Volume 6, Issue 2 (XI)
April - June 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

HINDUSTHAN EDUCATIONAL AND CHARITABLE TRUST
HECT

Hindusthan
College of Arts & Science

An Autonomous College - Affiliated to Bharathiar University
Approved by AICTE and Govt. of Tamilnadu
Accredited by NAAC-An ISO Certified Institution

International Conference
on
"Future Networking: Internet of Everything"
ICIOE 2019

Sponsored under
DBT STAR COLLEGE SCHEME
Ministry of Science and Technology
Govt. of India

Organized by
Departments of B.Sc (CS), BCA, B.Sc (IT) and B.Sc (CT)
Hindusthan College of Arts and Science
Coimbatore

March 21st 2019

Publication Partner
Indian Academicians and Researcher's Association

Hindusthan College of Arts and Science

Coimbatore

Affiliated to Bharathiar University

Approved by AICTE and Govt of Tamilnadu

Accredited by NAAC

An ISO Certified Institution

Guest Editor of Special Issue

Dr. R. Rangaraj
Head and Associate Professor
Department of Computer Science
Hindusthan College of Arts and Science, Coimbatore

Dr. S. Sasikala
Associate Professor
Department of Computer Applications
Hindusthan College of Arts and Science, Coimbatore

ORGANIZING COMMITTEE

Chief Patron

Mr. T. S. R. Khannaiyann
Chairman
Hindusthan Educational and Charitable Trust, Coimbatore

Chairman

Tmt. Sarasuwathi Khannaiyann
Managing Trustee
Hindusthan College and Charitable Trust, Coimbatore

Patrons

Thiru. K. Sakthivel
Trustee Administration
Hindusthan Educational and Charitable Trust, Coimbatore

Tmt. Priya Satishprabhu
Executive Trustee and Secretary
Hindusthan Educational and Charitable Trust, Coimbatore

Co-Chairman

Dr. A. Ponnusamy
Principal,
Hindusthan College of Arts and Science, Coimbatore

Programme Chairs

Dr. R. Rangaraj
Head and Associate Professor, Department of Computer Science

Dr. P. Senthilvadivu
Head and Associate Professor, Department of Computer Applications

Dr. V. Saravanan
Head and Associate Professor, Department of Information Technology

Ms. K. Mythili
Head and Associate Professor, Department of Computer Technology
Hindusthan College of Arts and Science, Coimbatore

Organizing Committee

Editorial

Members of Editorial Advisory Board

ABOUT HINDUSTHAN EDUCATIONAL AND CHARITABLE TRUST

Hindusthan Educational and Charitable Trust, one of the finest in education and teaching is strategically placed in the heart of the city, and since 1992 has established itself firmly in the fields of Arts, Science, Education and Technical Education. The Trust aims at providing education that is world class and on the par with global standards. The Trust firmly believes in education from "Pre-KG to PhD" and is true to its motto – 'Get the best in everything'. The Management has always stood by its commitment to the betterment of the student community and had at first established itself as a brand in the 'Power Sector' and today in the field of Education has reigned supreme with the 'Life Time Educational Achievement Award' for giving back to Society. The Trust also believes in making education affordable to the underprivileged students and hose from the weaker strata of the society are given educational scholarships. The various institutions run by Hindusthan Educational and Charitable Trust are:

Hindusthan College of Arts and Science

Hindusthan College of Engineering and Technology

Hindusthan Institute of Technology

Hindusthan College of Education

Hindusthan Polytechnic College

Hindusthan Matriculation and Higher Secondary School

Hindusthan Kangaroo Kids Pre School

ABOUT THE DEPARTMENTS

Bachelor of Science (Computer Science)

PG & Research Department of Computer Science has started its functioning From the Academic Year 1998 with one Under Graduation BSc (Computer Science) and post graduationMsc(Computer Science) in the academic year 2005 ,headed by Dr.R.Rangarajwith 19 years of Experience. The Department is also offering the research programmes M.Phil in part time and full time Course from 2005 onwards. The department holds 3 Doctorates and 6 pursuing Doctorates among 15 faculties with average experience of 14 years. The department has produced University Ranks and many of the candidate with Distinction.

The Department has Signed for 6 MOU's with various organizations in and around Coimbatore. The Faculty Members Includes Journal Publishing, Organizing and attending FDP Programmes Conference and Seminars. They also show high involvement in Publishing papers and article in Journals, Conferences and Seminars. They combine the very highest standards of teaching and mentoring to change students as eminent entrepreneurs, policy makers, researchers, theoreticians and consultants for achieving excellence. The Department Conducts National Level, Seminars, Guest Lectures and Industrial Visits for upgrading the Knowledge and Skills of the Students. The students are placed in the various reputed Companies.

Bachelor of Computer Applications

The Department of Computer applications has laid down several goals for students enrolled in our program and its vision is dedicated towards academic excellence in computer applications. The course in our curriculum is designed to help students achieve specific learning objectives to acquire the up-to-date technical knowledge and develop the skills needed for a successful start to careers in the computing industry.The infrastructure of the department is well equipped to meet the recent industrial standards and has experienced faculty in different areas of specialization. There are 12 well qualified faculty members headed by Dr.P.Senthilvadivu with nearly 19 years of teaching, research experience and having 6 Ph.D scholars.

Among the faculty members2are Doctorates and 6 pursuing Doctorates and 1 qualified SET with average experience of 13 years. One Faculty Member Dr.S.Sasikala, received “Dr.A.P.J.Abdul Kalam Young Scientist Award” and “Innovative Women Academician Award” for innovating a new dataset in research. The Faculty Members took part inBook and Journal Publishing, Organizing and attending FDP Programmes Conference and Seminars.Periodically staff meeting is conducted for the exchange of views and discussions for all around development of the department and welfare of the student. There are 570 students in the department. The Students are trained for placements and are motivated to attend interviews with various companies even if they are placed.

Bachelor of Science (Information Technology)

The Department of Information Technology was established in the year 2007. It has the vision to “Evolve into a Centre of Excellence for Education and Research in Information Technology” through academic excellence, value added courses to produce highly competent and socially conscious information technology professionals. The Department offers one UG programme B.Sc. Information Technology since 2007 and one PG programme M.Sc. Information Technology since 2011. The Department is headed by Dr.Saravanan.V with 14 years of Teaching and Research experience and supported by well experienced and qualified faculty members.The area of specialization of the department faculties fall into areas like DataMining, Wireless Sensor Networks, Data Analytics, Information Security, Cloud Computing etc., The department has established industry linkage with various companies like SunSystems, Aram Foundation, Kalvi Institute. Both the students and faculty have been trained in contemporary areas and for industrial solutions. The top recruiters of students of our department include many top software companies like TCS, Wipro, HCL, Tech Mahindra, Mahindra Satyam etc. Around 90% of our students get recruited in the top companies through campus recruitment.

Bachelor of Science (Computer Technology)

The Department of Computer Technology has been established in 2008. Its main aim is to provide Quality, Technical education to tomorrow’s techno crafts and software professionals to expose them to recent development, to motivate them towards success and prepare them to face the future challenges, with confidence and courage.

The Department has B.Sc (Computer Technology) as three year programme. There are 8 dedicated faculty members headed by Mrs.K.Mythili with nearly 20 years of teaching and Research experience. The members are actively participating in journal publication, attending conferences, seminars, workshop in National Level and International Level. The department supports 372 students has two batches in I, II, III year.

The department has signed a MOU with leading IT sectors such as Prime Solutions Live Stream Technologies for the benefit of students. The department association CTECH is inaugurated by eminent personalities to conduct national level seminars, state level technical symposium, workshop and guest lectures to enrich their knowledge, to provide a platform for the students to exhibit their talents and showcase their interest in various domains. The department produces university rank consistently year by year. Many of our department students has been placed in following companies WIPRO Technologies, Tech Mahindra, TCS, CTS, Accenture, Infosys, VEE technologies, KGISL, Velan InfoTech, Asec Technology, etc…

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.

ABOUT CONFERENCE

The IoT is being called the fourth industrial revolution, and is expected to have a value of over $10trillion by 2025. The Internet of Everything (IoE) is a concept that extends the Internet of Things (IoT) emphasis on machine-to-machine (M2M) communications to describe a more complex system that also encompasses people and processes. This conference creates a technical platform to elevate in this regard of IoE, IoT and state of the art development cared out in this domain. The Conference is an International forum for the presentation of technological advances and research results in the fields of Computer Studies. The conference will bring together leading researchers, engineers, developers, scientists and practitioners from academia and industry working in all interdisciplinary areas of Computer Studies to share their experience, and share their ideas. The conference of ICIOE 2019 is organized by PG and Research Department of Computer Science, Department of Computer Applications, Department of Information Technology, Department of Computer Technology, Hindusthan College of Arts and Science, Coimbatore, Tamilnadu, India.

International Journal of Advance and Innovative Research

Volume 6, Issue 2 (XI): April - June 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 2 (XI) : April – June 2019

CONTENTS

Research Papers

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019

ISSN 2394 - 7780

A STUDY ON TEACHING TECHNIQUES USED FOR THE ANALYSIS OF THE AUTISTIC CHILDREN USING DATA MINING TECHNIQUE

R. Subalakshmi
Assistant Professor, Department of Computer Science, P. S. G College of Arts & Science

ABSTRACT
This study was designed to examine the behavior of Autistic Children Behavior using Applied Behavior, (ABA) Analysis therapy, PECS (Picture Exchange Communication System) and Social Story. Data is collected by behavioral intrusion while teaching children diagnosed with autism spectrum disorder. The disorder is characterized by a wide variety of possible symptoms such as developmental disabilities, extreme withdrawal, lack of social behavior, severe language and attention deficits, and repetitive behaviors. The symptoms intensity ranges from almost unnoticeable to very severe. Because of this wide variety of symptoms and intensity, therapy needs to be individualized for every person. On the other hand, the teaching techniques involves Applied Behavioral Analysis (ABA), PECS (Picture Exchange Communication System) and Social Stories. Data Mining Techniques analyzes the improvement of the children and it helps them in improving their behavior.

Keywords: Applied Behavior Analysis, Picture Exchange Communication System, DataMining

I. INTRODUCTION

AUTISM spectrum disorder (ASD) has become one of the most prevalent mental disorders over the last few years and its prevalence is still growing every year. It is a serious developmental disorder that afflicts children and that is more common than childhood cancer. The disorder is characterized by a wide variety of possible symptoms such as developmental disabilities, extreme withdrawal, lack of social behaviour, severe language and attention deficits, and repetitive behaviours. The symptoms intensity ranges from almost unnoticeable to very severe. Because of this wide variety of symptoms and intensity, therapy needs to be individualized for every person.

Therapeutic interventions that leverage information technology (IT) are still in their infancy in this area. The researcher's a like point to the need for more research and applications to help integrate autistic persons in society and help them and their families achieve a higher quality of life. They argue that it would be most beneficial if computer-aided learning software would focus on three main impairments: social and interpersonal skills, communication difficulties, and rigidity of thinking. The research can be classified into these three groups. Social and interpersonal skill training refers to helping people with autism understand why other people behave as they do. Others focus on the second impairment: communication. The use of information technology varies from approaches that use low complexity technology, from the therapist's point of view, to high complexity. Others trained autistic people to point to pictures to aid communication. Even more technology-intensive are simulations used to teach verbal communication or social robots for diagnosis and treatment. Finally, there are also attempts to address the third major impairment: rigidity of thinking. However, compared to fields such as biology or commerce, information technology is much less used to capture and analyze the impact of interventions on a large scale, i.e. the impact of therapy on behaviours. Thus, the research uses advanced data mining approach to study systematic differences, or the lack thereof, in therapy outcome for autistic children.

Virtual reality enables e-learners to visualise the learning process, manipulate findings with relative complex sets of data and interact with current technologies (Kadir & Xu, 2011). The visualization process refers to visual representation in computers, auditory components or any other forms of sensory outputs displayed in a virtual world. According to Abdul-Kader (2008), the virtual reality can be classified into three categories; desktop virtual reality, fish tank virtual reality and immersive virtual reality. Additionally, he concluded that applications of virtual reality have the potential of developing into a wider spectrum, which can diverge from entertainment purposes to educational purposes. On the other hand, the most recent application of virtual reality is the interface to e-learning applications, which is also known as virtual reality based e-learning tool. The potential of virtual reality tool is demonstrated by its ability to facilitate learning processes while avoiding many problems characterizing traditional or conventional teaching learning methods.

A multitude of e-learning educational systems that were developed recently incorporates virtual environments. Most of the medical and scientific subjects are the leading e-learning applications that use virtual reality technology (Dimitropoulos et al., 2007; Huang et al., 2010; Albeanu, 2008). With this in mind, many virtual classrooms are set up to facilitate virtual learning in educational institutions and training centres. It is also noted

ISSN 2394 - 7780

that over the years, advancement in the virtual reality technology has opened up numerous application possibilities such as providing guidance for disabled children (Albeanu, 2008; Reid, 2011; Kandalaft et al., 2013). Therefore, in a hope of broadening the studies that have already been done, this research focused on enhancing and facilitating the learning process of the specified target group of autistic children.

Several countries abroad have been implementing caretaking service centres and nurseries to assimilate an education for these children with special needs. Therapy to assist autistic children's parents and caretakers to educate the autistic children effectively. Most of the children in these facilities suffer from poor social interaction, lack of communication skills, and portray unusual and distinguishing behaviours similar to the scenario elaborated by Zander (2004). On account of such issues, some specifically designed teaching methods have been made available to allow autistic children to learn better, for example; applied behavioural analysis (ABA), treatment and education of autism and related communication handicapped children (TEACCH), floortime, social story, and picture exchange communication system (PECS) etc. (Selpa & Marin, 2001).

Despite of all the possible advantages of implementing virtual reality based tools the teaching methods stated above still possess various disadvantages. These disadvantages could include any of the following: requiring special guidance, skills domination, imagination problems, equipment storage and deterioration of storage medium (Selpa & Marin, 2001). However, most researchers have considered virtual reality based learning tool to be an effective tool for autistic children to facilitate the teaching learning process (Albeanu, 2008; Reid, 2011; Kandalaft et al., 2013). To add on, VE provides great potential for people with autism because users can play a role in an environment designed to imitate definite social situations. The increasing sophistication of VEs means that skills and tasks can be practiced in realistic settings. This has been identified as an approach that gives encouraging support to enhance the children's social skills (Strickland et al., 1996).

Autism is a spectrum of closely-related disorders with a shared core of symptoms. Every individual on the autism spectrum has problems to some degree with social skills, empathy, communication, and flexible behaviour (Mesibov et al., 2000; Happé & Frith, 1996). Due to this, to educate autistic children on social skills, a flexible and interactive teaching method or technique should be established. This learning style must be an enjoyable learning process that allows them to gain more and experience the real scenario via the implemented system. However, the majority of the prevalent methods of teaching aids available to autistic children have certain drawbacks in terms of enhancing social skills. Alternatively, there are many applications available online to serve this purpose, but it might be time-consuming due to the time required to download such applications. Additionally, it might also require more digital storage space depending on the size of an application in certain mobile devices. In Malaysia, mobile technology is an emerging technology and is gaining wide popularity. However, this technology is not owned by the majority and therefore there is some limitation to the access of smart phone applications that cater to needs of autistic children. It has been observed that many parents do not own smart phone technology to provide behavioral training to their autistic children via virtual reality based behavioral training and learning resources due to the high cost.

Several online applications also demand the user to spend more time in constructing a social story, whereby, the user is required to create a virtual environment for a specific behavioral training. Apart from that, it is not an easy task to obtain a suitable graphic to be used as a teaching and learning material for autistic children. However, it is important to use effective graphics in the virtual environment as it is a more appealing tool for teaching these children. Hence, pictures used should be realistic and cater to educational needs (Simon et al., 1986).The research aimed to create a virtual environment for autistic children that includes a virtual agent which can role play to educate autistic children on 'how to behave' at specific places or scenarios. Aligned with this, the derived objectives of this research are as follows:

• To identify the virtual environment (VE) needed for the behavioural learning process of autistic children;

• To ascertain the virtual environment (VE) requirements to educate autistic children; and

• To evaluate the prototype for virtual reality based learning application which

II. RELATED WORKS

Bishop, (2003)investigated onSocial and interpersonal skill training refers to helping people with autism understand why other people behave as they do. He is working on a tool that can help an autistic person better understand social situations by using a mobile phone to provides translations for phrases such as "cat's got your tongue?" This phrase does not make sense when taken literally, which many autistic persons would do. In a small study they evaluated how the system would be received and found that people with autism would find it useful.

ISSN 2394 - 7780

Dauphin et al (2004) & Miller et al (2006) Dauphin et al focused on Communication and the use of information technology vary from approaches that use low complexity technology, from the therapist's point of view, to high complexity. For example, Dauphin et al used PowerPoint slides with video segments to teach sociodramatic play. Others trained autistic people to point to pictures to aid communication. This approach has been taken a step further by Miller et al who developed a communication system for use with personal digital assistants. Even more technology-intensive are simulations used to teach verbal communication or social robots for diagnosis and treatment.

Rajendran & Mitchell (2000)tried to improve interpersonal understanding and understanding of mental states of others with the Bubble Dialogue program. They trained children with sperger's syndrome, i.e., high-functioning individuals with autism. A virtual reality based learning tool that includes a virtual environment (VE) and virtual agents is an effective method to support the social communication skills of children with autism. In such conditions, where social skills can be practiced repeatedly, the result possess a less threatening, less social challenging, more controllable and comfortable process when compared to a face-to-face communication scenario .Besides this, it also allows the user to truly see on the screen rather than how the environment is actually encountered in real life.

Happé & Frith, 1996; Wing & Gould, 1979; Wing, 1998 in their paper Autism is comprised of severe enveloping impairments in several important areas of development in a person. These impairments could be any of the following examples; social interactions, communication, behavioural, and imaginative.

Sallows & Graupner, 2005; Pinker, 1999 in their paper The majority of autistic children encounter learning difficulties, even though some might have been equipped with an average intelligence .The disability of these children can also fall under the categories of epilepsy, visual and auditory problems.

Mesibov et al., 2000 in this paper Autism is related to the behavior of a person as an effect of unknown biological dysfunctions of the brain that has consequence on the development or reaction of the brain while handling information. This dysfunction can range from issues that lie between any of the received information, processed information or even interpreted information.

Zander, 2004 ., In his article entitled "Introduction on autism", asserted that social interaction is a main issue encountered by autistic children, whereby the children have difficulties in conducting eye contact, body language, facial expression, and modulation.

Besides this, he also concluded that the level of seriousness in autistic children varies from one individual to another in terms of intelligence and learning ability. This might be due to several causes such as depression, the nature of the autism disorder, epilepsy, genetic symptoms, etc. Hence, the need to develop an attractive and an effective method to teach these children arises. There are several effective teaching methods identified to be used while educating these autistic children. Table 1 below shows several popular teaching methods for these special children.

Teaching Method	Description
Applied Behavioral Analysis (ABA)	Learning method by using an alphabetical model in order for them to be more focussed, responsive and imitate (Birnbrauer & Leach, 1993; Sallows & Graupner, 2005).
PECS (Picture Exchange Communication System)	Parents and caretakers are required to participate in an intensive training on how to use binders and picture cards as it comprises of 6 phases which can be considered as rather time consuming (Bondy & Frost, 1994). Furthermore, this meta-analysis analyses the extant empirical literature for PECS relative to the targeted (functional communication) and the non-targeted concomitant outcomes (behaviour, social skills, and speech) for learners with autism, learners with autism and intellectual disabilities, and those with autism and multiple disabilities (Ganz et al., 2012).
Social Story	Social Story was developed by Carol Gray which began in 1993; it was used to teach disabled children by providing accurate information in challenging situations (Reynhout et al., 2008). Social Story also provides guidance by describing the patterns on performing an action in sequence.

Table-1: Teaching Methods for Autism Students

ISSN 2394 - 7780

Parsons et al., 2006. VE is one of the tools which can be used in teaching a social story for autistic children. Past research also highlights an individual case study conducted to produce a report based on an observation and comments from two autistic children using two different virtual environments such as virtual cafe and virtual bus environment.

III. DATA MINING TECHNIQUES

Objectives of the Study

The research uses information technology focuses specifically on the use of IT to train autistic children or to improve communication with them. This research is of tremendous value to are givers and autistic children to improve their quality of life. Additional research is needed in to find the cause and optimal matching of children to therapies. Data mining is optimal for this. Two approaches are possible. The first is the use of data mining to find biological associations, such as specific genes related to autism. This type of data mining research is similar to data mining in molecular biology and genetics. It can help fine-tune diagnosing and find underlying causes for drug related treatments. Third approach, mining the actual behaviours, may provide more specific insights into when specific therapies work, which behavioral profiles exist, and how these two factors may interact. It may also help fine-tune the autism diagnosis.

Scope of the study

Our work focuses on the use of technology to study the effects of behavioral therapy. Data mining techniques can be used on behavioral therapy data from two perspectives: to find what is characteristic for a one or a group of children (behavioral profile) and to discover what is characteristic for a specific therapy approach (therapy profile). The research use data mining techniques to examine how behavior changes for a group of children receiving a specific therapy (therapy profile).

Methodology

This study aims to analyse Autistic Children. The researcher assumed that certain Data Mining Techniques to change the behaviour of Autistic Children .Many children need extensive therapy for years to improve their behavior and facilitate integration in society. However, few systematic evaluations are done on a large scale that can provide insights into how, where, and how therapy has an impact. We describe how data mining techniques can be used to provide insights into behavioral therapy as well as its effect on participants. To this end, we are developing a digital library of coded video segments that contains data on appropriate and inappropriate behavior of autistic children in different social settings during different stages of therapy and In general, we found that therapy increased appropriate behavior and decreased inappropriate behavior. Decision trees and association rules provided more detailed insights for high and low levels of appropriate and inappropriate behavior. We found that a child's interaction with a parent or therapist led to especially high levels of appropriate behavior and behavior is most predictable while therapy is in progress.

Research Methods

This research used a mixed methodology uses behaviour analysis. The behaviour analysis method focuses on an interview and an observation survey. The interview was conducted as part of the preliminary study for this research. Besides conducting interviews, the student observation was also carried out during this face to face interaction session. The behavior method was then used to analyse findings of this research that uses the PECS teaching method for autistic children (Bondy & Frost, 1994). It is clear that PECS is a communication method that does not require speech and has been widely used in various researches pertaining to autistic children. It is based on an exchange of a picture of a real object by finding and reaching for someone's assistance to deliver the message effectively. With that exchange, the children themselves start the act of communication. Thus, the main objectives of using PECS set by the researchers are that the child initiates the communication, finds and approaches a communicative partner and uses only one picture in order to avoid a confusion about what he or she wants (Bondy & Frost, 2002).

IV. FUTURE ENHANCEMENT

The Teaching Techniques used in this study brings out the changes and improvement in the behavior of Autistic Children. Data Mining Techniques like Decision trees and association rules provided more detailed insights for high and low levels of appropriate and inappropriate behavior. In future some more techniques can be applied for teaching the Autistic Children.

