram Sonawane College of Commerce, Arts and Science, Wadeghar road, Kalyan (west)

ABSTRACT
Social media has become a potent tool for every professional today. The open and easy availability of data on social media often raises questions about its impact on human rights. This paper discuss the influence social media has on the cyber space and the resultant invasion of privacy that becomes pertinent in this respect. An attempt has been made to offer recommendations that would enable policy-makers to evaluate the current influx of information on social media and how that could be examined to eliminate future threats of data security and data privacy.

Keywords: social media, human rights, invasion of privacy.

INTRODUCTION

In today's digital era every next person is having or using a user account to get connected to social Networking Website and having access to social media to allows you to spread a right to freedom of information and expression. Some of the commonly used social Networking platforms are Whatsapp, Facebook, Instagram, Twitter and Linkedin, etc.

So lets us first try and exactly what is social media and how does it contributes in Social Networking? The website or an application that enables the users to create and account into website for interacting/ sharing or participating with people with similar interest to one's own (Ellison, Nicole & Boyd, 2013).

How to get into the Social Networking Communities and access the social Media? Identify community of your interest, check with the options available services and feature they offer, sign up into the community- that creates your account, now once you have created the account login into the account, start sharing your updates and start interacting with the community people by viewing there profiles and status updates and chats.

Now a days social Networking has become a symbol of status to every individual who has been creating user accounts and using social networking for getting connected with the social media.

What do you mean by Human Rights?- "the basic rights and freedoms to which all humans are entitled" – such as right to equality, Freedom from Arbitrary Arrest and Exile, Right to Fair Public Hearing, Right to be Considered Innocent until Proven Guilty, Freedom from Interference with Privacy, Family, Home and Correspondence.

What is cyber security? The definition developed by the Freedom Online Coalition's cyber security Working Group "An Internet Free and Secure" based on the ISO 27000 standard, Cyber Security is defined as "Cyber security is the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline".

How is human rights and cyber security related? The freedoms of expression and information in stated by The United Nations Human Rights Council (UNHRC) under the Article 19(**2**) of the International Covenant on Civil and Political Rights (ICCPR) include the freedom to receive and communicate information, ideas and opinions through the Internet.

In Article 19(**3**) of the ICCPR states an important clause as:

The exercise of the right provided in paragraph two of this article carries with it special duties and responsibilities. It may therefore be subjected to certain restrictions, but these shall only be such as are provided by law and are necessary:

(**a**) For respect of the rights or reputations of others;

(**b**) For the protection of national security or of public order, or of public health and morals.

The HRC has stated that "the same rights that people have offline must also be protected online" (mentioning, in particular, freedom of expression). Freedom of information should be balanced with other rights.(*Australian Human Right Commission.* Retrieved April 10, 2015.)

ISSN 2394 - 7780

CHALLENGES

Some of those cyber behaviors on social networks that affect the human rights are as listed below:

A user who is "offline" appears to be "online" (cyber bullying).(Dredge, Rebecca, John Gleeson, and Xochitl De la Piedad Garcia.(2014))

Many a time when you have not logged into your facebook, instagram or WhatsApp account you seem to be available. And the moment people see you available they starting sending the message requests.

Messages getting flooded by social Media Marketing (cyber bullying) (DeHue, Francine, Bolman, & Völlink,2008)

Many a time there are pages and advertisements on the social networking website. Just with curiosity if you check with the advertisements they ask you with your social networking details or they grab the details from your account and start overloading your inbox the spam messages.

Racial comments how beautiful or ugly one looks? (cyber racism). (Barker & Valerie, 2009) & (Schmidt, Anna, and Michael Wiegand ,2017)

When a user uploads an image (photograph) people start comments and being judgmental on the looks and appearance of the person with various versions of the comments with likes and dislikes.

Communal talks and shares- related to political or religious sentiments (hate speech). (Burnap, Pete & Williams, 2016).

The speech mentioned in terms of comments related to race, religion, ethnic origin, national origin, sex, disability, sexual orientation or gender identity targeting a particular user or community.

By this certain or uncertain behaviors of every responsible individual directly or indirectly we make the invasion of privacy and that leads to threat to human rights.

RECOMMENDATIONS

If every individual follows some simple practices then we can protect the invasion of privacy in human rights. (Naughton & John, 2013) and (*Face2Face Africa*, 2018)

1. **Make use of personal digital device for accessing your user accounts**
   While accessing internet and logging into the social media we should be careful while using the device through which we are going to access the internet. Because if you click on remember password button then your password will be remembered by the cookies of the system you are accessing the account. And information can be auto logged in
2. **Choose your network location carefully and then log into your account.**
   Do not access your social networking accounts through shared points or free wireless fidelities.
3. **Passwords should not be simple**
   When you will be using the passwords for signing up the accounts make sure that your passwords are not easily accessible by anyone. Difficult to guess. It should be proper composition of characters, digits and special characters.
4. **Be careful in content sharing**
   When you are sharing or commenting on some post of social media make use of correct words and expressions (especially when you are making use of emoji's) or make use of proper words and clear thoughts.
5. **Verify before you click when you are requested.**
   When you are visiting communities or groups you come across many advertisements. When you click or subscribe button read the instructions given against. Otherwise if the terms and conditions are not read your inbox will be flooded with the spams messages.
6. **Stay careful while shopping online**
   When you are buying or selling the products through e-commerce website read all the policy quotes mentioned and then agree the terms and conditions and buy the products and carefully select the payment portal. While selecting the online portals please selected and known trusted portals or payment partners for the portals.

ISSN 2394 - 7780

7. **Check messages and apps from your device (major threats).**
   Your phone is most susceptible device to receive the text message and shared links. So while surfing the internet you phone can capture the unknown links and download the apps and information available from unknown and untrusted sources because your app store is easily open ended application available at your device.

8. **Check the updated when your software are set on automatic updates**
   You should update your device with latest patches received from the authorized source. Your security and antivirus should schedule the scans at regular intervals.

9. **Accept the friend requests at your own risk.**
   We receive so many friend requests when we are online. We should have only those friends request to whom we actually know. Because all the profiles present on the social networking sites are always not real they may be either fake users or hackers account too.

CONCLUSION

Simple steps to precautions will lead to safe internet surfing and preserving privacy to human rights.

REFERENCES

1. "Background Paper: Human Rights in Cyberspace" (PDF). *Australian Human Right Commission*. Retrieved April 10, 2015.
2. Ellison, Nicole B., and Danah M. Boyd. "Sociality through social network sites." *The Oxford handbook of internet studies*. 2013.
3. Kwak, Haewoon, et al. "What is Twitter, a social network or a news media?." *Proceedings of the 19th international conference on World wide web*. AcM, 2010.
4. Kaplan, Andreas M., and Michael Haenlein. "Users of the world, unite! The challenges and opportunities of Social Media." *Business horizons* 53.1 (2010): 59-68.
5. Mesch, Gustavo S. "Parental mediation, online activities, and cyberbullying." *CyberPsychology & Behavior* 12.4 (2009): 387-393.
6. DeHue, Francine, Catherine Bolman, and Trijntje Völlink. "Cyberbullying: Youngsters' experiences and parental perception." *CyberPsychology & Behavior* 11.2 (2008): 217-223.
7. Vandebosch, Heidi, and Katrien Van Cleemput. "Defining cyberbullying: A qualitative research into the perceptions of youngsters." *CyberPsychology & Behavior* 11.4 (2008): 499-503.
8. Dredge, Rebecca, John Gleeson, and Xochitl De la Piedad Garcia. "Cyberbullying in social networking sites: An adolescent victim's perspective." *Computers in human behavior* 36 (2014): 13-20.
9. Barker, Valerie. "Older adolescents' motivations for social network site use: The influence of gender, group identity, and collective self-esteem." *Cyberpsychology & behavior* 12.2 (2009): 209-213.
10. Burnap, Pete, and Matthew L. Williams. "Us and them: identifying cyber hate on Twitter across multiple protected characteristics." *EPJ Data Science* 5.1 (2016): 11.
11. Williams, Matthew L., et al. "Policing cyber-neighbourhoods: tension monitoring and social media networks." *Policing and society* 23.4 (2013): 461-481.
12. Rice, Emma S., et al. "Social media and digital technology use among Indigenous young people in Australia: a literature review." *International journal for equity in health* 15.1 (2016): 81.
13. Rice, Emma S., et al. "Social media and digital technology use among Indigenous young people in Australia: a literature review." *International journal for equity in health* 15.1 (2016): 81.
14. Silva, Leandro, et al. "Analyzing the targets of hate in online social media." *Tenth International AAAI Conference on Web and Social Media*. 2016.
15. Gibbons, Thomas, and Thomas Gibbons. *Regulating the media*. Vol. 13. London: Sweet & Maxwell, 1998.
16. Mondal, Mainack, Leandro Araújo Silva, and Fabrício Benevenuto. "A measurement study of hate speech in social media." *Proceedings of the 28th ACM Conference on Hypertext and Social Media*. ACM, 2017.
17. Schmidt, Anna, and Michael Wiegand. "A survey on hate speech detection using natural language processing." *Proceedings of the Fifth International Workshop on Natural Language Processing for Social Media*. 2017.

ISSN 2394 - 7780

18. Oksanen, Atte, et al. "Exposure to online hate among young social media users." *Sociological studies of children & youth*18.1 (2014): 253-273.
19. Debatin, Bernhard. "Ethics, privacy, and self-restraint in social networking." *Privacy online*. Springer, Berlin, Heidelberg, 2011. 47-60.
20. Risse, Thomas, and Kathryn Sikkink. "The socialization of international human rights norms into domestic practices: introduction." *Cambridge Studies in International Relations* 66 (1999): 1-38.
21. "8 ways to stay safe online - Face2Face Africa". *Face2Face Africa*. 2018-02-06. Retrieved 2018-02-26.
22. Naughton, John (2013-09-16). "Internet security: 10 ways to keep your personal data safe from online snoopers". *The Guardian*. Retrieved 2018-02-26.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

APPROACHES APPLICABLE FOR WIRELESS SECURITY

Swapna Thakare
Research Scholar, Pune University

ABSTRACT
Wireless technology gives us many benefits as flexibility, portability, lower cost of installation. Wireless networks can easily accessed by laptop, cameras, game consoles, laptops etc. Due to this wireless technology becomes more popular day by day. Wireless technologies eliminates all limits and boundries of distance and location for communication and sharing information amongst peoples. Here we are discussed these wireless technologies and it's threats.

Keywords: WI-FI, WEP, SSID

I. INTRODUCTION
As wireless network are very flexible, it is becoming more and more popular everywhere. Wireless technology gives us many benefits as flexibility, portability, lower cost of installation. It covers a broad ranges of networks oriented towards various uses as per need. So risks are there in wireless technology. Few risks are as similar that of wired network. The most significant source of risk is airwave, the technology used in wireless network for underlying communication. Airwave is open to intruder. Also the loss of confidentiality, integrity and the threat of DOS(Denial Of Service) attack are also associated. Unauthorized access to system and data, corruption of data, consumption of network bandwidth, network performance degradation, launch an attack on other system can happen if no security is maintained. Once unauthorized user gets an access to the system he can access your servers, databases, email servers etc. There are two main security issues we need to focus –

Access- Only authorized users get access to sensitive data and can use wireless network

Privacy- nobody should be able to watch your authorized communication

II. SECURITY THREATS
There are major threats are as following:

#1: Easy to find the wireless LAN's. All wireless network should announce their existence by which the user can link up and provide the services by the network. Beacons, a special frames are used to announce this type of existence. Similarly the same information by which the user can join the network can also be used to launch an attack on a network. To avoid this we use strong access control and encryption.

#2: "Rogue" Access Points is an easy access to wireless LANs. Any user can purchase it and can connect to the corporate network without authorization. When Rogue is deployed by the end user it will results in great risk. This problems may not be identified by the end users as they might not be security expert .

#3: All the access point with default configuration may not activated wired equivalent privacy(WEP). If not taken the help of WEP the network access is usually there. Unauthorized user will never follow your service provider's terms and conditions. In case of Hot spot also the major concern was connectivity provider like hotels, airports etc.

#4: with the service and performance constraint, wireless LAN's has limited transmission capacity. All users shared this capacity with an access point. It is easy to imagine how local area application beats this limited capacity problem or how an attacker has made an attack of DOS.

#5: Session hijacking and MAC spoofing does not authenticates the frames. Each frame has a source address but there is no guarantee that it will be true one. Simply attackers can observe the MAC address of stations, which are active and adopt those address for malicious transmission.