ISSN 2394 - 7780

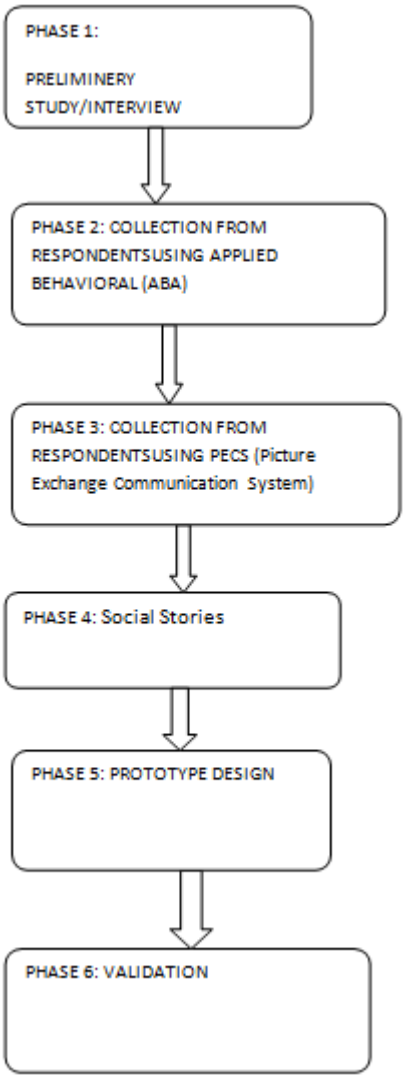


Figure-1: Six Phases

REFERENCES

1. J. Bishop, "The Internet for educating individuals with social impairments," Journal of Computer Assisted Learning, vol. 19, pp. 546-556, 2003.
2. M. Dauphin, E. M. Kinney, and R. Stromer, "Using Video-Enhanced Activity Schedules and Matrix Training to Teach Sociodramatic Play to a Child with Autism," Journal of Positive Behavior Interventions, vol. 6, pp. 238-250, 2004.
3. T. Miller, G. Leroy, J. Huang, S. Chuang, and M. H. Charlop-Christy, "Using a Digital Library of Images for Communication: Comparison of a Card-Based System to PDA Software," presented at First International Conference on Design Science Research in Information Systems and Technology, Claremont, CA, 2006.
4. G. Rajendran and P. Mitchell, "Computer mediated interaction in Asperger's syndrome: the Bubble Dialogue program," Computers and Education, vol. 35, pp. 189-207, 2000.
5. Happe, F. & Frith, U. (1996). The neuropsychology of autism. Brain - A jnl of Neurology, 119(4):1377-1400 Hardy, C., Ogden, J., Newman, J. & Cooper, S. (2002) Autism and ICT: A Guide for Teachers and Parents. London, UK: David Fulton Publishers Ltd.
6. Wing, L., & Gould, J. (1979). Severe impairments of social interaction and associated abnormalities in children: Epidemiology and classification. Journal of Autism and Developmental Disorders.
7. Wing, L. (1998). The history of Asperger syndrome. In Asperger Syndrome or High-Functioning Autism?, 11-28. Springer US.

ISSN 2394 - 7780

8. Sallows, G. O., & Graupner, T. D. (2005). Intensive behavioral treatment for children with autism: Four-year outcome and predictors. Journal Information,110(6).

9. Zander, E. (2004). An introduction to autism, AUTISMFORUM Handikapp & Habilitering, Stockholm.

10. Parsons, S., Leonard, A., & Mitchell, P. (2006). Virtual environments for social skills training: comments from two adolescents with autistic spectrum disorder.Computers & Education, 47(2), 186-206.

11. Bondy, A. S., & Frost, L. A. (1994). The picture exchange communication system. Focus on Autism and Other Developmental Disabilities, 9(3), 1-19.

12. Bondy, A., & Frost, L. (2002). A Picture's Worth: PECS and Other Visual Communication Strategies in Autism. Topics in Autism.Woodbine House, 6510 Bells Mill Rd., Bethesda, MD 20817.

13. Chorpita, B. F. (2014). Fear and anxiety are common emotions that are a neccessary part of the normal development of all children. 1 For some children, however, the levels of fear or anxiety. Child

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

AUMENTING SMART WATER MANAGEMENT SYSTEM USING RASPBERRY PI IOT

Dr. T. Thiruvenkadam[1], Rajkamal[2] and Dr. S. Sasikala[3]
Assistant Professor[1], Department of Information Technology, Adigrat University, Ethiopia
Student[2], BCA
Associate Professor[3], Hindusthan College of Arts and Science

ABSTRACT
Managing This Paper Proposes a system, that system performs water quality monitoring and Regulated water supply operation. We have some more sensor like Ph sensor, Flow sensor, Temperature Sensor and Turbidity sensor. By using this sensor value, we calculate the continually and taking the data, analyze after the any problem in the sensor value we will calculate to the water purity and sent the alert message to the authorized person by using the IOT Technologies. We have the purity sensor and pH sensor by using this we getting the sensor values at last we get the alert message.Clean drinking water is the most valuable resource for humans. Any imbalance in the water quality would seriously affect the health condition of the humans. Now a day's drinking water utilities are facing various challenges in real time due to limited water resources, global warming, growing population and pollution. Hence there is need of better methodologies for real time water quality monitoring. As the recent survey of WHO estimated that in India 77 million people face problems due to unsafe drinking water and 21% of the diseases are related to impure water. WHO also estimated that 1600 people die every day in India due to diarrhea.Conventional method of water quality monitoring involves the manual collection of the water at different areas and this water is tested in laboratory.

Keywords: IoT, Turbidity, pH Sensor, WIFI

I.INTRODUCTION

Water is one of the most essential commodities for human well-being and substantial for socio-economic development of a country. Water is not only life-sustaining drink for humans and all other organisms but also vital for industrialization and agriculture. Total amount of water remains constant throughout the planet and adequate to meet all demands of civilization but potable water reserves are rapidly depleting all across the world. Growing population, discharge of toxic chemicals, untreated sewage, climate change and other human activities definitely impact water resources in densely populated regions if not handled effectively. In addition, water is not evenly spread throughout the planet so non-uniform, unsustainable and inequitable allocation results in problem of scarcity and availability.

The world is increasingly looking forward to adaptation and use of new technologies to improve quality of life as well as reduce impact of human activities and consumption patterns on environment. Availability of clean water, its increasing demand from urbanization and growing population in cities, cost for management of water transmission, storage, treatment, distribution and billing for consumption are serious issues in underdeveloped and developing countries. Rapid changes in lifestyle and increased paying capacity have impacted use of water and related overheads on sewerage requirements. The prototype system relies on the use of simple Internet of Things (IoT) approach for Water metering in conjunction with a custom built Smartphone App.

The next wave in the era of computing will be outside the realm of the traditional desktop. In the Internet of Things (IoT) paradigm, many of the objects that surround us will be on the network in one form or another. Radio Frequency IDentification (RFID) and sensor network technologies will rise to meet this new challenge, in which information and communication systems are invisibly embedded in the environment around us.

This result in the generation of enormous amounts of data which have to be stored, processed and presented in a seamless, efficient, and easily interpretable form. This model will consist of services that are commodities and delivered in a manner similar to traditional commodities.

Cloud computing can provide the virtual infrastructure for such utility computing which integrates monitoring devices, storage devices, analytics tools, visualization platforms and client delivery. The cost based model that Cloud computing offers will enable end-to-end service provisioning for businesses and users to access applications on demand from anywhere. Smart connectivity with existing networks and context-aware computation using network resources is an indispensable part of IoT.

The importance of maintaining good water quality highlights the increasing need for advanced technologies to help monitor water and manage water quality. In particular the implementation of the WFD poses new challenges for water managers who have traditionally monitored water quality by taking samples and analyzing

ISSN 2394 - 7780

them in the laboratory.

In this paper we intend to present the design and development of a low cost system for real monitoring of water Theft in an IoT environment.The parameters such as flow of the water can be measured and also to intimate to the main control room. The control room to access the motor and gate valve depends up on the water flow and level. Whether the valve open particular area peoples will receive the water. If anyone misuses the water line and gets the illegal water connection, the water is automatically stopped using solenoid valve and only the authenticated person can able to open the valve again. This Paper Proposes a system, that system performs water quality monitoring and Regulated water supply operation. We have some more sensor like Ph sensor, Flow sensor, Temperature Sensor and Turbidity sensor. By using this sensor value, we calculate the continually and taking the data, analyze after the any problem in the sensor value we will calculate to the water purity and sent the alert message to the authorized person by using the IOT Technologies. We have the purity sensor and pH sensor by using this we getting the sensor values at last we get the alert message.

SYSTEM REQUIREMENT

HARDWARE

• RASPBERRY PI

• PH SENSOR

• FLOW SENSOR

• TURBIDITY SENSOR

• TEMPERATURE SENSOR

• SOLENOID VALVE

SOFTWARE

• THINGSPEAK CLOUD

• RASBIAN- JESSIE

• PHYTHON

SYSTEM SPECIFICATIONS

Raspberry pi

• SoC: Broadcom BCM2837 (roughly 50% faster than the Pi 2)

• CPU: 1.2 GHZ quad-core ARM Cortex A53 (ARMv8 Instruction Set)

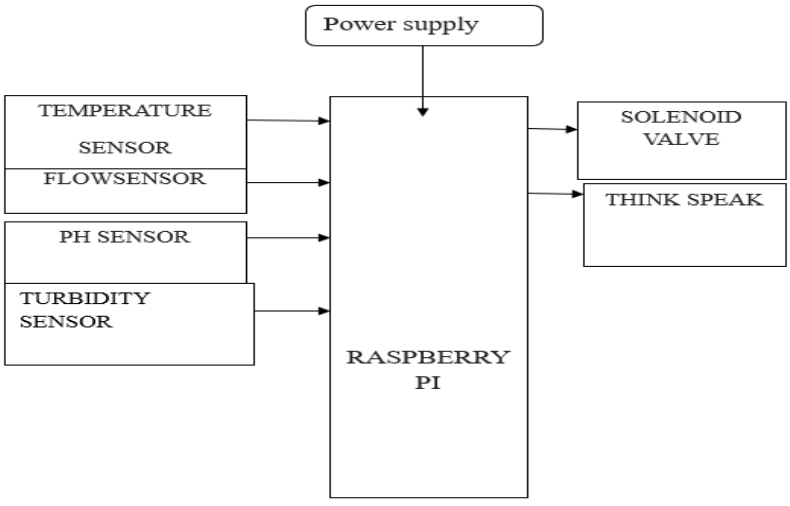
• GPU: Broadcom VideoCore IV @ 400 MHz

• Memory: 1 GB LPDDR2-900 SDRAM

• USB ports: 4

•Network: 10/100 MBPS Ethernet, 802.11n Wireless LAN, Bluetooth 4.0

III. SYSTEM STUDY



ISSN 2394 - 7780

EXISTING SYSTEM

In existing System, we monitoring the water quality by connecting PH sensor, conductivity sensor and turbidity sensor which is collected in raspberry pi and uploaded over the Cloud for analysis.

PROPOSED SYSTEM

In proposed system same setup, we have from Existing system but we have to add Flow sensor and Solenoid valve. Purpose of using flow sensor is to find out How much water is consumed by each house. And solenoidal valve is to Automatic Closing of pipe. This whole system will act as water quality and Water regulated supply system.

Whole system is based on Sensors connected to Raspberry pi to monitor the water quality and Regulated water supply. Raspberry – Single board Computer acts as a heart of the system to perform desired operation. All the sensor values are uploaded to cloud any person can monitor the parameters in any where in the world. Thingspeak – open source cloud provides the values in the form of Graphical representation by using this we can do analysis.

THINKSPEAK

ThingSpeak is an open data platform for monitoring your data online. You can set the data as private or public depending on your choice. ThingSpeak takes minimum of 15 seconds to update your readings. Its a great platform for building your IOT papers.

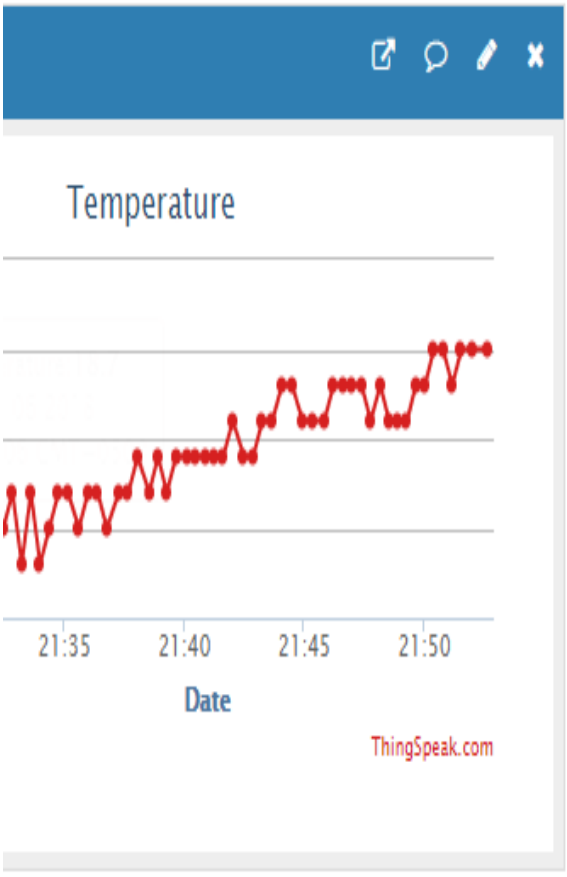
ThingSpeak is an “open data platform for the Internet Of Things”. To get started, you need to create a channel that specifies what you are plotting – title, range, number of fields, etc. You then update data in your channel with an HTTP request of the form:

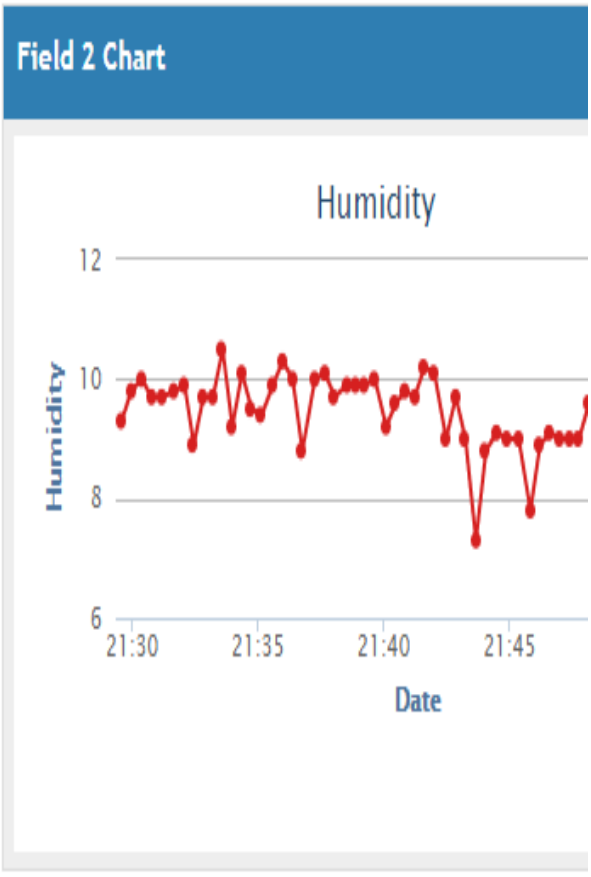
https://api.thingspeak.com/update?api_key=YOUR_CHANNEL_API_KEY&field1=99

The data stream itself can be viewed at the following URL:

https://api.thingspeak.com/channels/YOUR_CHANNEL_ID

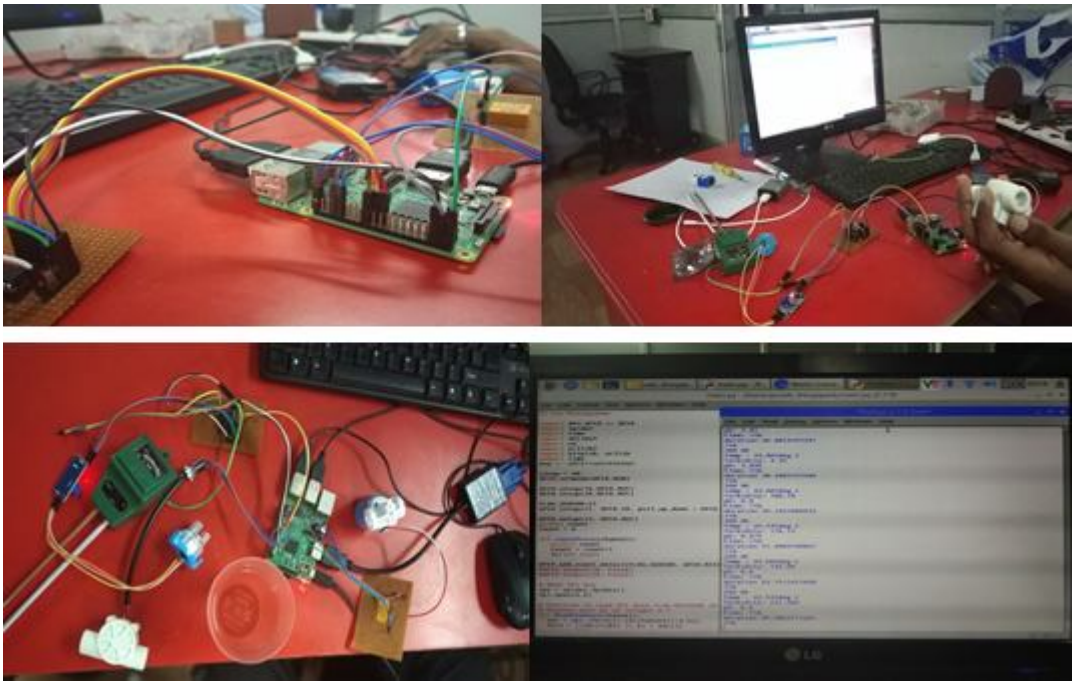
ThingSpeak provides a lot of options for displaying your channel’s data – make it public/private, changing extents, layouts, etc. The only limitation is the rate of data updates – it has to be no more frequent than 15 seconds. But the whole software is Open Source, which means you could host it on your own if you need faster updates.





ISSN 2394 - 7780

VI. IMPLEMENTATION AND TESTING
IMPLEMETATION



VII.CONCLUSION

The design and development of low-cost system for real time monitoring of water quality and controlling the flow of water by using IoT is presented. The proposed system consists of sensors for water quality monitoring and solenoid valve for controlling the water flow in the pipeline. These devices are low in cost, highly efficient and flexible. These are connected to Raspberry pi core controller and IoT module. Finally, sensed values viewed and controlling is performed by internet and also through Wi-Fi to mobile devices.

- Rain water harvesting can be done with which water supply can be done so that
  we could conserve water drastically.
  Routine watering of trees, plants can be done in order to avoid wastage of water by individual watering of their plants or trees.
- Internet of Things technology can help the water management industry respond to and stop leaks.Water leakage is managed by controlling water pressure, overseeing pipelines and other assets, and responding quickly when repairs are needed.
- Using technologies that include iot water sensors, sensor data communications, and analytics, IoT applications can help the water industry optimize performance and improve workplace efficiency.

ACKNOWLEDGMENT

We convey our sincere gratitude to the DBT, Ministry of Science and Technology for their support for the STAR COLLEGE SCHEME to strengthen the undergraduate courses through which we have a strong platform of learning the technology of the Internet of Things. We convey the heartful thanks to them for the support they have rendered.

REFERENCES

[1] CongcongSun ; Gabriela Cembrano ; Vincenc Puig ; Jordi Meseguer, ‘Cyber-Physical Systems for Real-Time Management in the Urban Water Cycle’, 2018 International Workshop on Cyber-physical Systems forSmart Water Networks (CySWater)

[2] Chanda Rajurkar ; S R S Prabaharan ; S. Muthulakshmi,“IoTbased water management”, 2017 International Conference on Nextgen Electronic Technologies: Silicon to Software (ICNETS2)

[3] M Suresh ; U. Muthukumar ; Jacob Chandapillai, “A novel smart water-meter based on IoT and smartphone app for city distribution management”, 2017 IEEE Region 10 Symposium (TENSYMP).

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

FISHERMAN BORDER SECURITY EMPOWERED WITH IOT ARDUINO BASED BOAT

Dr. K. M. Sharavana Raju[1], Dr. S. Sasikala[2] and Nisha. S[3]
Assistant Professor[1], Department of Computer Science, College of Computer Science & Information Systems, Jazan University, Kingdom of Saudi Arabia
Associate Professor[2] and Student[3], Hindusthan College of Arts and Science

ABSTRACT
The main idea of this paper is to Safe guard the fisherman from the Border Crossing, if the crossing the border means many times they get shout down by the other state people. So, we built one system that Safer guard the Fisherman that system consists of GPS and GSM. GPS is used to track the location of the boat and GSM will notify the location via messages. In border area we split in to two one is warning border and Notional border. If the boat reaches the Warning border means he fisher man get some alert Even he travelled and reach the nation border means his boat is automatically off. SMS Sent to the Indian Coast guard. This system is very much helpful for Fisherman. After that Coast guard come and save the fisherman's life. This system is very much helpful for Tamil Nadu Fisherman.

Keywords: IoT, FISHERMAN, GPS, WIFI, GSM

I. INTRODUCTION

The main idea of this paper is to Safe guard the fisherman from the Border Crossing, if the crossing the border means many times they get shout down by the other state people. So, we built one system that Safer guard the Fisherman that system consists of GPS and GSM.

Sri Lanka and India seaside nations are isolated by their sea borders. In Tamil Nadu about 20,000 vessels make spinning in the Bay of Bengal. The main aim is to give a well equitable user-friendly environment for Indian Fisherman to handle hazardous situation with the help of engine control. This paper comes with a consistent solution for this problem and protects the Indian fisherman from dangerous situation and being crossing the maritime boundary and save their life and improve the safety of fisherman. The system is designed by using GPS and GSM. A GPS route device is a device that precisely discovers natural area by getting data from GPS satellites. This device can track the GPS data every single time at whatever point the fisher man's cross the Indian border. It is a significant depression issue and encourages trouble in the both people and also their economic expenditures.

II. SYSTEM STUDY

EXISTING SYSTEM

Borderline measured manually

Difficult to communicate to navy control

Functions of this system based on time and distance

PROPOSED SYSTEM

Effective alert system for fisherman

Communication between fisherman boat and Navy control is reliable

Wireless communication used for transferring information

Display system for identifying boundary.

SYSTEM REQUIREMENTS

Hardware Tools

Microcontroller

RF Reader

Relay

Motor

Buzzer

System specification (Arduino)

ISSN 2394 - 7780

Microcontroller: ATmega328P

Operating Voltage: 5V

Input Voltage (recommended): 7-12V

In-Out Voltage (limit): 6-20V

Digital I/O Pins: 14 (of which 6 provide PWM output)

PWM Digital I/O Pins: 6

Analog Input Pins: 6

DC Current per I/O Pin: 20 mA

Software tools

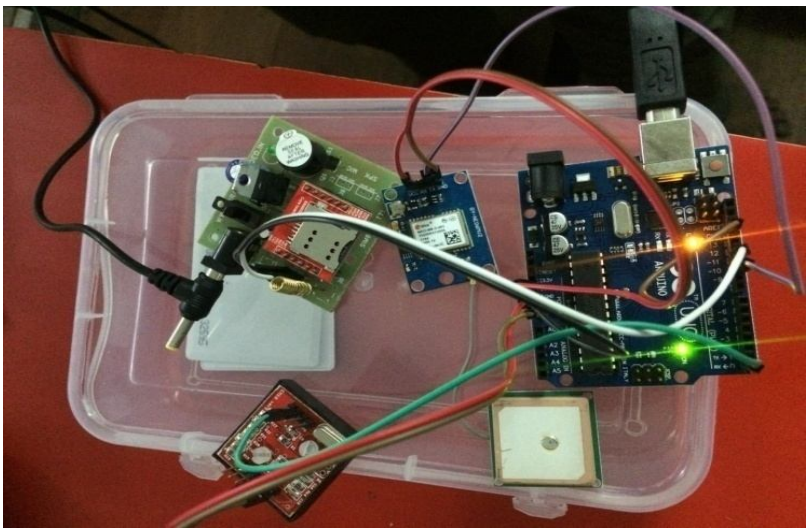
ARDUINO INO

LANGUAGE: EMBEDDED C

III. SYSTEM ANALYSIS

The GPS Modem will continuously give the signal which determines the latitude and longitude and indicates the position of the fishermen to them. Then it gives the output which gets read and displayed in the LCD. The same data is sent to the mobile of the fisherman and simultaneously the same data is sent to the Sea border security. An EEPROM is used to store the data, received by GPS receiver. The hardware which interfaces with microcontroller are LCD display, GSM modem and GPS Receiver. GPS (Global Positioning System) is increasingly being used for a wide range of applications. It provides reliable positioning, navigation, and timing services to world wide users on a continuous basis in all weather, day and night, anywhere on or near the Earth. 24 satellites inclined at 55° to the equator orbit the Earth every 11 hours and 58minutes at a height of 20,180 km on 6 different orbital Lanes and each one of these satellites has up to four atomic clocks on board. All we require is an accurate clock. By comparing the arrival time of the satellite signal with the on board clock time, at which the signal was emitted, the latitude and longitudinal degree of the boat's location is determined. The current design is an embedded application, which will continuously monitor a moving Boat and once the boat goes beyond the level of the defined layer the particular operation will be done. For doing so an PIC microcontroller is interfaced serially to a GSM MODEM AND GPS receiver.

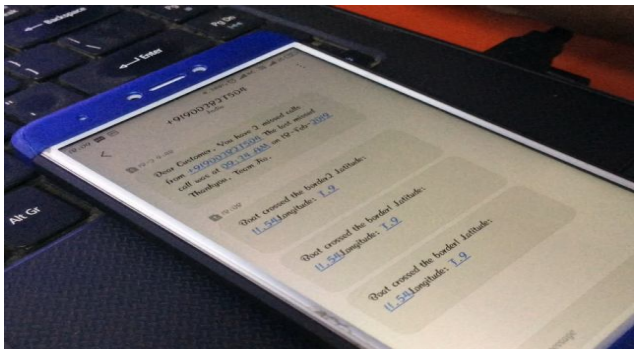
IV. SYSTEM IMPLMENTATION AND TESTING



The proposed system uses a GPS receiver which receives signal from the satellite and gives the current position of the boat. The proposed system is used to detect the border of the country through the specified longitude and latitude of the position, not only between Sri Lanka and India but all over the world. The particular layer level i.e. border can be predefined and this can be stored in microcontroller memory. The current value is compared with predefined values and if these values are same, immediately the particular operation will be done i.e, the microcontroller gives instruction to the alarm to buzzer. It also uses a message transmitter to send message to the base station which monitors the boats in the sea. The system provides an indication to both fisherman and to coastal guard. Thus it saves the lives of the fisherman and alerts the base station to provide help.

ISSN 2394 - 7780

Basically there are three different locations which are pre stored those location points are just few nautical miles away from border at each location each warning system is proclaimed at first location there will be warning buzzer and there will be exact display of distance between present location and border in LCD display and also there is a 50 percent reduction of boat speed if fishermen misses warning if he moved ahead then it shows distance information and also motor will stop now fishermen can start a boat once it is an indication that border is just few nautical miles away from the border if he ignored and moved on towards third location whole boat will stop and the location of that point is send to navy control room and they will come and verify the legitimacy of fishermen and they have to put an randomly generated key to start boat and same location is sent to family members through GSM. Thus we can stop fishermen before the border and lives of fishermen are saved.



Border alert system for fishermen is used to detect the boundary location and warn the fishermen in danger situations. It not only finds the GPS value, but also compares with the stored value in the microcontroller, and makes a decision as to whether the fishermen is in the warning range or not.

The boundary between India and Sri Lanka in the waters from Adam's Bridge to Palk Strait shall be arcs of Great Circles between the following positions, in the sequence given above, defined by latitude and longitude.

Maritime Boundary between Indian and Sri-Lanka

The boundary points are marked above. These points should be stored in microcontroller. The computation is done in microcontroller with these points. Thus vessel crossing the border is being calculated.

Consequence

Boat Position and Navigation System contains,

Location 1: buzzer indication

Location 2: motor speed control indication.

Location 3: motor stops.

Location 4: final verification

V. CONCLUSION

In the recent times the capture of Indian fishermen across Sri Lanka border has been increased. It is difficult for the fishermen to discover the borders and lost into other country borders. Our objective is to give wireless support to those fishermen and aside from to go out after them if they are found missing. This paper is a low-cost efficient method of wireless tracking. It also gives sufficient information to both ship and coastal guardians of anyone crossing the border. We can use the EEPROM to store the previous Navigating Positions up to 256

ISSN 2394 - 7780

locations. We can navigate up ton number of locations by increasing the memory of EEPROM. We can reduce the size of the kit by using GPS+GSM on the same module of GPS navigator. We can increase the accuracy up to 3m by increasingthe cost of the GPS receivers.

BENEFITS

1. The hijack of the ship by the pirates can be eradicated.

2. The lost ship wrecks due to natural calamities can be identified

3. By keeping the kits in the entire boats and by knowing the locations of all the boats we can use our kit to assist the traffic.

4. Incase of any accident on the sea. it can be detected by the system and the accident location of the boat is sent to the rescue team.

APPLICATION

1. We can use this device also as bomb detector

2. Location of any lost vehicle could be found

ADVANTAGES

1. Accuracy determination of location

2. Maintenance cost is low

3. Easily replaceable with traditional method of verification.

REFERENCES

1. R.M. Bhardwaj, "Overview of Ganga River Pollution", Report: Central Pollution Control Board, Delhi, 2011
2. NivitYadav, "CPCB Real time Water Quality Monitoring", Report: Center for Science and Environment, 2012
3. Tuan Le Dinh, Wen Hu, PavanSikka, Peter Corke, L. Overs, Stephen Brosman, "Design and Deployment of a Remote Robust Sensor Network: Experiences from Outdoor Water", 32nd IEEE Conf. on Local Computers, pp 799-806, Feb., 2007
4. Quio Tie-Zhn, Song Le, "The Design of Multiparameter On line Monitoring System of Water Quality based on GPRS", Report: Advanced Transducers and intelligent Control System Lab, Taiyuan Technical University, Taiyuan, China, 2010
5. Steven Silva, Hoang N Ghia Nguyen, Valentina, Tiporlini, Kamal Alameh, "Web based Water Quality Monitoring with Sensor Network: Employing ZigBee and WiMAX Technology", 36th IEEE Conf. on Local Computer Networks, 2011
6. Donge He, Li-Xin Zhang, "The Water Quality Monitoring System based on Wireless Sensor Network" Report: Mechanical and Electronic Information Institute, China University of GeoScience, Wu Hen, China, 2012
7. PavlosPapageorgiou, "Literature Survey on Wireless Sensor Networks", Report: University of Maryland, 16 July 2003
8. SatishTurken, AmrutaKulkarni, "Solar Powered Water Quality Monitoring System using Wireless Sensor Network", IEEE Conf. on Automation, Computing, communication, control, and compressed sensing, pp281-285, 2013
9. Liang Hu, Feng Wang, Jin Zhou and Kuo Zhao "A Survey from the Perspective of Evolutionary Process in the Internet of Things", International Journal of Distributed Sensor Networks, Article ID 462752, 2015
10. ThingSpeak-Understanding your Things-The open IoT Platform with MATLAB analytics, MathWorks
11. User Manual Arm7-LPC2148 Development kitPantech Solutions.
12. ESP8266 serial Wi-Fi wireless Transceiver Module for IoT, ESPRUINO-Wireless.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

LOAD BALANCING USING SLEEP SCHEDULING ALGORITHM IN MANET

M. Hemalatha[1] and Dr. S. Mohanapriya[2]
Assistant Professor[1], Department of Computer Applications, Hindusthan College of Arts & Science, Coimbatore
Head[2], Department of Computer Science, K. S. R College of Arts & Science for Women, Tiruchengode

ABSTRACT
A wireless impromptu system is an accumulation of wireless figuring gadgets that self-design to shape a system freely of any fixed framework. Numerous wirelesses specially appointed system gadgets, for example, advanced cells and tablets are normally controlled by batteries with a restricted task time. This represents a noteworthy test to the plan of low-control organize conventions. rest scheduling is generally embraced as an effective mechanism to additionally lessen control squandered in catching and inert tuning in. Nonetheless, the earlier work has for the most part treated energy-proficient directing and rest scheduling as two separate undertakings, which prompts a significant issue that neither one of the components can completely limit the system wide energy utilization. In this proposal, we contemplate how energy-effective steering can be facilitated with rest scheduling to build organize side energy efficiency. We distinguish an exchange off between the diminished transmit control at senders due to multi-receiver assorted variety and the expanded power at forwarders with the joining of composed rest scheduling.

Keywords: Load Balancing, Sleep Scheduling, Link Layer, Routing.

1. INTRODUCTION
In contrast to wired systems or cellular systems, a wireless ad hoc system has no fixed systems administration infrastructure. The basic components of the wireless ad hoc systems architecture are hubs with the capability of wireless communications. As appeared in Figure 1, a wireless ad hoc system is an accumulation of various hubs that maintain the system network through wireless communications. In wireless ad hoc systems, each hub may communicate straightforwardly to other people. Because of the constrained transmission range of radio, pairs of hubs that are not legitimately associated need intermediate hubs to advance their traffic. Each intermediate hub goes about as a switch to advance parcels for different hubs on account of multi-bounce associations. Contrasted and conventional infrastructure-based wireless systems, for example, cell systems and wireless neighborhood (WLAN), the fundamental favorable circumstances of wireless impromptu systems are exibility, minimal effort and heartiness. These characteristics of specially appointed systems start an assortment of utilizations and frameworks. At first, wireless specially appointed systems were chiefly thinks about in the domain of military or fiasco alleviation circumstance. All the more as of late, wireless specially appointed systems have likewise been imagined for business application, for example, giving Internet availability to hubs that are not in the transmission scope of a wireless passageway. By and large, the field of wireless impromptu system contains a few subfields including portable impromptu system (MANET, for example, in military communications where all hubs are thought to be versatile, wireless work arrange (WMN), a mix of specially appointed and infrastructure organize, wireless sensor organize (WSN) made up of sensor hubs for observing and following, and vehicular specially appointed system (VANET) extraordinarily for vehicle communications.

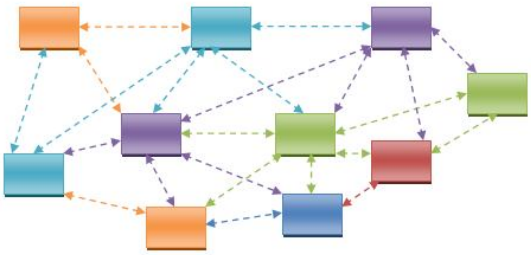


Figure-1: Illustration of Wireless Adhoc Network Architecture

Wireless specially appointed systems ordinarily comprise of registering gadgets fueled by battery. In this way, the structure of a vitality compelled wireless impromptu system represents a basic test identified with the vitality spending plan. The continuous research is essentially focused on arrangements that utilization the minimum conceivable vitality amid communications, along these lines drawing out the gadget activity lifetime. In this proposal, we center around two independent yet similarly imperative fronts of intensity sparing mechanisms: rest planning for the connection layer and vitality proficient steering in the system layer. In the accompanying, we initially give the power utilization examination of the wireless interface at a hub, and after

ISSN 2394 - 7780

that present two fundamental systems and investigate their offered advantages of vitality reserve funds. Regularly, the wireless interface hardware at a hub can work in any of four distinct modes: (1).Transmit mode when a hub transmits a bundle; (2).Receive mode when a hub gets a parcel; (3).Idle mode when a hub isn't transmitting or receiving a bundle. This mode devours control in light of the fact that the wireless interface must be up and prepared to get any conceivable traffic; (4).Sleep mode when a hub forces of the wireless interface hardware and along these lines it can neither transmit nor get bundles. Estimation results have demonstrated that the wireless interface devours the most noteworthy power in the transmit mode and next to no power in the rest mode. The power devoured in the inactive mode is anyway equivalent with the power required for the get mode. For example, Cisco Aironet Wireless CardBus Adapter regularly devours 1.78W, 1.08W, 0.67W and 0.02W in the over four modes individually. For wireless impromptu systems, there are primarily three wellsprings of unnecessary vitality consumption. The principal wellspring of vitality squander is crashes because of arbitrary access. In shared-medium wireless systems, there is a high open door for parcel transmission impacts to happen. At the point when a transmitted parcel is undermined because of crashes, it must be disposed of and retransmissions of the bundle cause additional vitality. One crucial focus of the MAC conventions is to stay away from impacts from meddling hubs. TDMA MAC has the characteristic favorable position of vitality sparing contrasted and the conflict based conventions by disposing of impacts. The second source is alluded to as inert tuning in, which relates to the vitality expended in the inactive mode. At the point when the all out traffic load over the system is generally low, hubs are thought to be worked in the inactive mode for quite a while. For example, most sensor systems creating exceptionally light traffic are intended to work for quite a while. In this way, inactive listening is an overwhelming component of vitality squander in such cases. The third wellspring of vitality squander is catching, amid which hubs gets control or information parcels that were not transmitted to them. Sadly, in a wireless impromptu system, it is much of the time the case that a bundle transmission starting with one hub then onto the next will be caught by every one of the neighbors of the transmitter. These hubs will devour control unnecessarily despite the fact that the parcel isn't coordinated to them. The reason is that the wireless interface does not have any component to not get that bundle. Note that vitality devoured by catching is equivalent to that in gathering. It is consequently a huge misuse of vitality, particularly when hub thickness is high and traffic load is overwhelming.

II. LITERATURE SURVEY

Jeungeun Song, YimingMiao ,Enmin Song, M. ShamimHossain and Mohammed F. Alhamid propose the RCR-based ideal transfer assignment and cooperative information conveyance (RCR-conveyance) plan to give a low-communication-overhead information transmission and an ideal obligation cycle for a given number of cooperative hubs when the system is dynamic, which empowers some portion of cooperative hubs to switch into inert status for further vitality sparing. The proposed plan altogether beats the current geographic steering plans and beaconless geographic routings in remote sensor systems with an exceptionally powerful remote channel and controls vitality consumption, while ETE dependability is adequately ensured. Hongbin Chen QianZeng and Feng Zhao proposed a proficient rest booking algorithm is advanced to handle the above issue in vitality collecting sensor systems. At first, we alter the likelihood based prediction and rest booking (PPSS) algorithm to follow the objective and further utilize another rest planning algorithm we proposed to wake tracking hubs when the objective is probably going to be missed (i.e., it is ineffective to wake next-minute tracking hubs). Besides, a double-storage vitality collecting architecture is utilized to expand remaining vitality of sensor hubs and to broaden organize lifetime. The proposed rest planning algorithm can improve tracking execution and drag out system lifetime contrasted and the PPSS algorithm and the proposed algorithm without vitality gathering. Jue Hong, Zhuo Li, Dianjie Lu and Sanglu Lu propose SALB, a resting plan mindful local communicate algorithm. In SALB, an average local algorithm for developing associated commanding set is utilized to shape the communicate spine. To ensure appropriate transmission of communicate messages, a rest mindful sending mechanism is actualized. Additionally, heuristic techniques are utilized to diminish the quantity of transmissions and the communicate idleness. Altered an established local algorithm for developing associated ruling set to frame the communicate spine and structured a sending mechanism to deal with the occasionally dozing issue of hubs. Sha Liu, Kai-Wei Fan, PrasunSinha proposed Current rest planning approaches for sensor arranges that address vitality consumption either possibly spare vitality when sitting or have high latencies and low channel utilization. Our commitment is a vitality effective rest booking convention called BSMac for sensor systems while keeping up high throughput and low inactivity. BSMac depends on another architecture called BoostNet in which the base station communicates basic booking coordination data utilizing vast transmission range to achieve all sensor hubs in a single jump. Hubs appointshues consecutively to the active connections along the traffic way, and hubs not on the information way work at a low obligation cycle. To accommodate diverse traffic designs, the quantity of hues is basic. To accomplish ideal throughput, the base station tests the system with various greatest number of hues occasionally. Niranjan Kumar Ray and

ISSN 2394 - 7780

Ashok Kumar Turukproposed a vitality protection system called Location Based Topology Control with Sleep Scheduling for impromptu systems. It utilizes the element of both topology control approach and power management approach. Like the topology control approach, it endeavors to diminish the transmission intensity of a hub, which is resolved from its neighborhood area data. A hub rests state dependent on the traffic condition as that of intensity management approach. A hub rests state just when its nonattendance does not make local segment in its neighborhood. We preformed broad simulation to contrast the proposed plan and existing ones. Simulation results demonstrate that the vitality consumption is lower with increment in the system lifetime and higher throughput in the proposed plan.

III. PROPOSED WORK

Sleep Scheduling in the Link Layer

As per the power consumption investigation at a remote hub, powering of the remote interface can incredibly diminish the vitality devoured by inactive tuning in and catching. Thusly, rest scheduling (additionally called obligation cycling) is ordinarily embraced as a connection layer power-saving mechanism in the remote specially appointed systems. This mechanism enables hubs to enter the low-power rest mode by turning of the remote interface at whatever point there is no correspondence request. By doing this, the channel time is isolated into rest periods and dynamic periods, as Figure 2 appears. In the rest time frame, a hub powers of its remote interface so as to spare vitality. Toward the start of every dynamic period, the hub awakens and prepares to transmit. An essential concern identified with rest scheduling is whether the postponement or throughput conduct is decayed. In this way, the urgent issue in the plan of rest scheduling conventions is to strike an exchange off between the general execution and power saving. Broad endeavors can be arranged into composed scheduling and random scheduling (additionally called nonconcurrent scheduling). By and large, organized rest scheduling methodologies can conceivably accomplish better execution with the centralized coordination of rest plans than random scheduling.

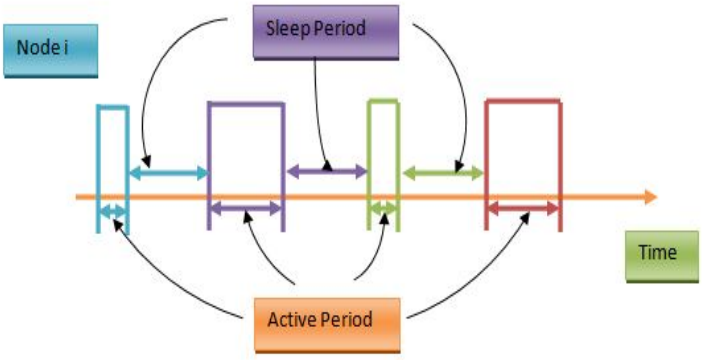


Figure 2: An Illustration of Operation Sleep Scheduling

Energy efficient Routing in the Network Layer

Vitality productive directing is proposed to lessen end-to-end transmission vitality cost of data communications in remote ad hoc systems. Distinctive courses comprise of various hubs in the topology and subsequently decide a unique transmission path related to vitality assets. Typically control aware directing protocols select a path interfacing a pair of source and destination hub that limits the total transmissions control over all the hubs in the chose path. Most existing force aware directing protocols assume that remote connections are reliable. In any case, in remote systems, various factors like ambient clamor, fading and impedance can lead to packet misfortunes because of transmission blunders. A retransmission mechanism is normally utilized in the connection layer to recuperate from packet misfortunes. Along these lines, the total transmission control associated with a pre-chosen path in the power-aware steering protocols fails to capture the actual vitality spent in packet conveyance thinking about potential retransmissions. Vitality productive reliable directing protocols that take account of the quality of remote connections are subsequently proposed to discover best paths requiring less number of retransmissions. It is worth to make reference to that those best path steering (BPR) protocols all pursue a conventional plan rule of traditional wired systems: the best courses are foreordained before data transmissions and all data streams from the source and destination pursue the chose courses until the path is updated. Pioneering directing (also called any path steering), an integrated directing and MAC strategy has as of late upset this guideline. Instead, artful steering protocols allow numerous forwarders to opportunistically convey packets to the destination, accounting for their time-variant channel conditions. The general idea of OR is that, for each destination, a lot of next-bounce candidate forwarders are chosen and prioritized. At the point when a data packet is to be forwarded, the most noteworthy priority hub among

ISSN 2394 - 7780

candidates that got it will be picked as the following bounce. It leverages the remote broadcast advantage (WBA) to mitigate the impact of packet misfortunes: the packet transmission for a hub can be heard by its neighboring hubs, so the probability of fruitful gathering by at least one hub inside these forwarders can be a lot higher than that of only one fixed next-jump. It is envisioned that OR avoids retransmissions as long as the packet makes forward advancement towards the destination and in this manner lessening the total vitality devoured. Or then again protocols are affirmed to beat BPR protocols regarding the total vitality consumption with lossy broadcast joins. One fundamental issue in planning a vitality productive OR protocol is the manner by which to choose and prioritize the forwarder rundown to limit the total vitality cost.

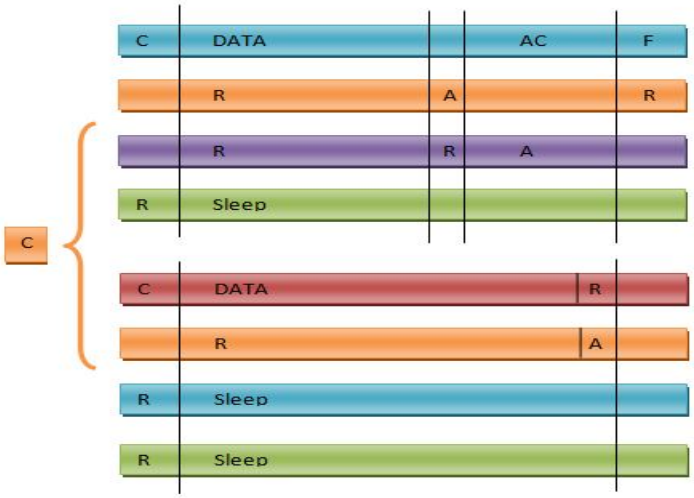


Figure 3: A timing diagram illustrating the routing operation within a single time slot

Coordinated Sleep Scheduling

We accept that the remote hubs are fit for controlling of the radio interface amid a certain period inside an availability. This enables a hub to enter the low-control dozing mode when it doesn't have a bundle to send or to get. In this investigation, we receive the capacity of coordinated rest scheduling to encourage the directing tasks regarding BPR and OR protocols, separately. In the received rest scheduling protocol, a vacancy is partitioned into two periods, to be specific WAKE and DATA periods, separately. By and large, every one of the hubs wake up toward the start of the WAKE time frame in one schedule vacancy. Amid the WAKE time frame, transmitters with the correspondence demand send a flagging parcel of traffic indicator to inform its planned beneficiary hubs. In the interim every single other hub hold tuning in to the channel for the conceivable traffic indicator from any of the neighbors. Amid the DATA time frame, every one of the hubs are permitted to intensity of the radio interface when it doesn't have a bundle to send or to get in this schedule opening. Such coordinated rest scheduling protocol has been broadly examined in research on intermittent rest scheduling. Figure 3 outlines the rest scheduling joined with various steering tasks with the BPR and OR standards, individually. In the accompanying, we talk about the framework of directing tasks joined with the capacity of coordinated rest scheduling utilizing the model appeared in Figure 3. Assume in this vacancy, the sender hub u has a data to transmit and v1; v2; v3 are three neighbor hubs inside its transmission range. For the BPR protocols, we expect that hub v1 is the beneficiary which has been determined ahead of time, while v1 and v2 are two candidate forwarders inside the forwarder rundown Fwd of OR protocol.