#6: Eavesdropping and Traffic Analysis does not provides any protection against attacks, which passively observe traffic.

III. SECURING WIRELESS NETWORKS
To provide the wireless network security many points we need to focus.

a. Use of Encryption technique– to secure our wireless network from attackers, encryption is an effective way. More wireless routers, base stations and access points have built-in encryption mechanism. Most of the manufacturers deliver wireless routers having the encryption technique as turned off. If want to secure your network, you must turn it on.

ISSN 2394 - 7780

b. Use of anti-spyware and anti-virus software, firewall- we can used anti-spyware and anti-virus to protect our network and also update it timely. If firewalls are there then make turn on.

c. Change the default identifier- firstly change the default identifier assigned for router by the manufacturer. Though your router does not broadcasting to all still hackers knows default ID's and they can use it access your network. Make strong password which has at least 10 characters and hard to break.

d. Change router's all pre-set- change all the default passwords for administration given by the manufacturer of your wireless router

e. Only allow specific computers to access your wireless network. Each computer can communicate with a network with its own unique Media Access Control (MAC) address. Usually Wireless routers can allow only devices with specific MAC addresses to access to your network.

f. When you are not using your wireless network turn it off. Hackers will not be able to access the wireless routers when it is shut down

g. Give the training to Users and educate them about the secure wireless. For more effectiveness these training must be repeated periodically.

h. in search of rouge hardware we need to audit the network regularly. In this, the network used to be scanned and mapped for all WLAN nodes and access points.

IV. CONCLUSION

To increase the productivity and to cut the cost, Wireless networking provides numerous opportunities. It is not possible to remove all the threats arising from wireless networking and very difficult to reach to the reasonable level of security. We can adopt a systematic approach for handling these risks. Within this paper I discussed about the threats and risks associated with wireless and provided commonly available solution to eliminate the risks.

REFERENCES

[1] Gast, M. 802.11 Wireless Networks: The Definitive Guide Creating and Administering Wireless Networks, O'Reilley Publishing, April 2002.

[2] PCI Security Standards Council

[3] "PCI DSS Wireless Guidelines". Retrieved 2009-07-16.

[4] "Fitting the WLAN Security pieces together". pcworld.com. Retrieved 2008-10-30.

[5] "Wireless Security". Thomas M. Thomas. Cisco.

[6] Norton, P., and Stockman, M. Peter Norton's Network Security Fundamentals. 2000.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

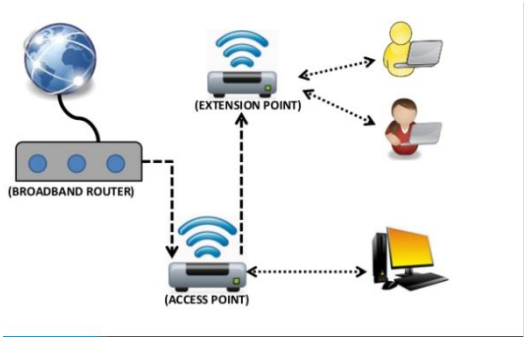
A TOUR ON WIRELESS SECURITY TECHNIQUES

Meghal Murkute
JVM'S Jr. College & Mehta Degree College, Navi Mumbai

ABSTRACT
This research paper is about the most important security protocols for wireless networks. Network security is a branch of cyber forensic that addresses enforcement of secure behaviour on the operation of wireless network. The definition of secure varies by application, and is usually outlined implicitly or expressly by a security policy that addresses Confidentiality, Integrity and availableness of electronic data that's processed by or stored on computer systems. It focuses on the Bluetooth, Infrared and Wi-Fi. The strengths and weaknesses of these solutions are discussed on further development and improvements.

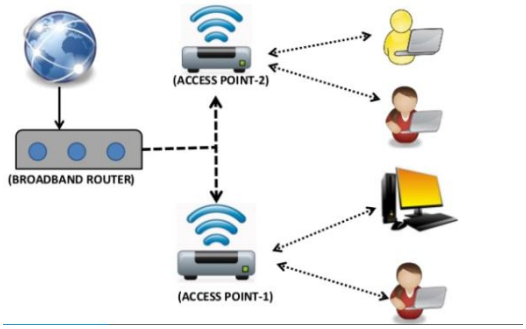
INTRODUCTION
Wireless network is also known as WLAN. It is developed on IEEE 802.11 standards. Wireless network include Bluetooth, Infrared, Wi-Fi, WiMAX, etc. Components used are wireless client receiver, access point and antennas. Types of wireless network are:-

i. Extension to wired network



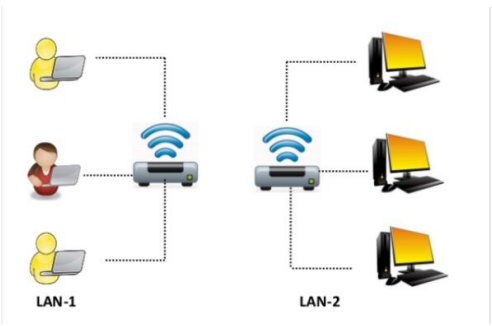
Home plug adapters can be used to extend a wired and wireless network. Generally they add pairs however you'll use quite two on a network.

ii. Multiple access point



Multiple access point is a technique that lets multiple mobile users to share the allotted spectrum in the most operative manner. The multiple access method permits various terminals to connect to the same multi-point transmission medium to transmit over it and share its capacity.

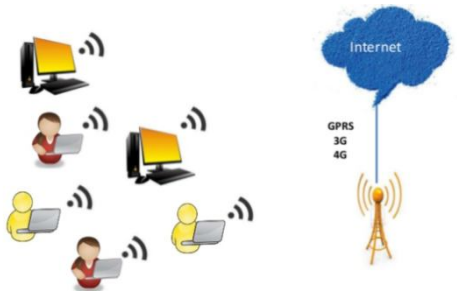
iii. LAN to LAN:-



ISSN 2394 - 7780

Connecting one of the main router's Ethernet ports to the secondary router's Ethernet port. This type of cascading needs the most and also the secondary routers to get on an equivalent local area network Internet Protocol (IP) to permit the computers and different devices to attach to each router. It is good way to expand your wired or wireless network.

iv. 3G or 4G hotspot



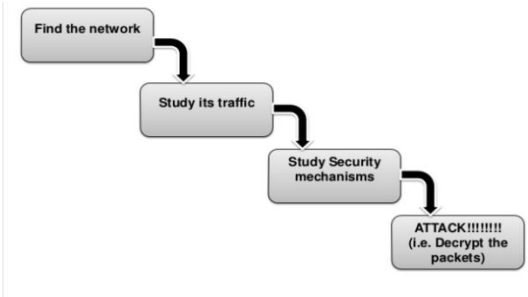
Mobile hotspots are a recent technology that allows you to connect your Internet-capable devices to the Internet through a portable device. The hotspot forms a Wi-Fi network and you can connect a number of computers or gadgets to the network for Internet access.

There are four Wi-Fi standards:-

1. 802.11a
2. 802.11b
3. 802.11g
4. 802.11n

Wireless security is that the interference of unauthorized access or harm to computers or information using wireless networks. The most common forms of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is an extremely weak security standard i.e. the password it uses can often be cracked. WEP is an old standard. It uses CRC-32 bit checksum. It was typically used by home users. It uses 64,128, 256 keys. WEP was replaced with WPA. WPA was welled improved with encryption and authentication method. Hardware changes not required. It was getting firmware update. The current standard is WPA2. It is having stronger data protection and network access control. It required hardware changes.

Mobile devices and wireless technology is getting develop gradually. Handheld device and desktop are replaced with mobile phone and notebooks. Most of the security or home devices have wireless technology. Wireless radio frequency signals spread beyond walls and buildings. The task of securing radio frequency is difficult. Hackers have found wireless network easy to hack. The risks to users of wireless technology have increased as wireless has become more popular. Hackers had not yet had time to handle on to the new technology, and wireless networks were not commonly found in the work place. However, there are many security risks associated with the current wireless protocols and encryption methods and in the lack of attention and lack of knowledge that exists at the user and corporate IT level.



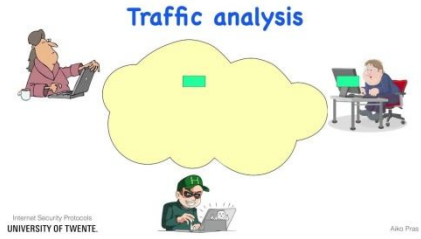
Attackers find the network and study its traffic. And then study its security mechanism and attack.

Attackers may attack your smartphone which is connected to wireless network and can fetch all the details like personal message, contacts, photo, bank details or it can access your camera, mic or location. Now days home devices, appliances and security are connected to a wireless network and if attacker tries to attack then he/she may have control over the devices and can miss use it.

ISSN 2394 - 7780

WIRELESS NETWORK THREATS ARE

1. **Traffic analysis:-**



It allow attacker to obtain 3 forms of information:-

i. The attacker identify that there is an activity on the network.

ii. Identification and physical location of wireless access point.

iii. Type of protocol being used during transmission.

2. **Passive eavesdropping**

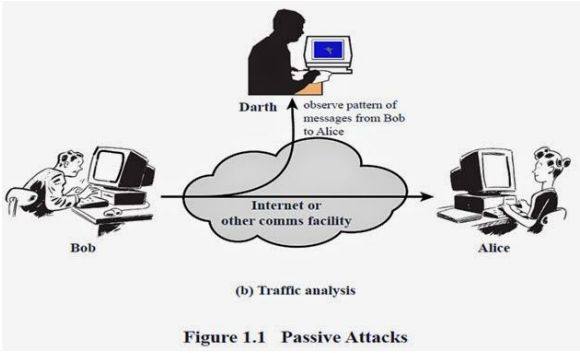
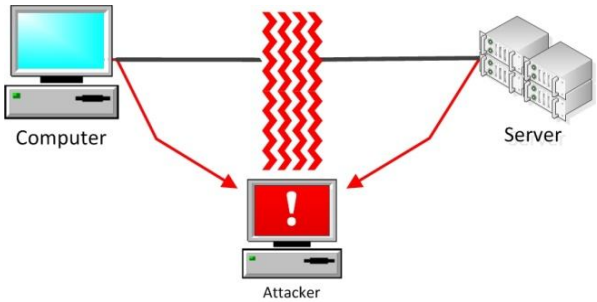


Figure 1.1 Passive Attacks

It allow attacker to obtain 2 forms of information:-

- The attacker can read the data transmitted.
- The attacker can read source, destination, size and time of transmission.

3. **Active eavesdropping**



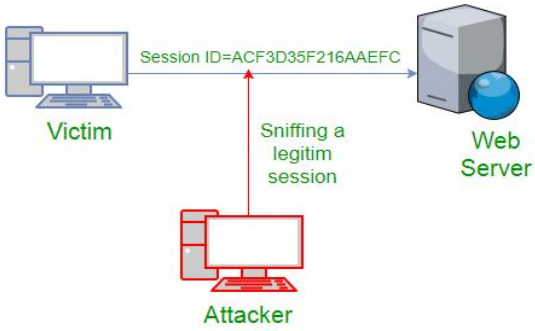
It allow attacker to modify the data into communication.

4. **Unauthorized access**

Due to the physical properties of WLAN, the attacker will always have access to the wireless devices on the network. If attacker successful gets unauthorized access to the network, then the attacker can use whole network services.

ISSN 2394 - 7780

5. Session high-jacking

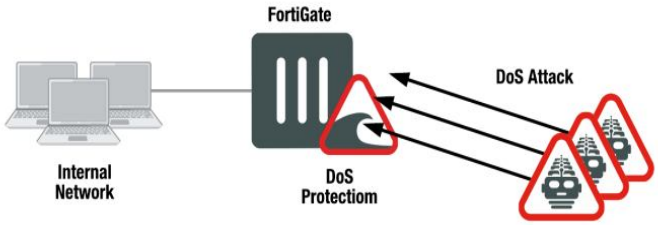


It is also known as cookie hijacking i.e. exploitation of a legitimate computer session additionally known as a session key to achieve unauthorized access to data or services during a system.

6. War driving

It is act of locating and possibly misusing connections to the WLAN while driving around city or using laptop or smartphone. The wiredriver generally configure their software to log any strong unencrypted signal using GPS receiver and connect to access point.

7. Denial of service attack



It is an attack which can disable network. It can slow the network speed or actually force it to stop working. It can come in 2 forms:-

i. A huge flood of packets that uses all network resources and forces to shut down.

ii. A very strong radio signal that completely take over radio wave and render the access point and radio card useless.

SOLUTION

1. Changing administrator passwords and usernames.
2. Upgrading Wi-Fi firmware time-to-time.
3. MAC address filtering
4. Stop publicly broadcast your network.
5. Do not connect to open network.
6. Do not auto-connect to the public network or hotspot point.
7. Use built-in firewall.
8. Turn off the network when not in use.
9. Login form must be implemented.
10. Do not connect if the network is slow.
11. Make sure any services or website you use are secure with SSL encryption.
12. Use licence antivirus.
13. Password must be a combination of special characters, number, and alphabets.

ISSN 2394 - 7780

CONCLUSION

We have overview of security techniques included in Wireless LAN. We have also discussed about the security issue wireless networks. It is hard to provide security for wireless network and great care and estimation is needed to get it correct. The problems with WEP are simple and it is not surprising that IEEE has created a task group to solve this problem quickly.

REFERENCES

1. https://ieeexplore.ieee.org/document/7987214
2. https://en.wikipedia.org/wiki/Wireless_security#Mobile_devices
3. https://whatsag.com/g/what_is_a_mobile_hotspot.php
4. https://www.wikihow.com/Cascade-Routers
5. https://en.wikipedia.org/wiki/Session_hijacking
6. https://en.wikipedia.org/wiki/Passive_attack

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

DATABASE SECURITY – ATTACKS AND THREATS

Khushi B. Patel & Preeti G. Verma
Jnan Vikas Mandal's Mehta Degree College

➢ ABSTRACT

A database is a collection of data which describes the activities of one or more related information. Security is the safety of facts and data from the unaccredited user. Database security refers to the collective measures used to protect and secure a database or database management software from illegitimate use and malicious threats and attacks. All the operation of data manipulation and data maintenance is done by database management system. It is a broad term that includes a multitude of processes, tools and methodologies that ensure security within a database environment. Its demand can be checked by the growth in the number of hacking of sensitive data from unaccredited user. Nowadays, we share our data by electrically which leads to hacking of data to save all those things. Database security is very much important so that our data can be safe. In this paper, I will be writing little bit security technique so that our facts or data can be secure and our database becomes stronger in security point of view. Databases should be preserved more than any systems in any organization. The motive of this paper is to highlight and threat types and their influence on sensitive data, and presents different security models.

➢ INTRODUCTION

Databases are warehouse of the most important and expensive information in the cooperative. Today, in many business organizations, the databases and data belongings are imperfectly protected. Information is outlined as a group of knowledge that's saved on a pc system's Winchester drive. Databases allow any authorized user to access enter and analyse data rapidly and comfortably. Databases must be preserved better than any other systems in the organizations. They allow data to be cherished and shared electronically and the amount of data contained in these systems persistent to grow at an exponential rate.

The user interface for databases is called database management system. DBMS are a software application that interacts with the permit user, other applications and the database itself to capture and analyse data. Advantage of using the database is it programmed different procedures, savings resources and man hours. Information will offer potency and speed within the fashionable geographical point. Database security demands allowing or prohibiting user actions on the information and also the objects within it. Organizations that are running successful demand the confidentiality of their database. They do not allow the unauthorized access to their information. They also demand the assurance that their data is protected against any harmful or accidental modification. Hacking is distinctive weakness in pc systems or networks to take advantage of its weaknesses to realize access.

ISSN 2394 - 7780

Data hacking describes the activities practiced by individuals, organizations, and nations, in order to gain unaccredited access to computer and technology dependent systems. These activities may involve the modification or modification of system's software and hardware in order to perform activities neither purposed by the author nor in line with the author's original objectives. The threats create a challenge to the organization in terms of integrity of the info and access. The threat can result from untouchable loss such as hardware robbery or untouchable loss such as loss of confidence in the organization activities. All these activities have been uncontrolled due to electronic commerce as opposed to typical trade involving physical goods.

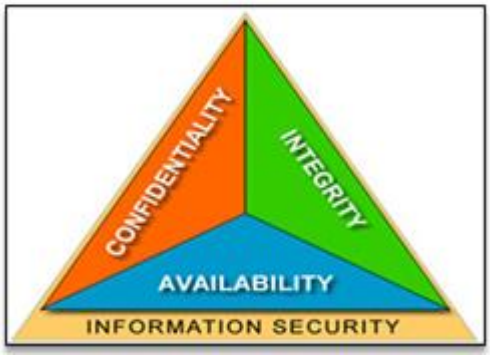
- **THREATS OF DATABASE SECURITY**

Database security issues have been more complex due to universal use and use of distributed client/server architecture as opposed to administration system. Databases are a firm main resource and therefore, policies and procedure must be put in place to protect its security and the truthfulness of data it contains. The objective of database security is to protect database from accidental or intentional loss. These threats pose a risk on the integrity of the data and its responsibility. Database security allows or declines the users from executing actions on the database. Database managers in an organization identify the warnings and make policies that take actions to migrate any risks.

Such actions embrace controls victimization passwords and username to manage users World Health Organization access the databases. The system created is termed direction security system that keeps user details and permits access once supplied with passwords and usernames. There are different threats to the database systems. Loss of availability means that data or systems cannot be accessed by any users. This most often arise from destroy of the hardware, applications or networks systems. This may conclude the activities of the organization as well delay in the operation in the day by day activities of the organization.

When users are given too much advantage in the system database they abuse them for harmful purposes. Another threat to database security is that of privileges elevation. This is when some user can convert extra privileges from ordinary user to administrator through taking database platform software susceptibility. This is done utilizing the software weaknesses in the database systems. This is when an organization exposes itself to risk of various types due to weaknesses in its internal system. This is due to weak is incentive mechanism. Denial of service is another drawback in information security.

- **CONTROL METHODS FOR DATABASE THREATS**



Confidentiality, Integrity and availability are the three major measures for data security. **Confidentiality** deals with the safety of data from unaccredited disclosures. **Integrity** deals with the safety of data from unaccredited modifications. **Availability** deals with the safety of data from unaccredited users.

ISSN 2394 - 7780

To remove the security threats every organization must consists a security policy which should be tooled for sure. In security policy validation plays a vital role because if validation is proper than there is less chances of threats. Different users have variance of access rights on different databases objects. Access management mechanisms touch upon managing the access rights. It is the basic technique to protect the data objects in the databases and is supported by the most of the DBMS.

1) **ACCESS CONTROL**

Access control is one of the elementary services that any Data Management System should provide. It's protected information from unauthorized browse and write operations. Errors is as major which might produce drawback in firm's operation

Access control systems include:

- **File permissions** - create, read, edit or delete on a file server.
- **Program permissions** – right to execute a program on an application server.
- **Data rights** – right to retrieve or update information in a database.

2) INFERENCE POLICY

It is very necessary to protect data at particular level. It can be applied when analysis of particular data is in the form of reality that is required to be prevented at a certain higher security level. It helps to determine the way to shield info from being free. The aim of the inference control is to avoid indirect announcement of information. There are three ways to unaccredited data declaration:

- **Correlated data** – typical channel when visible data X are semantically related with invisible data Y.
- **Missing data** – result of inquiry contains NULL values that mask sensitive data. Existence of that information could by find that means.
- **Statistical inference** – typical for databases that provide statistical information about entities.

3) **USER IDENTIFICATION /AUTHENTICATION**

User can be authenticated in number of ways before they are allowed to create database. Database authentication includes each identification and authentication of users. This is very basic requirement to ensure security since the identification process defines a set of people that are allowed to access data. To ensure security, the identity is authenticated and it keeps the sensitive data secure and from being modified by unauthorized user.

4) **ACCOUNTABILITY AND AUDITING**

Auditing is that the observation and recording of designed info actions, from both database users and non-database users. According is the process of maintaining an audit trail for user actions on the systems. Accountability and audit checks are required to confirm physical integrity of the information which needs outlined access to the databases which is handled through auditing and for keeping the records.

5) **ENCRYPTION**

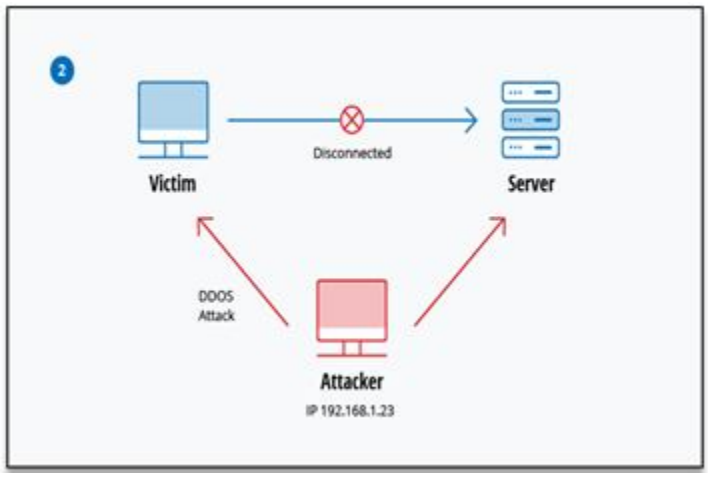
Encryption is that the method of changing info into a cipher or a code so it can't be clear to all or any people except people who hold a key for the cipher text. The cipher text or encoded text is termed as encrypted information. There are 2 states for information protection in information. Data may exit either: **At Rest** - data may be stored in database or in backend tape and **At Transit** - data travelling across the network which dictates different encryption solutions for the data in transit.

➢ **DIFFERENT TYPES OF ATTACKS**

Different types of attacks that can be carried out by an attacker after breaching through all layer of security are:

- **Direct attacks:** Directly hitting the target data is known as direct attack. These attacks are accessible and successful only if the database does not assist any protection system.
- **Indirect attack:** As its name implies indirect attacks are not directly executed on the target but data from or about the target can be collected through other transitional objects. For purpose to cheat the security system, some of the combination of different queries is used. These kinds of attacks are difficult to track.

ISSN 2394 - 7780



- **Passive attack**
  In this attack, attacker only examines data present in the database and do not perform any alteration. Passive attack can be carried out in the following ways:

8. **Static leakage**: In this attack, information about database plain text values can be attained by examining the snapshot of database at a particular time.
9. **Linkage leakage**: In this information about plain text values can be achieve by linking the database values to position of those values in index.
10. **Dynamic leakage**: Changes performed in database over a period of time can be observed and analysed and information about plain text values can be obtained.
11. **Active attack:** In active attack, actual database values are modified. These are more problematic than passive attacks because they can misguide a user. There are numerous ways that of playing such quite attack which are mentioned below:

REFERENCE

- **Spoofing:** In this attack, cipher text value is replaced by a generated value.
- **Splicing:** In this attack, a cipher text value is replaced by different cipher text value.
- **Replay:** It is a kind of attack where cipher text value is replaced with old version previously updated or deleted..

➢ CONCLUSION

Database security presents options that have to be seriously taken into consideration. Databases are a favourite target for attackers because of the data these are containing and also because of their volumes. Data warehouse is the ultimate goal. In today's technological world, database is unsafe to hosts of attacks. Efforts to ensure database security are considerably higher than for the others types of data. It is easier to implement an access list for an excellent variety of files than an access list for the weather of information. Database can be accommodated in several ways.

Different types of attacks and threats are there these days from that information ought to be protected. Organizations now are depending on data to make decisions on various

businesses operations that enhances their operations. It is advisable to keep sensitive information away from unaccredited access. Database security research paper has attempted to explore the issues of threats that may be self-possessed to database systems.

These embrace loss of confidentiality and loss of integrity.

Security of sensitive information is often an enormous challenge for a corporation at any level.

➢ REFERENCE

1. Mr. Saurabh Kulkarni, Dr. Siddha ling Urologic, Review of Attacks on Databases and Database Security Techniques, Facility International Journal of Engineering Technology and Database Security Techniques Research, Volume 2, Issue 11, November-2012.

ISSN 2394 - 7780

2. Sohail IMRAN, Dr Irfan Hyder, Security Issues in Database, Second International Conference on Future Information Technology and Management Engineering, 2009.
3. Emil BURTESCU, Database Security- Attacks and Control Methods, Journal of Applied Quantitative Methods, Volume 4, Issue 4, 2009.
4. Jiping Xiong, Lifeng Xuan, Jian Zhao and Tao Huang, Web and Database Security, Zhejiang Normal University.
5. Shelly Rohilla, Pradeep Kumar Mittal, Database Security: Threats and Challenges, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.
6. Deepika, Nitasha Soni, and Database Security: Threats and Security Techniques, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 5, May 2015.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

A BRIEF STUDY ON CYBER CRIME AND SECURITY

Pournima Raut
Computer Science Department, Bhavan's B. P. Vidya Mandir, Nagpur

ABSTRACT
The terms computer crime and cybercrime are more properly restricted to describing criminal activity in which the computer or network/Internet is a necessary part of the crime, these terms are also sometimes used to include traditional crimes, such as fraud, theft, blackmail, forgery and embezzlement, in which computers or networks are used. Cyber Crimes are also on the rapid expansion causing our sensitive data to be used without our permission. Governments are aware of this matter doing everything they can do secure our networks, but many say security is just an illusion.