WAKE Period: When a data packet is prepared for transmission, sender u transmits a RTS flagging packet with packet length LBPR RTS or LOR RTS in regards to the distinctive directing conventions, and every one of the hubs inside its communicate run v1; v2; v3 are required to get the packet. It contains the forwarder rundown and their needs. Note that for BPR conventions, just a single forwarder is indicated in the field of RTS. DATA Period: During the DATA period, a data packet with packet length Ld is transmitted. The directing activity shifts as for various steering conventions. In the accompanying, we present the point by point task of BPR as well as, individually.

•BPR Packet Transmission: Sender u unicasts the data packet to the predetermined recipient hub, v1, while hubs v2 and v3 turn of their radio amid the remainder of schedule opening to protect vitality. Just hub v1 is required to get the data packet. After an ACK reacted from recipient v1 is gotten at hub u, the data transmission is finished. Something else, sender u will retransmit this data packet in the following accessible schedule vacancy.

•OR Packet Transmission: Sender u multicasts the data packet to the different applicant hubs determined in the

ISSN 2394 - 7780

forwarder rundown fv1; v2g. Hub v3 then turns of the wireless interface to enter the rest mode as it isn't associated with the data transmission in this vacancy. Here we present a TDMA-like methodology in AC period for the OR conventions dependent on. At the point when a planned competitor gets the data packet, it reacts by an ACK packet. These ACK transmissions are conceded in time in a request of their needs. The main competitor with the most elevated need transmits the ACK when it effectively gets the data packet, the second one after a period equivalent to an opportunity to transmit an ACK, etc. At long last, sender u transmits a FI message that shows the hub v1 to assume the liability of forwarding the packet. The packet length of FI message is meant as LFI . The length of AC period is predefined as indicated by the greatest applicants Cm that can be utilized for pragmatic contemplations.

We expect that flagging packets, for example, RTS, ACK and FI, with a little packet length are not expose to transmission mistakes, while data packet transmissions when all is said in done encounter connect disappointments. It is worth to make reference to that those assumptions are made for the most part for straightforwardness of the computations of the normal vitality cost in the accompanying. Since the packets are generally short, it is reasonable to accept that the channel remains moderately consistent for the whole availability.

IV. EXPERIMENTAL RESULTS

Detection Time

Energy Efficient Neighbor Coverage Protocol(EENCP)	Secure Enhanced Adaptive Acknowledgement(SEAACK)	Probability Based Prediction and Sleep Scheduling(PPSS)	Proposed
550	350	600	240
690	280	780	320
750	450	800	600
880	500	950	530
920	690	1030	800

Table-1: Comparison table of Detection

This table portrays the correlation of location time of three existing strategy that is EENCP, SEAACK, PPSS technique and proposed technique. Comparing these four techniques we accept that proposed Method demonstrates least estimations of discovery time from 240 to 800. Though the other three demonstrates a most extreme discovery esteems not exactly proposed strategy.

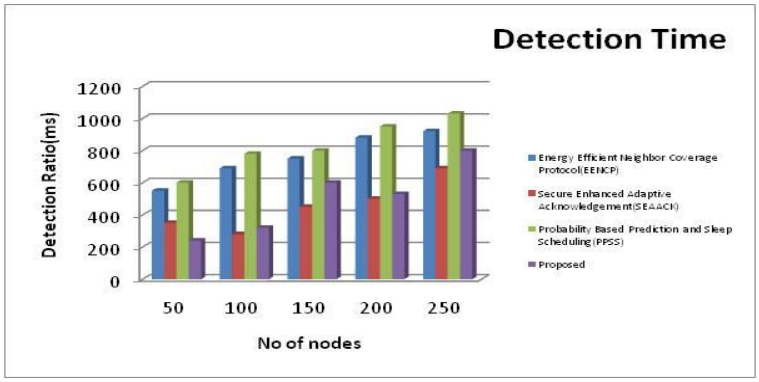


Figure-4: Comparison Chart of detection Level

This chart explains about the detection level of three existing methods and one proposed method. The variations of its range is been explained using no. of nodes in X axis and the detection ratio of the process in Y-axis. While analyzing and comparing proposed method with existing method, proposed Method shows minimum values of detection time from 240 to 800. Whereas, the other three existing methods involves more detection ratio.

False Positive

Energy Efficient Neighbor Coverage Protocol(EENCP)	Secure Enhanced Adaptive Acknowledgement(SEAACK)	Probability Based Prediction and Sleep Scheduling(PPSS)	Proposed
710	600	1000	500
790	650	1290	599
830	780	1450	810
1100	800	1610	1000
600	400	1700	499

Table-2: Comparison table of False positive ratio

ISSN 2394 - 7780

This table describes the comparison of false positive ration of three existing method that is EENCP, SEAACK, PPSS method and proposed method. Comparing these four methods we assume that the false positive ratio of proposed method is less when compared to existing methods.

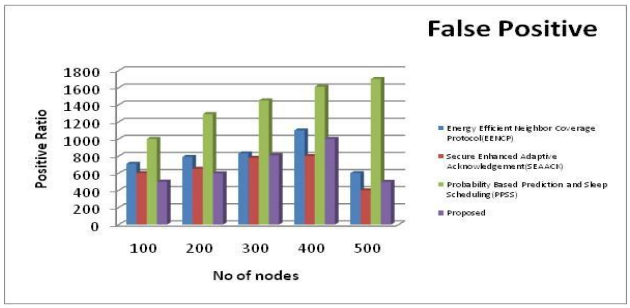


Figure-5: Comparison chart of false positive

The examination outline clarifies about the bogus positive proportion of three existing methods and one proposed method. The variations of its proportion is been clarified utilizing the positive proportion in Y hub and no of hubs in X-hub. The chart shows the correlation of false positive proportion on the proposed and three existing methods. The bogus positive of proportion in proposed method is less in minimum 499 to greatest 1000 when contrasted with other existing methods.

Impact of False Positive

Energy Efficient Neighbor Coverage Protocol(EENCP)	Secure Enhanced Adaptive Acknowledgement(SEAACK)	Probability Based Prediction and Sleep Scheduling(PPSS)	Proposed
500	1100	1000	489
650	1400	1320	620
790	1500	1450	750
900	1700	1699	888
1400	1900	1850	1300

Table-3: Comparison table of Impact of false positive

This table portrays the correlation table of effect of false positive proportion of three existing strategy that is EENCP, SEAACK, PPSS technique and proposed technique. Comparing these four techniques, we expect that the execution of proposed strategy indicates less effect of false positive incentive from 489 to 1300. Though the other three demonstrates a greatest effect of false positive proportion than proposed technique.

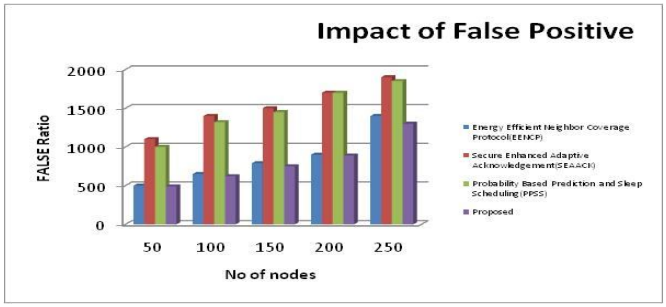


Figure 6: Comparison Chart of Impact of False positive

The examination outline clarifies the Impact of false positive proportion of existing techniques and proposed strategy. This demonstrates proposed strategy process the effect of false positive proportion from 489 to maximum 1300. While, the proportion dimension of three existing techniques EENCP, SEAACK, PPSS demonstrates maximum number of false proportion when contrasted with proposed strategy.

Impact of Malicious Node

Energy Efficient Neighbor Coverage Protocol(EENCP)	Secure Enhanced Adaptive Acknowledgement(SEAACK)	Probability Based Prediction and Sleep Scheduling(PPSS)	Proposed
790	550	500	430
850	650	600	580
910	750	735	625
980	850	800	788
1100	950	901	850

Table-4: Comparison Table of Impact of malicious node

ISSN 2394 - 7780

This examination table portrays the Impact of malevolent hub of three existing strategies EENCP, SEAACK, PPSS and proposed technique. Comparing these four strategies we accept that the proportion of impact of noxious proportion in proposed technique is less from 430 to 850. The current technique demonstrates a most extreme impact of malevolent hub than proposed strategy.

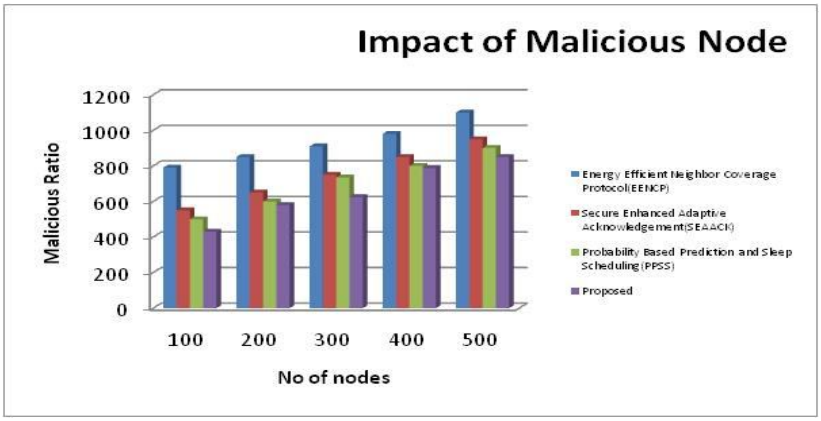


Figure-7: Comparison Chart of Impact of Malicious node

Comparison graph clarifies about the Impact of malignant hubs of three existing Methods and one proposed method. The comparison of these four methods is been clarified utilizing the quantity of hubs in X pivot and its malevolent proportion in Y-hub. The soundness dimension of proposed method is less from 430 to 850, when contrasted with existing methods.

V. CONCLUSION

We present the reenactment based assessment of various energy effective steering conventions with and without the capacity of coordinated rest scheduling. We consider broad framework performance measurements dependent on the all out energy consumption, throughput, and packet delay, just as energy consumption per packet. The outcomes demonstrate that coordinated rest scheduling affects the energy efficiency accomplished by various steering conventions. In the first place, we assess the effect of traffic load over the system on the general performances. At the point when the channel condition is generally great because of the lower traffic load, the EEOR convention can't ensure a higher energy efficiency as contrasted and the MHR convention. At that point, assessment of the hub thickness sway on the general performances demonstrates that MHR even outperforms EEOR in term of energy efficiency in high hub thickness situation. In spite of the improvement of packet conveyance probability accomplished by multi-beneficiary assorted variety gain in OR conventions, the impact of expanded energy consumption at potential forwarders ought to be considered when organize rest scheduling is bolstered.

REFERENCES

1. Sha Liu, Kai-Wei Fan, PrasunSinha, “Dynamic Sleep Scheduling using Online Experimentation for Wireless Sensor Networks”, 2014.
2. Niranjan Kumar Ray and Ashok Kumar Turuk, “A Hybrid Energy Efficient Protocol for Mobile Ad Hoc Networks”, Journal of Computer Networks and Communications Volume 2016.
3. M. T. Hyland, B. E. Mullins, R. O. Baldwin, and M. A. Temple, “Simulation-based performance evaluation of mobile ad hoc routing protocols in a swarm of unmanned aerial vehicles,” in 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW’07), vol. 02. IEEE Computer Society, 2007, pp. 249–256.
4. A. B. R. Kumar, L. C. Reddy, and P. S. Hiremath, “Performance comparison of wireless mobile ad-hoc network routing protocols,” International Journal of Computer Science and Network Security (IJCSNS), vol. 8, pp. 337–343, 2008.
5. A. Neumann, C. Aichele, M. Lindner, and S. Wunderlich, “Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N.) draft-wunderlich-openmesh-manet-routing-00,” Internet-Draft, Apr, 2008. [Online]. Available: http://tools.ietf.org/html/ draft-wunderlich-openmesh-manet-routing-00
6. A. Koul, R. B. Patel, and V. K. Bhat, “Distance and frequency based route stability estimation in mobile adhoc networks,” Journal of Emerging Technologies in Web Intelligence, vol. 2, no. 2, pp. 89–95, 2010.
7. J. Moy, “OSPF version 2,” RFC 2328, April 1998.[Online]. Available: http://tools.ietf.org/html/rfc2328

ISSN 2394 - 7780

8. C. E. Perkins and P. Bhagwat, “Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers,” in SIGCOMM Proceedings of the conference on Communications architectures, protocols and applications, vol. 24. London, England, UK: ACM, 1994, pp. 234–244.
9. T. Clausen and P. Jacquet, “Optimized Link State Routing Protocol (OLSR),” RFC 3626, Oct, 2003. [Online]. Available: http://tools.ietf.org/ html/rfc3626
10. T. Clausen, C. Dearlove, P. Jacquet, and U. Herberg, “The Optimized 198 BIBLIOGRAPHY
11. Link State Routing Protocol version 2,” Internet-Draft, March, 2012.[Online]. Available: http://tools.ietf.org/html/draft-ietf-manet-olsrv2-14
12. D. Yadav and G. S. Mishra, “Performance evaluation of proactive routing protocol for ad-hoc networks,” International Journal of Computer Science and Information Technology and Security (IJCSITS), vol. 2, no. 3, pp. 690–695, 2012.
13. D. Johnson, Y. Hu, and D. Maltz, “The Dynamic Source Routing protocol (DSR) for mobile ad hoc networks for IPv4,” RFC 4728, Feb, 2007. [Online]. Available: http://www.ietf.org/rfc/rfc4728.txt
14. C. E. Perkins, S. Ratliff, and J. Dowdell, “Dynamic MANET On-demand (AODVv2) Routing,” Internet-Draft, March, 2012. [Online]. Available: http://tools.ietf.org/html/draft-ietf-manet-dymo-22
15. K. Tripathi, M. Pandey, and S. Verma, “Comparison of reactive and proactive routing protocols for different mobility conditions in wsn,” in Proceedings of the International Conference on Communication, Computing and Security. ACM, 2011, pp. 156–161.
16. S. Barakovic, B. Sarajevo, Herzegovina, and J. Barakovic, “Comparative performance evaluation of mobile ad hoc routing protocols,” in Proceedings of the 33rd International Convention (MIPRO). IEEE, 2010, pp. 518–523.
17. C. Mbarushimana and A. Shahrabi, “Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks,” in 21st International Conference on Advanced Information Networking and Applications Workshops. IEEE, 2007.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

A STUDY ABOUT MULTI FACTOR AUTHENTICATION SYSTEM OF OTP AND BIOMETRIC

Dr. V. Kavitha[1] and S. Subhasini[2] and B. Sathyabama[3]
Associate Professor[1]& Assistant Professor[3], Department of MCA, Hindusthan College of Arts and Science
Assistant Professor[2], Department of Computer Applications (BCA), Hindusthan College of Arts and Science

ABSTRACT
One Authentication is the progression of identifying a user's uniqueness. It is a procedure of correlating an incoming request with a set of recognizing authentications. The identifications provided are related with a huge file in a database of the authorized user's details on a local operating system or the server of authentication. Security system will search all the conceptual objects that it knows and discover the exact one of which the actual user is presently applying. An original user can be mapped with other conceptual user object in the system, and therefore be granted permissions and rights to the user and that user must provide evidence to show his identity to the system. The procedure of determining claimed user unique user offered evidence is referred as authentication and the evidence which is offered by the user throughout process of authentication is termed as credentials. To implement the security multi factor authentication system, there are numerous authentication methods available. In that, one time password authentication method and biometric authentication methods are utilized to prove the effective security authentication procedures.

Keywords: Security, authentication, SMS, Biometric

I. INTRODUCTION

Authentication is one of the significant progression where a user identifies about themselves through sending the first person x to the system, that system authenticates their identity and checking that it equal values. Authentication remains an essential safeguard against the illegal and criminal usage to the device or any other sensitive online and offline applications. Authentication starts when a client tries to access the information. Basically the user must confirm their access identity and rights. When login the computer users must enter their login id and password for authentication purposes. These combination is providing access to the user and it must be avoided by the hackers. A technique of biometric is one of the better form of authentication according to the presence of the user and their biological makeup such as finger prints and retina. This technology prevents the illegal process from the hackers to break the system.

Generally, there are three kinds of authentication factoring systems available. At first, the one factor authentication system, also referred as Single factor authentication was proposed which is used to authenticate the subject. This system was typically adopted by the community due to its easiness and user friendliness. For an instance, the uses of a password which is used to confirm the rights of the users could be considered. It seems that, single factor authentication system is the weakest level of authentication.

Subsequently, the next system of two factor authentication was projected that couples the representatives data such as the combination of user name and password with the factor of individual rights such as a smartcard or phone. It look likes that, two factor authentication system is the moderate level of authentication. Consequently, the multi factor authentication was proposed to provide a higher level of safeguard and continuous protection of computing gadgets from unauthorized illegal access by using more than two credentials.

Multi factor authentication system involves some of the authentication methods such as Universal Second Factor (U2F) Security Keys, Physical one time Pin(OTP) Tokens, Biometrics, Smart cards, Mobile Applications, Short Message Service (SMS) Messages, Software Certificates. If an authentication methods offers the ability to shrink the number of authentication factors to a single factor it is by definition no longer a multi factor authentication to the user at any time.

II .MULTI FACTOR AUTHENTICATION METHODS

Generally, more number of authentications methods are available which is used to provide a security in various levels. Some of the multi factor authentication methods are discussed below. U2F Security Keys is one of the authentication method which uses a physical token or card termed as U2F authenticator as a second factor. The U2F security key utilizes public key cryptography to rectify the user's identity by signing an experiment response and request from a service which is passed through any mobile app or any web browser. OTP - Physical one time token is another kind of authentication method that exhibits a time limited one time pin on its screen. Time on both authentication service and physical token are processed and the it verifies the authentication details are correct for that user and permits or rejects the service.

ISSN 2394 - 7780

Biometric is the second factor of multi factor authentication system like iris scan or fingerprint which provide the authentication service through the passphrase along with the biometric data. This kind of security authentication is considered as the maximum security measure of multi factor authentication method. Smartcard authentication method utilizes a private key stored on it as a second factor. This method has a potential security vulnerability through the software involved to interact with the smart card. This method uses a time limited one time PIN or password provided through the mobile app as a second factor. The most significant advantage of this method is providing the services with minimum cost. The above said authentication methods are obtainable to provide security.

ONE TIME PASSWORD AUTHENTICATION METHOD

OTP refers One Time Password it also known as One Time Pin. This is a password that is authenticate for only transaction or one login session on any digital gadgets or computer devices. OTPs keep away from a number shortcomings that are correlated with conventional static password based authentication, a number of developments also integrate with two factor authentication through ensuring that the onetime password needs access to something a human has as well as something a human knows. The most significant improvement is addressed by OTPs is that in contrast to static password. These passwords are not helpless to repeat attacks. This refers that a potential interloper who maintains to record an OTP that was already utilized to log into a service or to accomplish a transaction will not be capable to misuse it, since it will no longer be suitable. Next advantage is that a user who utilizes the similar password for multiple systems, If the password for one of these is obtained by an attacker. OTPs are an possible replacement for traditional password authentication system. Moreover OTPs are not easy form human being to remember. Hence, it need added technology to perform. OTPs can be incorporate with limited usability of addition OTPs like SMS, Voice and Hybrid.

One Time Passwords via SMS

SMS based OTPs are providing more security. With a 98% open rate within 30 seconds, SMS is known for its high reliability. By sending One Time Passwords via SMS, the users are sure to reach their communications wherever they are. Then security providers have migrates to time based OTPs, which refers to TOTP.

One Time Passwords via Voice

Alternatively, the next type of authentication system is introduced called as OTP through Voice SMS. With Voice, the spoken password is obtained as a phone call on the user's mobile. The passwords will not be gathered on the user's phone and Voice allows you to reach users with limited sight.

One Time Passwords via Push

Another kind of OTP is cost effective channel Push. The user can view the OTPs through their apps which is installed in their gadgets, after that the OTP will be disappeared on their phone devices.

One Time Passwords via Hybrid

To make the smart solutions among the various OTP solutions. it make sure all passwords are delivered fruitfully.

OTP GENERATION AND VERIFICATION SOLUTION

A one-time password (OTP) is an automatically produced numeric or alphanumeric string of characters that authenticates the user for a single transaction or session. This is utilized by several online platforms to validate customer transactions and identity. User Authentication while creating transaction is the most considerable factor for many businesses. Phonon provides one of the most secure authentication methods by creating a token or random code and sends OTP via. SMS, Email and Voice Calls to the users. Once user gets the token or randomly generated code, then user can enter those details and validate it.

During OTP delivery to the user, Phonon maintains strict TRAI and NDNC compliance while sending messages and making calls to the registered phone numbers. For email delivery, Phonon uses Amazon SES Integration with SPF and DMAC / DKIM authentication to ensure that the mail is delivered to the Primary inbox of the user. OTP (One Time Password) security is maintained through a one-way hash based on the HMAC SHA algorithm.

Fig 1 depicts the functionality of one time password generation, which is the user, received the one time password, that code will be feed on to the system though the pin and token code by the user. That code must be evaluated by the authentication manager with the support of internet and RSA authentication technique. Then the final process of RSA authentication agent authenticated the rights through any corporate network. The principle of a one-time password (OTP) generator is to make it more difficult to gain unauthorized access to restricted resources, such as a mail account or a database with sensitive information. Static user login names and

ISSN 2394 - 7780

passwords can be accessed more easily by an unauthorized interloper given much attempts and time. By continuously altering the password, as is done with a one-time password, this risk can be greatly reduced. Conventional authentication solutions that issue one time passwords make use of a key fob or hardware token to generate OTPs. The cost and maintenance of these tokens, plus the distribution and management thereof, demands more logistical resources as well as additional costs.