In this report we will analyse the strength of the people who are trying to spoil the Cyber Ecosystem and the higher grounds where we can deceive them.

INTRODUCTION
Cybercrime is a type of crime or an illegal activity that is basically committed through a computer with the help of networking. Generally, however, it may be divided into one of two types of categories:

1) Crimes that target computer networks or devices directly;
2) Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device.

The ideal or most common word for this would be "Hacking"

The following are the examples of cybercrime-

a) Internet Fraud
b) Malware and malicious code/Spam
c) Denial-of-service attacks
d) Computing viruses
e) Cyber stalking/Cyberbullying
f) Fraud and identity theft
g) Phishing scams
h) Information warfare
i) Hate Crimes

Internet Fraud:
Whenever one tries to purchase a product from the internet, he/she is on a great risk of being victimized by internet fraud. So, it is very important for a person to research and study the sources from which he/she is purchasing the product. The e-commerce environment is stuffed with fake companies and organizations who distribute worst quality products to the customers and are greatly involved in stealing customers bank account data. These Internet crimes became a larger platform for crimes in the late 1990s and early 2000s. A single virus outbreak was blamed for 80$ Billion loss. In this scenario, HBL has introduced a 3-D secure e-commerce web certification which allows the user to recognize websites that can be trusted for online shopping. There are some famous websites which could be trusted on the basis of current circumstances for online shopping. Some of the trustworthy websites are given below:

- Flipkart.com.
- Amazon.in.
- Snapdeal.com.
- Jabong.com.

Malware: Malware is Malicious Software - deliberately created and specifically designed to damage, disrupt or destroy network services, computer data and software.

ISSN 2394 - 7780

There are several types

- Computer virus
- Worm
- Trojan horse
- Root kit
- Botnet
- Spyware
- Malware

Spam
Spam, or the unsolicited sending of bulk email for commercial purposes, is unlawful to varying degrees. As applied to email, specific anti-spam laws are relatively new, however limits on unsolicited electronic communications have existed in some forms for some time.

Spam originating in India accounted for one percent of all spam originating in the top 25 spam-producing countries making India the eighteenth ranked country worldwide for originating spam.

Cyberbullying.
Cyberbullying is done through digital devices for example Cell Phones, Computers, Tablets, iPhone, Ipads etc. Mentally torturing, harassment, Humiliation is cyberbullying. It includes sending, posting or sharing taunting, offending and sexual contents "publicly" or sending it to a specific person. The content could be personal data like pictures, email, chats etc.

Platforms for cyberbullying are given below:

1) Social Media such as Facebook, Twitter, Snapchat, Instagram.

2) Mobile Messaging.

80% teenagers use cell phones and some other related devices and 20% of them are bullied on daily basis.

Phishing
Phishing is a technique used by strangers to "fish" for information about you, information that you would not normally disclose to a stranger, such as your bank account number, PIN, and other personal identifiers such as your National Insurance number. These messages often contain company/bank logos that look legitimate and use flowery or legalistic language about improving security by confirming your identity details.

Cyber Criminals:
Someone who penetrates and breaks the security system of an organization or a network and exploits the flaws in that computer system is known as Hacker and process is known as Hacking.

There are many types of hackers.

1**) Script Kiddie:** Basically, they cannot be called hackers, because they just copy some kind of coded script and use it as a virus or use predefined software like maltego, hydra,Metasploit etc for penetration.

2) **White Hat Hackers:** They are known as Ethical Hacker or Legal Hackers. These types of hackers help organizations to make their system secure or they help victim company to prevent the viruses.

3) **Grey Hat Hackers:** They are nor Ethical Hackers neither Unethical Hackers. They don't harm people with their hacking nor steal anything, like money or personal information but sometimes they try to penetrate into a system.

4) **Black Hat Hackers:** They are famous as "Crackers". They find companies, organizations, especially bank that have weak and small security system and when they find it they steal the money, credit card information and etc

5) **Green Hat Hackers:** are types of hackers that really love hacking and care about it. They are unlike script-kiddies and they work hard and strive and struggle to become a legendary hacker.

6**) Red Hat Hackers:** Red Hat Hackers are the wanted criminals of the world. They steal money, steal data, harm the computer system, sometimes leaks the information to the outer world. It may include Terrorist.

ISSN 2394 - 7780

7) **Blue Hat Hackers**

History of Cyber Attacks:

Years	Types of Attacks
1997	Cybercrimes and viruses initiated, that includes Morris Code worm and other
2000	DDoS flooded Yahoo, eBay, CNN and ZDNet with huge data, blocking access for thousands of users for two to three hours.
2004	Malicious code, Torjan, Advanced worm etc.
2007	Identifying thief, Phishing etc.
2010	DNS Attack, Rise of Botnets, SQL attacks etc
2013	Social Engineering, DOS Attack, BotNets, Malicious Emails, Ransomware attack etc. Present Banking Malware, Keylogger, Bitcoin wallet, Phone hijacking, Anroid hack, Cyber warfare etc
2017	**WannaCry ransomware attack** was a May 2017 global cyber offence
2018	***SIM Swap Fraud, Cyber Attack on Cosmos Bank,*** Hackers hacked into the ATM server of the bank and stole details of many visa and rupee debit cards owners

Cyber Warfare:

Cyber warfare is a modern form of warfare in which countries attack each other for proving their strength or for gaining political/foreign policy victories.

Cyber warfare is an important evolutionary addition in the battle fronts that has the potential for significant effect on the citizens and especially on the computer scientists of the world.

Cyber warfare may be used as a political tool to increase the control of the government on the citizens and different organizations by keeping in checking their data and resources. Some of the techniques of the cyber-attacks include breaking into someone's personal computer or servers.

Cyber warfare became elite warfare when in the last United States elections Russian government Hacked into the election and moulded the results whatever they wanted it to be. This created a mass tension around the globe as it was one of the most powerful and unique display of power by one of the Superpower.

Another tactic is to create hindrance in the functionality of computers and the embedded equipment by using worms and viruses. In addition, some hackers use logic bombs and some other malware to malfunction the computer networks of important facilities.

The main scope and platform for the cyber warfare is internet and local network with a strong help from the ruling Government as generally they are the master planner of the attacks.

Applicable Laws are:

Country	**Laws**
United States	Access Device Fraud 18 U.S.C. & 1029 Computer Fraud & Abuse Act.18 U.S.C. & 1030 CAN-SPAM ACT. 15 U.S.C. & 7704
Canada	Criminal Code of Canada, Section 342.1 Criminal Code of Canada, Section 184 Computer Crime in Canada
United Kingdom	The Computer Misuse Act 1990(Chapter 18) The Regulation of Investigatory Powers Act 2000(Chapter 23)
Australia	Cybercrime Act 2001(Commonwealth) Crimes Act 1900(NSW): Part 6,ss 308-3081 Criminal Code Act Compilation Act 1913(WA)

ISSN 2394 - 7780

Malaysia	Computer Crimes Act 1997(Act 563)
Pakistan	Prevention of Electronic Crimes Ordinance 2007 Electronic Transactions Ordinance 2002
Singapore	Computer Misuse Act 1993(Chapter 50 A)
India	INFORMATION TECHNOLOGY ACT 2000 Online
Others	Council of Europe Convention on Cybercrime Global Survey of Cybercrime Law Unauthorized Access penal Laws in 44 Countries

Resources and the techniques used for Cyber Crimes:
There are many resources, but we will only discuss about most popular of them. Kali Linux is the operating system and python are the programming language which is widely used by the network penetrators.

Techniques used by hackers:
Brute Forcing: Probably the oldest technique out there, Brute forcing involves trying permutations and combinations of characters from a particular character set.

For instance, if a hacker must crack the password of a file. He will try all combinations for a given length and then move to the next length.

MITM: Man, in the Middle better known as MITM attack is a type of attack in which an intermediate device handles all requests that are made from it to a server.

Dictionary attack: Common dictionary words are used For predicting password.

Waterhole attacks: When the objective of the hacker is to gather as many sensitive information as he can they target public places like internet café, coffee shops or other most visited public places.

Fake Wi-Fi points: They can create fake wifi points in order to grab the sensitive data of the user who tries to log in from the wifi.

Keylogging: It is the process of creating a log(record) of all typed keystrokes on a system. All this data is then sent to the hacker's server periodically.

Modern Keyloggers provide features like snapshotting the victim's screen and even hide within other processes to not get detected.

Cookie Stealing: Cookies are used on almost every website around the internet. They are used to identify, remember and authenticate a particular user from the billions of other users on the website.

Backdoors: The points from which they penetrate into a system is known as the backdoor.

Usage of proxy networks for defence: Universities and institutions use proxy servers in order to defend their user from being attacked. This proxy network changes the IP address of their traffic who are accessing the internet so that a foreigner whose intentions are bad fails in tracking the genuine IP address of their member.

SQL Injection:SQL injection is the process by which a hacker may hack the database of a server by typing SQL queries in the input forms of websites.

DDOS Attack stands for distributed denial of service attack. In this, the victim is attacked from different sources. This makes it very difficult to defend the network from the attack.

The internet as a whole consists of three layers **world wide web, deep web and dark web.** Worldwide is the portion of internet consisting google search engine and the whole social media and many more websites. There are other different websites which our search engines cannot access therefore we can call them hidden or the webs which can be accessed via password or authorization. Which can only be logged in by using genuine authorization these are the deep web content that won't show up on our common search engine.

The other one is dark web which is quite popular in the underworld of criminals and unethical hackers. **Dark web** is part of worldwide that require a special browser to access.

The dark web is also called "Onionland" because of its content accessible only using services like Tor. It can be identified by the domain ". onion" whereas other normal websites identified by the domain .com.

ISSN 2394 - 7780

The dark web is used for illegal activities such as drug trade, media and confidential information exchange also for pedophiles and terrorists who want to hide their illegal activities use the dark web. People who want to hide their identity and want to search illegal articles use the dark web. Dark web is notorious for being the base of all cyber crime

Cross Site Scripting – XSS
Somewhat like SQL Injection, Cross Site Scripting inserts malicious client-side code in the input fields so when those fields are requested by some other user, They get exposed to those malicious scripts.
Things like security keys are used to prevent XSS attacks.

DNS Poisoning refers to introducing incorrect DNS address information into the DNS resolving server to make the user go to the same site located on the attacker's computer.

The Difference Between this and phishing is that in phishing attacks the URL is redirected to the hacker's website. But in DNS poisoning, the same URL is used but a different server is used.

CONCLUSIONS

Security is an illusion: Whatever technique we use to secure our networks it will be defeated in any time soon. This cycle keeps on running until meaning of security loses it's worth.

Develop best security practices:
People believe that security is an illusion, but we can do much more to give them a tough time. Technology tycoons like Facebook have thousands of their employees dedicated to the Cybersecurity wing, which allows their customers to trust them. The ones who know how to penetrate can also secure our networks as they know what a hacker looks for before penetrating a system.

Be proactive:
Do not wait until your networks are doomed in one way or another. Use every possible defence technique which cannot be deceived by the hackers.

Strict cyber laws should be deployed: Maximum people out there think we cannot/should not categorize Cyber Crimes into regular crimes. But as the events are happening and the world has started facing heavy losses because of cybercrimes it is becoming more and more clear that introducing strict cyber laws is the only way to handle these activities.

Increase security awareness among the masses: Most of the people do not give much more important to their data and they also imagine no one can really hurt them by grabbing their data but ironically the reality is opposite. Being tech people, we have a responsibility to create awareness among the masses about the dark side of the cyber ecosystem.