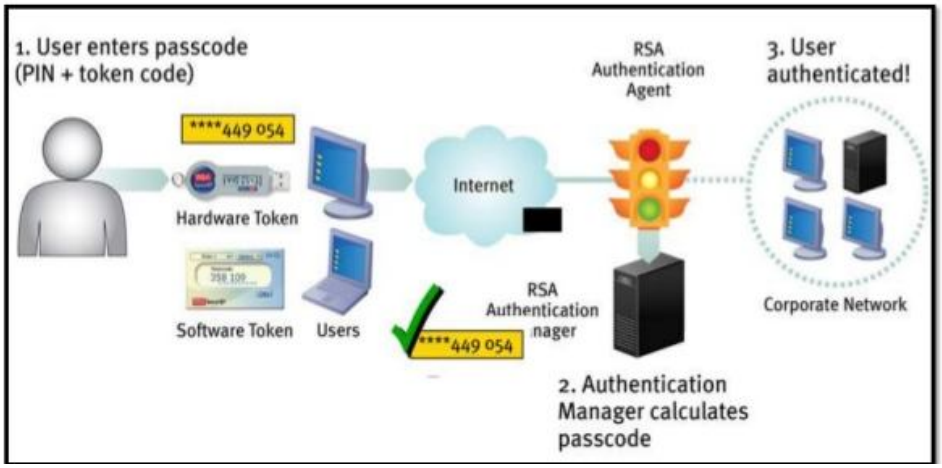


Fig-1: One Time Password Generator

BIOMETRIC AUTHENTICATION METHOD

Biometric is one of the most significant authentication method which is used to provide security process that relies on the unique biological characteristics of a human being to verify that the reliability of the person.

Fig-2: Biometric Authentication System

This kind of security authentication system compares a biometric data capture to stored in a database and confirm the authentic data in the database. The final authentication is confirmed whether both the samples of biometric data and its authentication is match. Likely, biometric authentication is utilized to control access to physical and digital resources like rooms, electric gadgets and construction building. Modern biometric verification has turn out to be almost instantaneous, and is more and more accurate with the arrival of computerized databases.

Fig 2 depicts the functionality of biometric authentication system from various devices. Biometric authentication system is a consumer identity confirmation process that absorb biological user input or scanning or analysis of some part of the human's body. This method is utilized to protect many different types of systems from logical systems make possible through any hardware approach points to physical systems sheltered through physical barriers, like secure facilities and sheltered research sites.

This kind of authentication method is the process of evaluating data for the human's characteristics to that mankind's biometric in order to establish similarity. These collected data stored and compared to other person's biometric data that must be authenticated and verified.

VARIOUS KINDS OF BIOMETRIC AUTHENTICATION TECHNOLOGIES

Generally, numerous kinds of biometric authentication techniques are available. Each techniques are utilized to receive the unique authentication from various devices and verify the authentication.

ISSN 2394 - 7780

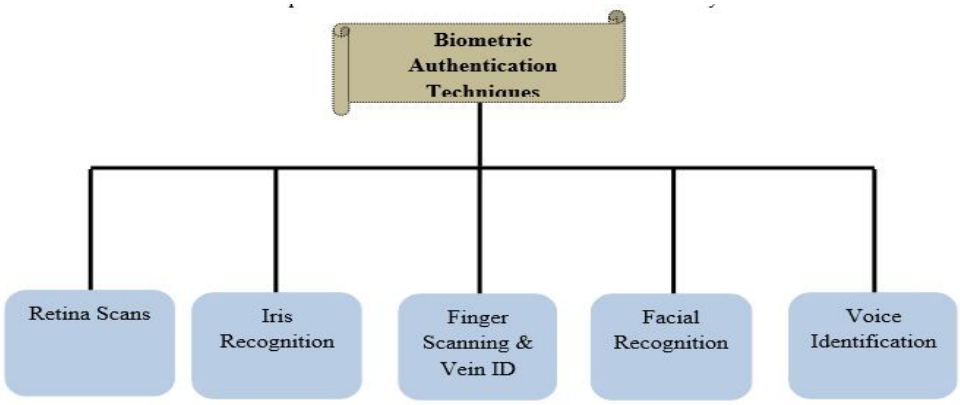


Fig-3: Various Kinds of Biometric Authentication Techniques

Fig 3 represents the different scan systems like retina scans, iris recognition, finger scanning and vein ID, Facial recognition and voice identification techniques. The first technique of retina scans create an image of the blood vessel pattern in the light sensitive surface lining the human being's inner eye. And next technique of iris recognition is utilized to discover individuals based on exclusive patterns within the ring shaped area surrounding the human being's eye. Subsequently, Finger scanning and finger vein ID are used. Finger scanning is the digital version of the ink and paper finger printing method, efforts with fine points in the pattern of raised areas and branches in a person's finger image and finger vein ID is established on the unique vascular pattern in an individual's finger. After that, the facial recognition system works with numeric codes described face prints, which discover 80 nodal points on the human face. Then the final authentication security method is voice identification, which rely on characteristics created through the shape of the speaker's mouth and throat, rather than more variable conditions.

CONCLUSION

Authentication is the progression of identifying a user's uniqueness. It is a procedure of correlating an incoming request with a set of recognizing authentications. The identifications provided are related with a huge file in a database of the authorized user's details on a local operating system or the server of authentication. To implement the security multi factor authentication system, there are numerous authentication methods available, which is used to provide more securable authentication to the authorized person. Among the various authentication methods, one time password authentication method and biometric authentication methods are utilized to prove the effective security authentication procedures. The purpose of these authentication systems protecting the legal secured and authorized objects from the illegal activities.

REFERENCES

[1]. Aceves, P. A., & Aceves, R. I. (2009). Student identity and authentication in distanceeducation: A primer for distance learning administrators. Continuing HigherEducation Review, 73, 143-152.

[2]. Adams, F. (2012). Who's who in distance education: Authentication and academic integrity.Distance Learning, 9(1), 13-19.

[3]. Al-Assam, H., Sellahewa, H., &Jassim, S. (2011). Accuracy and security evaluation ofmulti-factor biometric authentication. International Journal for Information SecurityResearch, 1/2(1), 11-19.

[4]. Kim, J. J., & Hong, S. P. (2011). A method of risk assessment for multi-factor authentication.Journal for Information Processing Systems, 7(1), 187-198.

[5]. King, C. G., Guyette, R. W., & Piotrowski, C. (2009). Online exams and cheating: Anempirical analysis of business student's views. The Journal of Educators Online,6(1), 1-11.

[6]. Makransky, G., &Glas, C. A. (2011). Unproctored internet test verification: Using adaptiveconfirmation testing. Organizational Research Methods, 14(4), 608-630.

[7]. Marais, E., Argles, D., & Von Solms, S. H. (2006) Security issues specific to e-assessments.Proceedings of the 8th Annual Conference on WWW Applications.

[8]. Gao, Q. (2012). Using IP addresses as assisting tools to identify collusions. International Journalof Business, Humanities and Technology, 2(1), 70-75.

[9]. Gathuri, J. W., Luvanda, A., &Kamundi, S. M. M. S. (2014). Impersonation challengesassociated with e-assessment of university students. Journal of Information Engineeringand Applications, 4(7), 60-68.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

WAVELET TRANSFORM TECHNIQUE FOR MAMMOGRAM IMAGE ENHANCEMENT

Dr. N. Revathy[1], T. Guhan[2], Dr. T. A. Sangeetha[3] and Dr. V. Kavitha[4]
Associate Professor[1,4], PG and Research Department of Computer Applications, Hindusthan College of Arts and Science, Coimbatore
Assistant Professor(SG)[2], Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore
Assistant Professor[3], Department of Computer Science, Kongu Arts and Science College, Erode

ABSTRACT
One of the most significant causes of increased women death rate in the world is due to Breast cancer. Mammography is the most effective method for early detection of breast diseases. The main aim of mammography is to detecting, non-palpable cancers during its premature stage. Conversely, mammograms are extremely complex to deduce being the fact that the pathological transformations of the breast are slight and their visibility is very poor with low contrast and noise. Mammograms have the significant information such as micro calcifications and masses, which are extremely complicated to detect because mammograms are of low-contrast. Cancer detection using mammography mainly concentrates on features of tiny micro calcifications, together with the number, size and spatial arrangement of micro calcification clusters and morphological features of individual micro calcifications. In the current scenario, Content-Based Image Retrieval (CBIR) techniques have gained considerable attention for medical images analysis. It is necessary to enhance the mammogram images because the mammogram images are very noisy, low-contrast, blur and fuzzy, for accurate identification and early diagnosis of breast cancer. In this paper, proposed efficient techniques to enhance the mammogram image using the wavelet transform technique (WTR) which is used to take clear decision in the medical field. The technique is to be measured with various performance factors. The results are also improved.

Keywords: Breast Cancer, Mammography, Image Enhancement, and wavelet transform technique.

I. INTRODUCTION

Breast cancer is one of the main reasons for death among women. Early detection and treatment are regarded as the most suggested approach to reduce breast cancer mortality. Breast cancer is a type of cancer caused by breast tissue, which occurs mostly in the inner lining of milk ducts or the lobules that supply the ducts with milk. Cancers originates from ducts are known as ductal carcinomas, while those originates from lobules are known as lobular carcinomas. Breast cancer usually occurs in humans and it occurs in other mammals too. Majority of human cases occur in women, male breast cancer can also occur.

Mammogram

Mammogram is a medical test that uses x-rays to take pictures of the internal structure of the breast. The testing is also known as "mammography."A mammogram is a radiograph of the breast tissue. It is an effective method of investigating the breast, typically for the diagnosis of breast cancer. Mammography is a radiographic examination of the breast and the most significant investigation to identify early stages of breast cancer.

But the digital mammography is very noisy, low-contrast, blur and fuzzy and hence there is a requirement for enhancing images. This is essential for enhancing the Peak Signal-to-Noise Ratio (PSNR) and reducing the Mean Squared Error (MSE) for accurate identification.

Mammograms are done for two reasons

i. Screening: When women participate on a routine basis to have mammograms done to find breast cancer at premature stage. This type of mammogram looks for the indications that breast cancer may be spreading, even though no symptoms are there.

ii. Diagnostic: This is typically done to check for breast cancer after a lump or any other sign/symptom has been found such as pain, nipple discharge, skin thickening, or a change in breast size or shape. It will be used as a second test if a screening mammogram finds something that is not normal.

One of the most important objectives of mammogram image enhancement is to enhance the contrast between regions of interest and the background. Also the medical images fluctuate extensively in terms of acquisition, noise characteristics and quality. Thus, there is a requirement to process an image on the image basis. This motivates the design and construction of effective mammogram image enhancement techniques using various transforms and fuzzy enhancement method.

ISSN 2394 - 7780

II. LITERATURE REVIEW

Digital mammography is one of the most suitable methods for early detection of breast cancer. However, the visual clues are faint and vary in appearance which makes diagnosis difficult and challenging. There is a significant requirement for developing methods for automatic classification of irregular areas in mammograms for aiding radiologists to improve the efficiency of screening programs and avoid unnecessary biopsies. Micro calcifications occur in mammogram image as small localized granular points with high brightness. It cannot be detected easily by naked eye because of its miniaturised dimension. Due to its small size, about 10-40% of micro calcification clusters are missed by radiologists.

Vetterliet al.,[11] pursued two dimensional transform that can capture the intrinsic geometrical structure that is key in visual information. The important challenge in exploring geometry in images comes from the discrete nature of the data. Hence, unlike curvelets, which develop a transform in the continuous domain and then discretize for sampled data. They constructed a discrete-domain multi-resolution and multi-direction expansion using non-separable filter banks. This formation results in a flexible local, multi-resolution, and directional image expansion using contour segments and it was named as contourlet transform. The discrete contourlet transform has a fast iterated filter bank algorithm that requires N operations for N-pixel images. Furthermore, they established a precise link between the developed filter bank and the associated continuous domaincontourlet expansion via a directional multi-resolutionanalysis framework. They showed that some numerical experiments demonstrate the potential of contourlet in several image processing applications.

Cunha et al.,[12] discussed the non sub-sampled contourlet transform (NSCT) and study its applications. The construction is based on a non sub-sampled pyramid structure and non sub-sampled directional filter banks. The result is a flexible multi-direction, multi-scale, and shift-invariant image decomposition that can be efficiently implemented by a trous algorithm. They also studied the filter design problem and designed a framework based on the mapping approach. They exploited the less stringent design condition of the non sub-sampled filter bank to design filter that lead to a NSCT with better frequency selectivity and regularity when compared to the contourlet transform. NSCT allows for a fast implementation based on a lifting or ladder structure that only uses one-dimensional filtering in some cases. In addition, this design ensures that the corresponding frame elements are symmetric, regular, and the frame is close to a tight one. They also assessed the performance of NSCT in image denoising and enhancement applications.

III. METHODOLOGY

Mammography is a specific kind of imaging that utilizes a low-dose x-ray system to check breasts. A mammography exam is called as mammogram, used to assist in the premature detection and early diagnosis of breast cancer and related diseases in women. An x-ray is noninvasive medical tests that assist physicians in diagnosing the disease. Imaging with x-rays involves exposing a part of the body to a tiny amount of ionizing radiation to generate pictures of the inside of the body. X-rays are the traditional and most commonly used form of medical imaging.

A. Wavelet Transform

The Wavelet transform (WT) is a powerful mathematical tool, with several applications in computer graphics and image processing [19]. The wavelet analysis is done by applying a function called the mother wavelet (usually denoted by $\psi(x)$) to a signal/image, which allows not only to identify its frequency components, but also the spatial location where these components appear. The notion of scale is very important in the wavelet theory such as the coarser the scale of analysis, the fewer details of the signal is caught. On the other hand, finer scales capture more details of the processed signal/image. Model for digital enhancement in the wavelet domain is presented.

It explores wavelet coefficients to ensure the proper preservation of the image structure and correct filling of the enhanced region with block-based texture synthesis. The method takes an image I and a user defined in painting mask Ω as input, and decomposes both images using a decimated Wavelet Transform. Wavelet Coefficient is then propagated into the enhanced region, and the inverse Wavelet Transform is applied to obtain the final reconstruction image[13].The wavelet transform is a type of multi-scale analysis that decomposes input signal into high frequency and low frequency approximation component at different resolutions.

To enhance the features, the selected coefficients are adjusted by multiplying with an adaptive gain value. The enhanced image is then reconstructed using adjusted wavelet coefficients.

For wavelet coefficient propagation into the enhanced region, there are two important steps that must be executed at each iteration in the algorithm. After the data have been prepared, the proposed model iteratively fills the in painting region, until it is completely filled. At each iteration, a block with varying size is selected as

ISSN 2394 - 7780

the filling target, based on its geometric aspects and the energy of the wavelet coefficients in neighboring regions. Once this block is determined, the patch filled is selected by considering the structural aspects and the texture in the neighborhood of the in painting block. The next inner steps of this model are especially the approach for determining the priority of in painting blocks and the metric used in the block-based wavelet texture synthesis.

Mencattini et al., proposed a novel algorithm for image denoising and enhancement based on dyadic wavelet processing [17]. The denoising stage is based on the limited iterative noise difference evaluation. In addition, in the case of micro calcifications, it is proposed an adaptive change of improvement degree at various wavelet scales, while in the case of mass discovery an original segmentation technique combine with dyadic wavelet information by processing mathematical morphology is evaluated. The new approach consists of using the similar method core for giving out images to distinguish both micro calcifications and masses.

The Wavelet Transform in which, it processes the digital enhancement of mammogram images in the wavelet domain. In the Wavelet Transform in which it consists of many steps like data presentation, searching of the best block to fill, Edge strength, edge orientation and the confidence term. The drawback of Wavelet Transform is the method in which problem of filling the missing data will occur and the PSNR value is very low. So Curvelet transform is used for further enhancement study.

IV. EXPERIMENTAL RESULT

The Experimental results of the wavelet transform are explained below. Two datasets are taken from the UCI Machine Learning Repository. The datasets used in the proposed method are

- Wisconsin Diagnostic Breast Cancer (WDBC)
- Breast Cancer Dataset

Besides, the quality of the images are evaluated using the traditional distortion measurements such as

- Mean Squared Error (MSE)
- Peak Signal-to-Noise Ratio (PSNR)

For these images the mean square error and peak signal to noise ratio is calculated to find the better transformation. The input mammographic denoised image is shown in the Figure1.

Image Enhancement Technique	Database	Mean Square Error
Wavelet Transform Technique	Wisconsin Diagnostic Breast Cancer Dataset	4.514908

Image Enhancement Technique	Database	Peak Signal to Noise Ratio(PSNR)
Wavelet Transform Technique	Wisconsin Diagnostic Breast Cancer Dataset	42.315603

MSE of the output image is defined as

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|x(i,j) - \hat{x}(i,j)|^2}{MN}$$

where $x(i,j)$ is the original image, $\hat{x}(i,j)$ is the output image, and MN is the size of the image.

MSE is calculated for wavelet transform technique all .

Peak Signal to Noise Ratio (PSNR)

PSNR is defined as

$$PSNR = 20 \log_{10}\left[\frac{(2^n - 1)}{\sqrt{MSE}}\right] \text{ (dB)} \qquad (1.2)$$

where n is the number of 8bits/pixel used in representing the pixel of the image.

PSNR is calculated in the Wavelet Transform enhancement technique.

ISSN 2394 - 7780

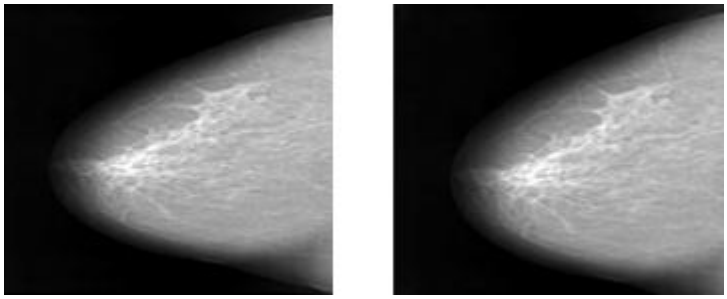


Figure-2: Enhanced Image Using Wavelet Transform

In figure 2 Enhanced Image Using Wavelet Transform techniques, the performance factors of mean square error (MSE) and peak signal noise ratio (PSNR) are calculated which is applied to improve the quality of the image. Hence, the input image of mammographys quality is enhanced and improves while comparing other image enhancement techniques. In image denoising, discovering major image descriptions and change the degree of noise smoothing appropriately. Hence the image needs to purify it for discovering the quality image with the support of Wavelet transform technique.

V. CONCLUSION AND SCOPE FOR FUTURE WORK

Presently one of the major significant causes of cancer death between young and middle aged women is breast cancer. Mammography is the most important technique in the medical field used by radiologists for preventing and diagnosis of breast cancer through the images. For detecting the premature breast cancer, digital mammogram is an excellent technique. Digital mammogram is used to capture electronic images of the breast and acquire it in the computer. Generally the mammogram images are low contrast, very noisy, fuzzy and blur. Because of these reasons the mammogram are enhanced for attaining accurate and more clarity images to identify the breast cancer. Hence these images need high computational abilities. In this paper, the mammogram images are enhanced using wavelet transform technique. The experimental result concentrates the performance factors of MSE and PSNR measures. As a future work, using some other transform techniques are used to detect and improve the mammogram images with more accurate result.

REFERENCES

1. H.D.Cheng, X. Cai, X. Chen, L. Hu, X. Lou, “Computer aided detection and classification of micro calcification in mammograms: a survey”, Pattern recognition vol. 36,pp. 2967-2991, 2003.
2. D.NarainPonraj, M.Evangelin Jenifer, P. Poongodi, J.Samuel Manoharan, “A Survey on the Preprocessing Techniques of Mammogram for the Detection of Breast Cancer”, Journal of Emerging Trends in Computing and Information Sciences, vol. 2, no. 12, pp 656-664, December 2011.
3. http://en.wikipedia.org/wiki/Breast_cancer.
4. T.S.Subashini, V. Ramalingam and S. Palanivel, “Pectoral Muscle removal and Detection of masses in Digital Mammogram using CCL”, International Journal of Computer Applications, vol. 1, no. 6, pp. 66-70, 2010.
5. Keir Bovis and Sameer Singh, “Enhancement Technique Evaluation using Quantitative Measures on Digital Mammograms”, Proc. 5th International Workshop on Digital Mammography, Toronto, Canada, M.J. Yaffe (ed.), Medical Physics Publishing, pp. 547-553, 2000.
6. R. Krishnamoorthy, N. Amudhavalli and M.K. Sivakkolunthu, “An Adaptive Mammographic Image Enhancement in Orthogonal Polynomials Domain”, International Journal of Computer and Information Engineering, vol. 4, no. 2, pp. 120-128, 2010.
7. B. Verma, P. Zhang, “A novel neural-genetic algorithm to find the most significant combination of features in digital mammograms”, Applied Soft Computing vol. 7, pp. 612-625. 2007.
8. R.G. Bird, T.W. Wallace, B.C. Yankaskas, “Analysis of cancers missed at screening mammography”, Radiology, vol. 184, pp. 613-617,1992.
9. H.Burhenne, L. Burhenne, F. Goldberg, T. Hislop, A.J. Worth, “Interval breast cancers in the screening mammography program of British Columbia: Analysis and classification,” vol. 162, pp.1067–1071,1994.
10. J. K. Romberg, M. B. Wakin, and R. G. Baraniuk, "Multi-scale geometric image processing", In Proceedings of the SPIE: Visual Communications and Image Processing, pp. 1265-1272, 2003.

ISSN 2394 - 7780

11. M. N. Do and M. Vetterli, "The contourlet transform: an efficient directional multi-resolution image representation," IEEE Trans. Image Process, vol. 14, pp. 2091-2106, 2005.
12. A. L. Da Cunha, J. Zhou, and M. N. Do, "The Non sub-sampled Contourlet Transform: Theory, Design, and Applications," IEEE Trans. Image Process, vol. 15, pp. 3089-3101, 2006.
13. E. J. Candès and D. L. Donoho, "Curvelets," [Online] Available:http://www.stat.stanford.edu/~donoho/Reports/1999/curvelets.pdf, 1999.
14. A. Cohen, C. Rabut, and L. L. Schumaker, Eds. Nashville, "Curvelets—A surprisingly effective non adaptive representation for objects with edges," in Curve and Surface Fitting: Saint-Malo 1999, TN: Vanderbilt Univ. Press, 1999.
15. Starck, Murtagh, E.J Candes , D.L. Donoho, "Gray and Color Image Contrast Enhancement by the Curvelet Transform," IEEE Transactions on Image Processing .vol. 12, pp. 706- 716, June 2003.
16. Jean-Luc Starck, Emmanuel J. Candes, and David L. Donoho, "The Curvelet Transform for Image Denoising" IEEE Transactions on Image Processing, vol. 11, no. 6, June 2002.
17. Y. Kiran Kumar, "Comparison Of Fusion Techniques Applied To Preclinical Images: Fast Discrete Curvelet Transform Using Wrapping Technique & Wavelet Transform", Journal of Theoretical and Applied Information Technology © 2005 - 2009 JATIT.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

PALM PRINT AUTHENTICATION FOR BIOMETRIC PRIVACY USING VISUAL CRYPTOGRAPHY

Dr. M. Suganya and Dr. R. Padmapriya
Associate Professor, Department of Computer Science, Rathnavel Subramaniam College of Arts & Science, Sulur

ABSTRACT
Managing Biometrics deal with automated methods of identifying a person or verifying the identity of a person based on physiological or behavioral characteristics. Preserving the biometric privacy such as digital biometric data (eg. face, iris, retina and fingerprint) is very important nowadays. In some traditional cases, the security systems are processed by passwords, personal identification numbers, and identification cards. In these cases, several problems occur due to the card was stolen and password hacking. Hence, to avoid such limitations it is necessary to implement the digital biometric data units in terms of face, iris, palm, fingerprints and voice. Among these data, the palm print is considered in this work to explore the possibility of cryptography. Initially, the palm images are selected and stored in the database to cross-check the identity of private images which is considered as input, then the enrollment is made by comparing the public host images. The image is authenticated with the help of database with images. Finally, the decision is taken by matching the originally targeted palm image.