REFERNCE

- http://www.theitstuff.com/top-10-hacking-techniques-2
- http://www.encyclopedia.com/science-and-technology/computers-and-electrical-
- engineering/computers-and-computing/internet-fraud
- https://www.cybrary.it/0p3n/types-of-hackers/
- http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5634434
- http://www.cyberlawsindia.net/index1.html
- https://www.irjet.net/archives/V4/i6/IRJET-V4I6303.pdf
- Ross J. Anderson: Security Engineering: A Guide to Building Dependable Distributed Systems, ISBN 0-471-38922-6
- Morrie Gasser: Building a secure computer system ISBN 0-442-23022-2 1988
- Donovan: Management Information Systems for the information age, ISBN 0-07-091120-7
- E. Stewart Lee: Essays about Computer Security Cambridge, 1999
- Peter G. Neumann: Principled Assuredly Trustworthy Composable Architectures 2004
- Paul A. Karger, Roger R. Schell:
- Thirty Years Later: Lessons from the Multics Security Evaluation, IBM white paper.
- Bruce Schneier: Secrets & Lies: Digital Security in a Networked World, ISBN 0-471-25311-1

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

BASIC CYBER FORENSIC ANALYSIS AND INVESTIGATION TECHNIQUES

Roopa Rajkumar Kulkarni
Department of Information Technology, Bhavna Trust Junior and Degree College of Science and Commerce, Deonar, Mumbai

ABSTRACT
Cyber forensics is the application of investigation & analysis techniques which are preservation, collection, validation, identification, analysis, interpretation, documentation, presentation of evidence from a particular computing device which can be presented in the court of law. Cyber Investigation is the process where the law authenticated officers use to track the criminals.

INTRODUCTION
Our country is developing rapidly in the field of ICT. People are educated .Education is like wealth, If one is educated they can use their talent in various fields of arts science, commerce , agriculture ,medical science, technology etc.

Technology has developed rapidly to such an extent where it has become easy to access internet even in remote areas. People use Pc, laptop etc for their specific purpose but if they do not know how to secure their PC they may become a victim to hacker.

PHASES OF A CYBER FORENSICS INVESTIGATION
The investigating officer has to collect all the data from the PC of the victim using specific tool which will collect all the data without alteration.

The system which has been taken to custody has to be kept safely along with the relevant material and data so that an unauthorised person will not access the data , storage device. The connection of the internet has to be removed if it is connected.

They have to find all the files that are protected ,hidden, encrypted, with password or deleted but must ensure that the hidden files are not overwritten, make a copy of all the storage device ,hard drive and all the files of the computer ,keep the original PC as it is safely , work on the copy to find evidence

Get back as much deleted information as possible using applications that can find and retrieve deleted data find the contents of all hidden files with programs designed to detect the presence of hidden data.

Decrypt and access protected files.

Observe special areas of the computer's disks, including parts that are normally inaccessible. (unused space on a computer's drive is called unallocated space could contain files or parts of files that are relevant to the case.)

Documentation of every step of investigation has to be done so that it will be a proof that the officer has done the investigation without altering the evidence. It may take years for the case to be solve so documentation has to be proper. It should also include the location of crime , hidden and encrypted file

Even when an investigation is complete, They may still need to provide testimony in court .

CONCLUSION
In this world of computers and threats from hackers, keeping the data of the computer safe is necessary. .Internet is the key way for the attacker with malicious intent to attack the computer with less security

There are many ways to keep your system secure and to detect the fraud. Maximum security level applied to the computer with internet services it becomes difficult for the hacker to enter the system for malicious activity.

Some few points to be followed to protect your system from malicious activity

Install Firewall

Install Antivirus Software

Install Anti-Spyware Software

Use Complex and Secure Passwords

Check on the Security Settings of the Browser

ISSN 2394 - 7780

There are families wherein only aged people stay in the house and their children are staying away from them due to their job, when they want to communicate with their children or do some financial transaction online, they may make a mistake while using the internet facility either due to old age or due to less knowledge of internet and computer.

There must be some facility provided for aged people to use the internet in a safe manner so that they do not become the victim for any fraud online

When a fraud has taken place in a house where only aged people live it becomes difficult for investigation because the investigation officer has to disturb them every now and then which may be difficult for the aged person also, so it would be better if there be a machine which records all the details of the crime location in one sitting and if further investigation or search has to be done a scanner has to be fixed in the crime location and the investigating officer can scan the crime location from his office without actually going to the crime location

REFERENCES

- www.theinvestigators.co.nz/news/what-is-a-cyber-investigation/
- https://searchsecurity.techtarget.com/definition/computer-forensics
- https://computer.howstuffworks.com/computer-forensic2.htm
- https://antivirus.comodo.com/blog/computer-safety/5-simple-steps-protect-pc/
- http://ithare.com/a-beginners-guide-to-computer-forensics/
- https://en.wikipedia.org/wiki/Cybercrime#Agencies
- https://ijcsmc.com/docs/papers/November2017/V6I11201734.pdf

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

INTERNET BANKING AND SAFETY ISSUES

Veena M. Nirgudkar
HOD, Law Department, JVM's Mehta College, Navi Mumbai

ABSTRACT
Now a day's most of the bank provides various E-banking services like electronic Bill payment, phone, bark/tele banking, internet banking, debit/credit card payment, electronic fund transfer. Internet banking is fastest growing sector.

In order to increase the efficiency and profitability information techno logy has proved to be very useful and convenient source. Now it's possible to have " ANY TIME , ANY WHERE, ANY WAY BANKING"

It is total shift from traditional banking practice there is sudden rise in various banking related frauds and scams reported because of high risk in internet banking services.

RESEARCH OBJECTIVES
1 To understand the awareness of internet banking

2 To understand about the cyber safety issues and web securities issues involved in this area

3 To understand the high risk in electronic transactions and internet banking services

4 Preventative and corrective measures

5 Safety standards and regulatory measures .

LIMITATIONS OF THIS STUDY
This study is supported by the facts more than the data hence it restrict the discussion to preventations of frauds and scams in internet banking by way of suggesting precautionary measures as well as better and efficient regulatory mechanism .

METHODOLOGY
This study is based on secondary data derived from various Journals, websites , books and white papers.

OVERVIEW
Recent survey has shown that the customer awareness regarding internet banking services is seen as under

1 Nearly 34% people are not aware about electronic bill payments

2 24% people are not aware about electronic fund transfer

3 However 94% of them are aware about ATM and Credit Card/ Debit Card Payment facility.

MOST OF THE BANK OFFERS VARIOUS INTERNET BANKING SERVICES FOR FOLLOWING REASONS,
1 Convenience

2 Speed

3 Efficiency

4 Low Cost

5 Services can cover large section of consumers

6 Cost effective and time Saving

However it is observed that internet banking is also perceived as high risk zone for electronic frauds and scams .Most of the people therefore do not prefer internet banking for various reasons which are as follows;

LACK OF SKILLED STAFF
1 Poor infrastructure & Low speed internet and poor connectivity

2 Lack of security and confidentiality

3 Limited knowledge and skill about internet at information technology.

4 Lack of evidence and faith.

5 Inadequate and inefficient regulatory mechanism.

ISSN 2394 - 7780

CONCLUSION

To conclude the above discussion it can be said that awareness and education is the key and solution to this problem.

R.B.I has issued strict mandates through its websites in this regard.

Most of the fauads occurred when there is laxity in security issues so as corrective measures the systems must be upgraded regularly and the consumers must be trained and informed accordingly.

It's necessary to have a strict legal mechanism to deal with malwares, social engineering, **DDOS** i.e. **Distributed Denial of Services**, and phishing

LIST OF REFERENCES AND BIBLIOGRAPHY

1 Report of National Institute of Public Finance and Policy.

2 White paper presented in parliament on black money

3 Report on Crimes in India by National Crime Record Bureau..

4 Various Websites and Journals.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019
ISSN 2394 - 7780

CYBER INTELLIGENCE, CYBER FORENSICS AND INVESTIGATION

Pranita Ingale

ABSTRACT

The objective of cyber Security is to safeguard programs, application, networks, computers and data from attack. In a computing context, security includes both cyber and physical security. Cyber security refers to the body of technologies, processes etc designed to guard networks, devices, programs, and information from attack, damage, or unauthorized access. Cyber security may additionally be brought up as data technology security. Cyber security includes of the hardware, application, networks and protecting against harm that may come via networks. In this paper we intend to plan a study of Cyber Security and its components. We additionally offer numerous security aspects connected with cyber security.

INTRODUCTION

What Is Cyber-Security?

Despite the recent increase of public media coverage, cyber security has been the subject of serious discussion in government, industry and academics. Cyber security is that the combination of policies and practices to forestall and monitor computers, networks, programs and datafrom unauthorized access or attacks that are aimed for exploitation.

The Importance of Cyber Security

Cyber security is very important as a result of government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that information are often sensitive data or other types of data for which unauthorized access or exposure could have negative consequences. As the volume and class of cyber attacks grow, corporation and organizations, particularly those who square measure tasked with safeguarding data with reference to national security, health, or monetory records, need to take steps to protect their information. As early as March 2013, the nation's prime intelligence officers cautioned that cyber attacks and digital spying are the top threat to national security, eclipsing even terrorism.

The three pillars of cyber security

1. People: Everyone needs to be aware of their role in preventing and reducing cyber threats, and specialised technical cyber security staff need to stay fully up to date with the most recent skills and qualifications to mitigate and answer to cyber attacks.

2.Processes

Processes are crucial in shaping the organisation's activities, roles and documentation accustomed to mitigate the risks to the organisation's data. Cyber threats modify quickly, thus processes got to be frequently reviewed to be able to adapt aboard them.

3.Technology

By characteristics of the cyber risks that your organisation faces you'll then begin to seem at what controls to place in situation, and what technologies you'll need to do this. Technology is deployed to forestall or cut back the impact of cyber risks, looking on your risk assessment and what you consider a suitable amount of risk.

- **Application Security**
  Application security is the use of software, hardware, and procedural methods to protect applications from external threats. Application security contains measures or counter-measures that are taken during the development life-cycle to protect applications from threats. Security measures built into applications and a sound application security routine minimize the likelihood that unauthorized code will be able to manipulate applications to access, steal, modify, or delete sensitive data. Some of the techniques used embrace input parameter validation, session management, user authentication and authorization, etc.

- **Information Security**
  Information security is a set of strategies for managing the processes, tools and policies necessary to prevent, detect, document and counter threats to digital and non-digital information. Information security programs square measure designed round the core objectives like maintaining the confidentiality, integrity and availability of IT systems and business data. This refers to the protection of knowledge and data from larceny, unauthorized access, breaches, etc. in order to uphold user privacy and forestall fraud.

ISSN 2394 - 7780

❖ **Email Security**
Email gateways are the number one threat vector for a security breach. It blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.

❖ **Mobile Device security**
Cyber criminals are increasingly targeting mobile devices and apps. Within consecutive three years, ninety percent of IT organizations could support company applications on personal mobile devices.

❖ **Web Security**
This is used to prevent and protect websites from cyber security risks on the internet. Holistic web site security programs can cowl the website's information, applications, supply codes and files. There contains a steady rise within the variety of information breaches on websites within the past few years leading to identity thefts, downtime, financial losses, loss of reputation and brand image, etc. The main reason for this has been the misunderstanding among website homeowners that their web site is protected by web site hosting supplier. Thus, leaving them vulnerable to cyber-attacks. Some of the important techniques and tools used for website security are website scanning and malware removal, website application firewall, application security testing, etc

❖ **Wireless Security**
Wireless networks aren't as secure as wired ones. Without demanding security measures, putting in a wireless Local Area Network are often like golf stroke LAN ports everyplace as well as the parking zones. To prevent an exploit from taking hold, user need products specifically designed to protect a wireless network.

❖ **Endpoint security**
This allows organizations to guard their servers, workstations and mobile devices from remote and native cyber-attacks. Endpoint security effectively secures the network by obstruction tries created access these entry points. File integrity monitoring, antivirus and anti-malware software, etc. are major techniques used.

➢ **Types of cyber security threats**
The process of maintaining with new technologies, security trends and threat intelligence can be a tough task. However, it's a necessity so as to shield data and alternative assets from cyber threats, that take several forms.

- **Ransom ware :** is a type of malware that involves an attacker locking the victim's computer system files via encryption and demanding a payment to decrypt it.
- **Malware:**
- **Social engineering :** Tricking humans on social basis to gain sensitive information.
- **Phishing :** It is a form of sending emails in-order to gain customers data such as credit card details, bank details etc .

➢ **What cyber security can prevent**
The use of cyber security will facilitate forestall cyber attacks, knowledge breaches and fraud and may aid in risk management. When a corporation includes a sturdy sense of network security and a good incident response set up, it's higher ready to forestall and mitigate these attacks. For example, end user protection defends information and guards against loss or theft while also scanning computers for malicious code.

➢ **Cyber Security Parameters**
The parameters for Cyber security are as follows:
1. Identify threats
2. Identify vulnerabilities
3. Access risk explore
4. Establish contingency plan
5. Respond to cyber security accident

How to protect against cyber security attacks
The best way to mitigate the effects of a cyber attack is to build a solid foundation which will help to grow your cyber security technology stack.

ISSN 2394 - 7780

The problem arises once we begin adding IT security solutions from totally different makers the graininess of their configuration settings – technology gaps can invariably be gift.

And technology gaps will always appear for one simple reason: developers will always keep some portions of their code proprietary as part of their competitive advantage. Hence, true compatibility and ability could solely be ninetieth. These are known as technology gaps. It is through these gaps that attacks typically occur.

A solid cyber security foundation will identify these gaps and propose the appropriate action to mitigate the risk of an attack, enabling you to build a robust cyber security strategy.

Leadership commitment

It's terribly tough to determine, implement and maintain effective processes. Top management should be ready to take a position in cyber security measures. Cyber security ought to tend acceptably priority by the board to support more investment in technology, resources and skills.

Security attacks and types

Security Attack is any action that compromises the security of information owned by an organization using any process that designed to detect. There are many kinds of attacks, however most typically common security attacks are delineate below:

- **Denial of Service Attacks** : These attacks are mainly used to unavailable some resources like a web server to users. These attacks are very common today. The resource cannot method the flood of requests and either slows or crashes.
- **Brute Force Attacks** : These attacks try to kick down the front door. It's a trial-and-error commit to guess a system's parole. One in four network attacks could be a brute-force try.
- **Browser Attacks** : These attacks target end users who are browsing the internet. The attacks might encourage them to inadvertently transfer malware. These attacks used fake software update or application. Websites are also force to download malwares. The best ways in which to avoid browser-based network attacks is to frequently update internet browsers.
- **Shellshock Attacks** : These attacks are refers to vulnerabilities found in Bash, a common command-line shell for Linux and UNIX systems. Since several systems area unit never updated, the vulnerabilities are still present across the Web. The problem is therefore widespread that Shellshock is that the target of all networks.
- **SSL Attack :** These attacks are intercept data that is sent over an encrypted connection. These attacks successfully access to the unencrypted information. These attacks are also very common today.
- **Backdoor Attacks** : These attacks are used to bypasses normal authentication to allow remote access. These attacks are added in software by design. They are intercalary within the Programs or created by sterilization associate degree existing program. Backdoors is less common types.
- **Botnet attacks** : These attacks are hijackers. They are computers that are controlled remotely by one or more malicious actors. Millions of computers are often caught in a very botnet's snare.

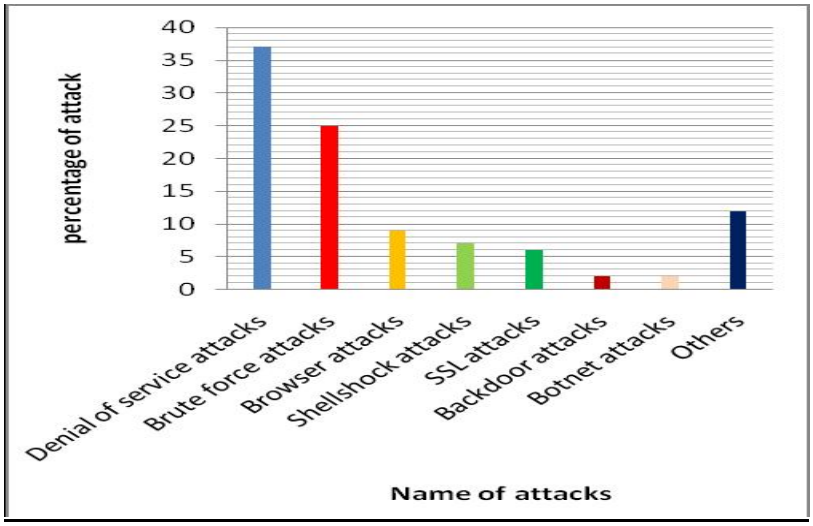


Figure Percentages of Various Attacks

ISSN 2394 - 7780

Guiding Principles for Public Policies to Advance Cyber security Analysis and Education :

1. Cyber security Analysis and Education as Public Policy Priorities : Strengthening cyber security analysis, education, and workforce development are vital to achieving overall cyber security policy objectives.

2. Cyber security as Many-sided and Multidisciplinary: Analysis and education policy approaches are effective given that they comprehend the many-sided and multidisciplinary nature of cyber security.

3. Cyber security and Privacy as Complementary : Security and private area unit are complementary issues, rather than tradeoffs. Planning should address both aspects.

4. Incorporate Security and Privacy : Security and privacy ought to be inbuilt as part of the culture, approaches, processes, systems, and technical infrastructures.

5. Cyber security Analysis and Development Funding: Analysis and development funding is indispensable to cyber security and innovation and desires to handle each security and privacy.

6. Research Opportunities in Higher Education: It provides opportunities for students and faculty to engage in high-impact research that are important to growing a strong research community.

7. Legal Protections for Privacy and Security Researchers : Governments ought to offer legal protections for people conducting legitimate and helpful computing privacy and security analysis.

8. Cyber security Education and Workforce Pipelines : Expanded access to cyber security and computing education at all levels is needed to prepare, build, and improve the workforce. Policy approaches should address diversity and inclusiveness.

9. Pedagogue Skilled Development : current skilled development permits educators to achieve and update their information and skills, and supports high-quality instruction to boost student learning.

10. Public-Private Coordination: Improved coordination of general public and personal sectors is required to deal with cyber security analysis and education.

11. Public Engagement : Cyber security public informative boards, research review boards, and public forums should include representation from the computing field.

12. International Cooperation : Cyber security challenges and advantages flow across borders and globally interconnected systems

CONCLUSION

Computer security may be a large topic that's changing into a lot of necessary as a result of the globe is changing into extremely interconnected, with networks getting used to hold out essential transactions. Cyber crime continues to diverge down completely different methods with every twelve months that passes then will be the safety of the data. There is no perfect solution for cyber crimes but we should try our level best to minimize them in order to have a safe and secure future in cyber space.

REFERENCES

- http://www.cs.georgetown.edu/~denning/index.html
- http://www.ists.dartmouth.edu/ISTS/
- http://www.crime-research.org/
- http://www.ijcsmc.com/docs
- http://digitalguardian.com
- http://www.cyberdegrees.org

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

NECESSITY OF CYBER SECURITY AWARENESS AMONG GRADUATE STUDENTS: A CASE STUDY OF BHARATI VIDYAPEETH NAVI MUMBAI

Prof. Abhijit S Desai and Prof. Manish Kumar Dubey
Bharati Vidyapeeth's Institute of Management and Information Technology, Navi Mumbai

Abstract
Cyber security is becoming a necessity for the students who are willing to complete the projects using SDLC life cycle. In spite of so many security measures and tools available for the purpose of securing your digital assets, there is a need of awareness about it amongst the students. Nowadays, graduate students are equipped with latest gadgets, which helps them in learning process. This study aims to understand the levels of cyber security awareness amongst the graduate students of Bharati Vidyapeeth Educational Complex, Navi Mumbai. In this study, 125 graduate students from various disciplines are selected as respondents. A survey instrument was prepared on the basis of parameters about cyber security awareness and circulated among the students. The responses were tabulated and analysed to measure the level of cyber security awareness among the students. This study reveals that compared to previous studies, now awareness about cyber security is increased but not at significant level. Therefore, there is a necessity to increase the awareness of cyber security along with its tools among the graduate students.

Keywords: Cyber security awareness, digital assets, gadgets, security tools.

Introduction

Technological advancements in the recent years made the challenges in the implementation of cyber security. Today's students are using payment gateways to implement in their academic projects without having awareness about various cyber threats for making secure payments online. This is not only the case where cyber security is implemented; there are several other incidents also where cyber security is playing important role in the project. Students who are beginners and implementing digital payments gateway, we conclude that this study is important in the aspect of creating and analyzing awareness of cyber security. Social media also allow to implement the cyber security.

For this study, researchers has included a number of graduate students of computer application course to measure the extent of security awareness level among them.

Cyber Security awareness

Security awareness is knowledge combined with attitudes and behaviors that serve to protect our information assets. Being cyber security aware means you understand what the threats are and you take the right steps to prevent them.

Security awareness in terms of cyber security describes the information threats that allows to enter in anybody's computing environment and restricting to perform necessary steps. There is a need of formal security awareness training workshops and seminars for all students before completion of their course and those who are using online payment gateways to make digital payments should ensure that proper security measures are available and properly implemented.

Security awareness are forced to implement for secure digital payments and giving user a message the payment is secured for both the parties, sender as well as receiver also.

Awareness is defined in NIST Special Publication 800-16 as follows: "Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance".

Cyber security

Cyber security is one of the important parameter to implement modern computer societies by the user for daily computing activities. Businesses are now turning to the Internet to increase their exposure as well as extending services, such as online banking and online shopping. The growth of users using the digital payments is increasing day by day, therefore the digital payment has become the important component to make the payment to the receiver. Multiple levels of securities is implemented to make the secure payments.

ISSN 2394 - 7780

Methodology of the study

For the present study undertaken by the researchers, 125 graduate students of Computer Applications course from Bharati Vidyapeeth's Educational complex Navi Mumbai were selected as respondents. Taking into the consideration of cyber security awareness aspect, a well drafted survey instrument was designed and circulated among the selected respondents. Before filling up the responses in the survey instrument, respondents were briefed about the nature of questions and objective of the study undertaken, which helped the respondents to provide proper and correct answers while filling up the questionnaire.

All responses given by the respondents were tabulated using MS-EXCEL worksheet and later used for the analysis purpose. A detailed analysis was carried out to check the validity of the assumptions made at the beginning of the study. Next section of the present research paper is about data analysis and interpretation of the study undertaken.

Data analysis and Interpretation

Following table shows the questions included in the questionnaire designed to assess awareness and a sense of security for graduate students.

Q. No.	Question
1	Do you set your operating system to automatically download and apply updates?
2	Do you use any of the security application?
3	Approximately how often do you update the definition files for your antivirus programs?
4	How many different passwords do you use for different websites? Less than 4/ 4-10/ More than 10
5	Do you share any of your passwords with other people?
6	Do you set your web browser to save passwords (including payment gateways) for you?
7	Is it important to worry about cyber security?
8	Keeping my digital assets secure, helps keep other's digital assets secure.
9	I am very careful about downloading from the internet.
10	I am very careful about opening attachments or links received in an email or message
11	I am very careful about performing any online payment transactions using payment gateways.
12	Would you attend a free 3-hour workshop/seminar on cyber security awareness, if any such is offered by the institute/college?

Table - 1: Questions related to the cyber security awareness

Responses given by the respondents were recorded, where the data is analyzed on the basis of answers given to the various questions mentioned in the above table. The responses were aggregated to find out the awareness level of the student about cyber security.

The table below shows number of male and female students selected as a part of the respondents. There are 44 % male students and 56 % female students selected as respondents.

Item	Category	Frequency	Percentage	Cumulative Percentage
Gender	Male	55	44%	44%
	Female	70	56%	100%
	Transgender	0	0%	0 %
Total		125	100%	100%

Table - 2: Respondents based on the Gender

The selected respondents also categorized by the year of graduation of their studies. The table below shows number of male and female students selected as a part of the respondents. There are 43.2% first year students, 26.4% second year students and 30.4% students from third year.

ISSN 2394 - 7780

Item	Category	Frequency	Percentage	Cumulative Percentage
Year of Graduation	First Year	54	43.2%	43.2%
	Second Year	33	26.4%	69.6%
	Third Year	38	30.4%	100%
Total		125	100%	100%

Table - 3: Respondents based on the Year of Graduation

Responses of the student were tabulated on the extent of awareness and non awareness of students for each question from the questionnaire, which is shown in the following tabular format.

Q. No.	Male students(55)		Female Students(70)	
	Awareness		Awareness	
	Count	Percentage	Count	Percentage
1	45	81.82	62	88.57
2	42	76.36	58	82.86
3	25	45.45	33	47.14
4	12	21.82	26	37.14
5	22	40.00	9	12.86
6	34	61.82	46	65.71
7	37	67.27	55	78.57
8	31	56.36	60	85.71
9	36	65.45	55	78.57
10	38	69.09	49	70.00
11	41	74.55	53	75.71
12	29	52.73	65	92.86
	Average	59.39	Average	67.98

Table - 4: Cyber security awareness based on gender

It is observed that, the cyber security awareness is 59.39 % among male students and 67.98% in female students.