Keywords: De-identification, Privacy, Palm Vein Authentication, Visual Cryptography.

I. INTRODUCTION
Biometrics is one of the human characteristics, used for identification and security purposes. It has several advantages when compared with non-biometric applications, such as no external equipment is a need, there is a unique identification hence, data theft is avoided and biometric is always distinctive and made with characteristics. Some examples of biometric are listed as a fingerprint, palm veins, face recognition, DNA, palm print, recognition, retina, and scent.

Biometrics is defined as an automatic identification of an individual based on their behavioral or physiological characteristics. Some of the biometric applications are in entry controls in airport, ATMs and Government programs. Apart from these uses the biometric security is used for real-time applications such as internet banking, household applications and so on. Kataria et al., (2013) made a survey of the biometric techniques. In traditional cases the system is accessed by two step process, first, the process by which the user professes an identity by providing a username and a password used for the purpose of identification. Next, the verification process is made by authenticating the user. Biometric is well suited for both the type of identification and authentication. Commercially, biometric is used in workstations, for access the control over voice or face recognition system, for door security, for portable media such as mobile hard drives and USB sticks.

The biometric authentication system is used to process the registered user's image which is stored in the database. If a new user needs to access the system then it is necessary to register the detail by enrollment process, which is shown in figure 1. Here the information is characteristics by the person. The information stores the data by means of templates. After registration, the user data is collected as private image and recognized by verifying the image which is previously registered an image.

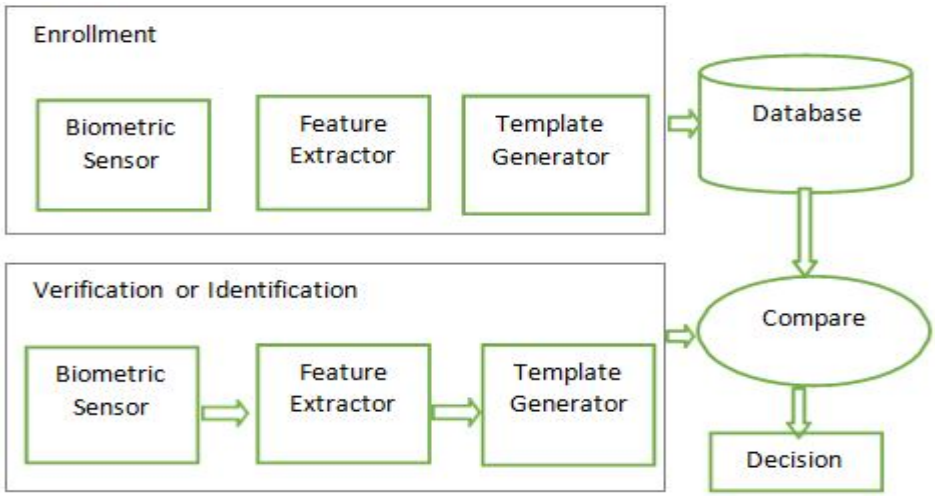


Fig-1: Biometric Authentication Process

ISSN 2394 - 7780

The authentication process is common for all types of biometric process, in this research palm print is considered it is similar to fingerprints, palms of the human hands contain a unique pattern of ridges and valleys. Generally, the area of the palm is much larger than the area of a finger and compared with the result, palm prints are expected to be even more distinctive than the fingerprints.

The registered palm pattern is stored in the database along with the personal details of the client, as shown in figure 2, if a palm is placed in the scanner then the special characteristic of the reduced hemoglobin coursing through the palm print is absorbed near- infrared light. This process takes a snapshot of the outer skin, hence, it is very hard to read or steal.The scanners used for palm print need to capture a large area, hence, it is bulkier and more expensive than the fingerprint. Human palms also contain additional features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, it results in cheap. If a high-resolution palm print scanner is used then the geometry features such as width, length, and area of a palm, ridge and valley features such as minutiae and singular points such as deltas, principal lines, and wrinkles may be combined to build a highly accurate biometric authentication system. Generally, in palm print based authentication system hand image of an individual is collected and then processed by preprocessing steps like image threshold ing, border tracking, segmentation, and ROI location are sequentially executed to obtain a square region which possesses the palm- print data.This section illustrated about basic palm registration process and general biometric applications. Section 2 reviews some traditional methods and applications implemented in several applications. Section 3 state's methodology with visual cryptography, in section 4, the experimental results were made for proposed design evaluation. Finally, the paper is summarized in section 5.

II. LITERATURE SURVEY

The automated biometric authentication system is recently developing rapidly, but since it is necessary to enhance the system to outperform the task. This section reviewed in detail about the biometric applications and implementation.Past many researchers were focused on security applications and stated a lot of challenges in biometric. An introduction to biometric authentication systems is made by Wayman et al., (2005), they stated generic biometric system with some of the applications. They also stated some of the security and privacy issues.

Lin and Fan (2004) presented an approach for personal verification using palm-dorsal vein thermal images in patterns. The characteristics of this method is that has no prior knowledge about the objects and the parameters can be set automatically. They have adopted an Infrared (IR) camera to capture the thermal images of the palm-dorsa. Feature Points of the Vein Patterns (FPVPs) are extracted within the region of convergence by modifying the basic tool of watershed transformation based on the properties of thermal images. Finally, the hierarchical integrating function is applied to integrate multiple features and multi- resolution representations. They have made a logical and reasonable method to select a trained threshold for verification.

In biometric technology, the finger vein authentication plays a major role in security and convenience. The image captured by the camera under IR light consists of veins and its backgrounds such as muscles, bones, and tissues. Mulyono and Jinn (2008) proposed a method to enhance the image quality. The noise produced by the camera and the light effect reduces the quality of the Image. They processed the image with adaptive threshold method and matched them using improved template matching.

Based on the real-time applications, to ensure customer security, Suruga bank launched its “Bio Security Deposit” in July (2004), the world’s first financial service to use Palm Secure. This service features high security for customers using vein authentication, it does not require a bank card or passbook and prevents withdrawals from branches other than the registered branch and ATMs thereby minimizing the risk of fraudulent withdrawals. Zhang et al., (2007) proposed personal authentication using palm vein. They included infrared palm images capture, detection of Region of Interest, Palm vein extraction by multi-scale filtering and matching.

Wang and Leedham (2006) made a near and far-infrared imaging for vein pattern biometrics. Badawi (2006) made a hand vein biometric verification prototype for testing performance and patterns similarity. Li et al., (2010) made a palm vein biometric recognition based on curvelet. Wang et al., (2008) presented a person recognition system by fusing palm print and palm vein images based on “Laplacianpalm” representation. Wang et al., (2007) made an infrared imaging of hand vein patterns for biometric purposes.

Noh et al., (2016) represented some overview and challenges of palm vein biometric system. Akbar et al., (2016) made a palm vein biometric identification system using local derivative pattern.Lu et al., (2016) palm vein recognition using directional features derived from local binary patterns.Lan et al., (2010) made a design based on FPGA-based palm vein acquisition system. Dere et al., (2016) designed a human identification model

ISSN 2394 - 7780

using palm vein images.

III. RESEARCH METHODOLOGY

From the literature, it is noticed that biometric privacy is improved by the various recognition system, identification model and implemented in some real time systems. This section gives the brief explanation of visual cryptography and methodology used for palm print based biometric system. The biometric units may differ according to the applications, in this research palm print is considered for the process. The proposed approach is made with palm print processing, initially, enrollment process for accessing the secure resource is shown in figure 3.The image is captured by the scanner and stored in the format of the image. The scanned image is a digital image, there is a need to make it as multiple segments called as super-pixels. Then normalization process taken place for changing the range of pixel intensity values, it is carried by sheet models. Finally, the feature extraction is made by convolving the normalized palm print pattern into one-dimensional wavelet.

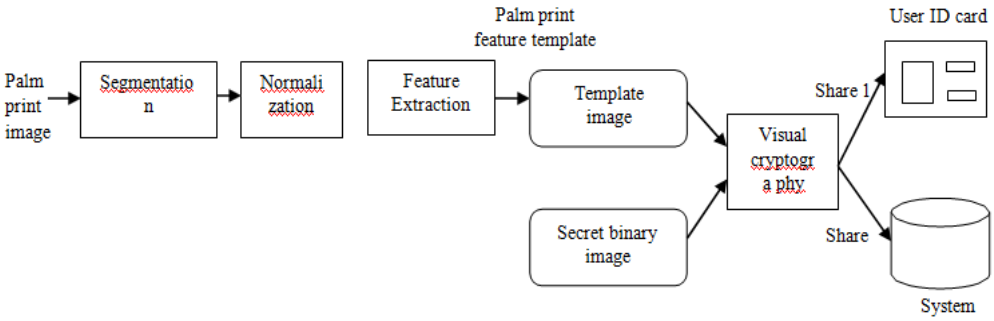


FIG.3. ENROLLMENT PROCESS OF PALM PRINT PROCESSING

After template image generation the secret binary image is compared with the template image to encrypt the pictures. This process is done by a cryptographic technique called as visual cryptography. The encrypted and decrypted images are transferred through this unit and stores the data in the database.A simple algorithm for visual cryptography is given by encrypted images.

Step 1: Create an image of random pixels with the same size and shape as original image consider it as random1.

Step 2: Create a second image whose pixels are matched with XOR of first image and original image, it is represented as

$$random2 = random1 \oplus random2$$

Step 3: Finally, the step1 and Step2 are merged with XOR operation and listed as,

$$random1 \oplus random2 = random1 \oplus (random1 \oplus original) = original\,.$$

The enrollment process made by collecting the private biometric data and sent to a trusted third-party entity.Once the trusted entity receives the image, then the biometric data is decomposed into two images and the original data is rejected. The use of palm print as hosts for a private palm print image has several benefits in the context of biometric applications. First, the demographic attributes of the private palm print images such as a vein, muscles, extra skin surface in the palm, etc. can be retained in the host images. Second, a set of public palm print images may be used to host the private palm print database. Here a small set of public palm print images can be used to encrypt the entire set of private palm print images. Finally, the feature template is XOR-logic with the palm print template from the original database. The last condition states that the matching will be done in a similar manner.Visual Cryptography (VC) is a method used for secret sharing, in this research a secret image called palm print image is encoded into transparencies, and the stacking of any out of transparencies reveals the secret image. After encryption, there is no way to decrypt-except visual cryptography. Hence, this system is secure for image processing applications. It is one of the best technique used to protect the data such as biometric templates. Naor and Shamir (1994) introduced the visual cryptography scheme (VCS) to allow the secret sharing of images without any cryptographic computations in simple and easymanner.

IV. EXPERIMENTAL RESULTS

The performance analysis for palm print is made with real time data which is collected and shown in figure 5, here the frame is segmented and processed by the encoding scheme. The overall implementation process is made by MATLAB open source unit.

ISSN 2394 - 7780

Tabl-I: Equal error rates (%) at different threshold values

Sl.No	Threshold Values (TH)	Equal Error Rate (EER) (%)
1	128	32.1
2	164	19.2
3	188	6.14

The experimental results were analyzed with the Equal Error Rate (EER) with respect to the threshold value. In the case of palm print image templates, the proposed method encrypt and send the data over an enrollment process and retrieved by the de- identification unit. The table I shows the result of reconstructed palm print images with the threshold value of 188 and its error rate is almost 6.14%, these results provides the exact securing of palm print images.

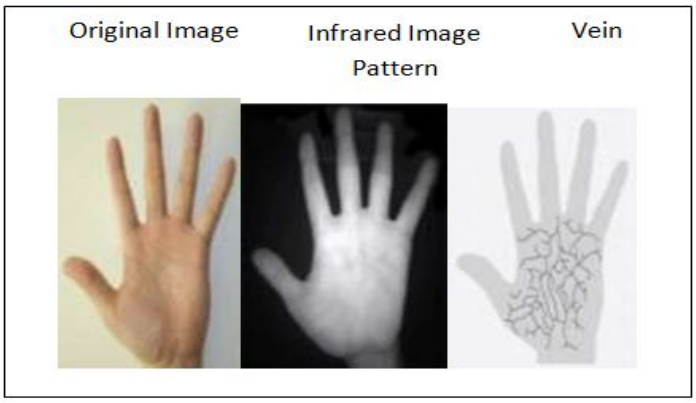


Fig-5: Original Image versus palm print patterns

Table-II: Experimental Results For Individual Sheet Images

	EER (%)
Reconstructed vs Reconstructed	2.3
Sheet 1 vs Sheet 1	22.2
Sheet 2 vs sheet 2	31.3

The main aim of measuring the error rate is to improve the reconstruction of the original image and to make a secure biometric authentication unit. From the results, it is summarized that the proposed method with visual cryptography is effective for implementing secure biometric authentication unit.

V. CONCLUSION

The design of the novel biometric system is essential in recent days to eliminate the smart cards and passwords. Hence, it requires a special unit to design the biometric system. This research gives a new direction in the field of biometric cryptosystems analyzed with the palm print image templates. The experimental results were shown that error rate is reduced if the threshold value increases. The comparison of the previously stored image is compared with the new image which is captured by a camera or by the scanner. The scope of future work is, to implement this proposed method in a real time end to end processing by reducing the errorrates.

REFERENCES

1. Kataria, A. N., Adhyaru, D. M., Sharma, A. K., & Zaveri, T. H. (2013, November). A survey of automated biometric authentication techniques. In 2013 Nirma University International Conference on Engineering (NUiCONE) (pp. 1-6). IEEE.
2. Wayman, J., Jain, A., Maltoni, D., &Maio, D. (2005). An introduction to biometric authentication systems (pp. 1-20). Springer London.
3. Lin, C. L., & Fan, K. C. (2004). Biometric verification using thermal images of palm-dorsa vein patterns. IEEE Transactions on Circuits and systems for Video Technology, 14(2), 199-213.
4. Mulyono, D., & Jinn, H. S. (2008, April). A study of finger vein biometric for personal identification.In Bio metrics and Security Technologies, 2008.ISBAST 2008. International Symposium on (pp. 1-8). IEEE.
5. Zhang, Y. B., Li, Q., You, J., & Bhattacharya, P. (2007, June). Palm vein extraction and matching for personal authentication. In International Conference on Advances in Visual Information Systems (pp. 154-164).Springer Berlin Heidelberg.

ISSN 2394 - 7780

6. Wang, L., &Leedham, G. (2006, November). Near-and far-infrared imaging for vein pattern biometrics. In 2006 IEEE International Conference on Video and Signal Based Surveillance (pp. 52-52). IEEE.
7. Badawi, A. M. (2006). Hand Vein Biometric Verification Prototype: A Testing Performance and Patterns Similarity. IPCV, 14, 3-9.
8. Li, Q., Zeng, Y. A., Peng, X., & Yang, K. (2010). Curvelet-based palm vein biometric recognition. Chinese Optics Letters, 8(6), 577-579.
9. Wang, J. G., Yau, W. Y., Suwandy, A., & Sung, E. (2008). Person recognition by fusing palm print and palm vein images based on "Laplacianpalm" representation. Pattern Recognition, 41(5), 1514-1527.
10. Wang, L., Leedham, G., & Cho, S. Y. (2007). Infrared imaging of hand vein patterns for biometric purposes. IET computer vision, 1(3/4),113.
11. Noh, Z. M., Ramli, A. R., Saripan, M. I., & Hanafi, M. (2016). Overview and challenges ofpalm vein biometric system. International Journal of Biometrics, 8(1), 2-18.
12. Akbar, A. F., Wirayudha, T. A. B., &Sulistiyo, M. D. (2016, May). Palm vein biometric identification system using local derivative pattern. In Information and Communication Technology (ICoICT), 2016 4th International Conference on (pp. 1-6). IEEE.
13. Lu, W., Li, M., & Zhang, L. (2016). Palm Vein Recognition Using Directional Features Derived from Local Binary Patterns. Structure,9(5).
14. Lan, X., Chen, P., & Sun, Z. (2015, May). The design of FPGA-based palm acquisition system.In Computer Science and Applications: Proceedings of the 2014 Asia-Pacific Conference on Computer Science and Applications (CSAC 2014), Shanghai, China, 27-28 December 2014 (p. 251). CRCPress.
15. Dere, S. N., Gurjar, A. A., &Sipna, C. O. E. T. (2016). Human Identification Using Palm-Vein Images: A New Trend in Biometrics. International Journal of Engineering Science, 2298.
16. Naor, M., & Shamir, A. (1994, May). Visual cryptography. In Workshop on the Theory and Application of-of Cryptographic Techniques (pp. 1-12). Springer BerlinHeidelberg.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

SECURE INCORPORATE OF IOT AND CLOUD COMPUTING

S. Subhasini[1], Dr. V. Kavitha[2] and B. Satyabama[3]
Assistant Professor[1], Department of Computer Applications (BCA), Hindusthan College of Arts and Science
Associate Professor[2] and Assistant Professor[3], Department of MCA, Hindusthan College of Arts and Science

ABSTRACT
Mobile Cloud Computing is a innovative technology which refers to a communications where both information storage and facts processing function outside of the mobile device. Another recent expertise is Internet of Things. Internet of Things is a new technology which is increasing quickly in the ground of telecommunications. More specifically, IoT associated with wireless telecommunications. The main objective of the communication and support between things and objects which sent through the wireless networks is to fulfil the purpose set to them as a shared entity. In adding up, there is a speedy development of both technologies, Cloud Computing and Internet of Things, view the pasture of wireless communications. In this paper, we present a survey of IoT and Cloud Computing with a centre of attention on the security issues of both technologies. particularly, we join the two aforementioned technologies (i.e Cloud Computing and IoT) in order to observe the common features, and in order to notice the benefits of their integration. Concluding, we present the involvement of Cloud Computing to the IoT technology. Thus, it appears how the Cloud computing technology improves the task of the IoT. ultimately, we re-examine the security challenges of the addition of IoT and Cloud Computing.

Keywords: Internet of Things, Cloud Computing, Mobile Cloud Computing, Security, Privacy.

I. INTRODUCTION

Authentication The Internet of Things is collected of three main parts:

1. The "things" (objects).

2. The statement networks that join them.

3. The computer systems by means of data usage from and to objects.

For example, home protection systems previously allow you to make sure remotely the locks on your doors, But what if it was likely to act proactively on your behalf? Imagine you opened the windows to ventilate your house before arriving, based on your concealed preferences, weather environment, and the distance from your house.

II. INTERNET OF THINGS

The Internet of Things is an association of devices that pass on, share, and utilize data from the physical situation to supply services to individuals, corporations, and society. The objects-things purpose either separately or in connection with other objects or individuals, and have unique IDs (identifiers). Also, the Internet of Things has related applications in health, transport, environment, energy or types of plans: sensors, devices worn/carried (wearable), e.g. watch, spectacles, residence automation.

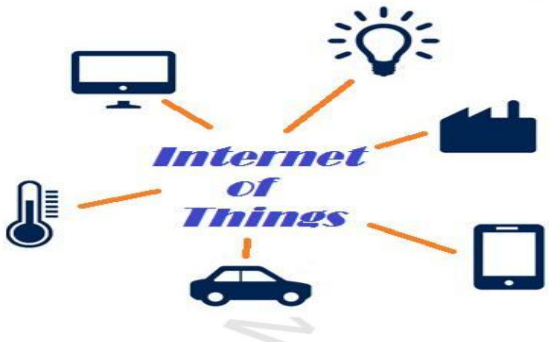


Figure-1: Internet of Things Technology.

Internet of Things: Advantages of the data

Opportunities where the streaming information will create new markets in order to inspire positive change or to enhance existing services are examined by businesses. a few examples of the heart of these developments are scheduled below :

a) Smart way out in the bucket of transport: Smart solutions in the bucket of transport, attain a cut of traffic on

ISSN 2394 - 7780

the roads, reduce fuel utilization, set priorities in vehicle fix programs, and save lives.

b) Smart control grids incorporating more renewable: Smart power grids incorporating more renewable improve system consistency, and reduce the charges consumers, thus providing cheaper electricity.

c) Remote monitoring of patients: Remote monitoring of patients provides simple access to health care, improves the value of services, increases the number of people served, and saves money.

III. CLOUD COMPUTING

Cloud computing produce computing, storage space, services provider, and applications with the Internet. In common, to provide smart phones energy efficient and computationally capable, major changes to the hardware and software point are essential. This entails the support of developers and manufacturers.

Mobile cloud computing is defined as an addition of cloud computing technology with mobile devices in order to make the mobile devices resource-full in terms of computational power, memory, storage, energy, and context awareness.

At hand are two perspectives in which the expression Mobile Cloud refers: a) infrastructure based, and b) ad-hoc mobile cloud. In the relations based mobile cloud, the hardware communications remains stagnant and also provides services to the portable users..

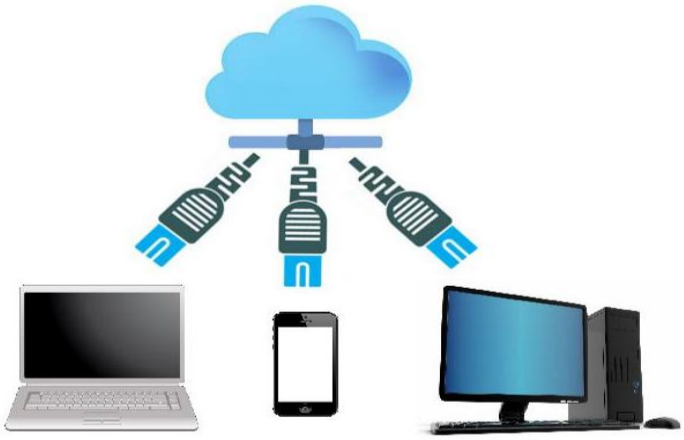


Figure-2: Cloud Computing Technology.

Cloud Computing Features

As all technologies, so the Cloud Computing technology has some quality which determine its function.

Storage over Internet

Storage over Internet can be distinct as a technology framework that uses Transmission Control Protocol/Internet Protocol (TCP/IP) networks to link servers and storage devices, and to assist storage way out deployment. The Storage over Internet technology is also known as Storage over Internet Protocol (SoIP) technology. With the grouping of the best storage and networking industry approaches, SoIP provides high-performance and scalable IP storage solutions.

Service over Internet

The main purpose of the Service over Internet is to be dedicated to help customers all over the world in order to change aspirations into achievements by harnessing the Internet.

Applications over Internet

The programs which can be written to do the job of a current manual task, or virtually anything, and which perform their job on the server (cloud server) via an internet relationship rather than the established model of a program that has to be installed and run on a confined processor are the Cloud Applications, or as a technical definition Applications in excess of Internet.