Q. No.	**First Year students(54)**		**Second Year Students(33)**		**Third Year Students (38)**	
	Awareness		**Awareness**		**Awareness**	
	Count	**Percentage**	**Count**	**Percentage**	**Count**	**Percentage**
1	22	40.74	28	84.85	34	89.47
2	30	55.56	22	66.67	33	86.84
3	21	38.89	28	84.85	30	78.95
4	29	53.70	21	63.64	32	84.21
5	33	61.11	28	84.85	34	89.47
6	32	59.26	23	69.70	31	81.58
7	28	51.85	22	66.67	28	73.68
8	30	55.56	28	84.85	34	89.47
9	29	53.70	24	72.73	27	71.05
10	27	50.00	28	84.85	28	73.68
11	30	55.56	25	75.76	34	89.47
12	29	53.70	27	81.82	29	76.32
	Average	52.47	Average	76.77	Average	82.02

Table - 5: Cyber security awareness based on the Year of Graduation.

It is observed that the cyber security awareness is 52.47 % in First year students, 76.77 % in second year students and 82.02 % in third year students.

Findings, Suggestion and Conclusion

From the present research study, researchers found that the awareness in increased among the students while completing their graduation by attending seminars/workshops and training programs. It is also identified that girl students are more aware compared to the boys. Some of the students needed more awareness by providing

ISSN 2394 - 7780

them seminar on particular topics on cyber security. It is also recommended that institutes should conduct regular seminars on cyber security awareness for its students.

References

[1] Pci data security standard (pci dss) october 2014 security awareness program special interest group pci security standards council.

[2] NIST, Information technology security training requirements: A role- and performance-based model, NIST —SP800-16, USA, 1998, available at http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf (last visited on 21 July 2008).

[3] building an information technology security awareness and training program mark wilson and joan hash, nist special publication 800-50.

[4] computer security division information technology laboratory national institute of standards and technology gaithersburg, md 20899-8933 october 2003.

[5] Infoworld.com, "What Cloud Computing Really Means," April2008, http://www.infoworld.com/ article/08/ 04/07/15FE-cloud-computing-reality_1.html.

[6] eweek.com, "Americans Confused as Ever Over Cyber-Security", October 2008, http://www.eweek.com/c/a/ /Security/Americans-Confused-As-Ever-Over-Cyber-Security/

[7] Darkreading.com, "CSRF Flaws Found on Major Websites", September 2008, http://www.eweek.com/ c/a /Security/Americans-Confused-As-Ever-Over-Cyber-Security/

[8] http://www.jadwa.com/ar/article/global/terms-conditions.html.

[9] survey on security awareness among social networking users in malaysia , iskandar ishak, fatimah sidi, marzanah a. jabar, nor fazlida mohd sani, aida mustapha, siti rozana supian ,australian journal of basic and applied sciences, 6(12): 23-29, 2012, issn 1991-8178.

[10] measuring computer security awareness on internet banking and shopping for internet users , 1fatimah sidi, 2marzanah a. jabar, 3aida mustapha, 4nor fazlida sani, 5iskandar ishak, 6siti rozana supian , journal of theoretical and applied information technology 20th july 2013. vol. 53 no.2, issn: 1992-8645.

[11] 11 the need for effective information security awareness, fadi a. aloul, journal of advances in information technology, vol. 3, no. 3, august 2012.

[12] andrew valentine, 2006, 'enhancing the employee security awareness model', cyber trust's icsa labs, p.17-19.

[13] a quantitative study on japanese workers' awareness to information security using the data collected by web-based survey, american journal of economics and business administration 2 (1): 20-26, 2010, issn 1945-5488.

[14] W. Hubbard. Methods and Techniques of Implementing a Security Awareness Program. SANS Institute, 2002.

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

REVIEW OF IOT FORENSIC INVESTIGATION

Amit Gangal
RTO, Wadala, Mumbai

ABSTRACT

Challenges for IoT-based forensic investigations include the increasing amount of objects of forensic interest, relevance of identified and collected devices, blurry network boundaries, and edgeless networks. As we look ahead to a world of expanding ubiquitous computing, the challenge of forensic processes such as data acquisition (logical and physical) and extraction and analysis of data grows in this space. Containing an IoT breach is increasingly challenging - evidence is no longer restricted to a PC or mobile device, but can be found in vehicles, RFID cards, and smart devices. Through the combination of cloud-native forensics with client-side forensics (forensics for companion devices), we can study and develop the connection to support practical digital investigations and tackle emerging challenges in digital forensics. IoT brings anything and everything "online" in a connectedness that generates an explosion of connected devices, from fridges, cars and drones, to smart swarms, smart grids and intelligent buildings. The explosive growth of smart objects and their dependency on wireless technologies for communication increases the vulnerability of Internet of Things (IoT) to cyberattacks. Cyberattacks faced by IoT present daunting challenges to digital forensic experts.

Keywords : Digital Forensics, IoT, Security, Cybercrime.

INTRODUCTION

The Internet of Things (IoT) devices, such as smartphones, washing machines, and medical implants, has empowered people to share facts with each other. These devices can communicate with each other directly or via Application Programming Interface (API) over the Internet, and they can be controlled by learned devices with high computing capabilities, such as cloud servers, that augment smartness to low-computing devices. The smartness and communication capabilities of IoT devices o□er many beneficial applications to common people, companies, industry, and governments. IoT application is also extended in the areas of transportation, healthcare, and smart cities. In addition, the market trend of IoT is increasing. However, emerging IoT technologies face various security attack-sand threats. Notable threats include virus attacks, mass surveillance, and Denial of Service (DoS) attacks, and disruption of IoT networks. To investigate these attacks, well-trained teams must conduct a digital investigation, known as IoT forensics. The sources of evidence in IoT forensics include home appliances, cars, medical implants, sensor nodes, and tag readers, among others. In traditional forensics, the sources of evidence can be computers, mobile phones, servers, or gateways. The evolutionary background of IoT lies in the advancement of the technology on micro sensor devices in the later 90s. Specifically, the advancements in microprocessors, memory technology and more importantly micro sensing devices led to the development of tiny sensors. These sensors are then equipped with radio communication capability on battery energy which enabled unattended intelligent sensing devices that can gather, process and transmit data. Early sensors have very scarce resources in terms of memory which makes data storage almost impossible for forensics purposes. Typically, there were two cases where memory was used:

1) User memory used for storing application-related or personal data; and
2) Program memory used for programming the device. This memory also contains identification data if the device has any.

DIGITAL FORENSICS

In IoT it is a challenge especially when it comes to accuracy due to the intensity of analysis. This results in data sometimes losing its granularity as systems may store, use, or present different semantics however, it does have the ability to adopt dissimilar formats, and may hold a proprietary format. Taking into the heterogeneity of data that IoT devices generate it is even more challenging. The following questions must be answered before the investigation is being performed in order to avoid inadmissibility of evidence.

- Can data be collected from the devices using available tools?
- Is the data propriety?
- How can it be analysed?
- Are forensic tools compatible with this data?

ISSN 2394 - 7780

Most of the challenges in IoT forensics are also available particularly at the data storage and network levels. However, with the rapid tendency towards the usage of effcient, low memory footprint and low power devices in the industry, devices will be less likely to keep data stored in memory.

IoT FORENSICS

IoT technology is a combination of many technology zones: IoT zone, Network zone and Cloud zone. These zones can be the source of IoT Digital evidences. That is, an evidence can be collected from a smart IoT device or a sensor, from an internal network such as a firewall or a router, or from outside networks such as Cloud or an application. Based on these zones, IoT has three aspects in term of forensics: Cloud forensics, network forensics and device level. Most of IoT devices have the ability to cross Internet (direct or indirect connect) through applications to share their resources in the Cloud. With all valuable data that store in the Cloud, it has recently became one of the most important targets for attackers.

TRADITIONAL DIGITAL FORENSICS AND IoT FORENSICS

In traditional forensics, the examiner can hold the digital equipment and then apply the investigation process to extract the evidence. However, in IoT forensics, it is a different scenario, the evidence could be separated in multi-location which is rising many challenges in terms of acquisition of data from the Cloud. In addition, examiners have limited control and access to seize the digital equipment and getting an exact place of evidence could be a challenge. Besides, data could be stored in a different location in the Cloud, resulting in no evidence could be seized. As all Cloud services use Virtual Machine as servers, data volatile like registry entries or temporary Internet files in these servers could be erased if they not synchronized with storage devices. For instance, if these servers are restarted or shutdown, the data could be erased. Network Forensics include all different kinds of networks that IoT devices used to send and receive data. It could be home networks, industrial networks, LANs, MANs and WANs. For instance, if an incident occurs in IoT devices, all logs that traffic flow that has passed throw, could be potential evidence such as firewalls. Device Level Forensics include all potential digital evidence that can be collected from IoT devices like graphics, audio, video. Videos and graphics from CCTV camera or audios, can be great examples of digital evidences in the device level forensics.

CHALLENGES IN IOT FORENSICS

Following are the challenges in IoT forensics:

- Data location.
- Lifespan limitation of digital media.
- Cloud service requirement.
- Lack of security.
- Device type.
- Data format.

IoT technology has presented a significant shift in investigation field, especially in how it interacted with data. However, there are some challenges in terms of IoT forensics. Many of IoT data are spread in different locations which are out of the user control. This data could be in the Cloud, in third party's location, in mobile phone or other devices. Therefore, in IoT forensics, to identify the location of evidence is considered as one of the biggest challenges can investigator faced in order to collect the evidence. In addition, IoT data might be located in different countries and be mixed with other users information. One of the challenges is the period of survival of the evidence in IoT devices before it is overwritten. Transferring the data to another thing such as local Hub or to the Cloud could be an easy solution to solve this challenge. However, it present another challenge that related to securing the chain of evidence and how to prove the evidence has not been changed or modified. Security lack Evidence in IoT devices could be changed or deleted because of lack of security, which could make these evidence not solid enough to be accepted in law court. For instance, in the market, some companies do not update their devices regularly or at all or sometimes they stop supporting the device's framework when they focus on a new product with the new infrastructure. As a result, it could leave these devices vulnerable as hacker found a new vulnerability. Usually, evidence source is types of a computer system such as computer and mobile phone. However, in IoT, the source of evidence could be objects like a smart refrigerator or smart coffee maker. Therefore, the investigators will face some challenges. The format of the data that generated by IoT devices is not matching to what is saved in the Cloud. In addition, user have no direct access to his/her data and the data presents in different format than that in which it is stored. Moreover, Data could be process using analytic functions in different places before be stored in the Could. Hence, in order to be accepted in a law court, data form should be returned to original format before performing analysis.

ISSN 2394 - 7780

CONCLUSION

The IoT offer a significant source of potential evidence, however due to their heterogeneous nature and the ways in which data is distributed, aggregated, and processed, there are challenges that the digital forensics investigations must overcome. For this purpose, new techniques are required to not only overcome the hurdles, but also influence the architecture and processes in order to gain access to this rich source of potential evidence in the IoT environments. In this paper, we explained digital forensics challenges in IoT environments. We also analysed and explained currently available solutions to overcome some of those challenges from different perspectives.

REFERENCES

- https://www.engpaper.com/iot-2018.htm
- https://ieeexplore.ieee.org/xpl/RecentIssue.jsp?punumber=6488907
- http://www.academia.edu/Documents/in/IOT

International Journal of Advance and Innovative Research
Volume 6, Issue 1 (XXXIV): January - March, 2019

ISSN 2394 - 7780

ADVANCE FORENSIC INVESTIGATION

Pallavi V. Deshmukh and Shakuntala P. Kulkarni
J.V.Ms Mehta Degree College, Navi Mumbai

ABSTRACT

The Discipline of Digital Forensics deals with the Identification, collection, analysis, and presentation of digital evidence from various types of digital/electronic storage media in a Litigation/Cybercrime or information security incidents. The proliferation of IoT devices and the increased number cyber security incidents on the IoT devices/applications has necessitated the collection and analysis of digital evidence from different types of IoT devices and came to be known as IoT Forensics, a subdivision of Digital Forensics. IoT Forensics requires a multi-faceted approach where evidence may be collected from a variety of sources such as sensor devices, communication devices, cloud storage etc.

The purpose of IoT forensics is to identify and obtain digital evidence from IoT devices for legal or investigative purposes.

A stream of digital forensic focusing on recovery and analysis of data of drone device used in crime as Drone forensic. Drone being a wireless device, subsystem of Drone is included in wireless forensic model. Server is also included in the operation. Server controls Drone at ground level. Information is present in the server at ground level.

Keywords: IoT forensics, Drone forensics, Digital forensics

INTRODUCTION

Cyber Crime means criminal activities carried out where either computer is used for crime or computer is a victim. The information stored on the computer is the target of the crime, with the intention of damaging its integrity, confidentiality or availability. Cybercrime is increasingly affecting a variety of domains: Government systems, large organisations, small to medium enterprises, E-commerce, online banking, and critical infrastructure.

Previously, criminal investigations generally relied on the analysis of physical evidence, the study of the crime scene, witnesses and interviews with suspects. In case of Cyber Crime the evidence is in the form of digital evidence. The vulnerability of Internet of Things (IoT) to cyberattack increases as there is increase in the use of smart objects and there is also an increase in the dependency on wireless technologies. Cyberattacks faced by IoT present daunting challenges to digital forensic experts. Various forensic techniques are adopted to investigate such attacks.

Internet of Things (IoT) refers to a network of connected physical devices, smart home appliances, wearable electronic devices and embedded electronic items etc. with different types of sensors for seamless connectivity and transfer of data amongst them. Some common examples for the IoT devices include Smart home accessories such as smart locks, sensors for temperature, ambient light, water, gas etc., and wearables such as smart watches, glasses, pacemakers and fitness gear and includes components such as M2M (Machine to Machine communications), RFID sensors, wearable and context-aware computing. Interception of cardiac devices such as pacemakers, Patient/Infant monitoring systems, Launching DDOS attacks using compromised IoT devices (Mirai Botnet), Hacking/Interception of In-Vehicle Infotainment (IVI) systems, Hacking of various CCTV and IP cameras are some of the examples of IoT device hacking incidents.

Drone is also known as UAV (Unnamed Aerial Vehicle). There is a great increase in the criminal cases involving drone. The Drone Forensics is a subsystem of Wireless Forensics (Wi-Fi Forensics). Wireless Forensics is a part of Digital Forensics. So Drone forensics is a category of Digital forensics.

An aircraft which has no pilot on board or a remotely controlled aircraft is known as UAV (Unmanned Aerial Vehicle). This UAV is often called Drone. Drone rules and regulations are set by Federal Aviation Administration (FAA) which is a US body. Certificate of Authorization (COA) is needed from FAA to fly UAV in the US for non- recreational purpose.

BACKGROUND

IoT has many emerging devices and trends. The IoT has the same monitoring requirements from cloud computing. But the challenges related to IoTdepend on the characteristics of volume, variety, and velocity. The IoT does not replace the existing ICT or operational technology networks; rather, it enhances these networks and relies on them in many ways. There is an estimation that by 2020 there will be 50 billion IoT devices. There is requirement to

ISSN 2394 - 7780

pay specific attention to transportation, storage, access, and processing of the huge amount of data generated by these devices. The IoT merges the data of the real and digital world, with the help of new IoT devices which are being created that store data. This is a problem for forensic expert as they have to find new ways to extract and safeguard the data. They also have to take care that the evidence is not manipulated while extracting. Solution has to be found to these problems related to extracting, storing and analyzing data seized from IoT devices. Solution can be found by analysing how these evidence can be correctly seized, stored, extracted, and analysed. Presently, there is a standardised methodology for retrieving evidence from hard drives, laptops, computers and mobile phones but there are no clear procedures for IoT-based investigations.

Drone has been used in crime like killing human, unlawful video or image capturing etc. If Drone can be used in doing crime then Drone can also be used in investigating a crime.The main intention of inventing Drone was that it can be used for recreational activities. It can also be used for education purpose, entertainment purpose, security purpose. Drone could also be used during wars to spy the enemies and their activities. Drone if deployed with weapons can cause mass destruction. A technology which was designed for good purpose, started being harmful as it is used for bad deeds. So the evolvement of drone in crime has sought the attention of forensic researchers towards Drone Forensics. Drone Forensics involves the forensics of the drone device, extracting and analyzing data from that device.

CHALLENGES

There are many challenges related to IoT devices. Challenges include the many objects of forensic interest, blurry network boundaries, and edgeless networks. The challenges also include extraction of physical and logical data, analysis of the data, storage of the data. IoT breach is a major challenge. Evidences to be extracted are no longer restricted to a PC or mobile device, but can be found in vehicles, RFID cards, and smart devices. IoT has major challenged for investigation. Same is the case with IoA (Internet of Anything). IoA brings anything and everything “online” in a connectedness that generates an explosion of connected devices, from fridges, cars and drones, to smart swarms, smart grids and intelligent buildings. There is a need to identify methods for performing IoT-based digital forensic analysis. The goal is to develop digital forensic standards that can be used for IoT and IoA security. Standards can also help IoT-based investigations. Digital evidence are in the form of many things.Hard drive of the computer of the criminals, laptop, external hard drives, mobile phone devices, etc. are the places where the main evidence can be found. There can be large amount of data, data can be of different format. Data is stored in different devices. So to extract the data and analysing of the data can be time consuming. Hence, there is a need to change the method to aextract and analyse the data from IoT devices to save time. TheIoA brings anything and everything “online” . The devices like fridges, cars and drones, to smart swarms, smart grids and intelligent buildings are all brought online in this Internet of Anything era. The main IoT/IoA challenge from a forensic point of view is that of data acquisition. Exactly where the data is stores and from where the data can be extracted is the main challenge of the forensic expert. Another major challenge related to civilian drone usage is privacy. The concern of the common people is that drone may take illegal photos of the people without them being aware of that. There should be proper law enforcement for the usage of drone. There should be proper balance between what use of drone is acceptable for private use and what is not. Drones are not simply flying machines, but contain information. Drone collects lot of information, hence it becomes troublesome that what all information must be used and what not to use. It is also a challenge to identify the data collected by drone which can be accepted in the court of law. It is being said that data acquired using a drone should be considered to be valid like data collected usingany other tool like mobile phones, smart watches, etc.

CONCLUSION

As there is significant increase in the ToT devices, there is a need to develop a standard procedure for the investigation of the crime related to IoT devices. There is major challenge in extracting and analysing data related to IoT devices. Since as of now there is no methodology to investigate IoT devices, investigation completely relies on mechanical and physical nature of the smart device. Currently computer forensic and cyber security investigators are exploring the IoT from the perspective of a computer forensic analyst with regards to evidence handling, evidence extraction, and analysis of the collected data. Sensors which are fixedin homes and buildings, sensors built into cars and wearable devices which are moving sensors, communication devices, can be used as source od data. Evidence can be collected from these devices.There are many challenges related to ToT devices which remain unanswered. Further study in this emerging field will give more methods to extract and analyse data related to IoT devices.

The different types of drones can be differentiated by the type (whether it is fixed-wing, multirotor or something else), the degree of autonomy, the size, weight, and the power source. These different technical specifications

ISSN 2394 - 7780

are factors which are used for determining the drone's capabilities. The capabilities of the drone are measured in terms of it's range, flight duration, and loading capacity. Drone collects a lot of information. It may invade someone's privacy also. So there is a need to give guidelines to what extent drone can be used. When the data is extracted from the drone, there is also a challenge to identify data that can be accepted in the court of law.

REFERENCES

1) K. Pieper, M. Tang, and M. Edwards, "Flint water crisis caused by interrupted corrosion control: Investigating 'ground zero' home," Environ. Sci. Technol., vol. 51, no. 4, 2017, pp. 2007–2014.

2) A. Sheth, "Computing for Human Experience: Semantics-Empowered Sensors, Services, and Social Computing on the Ubiquitous Web," IEEE Internet Computing, vol. 14, no. 1, 2010, pp. 88–91

3) Applications of Unmanned Aerial Vehicle (UAV) Technology for Research and Education in UAE Khaula Alkaabi* and Abdelgadir Abuelgasim Department of Geography and Urban Planning, College of Humanities and Social Science

MANUSCRIPT SUBMISSION

GUIDELINES FOR CONTRIBUTORS

1. Manuscripts should be submitted preferably through email and the research article / paper should preferably not exceed 8 – 10 pages in all.
2. Book review must contain the name of the author and the book reviewed, the place of publication and publisher, date of publication, number of pages and price.
3. Manuscripts should be typed in 12 font-size, Times New Roman, single spaced with 1" margin on a standard A4 size paper. Manuscripts should be organized in the following order: title, name(s) of author(s) and his/her (their) complete affiliation(s) including zip code(s), Abstract (not exceeding 350 words), Introduction, Main body of paper, Conclusion and References.
4. The title of the paper should be in capital letters, bold, size 16" and centered at the top of the first page. The author(s) and affiliations(s) should be centered, bold, size 14" and single-spaced, beginning from the second line below the title.

First Author Name1, Second Author Name2, Third Author Name3

1Author Designation, Department, Organization, City, email id

2Author Designation, Department, Organization, City, email id

3Author Designation, Department, Organization, City, email id

5. The abstract should summarize the context, content and conclusions of the paper in less than 350 words in 12 points italic Times New Roman. The abstract should have about five key words in alphabetical order separated by comma of 12 points italic Times New Roman.
6. Figures and tables should be centered, separately numbered, self explained. Please note that table titles must be above the table and sources of data should be mentioned below the table. The authors should ensure that tables and figures are referred to from the main text.

EXAMPLES OF REFERENCES

All references must be arranged first alphabetically and then it may be further sorted chronologically also.

- **Single author journal article:**

Fox, S. (1984). Empowerment as a catalyst for change: an example for the food industry. *Supply Chain Management*, *2*(3), 29–33.

Bateson, C. D.,(2006), 'Doing Business after the Fall: The Virtue of Moral Hypocrisy', Journal of Business Ethics, 66: 321 – 335

- **Multiple author journal article:**

Khan, M. R., Islam, A. F. M. M., & Das, D. (1886). A Factor Analytic Study on the Validity of a Union Commitment Scale. *Journal of Applied Psychology*, *12*(1), 129-136.

Liu, W.B, Wongcha A, & Peng, K.C. (2012), "Adopting Super-Efficiency And Tobit Model On Analyzing the Efficiency of Teacher's Colleges In Thailand", International Journal on New Trends In Education and Their Implications, Vol.3.3, 108 – 114.

- **Text Book:**

Simchi-Levi, D., Kaminsky, P., & Simchi-Levi, E. (2007). *Designing and Managing the Supply Chain: Concepts, Strategies and Case Studies* (3rd ed.). New York: McGraw-Hill.

S. Neelamegham," Marketing in India, Cases and Reading, Vikas Publishing House Pvt. Ltd, III Edition, 2000.

- **Edited book having one editor:**

Raine, A. (Ed.). (2006). *Crime and schizophrenia: Causes and cures.* New York: Nova Science.

- **Edited book having more than one editor:**

Greenspan, E. L., & Rosenberg, M. (Eds.). (2009). *Martin's annual criminal code:Student edition 2010.* Aurora, ON: Canada Law Book.

- **Chapter in edited book having one editor:**

Bessley, M., & Wilson, P. (1984). Public policy and small firms in Britain. In Levicki, C. (Ed.), *Small Business Theory and Policy* (pp. 111–126). London: Croom Helm.

- **Chapter in edited book having more than one editor:**

Young, M. E., & Wasserman, E. A. (2005). Theories of learning. In K. Lamberts, & R. L. Goldstone (Eds.), *Handbook of cognition* (pp. 161-182). Thousand Oaks, CA: Sage.

- **Electronic sources should include the URL of the website at which they may be found, as shown:**

Sillick, T. J., & Schutte, N. S. (2006). Emotional intelligence and self-esteem mediate between perceived early parental love and adult happiness. *E-Journal of Applied Psychology, 2*(2), 38-48. Retrieved from http://ojs.lib.swin.edu.au/index.php/ejap

- **Unpublished dissertation/ paper:**

Uddin, K. (2000). A Study of Corporate Governance in a Developing Country: A Case of Bangladesh (Unpublished Dissertation). Lingnan University, Hong Kong.

- **Article in newspaper:**

Yunus, M. (2005, March 23). Micro Credit and Poverty Alleviation in Bangladesh. *The Bangladesh Observer*, p. 9.

- **Article in magazine:**

Holloway, M. (2005, August 6). When extinct isn't. *Scientific American, 293*, 22-23.

- **Website of any institution:**

Central Bank of India (2005). *Income Recognition Norms Definition of NPA.* Retrieved August 10, 2005, from http://www.centralbankofindia.co.in/ home/index1.htm, viewed on

7. The submission implies that the work has not been published earlier elsewhere and is not under consideration to be published anywhere else if selected for publication in the journal of Indian Academicians and Researchers Association.

8. Decision of the Editorial Board regarding selection/rejection of the articles will be final.