IV. IOT AND CLOUD COMPUTING INTEGRATION

Moreover, a new creation of services, based on the idea of the ‘cloud computing’, has made its appearance in the Some of the main features of the Cloud Computing technology which relate to the characteristics of both Internet of Things are: a) Storage over Internet, b) Service over Internet, c) Applications over internet, d) power efficiency and e) processing capable. Tables 2 lists the description of Mobile Cloud Computing regarding the convenience this technology offers when combined with the characteristics of IoT.

ISSN 2394 - 7780

Table-1: Assistance of Cloud Computing in Internet of Things.

Internet of Things characteristics		Storage over	Service over	Applications	Energy	Computationally
		Internet	Internet	over Internet	efficiency	capable
Smart solution in the bucket of transport	X	X	X		X	
Smart power grids incorporating more renewable	X	X		X	X	
Remote monitoring of patients		X	X		X	
Sensors in homes and airports	X	X	X	X	X	
Engine monitoring sensors that detect & predict maintenance issues		X	X	X	X	

Through the integration of IoT and Cloud we have the opportunity to expand the use of the available technology that provided in cloud environments. Applications and information that use the Internet of Things technology with this integration can be used through the cloud storage. The integration of IoT and Cloud technologies represented in Figure 3. The cloud offers to mobile and wireless users to access all the information and the application that needed for the IoT connectivity.

Protection issues in IoT and Cloud Computing integration Consequently, some challenges about the security issue in the integration of two technologies are listed

a. Heterogeneity. A big challenge in Cloud Computing and IoT integration is related to the wide heterogeneity of devices, operating systems, platforms, and services available and possibly used for new or improved applications

b. Performance. Often Cloud Computing and IoT integration's applications introduce specific performance and QoS requirements at several levels (i.e. for communication, computation, and storage aspects) and in some particular scenarios meeting requirements may not be easily achievable .

c. Reliability. When Cloud Computing and IoT integration is adopted for mission-critical applications, reliability concerns typically arise e.g., in the context of smart mobility, vehicles are often on the move and the vehicular networking and announcement is often intermittent or unpredictable.

d. Big Data. With an approximate number of 35 billion strategies that will be networked by 2020, exact attention should be paid to transportation, storage space, right of entry, and processing of the huge amount of data they will produce.

Table-2: Impact of IoT & Cloud Computing security challenges.

IoT & Cloud Computing security challenges	Heterogeneity	Performance	Reliability	Big Data	Monitoring
Internet of Things		X	X	X	X
Cloud Computing	X	X		X	

The ubiquity of mobile strategy and sensor occurrence, definitely call for scalable computing platforms.

e. Monitoring. As mainly predictable in the literature, monitoring is an significant activity in Cloud environments for capability planning for control resources,performance and security, and for correcting the bug.

Future Efficient IoT and Cloud Computing security model

The AES algorithm provides the capability to have speed key group time a good key agility. So, if we use this algorithm in the functionality of DF representation, we might have a reliable relay technique with an encryption of a speed key setup. Therefore, instead the trust relay use that DF and AF technique offers and we can get hold there is no serious weak keys in AES.

V. CONCLUSION

The Cloud Computing expertise offers a lot of possibilities, but also places a number of boundaries as well. Cloud Computing refers to an communications where both the data storage and the data handing out happen external of the mobile device. In this paper, we present a survey of Internet of Things Technology, with a

ISSN 2394 - 7780

description of its operation and use. In addition, we present the main character of the Cloud Computing and it's operate offs. Cloud Computing refers to an infrastructure where both data storage and data processing happen outside of the mobile mechanism Also, the Internet of Things is a new expertise which is rising quickly in the field of telecommunications, and particularly in the up to date field of wireless telecommunications.

REFERENCES

1. LuigiAtzori et al, "The Internet of Things: A survey," Computer Networks, no. 54, p. 2787–2805, 28/10/2010.
2. Sandip Roy et al, "A Fog-Based DSS Model for Driving Rule Violation Monitoring Framework on the Internet of Things," International Journal of Advanced Science and Technology, pp. 23-32, 01/03/2015.
3. Swan, Melanie (8 November 2012). "Sensor Mania!The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0". Sensor and Actuator Networks 1 (3): 217–253. doi:10.3390/jsan1030217.
4. Mohammad A. Alsmirat; YaserJararweh; Islam Obidat; Brij B. Gupta, "Internet of Surveillance: A Cloud supported Large Scale Wireless Surveillance System," the Journal of Supercomputing, Springer, 2016.
5. J.MongayBatalla and P. Krawiec, "Conception of ID layer performance at the network level for Internet of Things", Springer Journal Personal and Ubiquitous Computing, Vol.18, Issue 2 (2014), Page 465-480.
6. Y.Kryftis, G. Mastorakis, C. Mavromoustakis, J. MongayBatalla, E. Pallis and G. Kormentzas, "Efficient Entertainment Services Provision over a Novel Network Architecture". To be published in IEEE Wireless Communications Magazine, 2016.
7. M. R. Rahimi et al, "Mobile Cloud Computing: A survey, State of Art and Future Directions", Mobile Networks and Applications, Volume 19, Issue 2, pp. 133-143, 01/04/2014.
8. T.Keskin and N. Taskin, "A pricing model for cloud computing service" 47th Hawaii International Conference on System Science, pp. 699-707, 01/10/2014.
9. S.Fremdt, R. Beck and S. Weber, "Does Cloud Computing Matter? An analysis of the Cloud Model software-as-a-service and its impact on operational agility" 46th Hawaii International Conference on System Sciences, pp.1025-1034, 01/10/2013.
10. S.Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications, vol. 1, no. 34, pp. 1-11, 11/07/2010.
11. HassanTakabi and James B.D. Joshi, «Security and Privacy Challenges in Cloud Computing Environments», IEEE COMPUTER AND RELIABILITY SOCIETIES, pp. 24-31, 01/11/2010.
12. George Suciu et al, "Smart Cities Built on Resilient Cloud Computing and Secure Internet of Things," in 2013 19th International Conference on Control Systems and Computer Science, Bucharest, 2013.
13. Fei Tao et al, «CCIoT-CMfg: Cloud Computing and Internet of Things-Based Cloud Manufacturing Service System», IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, vol. 2, no. 10, pp. 1435-1442, 02/05/2014.
14. Jiehan Zhou et al, «CloudThings: a Common Architecture for Integrating the Internet of Things with Cloud Computing», in Huazhong University of Science and Technology, Wuhan, 2013.
15. Juan Antonio Guerrero Ibáñez et al, "Integration Challenges of Intelligent Transportation Systems with Connected Vehicle, Cloud Computing, and Internet of Things Technologies," IEEE Wireless Communications, pp.122-128, 01/12/2015.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

A DELAY-TOLERANT SECURITY FRAMEWORK FOR MOBILE DATA COLLECTION

Pannerselvam[1], V. Liyandernoyalraj[2] and Dr. N. Revathy[3]
Student[1,2] and Associate Professor[3], Department of Master of Computer Applications, Hindusthan College of Arts and Science, Coimbatore

ABSTRACT
The concept of mobile health comprises the combination of mobile computing technology with medical sensors and communication devices, creating solutions for improving health care. The concept is also related to that of electronic health processing, but while the latter is more focused on fixed computing facilities (e.g., desktop computers), the former aims to explore more intensively the advances in wireless communication, ubiquitous computing.

Mobile Health (mHealth) proposes health care delivering anytime and anywhere. It aims to answer several emerging problems in health services, including the increasing number of chronic diseases, high costs on national health services, and the need to provide direct access to health services, regardless of time and place. mHealth systems include the use of mobile devices and apps that interact with agent and health manager. However, mobile devices present several constraints, such as processor, energy, and storage resource limitations. The constant mobility and often-required Internet connectivity also exposes and compromises the privacy and confidentiality of health information.

In this applications typically involve remote data collection of Primary Health Care indicators, such as family-related data, sanitary conditions, identification of common diseases in a given region, or tracking people with chronic conditions/diseases.

Nowadays security is one of the most imperative requirements for the success of systems that deal with highly sensitive data, such as medical information. However, many existing mobile health solutions focused on collecting patients' data at their homes that do not include security among their main requirements. This paper, a lightweight security framework focused on highly sensitive data collection applications.

This paper provides many security services for both stored and in-transit data, displaying interesting features such as tolerance to lack of connectivity (a common issue when promoting health in remote locations) and the ability to protect data even if the device is lost/stolen or shared by different data collection agents.

I. INTRODUCTION
Current mobile technologies in recent years there has been increased research on wireless telemedicine using current mobile communication systems. However, the increased equipment cost (such as satellite-based systems) and the limited bandwidth of the current generation of cellular telecommunication systems have restricted the wider use of these systems within the most promising segments of the health care structures in general. However, in recent years some emerging 2.5G- and 3G-based m-health systems with Bluetooth medical wireless

The next generation of m-health systems the next few years will witness a rapid deployment in both UMTS and mobile Internet based m-health systems with pervasive computing technologies. The increasing data traffic and demands from different medical applications and roaming application will be compatible with the data rates of 3G systems in specific mobility conditions.

II PROBLEM DEFINITION
In this proposed system we discuss more requirements and merits are there, that is

1. Tolerance to Delays and Lack of Connectivity
Many data collection systems are deployed in remote locations, where network access is not continuously available, implying that frequent connectivity losses are expected to occur c consequently, the mobile device should be able to authenticate the user in an offline manner and also employ mechanisms for temporarily storing acquired data in a secure manner, using encryption. Even though an entirely offline mode of operation should be allowed, if the data need to be delivered quickly, the mobile device should be capable of doing so as soon as a communication channel is detected and without intervention from the user, allowing a reasonably fast data upload process even in regions with intermittent connectivity.

2. Protection against Device Theft or Loss
This method employed for temporary data storage should also provide protection against unauthorized access or modification. Ideally, this protection should remain effective even if the mobile device in which the data are

ISSN 2394 - 7780

stored is stolen, while the user's session is still active (i.e., the user is still "logged in" to the device) and the device's volatile memory is accessed. In other words, the security solution should enable some level of forward secrecy, preventing attacker from using information in the device's memory to access undelivered, locally stored data. However, imposing forward secrecy may not be suitable for all situations, since it may be useful to allow agents to recover the information from previously saved forms, e.g., because they were only partially filled or contained incorrect data. Hence, the security framework should be flexible enough to support different forward secrecy configurations according to the application's needs.

3. Secure Data Exchange between Mobile Device and Server

Aiming to create a solution that does not depend on secure communication tunnels for data delivery, our approach is to independently authenticate every piece of data that travels from and to the mobile device. The protocol itself has no strict need for creating and authenticating a session before data delivery. Especially in scenarios where the communication infrastructure is far from ubiquitous and the devices have low computational power? This happens because the data temporarily stored in the device already needs to be encrypted and, thus, adding an extra security layer for protecting its delivery can be seen as an unnecessary overhead.

4. Lightweight and Low-Cost Solution

Low-budget projects may impose restrictions on the computational capabilities of the mobile devices employed for collecting data, including limitations on processing power and available memory. Therefore, the security framework should rely as much as possible on lightweight cryptographic mechanisms such as those based on symmetric keys (as opposed to public key cryptography).Moreover, the security mechanisms deployed should not depend on hardware capabilities not usually available in commercial mobile devices although it should be able to take advantage of such capabilities if present.

5. Device Sharing

Budget limitations or practical reasons may lead to the sharing of mobile devices by multiple agents. The security solution should allow access to registered users from any (possibly multiple) devices in which the data collection application is installed. Hence, users should be able to share devices in a straightforward manner, without incurring privacy and access control issues that might arise from a same device carrying data from different agents.

6. Usability

In this application, the staff responsible for data collection may include people with little education background and/or little experience with computers. Even though this can be overcame with intense training, frustrating experiences may become an extra barrier for the system's acceptance. Therefore, despite the need of strong security mechanisms for protecting digital forms, it is important to keep in mind that they must not impair the system's usability

III MODULES

This project contains two modules:

- Admin
- Agent

The admin module in this project deals with the agents' registration, survey creation, send notifications, monitor the agents and view the reports of the survey

Modules in admin

- Survey management
- Agent management
- Survey start
- Question management
- View survey information
- Send notifications
- Summarization

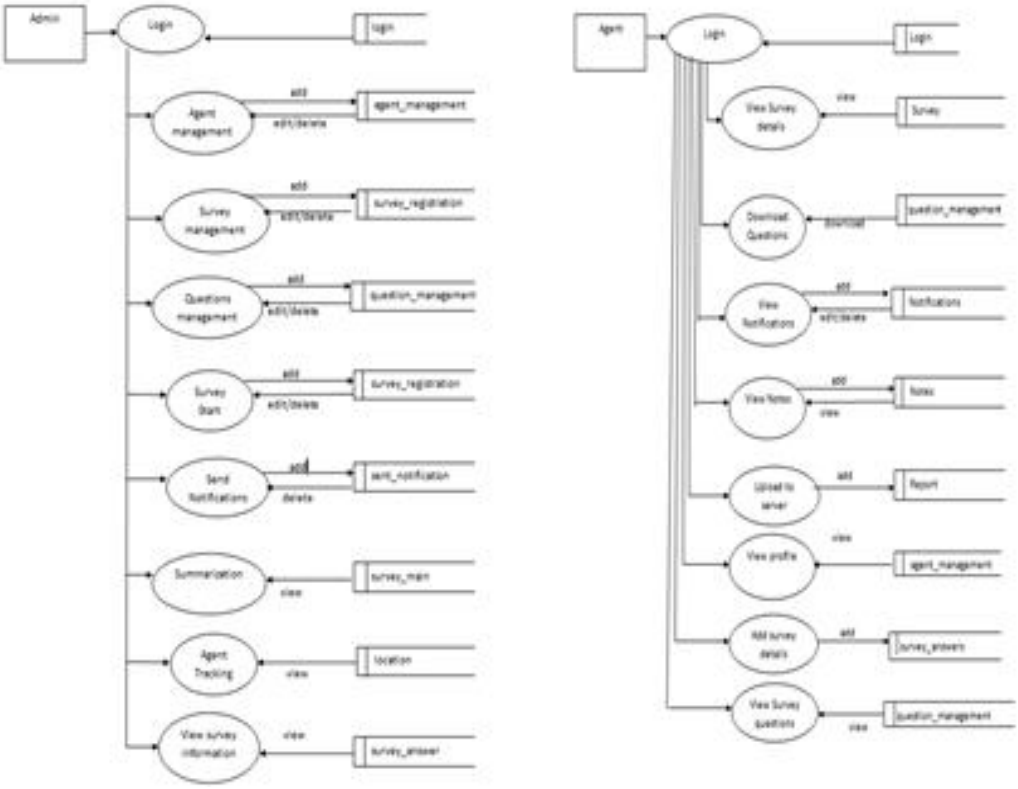
The agent module in this project is conduct survey. Other features for the agents is add notes, view questions, upload the survey details to server, view questions and view the profile of the agents

ISSN 2394 - 7780

Modules in agent

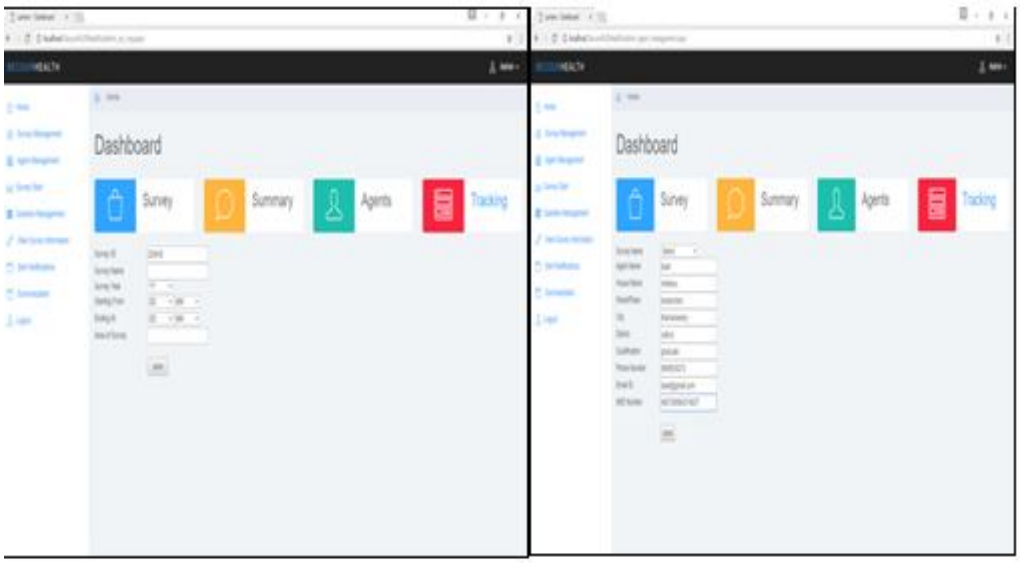
- View profile
- View survey details
- Add survey details
- View survey questions
- View notes
- Download questions
- Upload to server
- View notification

Admin **Agent**



Survey management

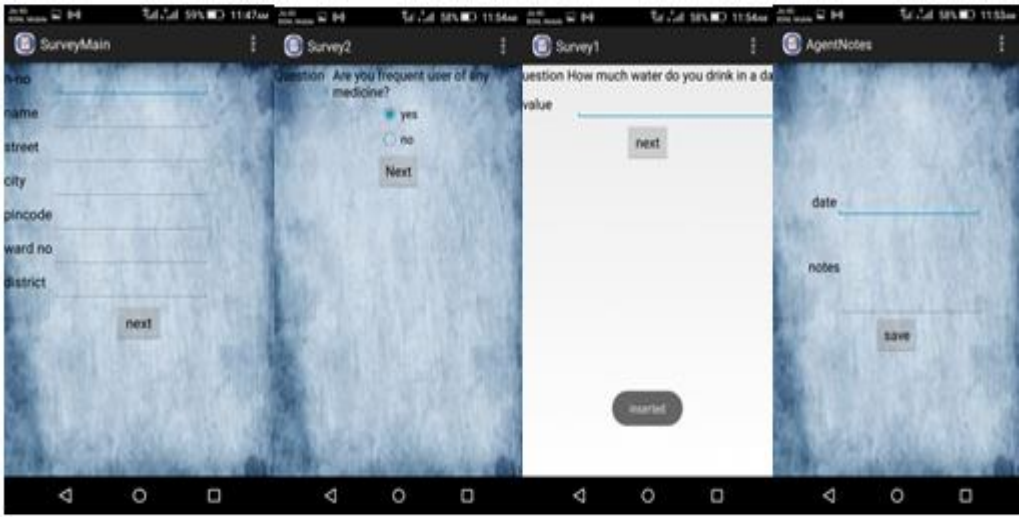
This form is used add new survey



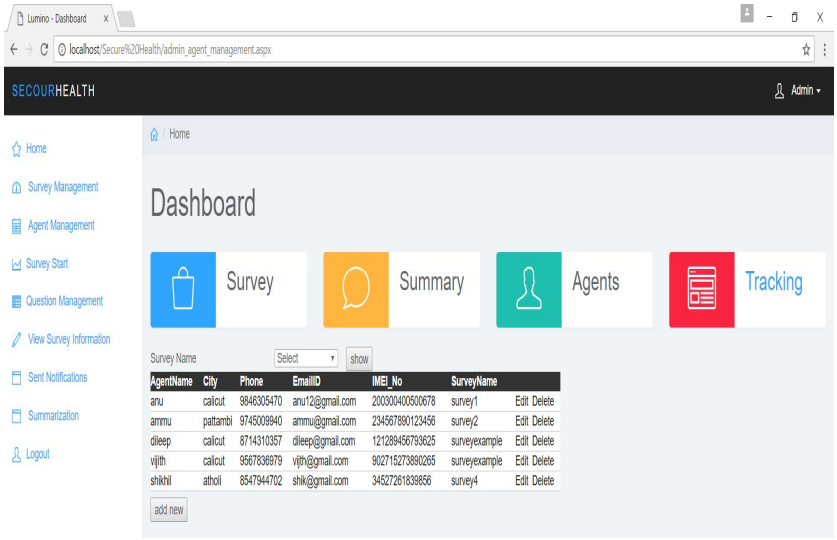
ISSN 2394 - 7780

Agent management
This form is used to register new agents

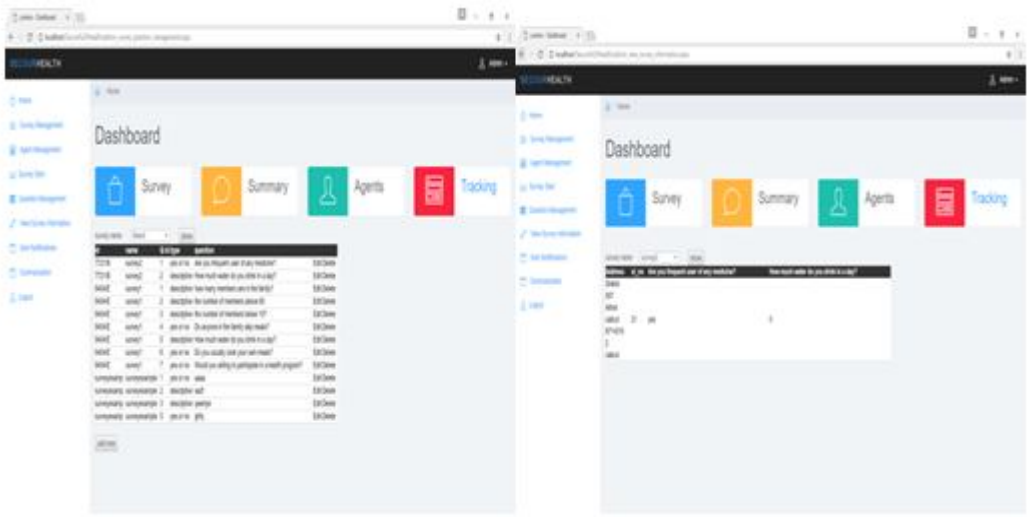
Android Screen shots
Add survey details



Agent management
This form is used to view the agent details

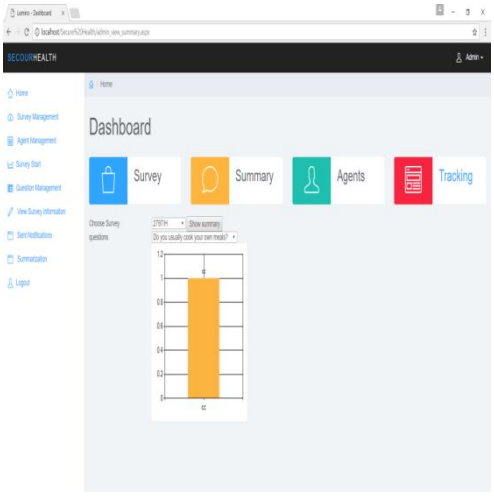


Question management
This form is used to displays the questions



ISSN 2394 - 7780

Summarization
This form is to display the summarized form of the survey



IV. IMPLEMENTATION

To assess the behavior of the SecourHealth framework in a real environment, we integrated the proposed mechanisms into the Geo Health system, an Android-based application currently being used in the city of Sao Paulo as part of a governmental initiative for health data collection called "Family Health Program." This initiative involves teams of data collection agents responsible for assisting families in a well-defined geo graphical area, surveying several primary care conditions and promoting actions such as prevention, recovery, and rehabilitation. Partially filled forms are stored in the device's local memory so they can be filled later . After consolidation, the forms are put in a first-in-first-out queue and sent as soon as possible to the server. All collected data are geo referenced, providing health managers with a clear view of the population's conditions in the surveyed regions. The original Geo Health architecture uses password for protecting the access to the application. More precisely before the accessing the application, the user needs to send its password to the server to be validated and, incase of success, the password is stored in the mobile device's memory. HTTPS is used for securing all communications, including the password registration and data delivery. The data in this protected tunnel are not otherwise encrypted or authenticated. Even though this approach does not incur in any serious security issue for in-transit data, it leads to some undesirable overhead due to the repeated establishment of TLS/SSL sessions and it requires the password to remain in memory all the time. Moreover, no security mechanism is employed for protecting the information kept in the mobile device's memory while no communication channel is available. The SecourHealth empowered Geo Health system overcomes these issues in the following manner.

1) User Registration: Even though the registration of a new user still employs HTTPS, the password is not sent in clear inside this tunnel but becomes part of the challenge response protocol described in Section IIIB. When compared to "plain" Geo Health, this process adds some extra overhead before users can use a new device. Nevertheless, since this needs to be done only once and the whole process is very similar to the regular password registration, this burden is not significant in practice.

ISSN 2394 - 7780

2) Secure Storage: Partially filled forms are periodically saved by the system in an automatic manner. Hence, they are encrypted (but not authenticated) using Knofs, so they can be repeatedly accessed by the agents. Consolidated forms are not expected to be changed, since they are likely to be sent to the server automatically soon after being saved. Therefore, the system uses Ksfs for encrypting and authenticating them. Kwfs is not used in the system and, thus, it is not generated.

3) Data Exchange: Data exchange with the server is performed without the prior establishment of an HTTPS channel, accelerating the delivery of consolidated forms. Downloading data from the server normally do not involve challenges issued by the server. There as on is that the policy adopted in Geo Health when users request some data are already quite strict: the server has a list of families to be visited by each agent and usually prevents access to information not belonging to such families. Challenge issuing is, thus, limited to when an agent requests information about a number of families well above the average in the same day or in exceptional cases (e.g., unplanned emergency visits to families not assigned to the requesting agent). Namely, for the current average of six families visited per agent per day, a challenge would be issued when the agent requests information about the tenth family in less than 24 h.

V. CONCLUSION

Security is one of the most imperative requirements for the success of systems that deal with highly sensitive data, such as medical information. Unfortunately, however, many existing Mobile Health applications for data collection do not include security mechanisms able to protect both the locally stored and in-transit medical data gathered by them. Aiming to close this gap, this work proposes SecourHealth, a lightweight security framework designed specifically for this class of applications. SecourHealth provides many security services for both stored and in-transit data, coping with this scenario's typical constraints such as tolerance to lack of connectivity, the need of enabling device sharing, and transparency to users. The set of tools offered in this manner can be integrated into existing solutions or used in the design of more secure Mobile Health data collection applications from the start. Indeed, our experimental results when integrating SecourHealth into the Geo Health solution show that it is possible to provide strong security for the data while introducing minimal overhead to the collection process. Finally, it is worth noting that even though SecourHealth was designed to prevent outsider rather than insider attacks (e.g., agents who simply copy old information into forms instead of effectively following their visitation schedule), it can also be used as a tool for discouraging the latter: since the proposed solution prevents outsiders from illegally accessing or tampering with the system's data, it gives managers the ability to identify misbehavior from insiders and act accordingly.

SCOPE FOR FUTURE ENHANCEMENT

As future work I intend to address one of the main challenges faced by Mobile Health solutions together with security: standardization. Namely I plan to consider the integration of the mechanisms proposed in SecourHealth into standard frameworks for data collection. Another potential use of SecourHealth is as an integrating part of other typical Mobile Health applications that relay on mobile devices for exchanging data with a server. One example is remote monitoring systems, in which a set of sensors continuously supervise a patient's health conditions at his/her home, periodically delivering the acquired data to a server using a mobile device as gateway.

REFERENCES

1. R. Istepanian, E. Jovanov, Y. Zhang, "Guest editorial introduction to the special section on m-health: Beyond seamless mobility and global wireless health-care connectivity", *IEEE Trans. Inf. Technol. Biomed.*, vol. 8, no. 4, pp. 405-414, Dec. 2004.
2. S. Tachakra, X. Wang, R. Istepanian, Y. Song, "Mobile e-health: The unwired evolution of telemedicine", *Telemed. e-Health*, vol. 9, no. 3, pp. 247-257, 2003.
3. "mHealth: New horizons for health through mobile technologies", *Global Observatory for eHealth series vol. 3. World Health Org. Geneva*, 2011.
4. L. Iwaya, M. Gomes, M. Simplicio, T. Carvalho, C. Dominicini, R. Sakuragui, M. Rebelo, M. Gutierrez, M. Näslund, P. Håkansson, "Mobile health in emerging countries: A survey of research initiatives in Brazil", *J. Amer. Med. Inform. Assoc.*, vol. 82, no. 5, pp. 283-298, 2013.
5. C. Hertzman, N. Meagher, K. McGrail, "Privacy by design at population data BC", *J. Amer. Med. Inform. Assoc.*, vol. 20, no. 1, pp. 25-28, 2013.
6. J. Sa, M. Rebelo, A. Brentani, S. Grisi, M. Gutierrez, "GeoHealth: A georeferenced system for health data analysis in primary care", *IEEE Latin Amer. Trans.*, vol. 10, no. 1, pp. 1352-1356, Jan. 2012.

ISSN 2394 - 7780

7. *D. Shao*, A proposal of a mobile health data collection and reporting system for the developing world, *2012*.
8. Norris, R. Stockdale, S. Sharma, "A strategic approach to m-health", *Health Informatics J.*, vol. 15, no. 3, pp. 244-253, 2009.
9. K. Patrick, W. Griswold, F. Raab, S. Intille, "Health and the mobile phone", *Amer. J. Preventive Med.*, vol. 35, pp. 177-181, 2008.
10. Sunyaev, J. M. Leimeister, H. Krcmar, "Open security issues in german healthcare telematics", *Proc. 3rd Int. Conf. Health Informatics*, pp. 187-194, 2010.
11. "A 'Conceptual' Privacy Impact Assessment (PIA) on Canada's Electronic Health Record Solution (EHRS) Blueprint Version 2", *Canada Health Infoway Montreal Quebec*, 2008.
12. *Earth Institute. Barriers and Gaps Affecting mHealth in Low and Middle Income Countries: A Policy White Paper.*, 2010.
13. W. A. Kaplan, "Can the ubiquitous power of mobile phones be used to improve health outcomes in developing countries?", *Globalization Health*, vol. 2, no. 9, 2006.
14. J. G. Hodge, "Health information privacy and public health", *J. Law Med. Ethics*, vol. 31, no. 4, pp. 663-671, 2003.
15. F. Mancini, K. Mughal, S. Gejibo, J. Klungsoyr, "Adding security to mobile data collection", *Proc. 13th IEEE Int. Conf. e-Health Netw. Appl. Serv.*, pp. 86-89, 2011.
16. R. Correia, F. Kon, R. Kon, "Borboleta: A mobile telehealth system for primary homecare", *Proc. 23rd ACM Symp. Appl. Comput.*, pp. 1343-1347, 2008.
17. J. Black, Authenticated Encryption, Berlin, Germany:Springer, 2005.
18. Kaliski, *PKCS#5: Password-Based Cryptography Specification Version 2.0*, 2000.
19. L. Almeida, E. Andrade, P. Barreto, M. Simplicio, "Lyra: Password-based key derivation with tunable memory and processing costs", *J. Cryptographic Eng.*, pp. 1-15, 2014, to appear.
20. "Generic Authentication Architecture (GAA) version 6.9.0", Jun. 2006.
21. S. Holtmanns, V. Niemi, P. Ginzboorg, P. Laitinen, N. Asokan, Cellular Authentication for Mobile and Internet Services, New York, NY, USA:Wiley, 2008.
22. Florencio and C. Herley, "A large scale study of web password habits", *Proc. 16th Int. Conf. World Wide Web*, pp. 657-666, 2007.
23. J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, L. F. Cranor, "Crying wolf: An empirical study of SSL warning effectiveness", *Proc. 18th Conf. USENIX Security Symp.*, pp. 399-416, 2009.
24. J. Engler, C. Karlof, E. Shi, D. Song, "PAKE-based web authentication: The good the bad and the hurdles", *Proc. IEEE* Web 2.0 Security Privacy Workshop, pp. 1-9, 2009.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

SECURE AND IDENTIFY HACKING IN ROUTING SYSTEM

M. Logesh[1] and A. Kriuthika[2]
Student[1] and Assistant Professor[2], PG and Research Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore

ABSTRACT
Packet forwarding is the procedure to route the packet from source to destination via routers. Using any database form the routing table with columns like source address, destination address and router addresses. The ip addresses in the routing table, are the path selected by the user according to the respective path the packet will be forward and finally reach destination. Source generate a packet and forward to ip address. Source need to know whether the packet received by authenticated router or not thus each router send an acknowledgement packet to the source. Thus each and every router follows the same procedure to avoid unauthenticated router access in a routing process. Before send the packet, source generates the signature with peer ID of destination then forwards the packet to the ip address as per routing table. Then source compare the acknowledgement with the predefined routing table if any ip mismatch then it will be consider as unauthorized ip.

Keywords: Router, P2P (peer id) , Packets , Source , Destination.

I. INTRODUCTION

Queries are routed towards the target with a certain ID. When one or more nodes are malicious, they may prevent correct message routing. Alternate routing paths can be used to circumvent them. As a result, the routing latency consists of two parts: normal routing latency and extra routing latency incurred by bypassing malicious nodes. In this paper, we propose tracer routing, an efficient routing strategy designed to control the routing path while reducing the normal routing latency. Combined with a peer-ID based signature scheme, it can offer the initiator of each query to identify malicious nodes. A key feature of our scheme from other protocols is that alternate routing is constructed only detecting malicious nodes. Our simulation shows that the routing success rate our scheme can achieve is better than previous protocols.

We define a secure routing primitive that can be combined with existing techniques to construct secure applications on structured p2p overlays. Subsequent sections show how to implement the secure routing primitive under the fault and network models that we described in the previous section. The routing primitives implemented by current structured p2p overlays provide a best-effort service to deliver a message to a replica root associated with a given key. With malicious overlay nodes, the message may be dropped or corrupted, or it may be delivered to a malicious node instead of a legitimate replica root. Therefore, these primitives cannot be used to construct secure applications.

MODULE DESCRIPTION

User interface design

Interface design is involved in a wide range of computer systems, to cars, to commercial planes; all of these involve much of the same basic human interaction yet also require some unique skills and knowledge. As a result, designers tend to specialize in certain skills centered around their expertise, whether that be software design, user research, web design, or industrial design.A user interface module is design for language editor; language conversion options and conversion result option everything available in screen. This module provides user friendly GUI options.

Peer Message Sender

Source peer get message from user and forward the packet to destination. This packet flow under the routing table. Source node received acknowledgement from current router. **Encryption** is a method which allows information to be hidden so that it cannot be read without special knowledge or tools. Once this is done the information is **encrypted**.

Peer Registration

Register new Peer to key distribution center. User give peer name and ip address peer id automatically generated and store to database. Sender get particular peer key and encrypt data. Receiver gets data from router and get key from key distribution center, and decrypt data using that key.

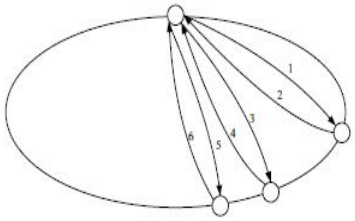
ISSN 2394 - 7780

II. SYSTEM ANALYSIS

Existing system

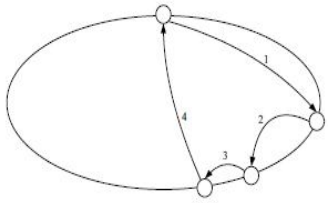
Iterative routing: Nodes communicate only with the originator. The tick mark denotes. The position of the queried key in the ID space. The square shows the key's successor node. The Triangles and arrows show a lookup path. The last node before the tick mark is the key's predecessor.

Iterative routing is not efficient, but it gains some benefits due to its manageable behavior. The intermediate peers reply with the IP address of the next hops to the initiator, the initiator can send the message to the peer in the next hop directly.



Iterative Routing

Recursive routing: Each node forwards the query to the next node. During the lookup process no information is send back to the originator, resulting in less packet overhead.



Recursive Routing

We consider three kinds of attacks

In case 1, the intermediate peer *x* pollutes or forges the content of the query. The next hop will still receive the original query since initiator sends the query by itself.

In case 2, peer *x* drops the query. If no relay from the next hop is received in a given timeout, initiator will determine that *x* drops it.

In case 3, peer *x* returns initiator an incorrect next hop. If the incorrect next hop colludes, the fact that initiate cannot verify the identity of the next hop makes determining which peer Sends the incorrect reply impossible. This challenge causes us to believe that the technique of verifying the ID of remote peer is necessary. Combined with Peer-ID based signature scheme, initiator can identify the malicious node *x*.

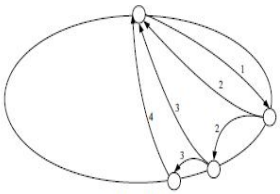
III. PROPOSED SYSTEM

Tracer routing: To make the routing strategy perform best, we present an efficient routing strategy, called tracer routing (Figure 1). Tracer routing enables the initiator to trace the whole routing process. It can reduce *normal* routing latency from $2h * t$ to $(h + 1) * t$. The basic principle of the routing strategy is as follows. In each step, the intermediate peer *x* not only forwards the query to the next hop, but also returns the IP address of the next hop to initiator. With the additional information, the initiator has the knowledge about the whole routing process. Each intermediate peer directly forwards the query to the next hop, thus the query can be routed quickly. Combined with the peer-ID based signature scheme, tracer routing offers a good tradeoff between routing efficiency and security.

We propose to address routing message attack by combined tracer routing with Peer-ID based signature scheme. Note that Peer-ID based signature scheme is not necessary. Any techniques of verifying the Peer-ID of remote peer can work with tracer routing. In our scheme, the initiator appends a signature to a query. When a intermediate peer *x* receives

The message (including query and its signature), *x* verifies the message and discards the polluted or forged one using the initiator's public key. Recall that the public key is the Peer- ID of initiator. Then *x* forwards the message it received to the next hop. At the same time, *x* sends an acknowledgement (including the Peer-ID of the next hop, query and the signature generated using the private key of *x*) to initiator. The process is repeated until the query reaches the target.

ISSN 2394 - 7780



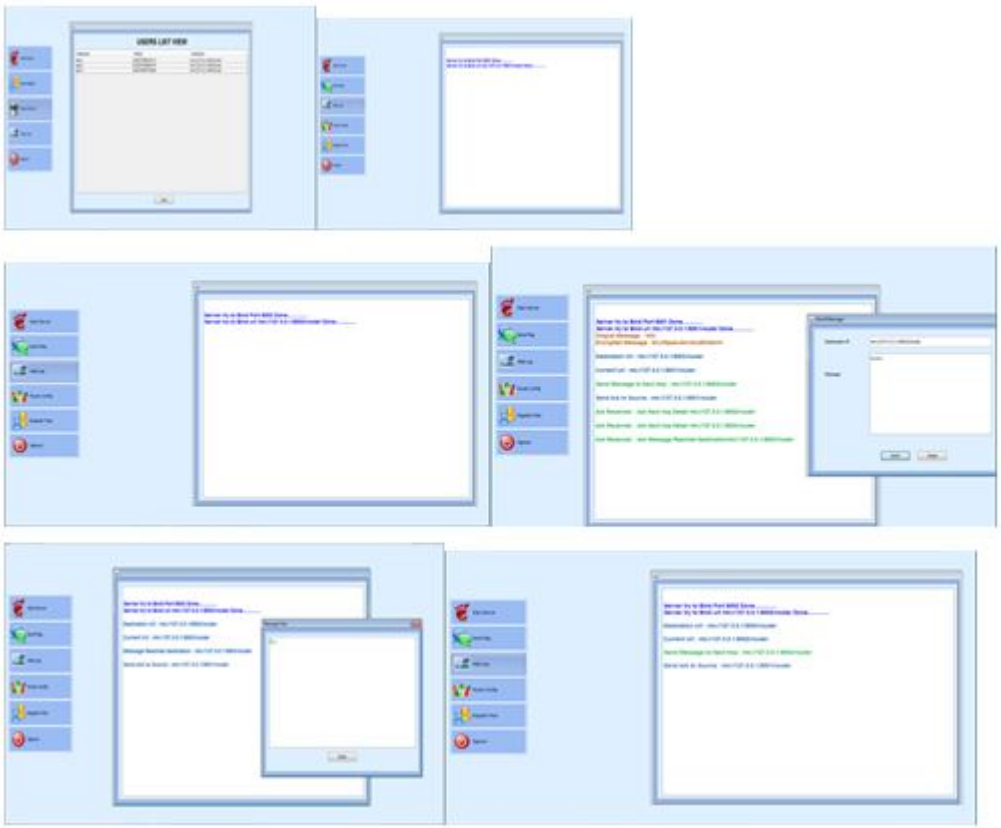
Tracer Routing

Message routing: At each routing step, a node seeks to forward the message to a node in the routing table whose node Id shares with the key a prefix that is at least one digit (or *b* bits) longer than the prefix that the key shares with the current node's id. If no such node can be found, the message is forwarded to a node whose node Id shares a prefix with the key as long as the current node, but is numerically closer to the key than the current node's id. If no appropriate node exists in the routing table or neighbor set, then the current node or its immediate neighbor is the message's final destination.

IV. SYSTEM IMPLEMENTATION

The purpose of System Implementation can be summarized as follows

It making the new system available to a prepared set of users (the deployment), and positioning on-going support and maintenance of the system within the Performing Organization (the transition). At a finer level of detail, deploying the system consists of executing all steps necessary to educate the Consumers on the use of the new system, placing the newly developed system into production, confirming that all data required at the start of operations is available and accurate, and validating that business functions that interact with the system are functioning properly. Transitioning the system support responsibilities involves changing from a system development to a system support and maintenance mode of operation, with ownership of the new system moving from the Project Team to the Performing Organization.



V. CONCLUSION

Peer-to-peer overlay networks, both at the network layer and at the application layer. We have shown how techniques ranging from cryptography through redundant routing to economic methods can be applied to increase the security, fairness, and trust for applications on the p2p network. Because of the diversity of how p2p systems are used, there will be a corresponding diversity of security solutions applied to the problems. has presented the design and analysis of techniques for secure node joining, routing table maintenance, and message forwarding in structured p2p overlays. These techniques provide secure routing, which can be combined with existing techniques to construct applications that are robust in the presence of malicious participants.

ISSN 2394 - 7780

REFERENCES

1. Scott Oaks, Henry Wong, Mike Loukides (Editor), "Java Threads Java Series", O'Reilly &Associates.
2. Patrick Naughton, Herbert Schildt, "Java™ 2: The Complete Reference", Third Edition, Tata McGraw-Hill Publishing Company Limited.
3. David Flanagan, "Java in a Nutshell", 2nd Edition, May 1997.
4. Mark Grand and Jonathan Knudsen, "Java Fundamental Classes Reference", Tata McGraw-Hill Publishing Company Limited, 1st Edition, May 1997.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

BAGGAGE TRACKING BEHAVIOR BY RFID AND IOT

S. Saranya[1], P. Deepika[2], Dr. S. Sasikala[3] and S. Geethamani[4]
Assistant Professor[1,2], Department of Computer Application, Hindusthan College of Arts and Science
Associate Professor[3], Department of Computer Application, Hindusthan College of Arts and Science
Assistant Professor[4], Department of Computer Science, Sri Ramakrishna College of Art & Science for Women

ABSTRACT
The baggage tracking system is designed to track the bags which missing or theft from community and other areas. There is constantly a risk of stealingthe bags. the proposed system of baggage tracking system using RFID and GPRS has overcome the problem. The most common Loop holes experienced inAviation industry for Baggage Handling aremislaid baggage, lost baggage and damage tobelongings.we providing animproved and safe system tothe public, we have proposed a design ofbaggage tracing and handling system usingsmart RFID tags and IoT which is based oncloud server.we can pathway the location of the bag as it travels, as the indicators are dropped which in a way gives us the position of the bag as it travels away from the holder. In this thesis, the IoT apparatuses are being used like Arduino Board and a GPS Module in order to track thebaggageand a frontend or mobile application is created in order to monitor.

Keywords: RFID, LCD,internet of things, object identification, GPS (latitude & longitude)

I. INTRODUCTION

Internet of Things (IoT) is the networking of corporalsubstances that contain electronics implanted within their construction in order to connect and sense relations each other or with respect to the peripherallocation. In the future years, IoT-based expertise will proposition advanced levels of services and virtually change the methodpublicmain their daily lives. Advancements in gene therapies,agriculture,medicine, power, smart cities, and smart home.

The adaptability of IoT has become very general in current years. There are many rewards to having a device created on IoT. Mckinsey Global Institute reports that IoT business will spread 6.2 trillion in income by 2025**.** There are numerous of applications are offered in the market in different areas.1) Personal Home Automation System2) Enterprise3) Utilities4) Energy Management5) Medical and Health Care6) Transportation7) Large scale deployment

II. METHODOLOGY

This section displays the several basic information and is used as a framework to effectively attain the major objectives. The most common Loop holes experienced in Aviation industry for Baggage Handling are mislaid baggage, lost baggage and damage to belongings. So, for providing a better and secure system to the passengers, we have proposed a design of baggage tracing and handling system using smart RFID tags and IoT which is based on cloud server.

The proposed technology will allows you to track your bags throughout the journey directly on your Smartphone using Wi-Fi, GPS technology.

III. RFID DESCRIPTION

The RFID system is used to verification and map out the movement of a luggage, when it's missing through radio frequency communication. A radio frequency identification reader (RFID reader) is a device used to collect the data from an RFID tag, which is used to track character objects. Radio waves are used to transmit the data from the tag to a reader. RFID is a technology like in theory to bar codes. In RFID tag it will not have to be scanned straight, nor does it need a line-of-sight to a reader. The RFID tag it must be surrounded by the range of an RFID reader, which ranges from 3 to 300 feet, in order to be read. RFID technology allows numerous items to be rapidly scanned and enables fast recognition of a particular product, when it is bounded by several other items.

This system has two parts they are reader and the transponder. It's also known as the tag. It is composed of an antenna and a silicon microchip. It has a unique recognition number and carries the information. This data represents the private information of the baggage owners or an identity code that is stored in binary format. Tags can be either passive or active. The proposed system uses passive tags due to their wide use and low-cost. These tags do not have a power source instead they get power from the incident electromagnetic field. The tag reader is skilled of powering and communicating with a tag. The tag antenna captures the energy and transfers the tag's ID (the tag's chip coordinates this process). The encapsulation sustains the tag's integrity and shields

ISSN 2394 - 7780

the antenna and chip from ecological conditions. When the tag was in RF field, it draws the power and transmits the stored information in the memory. In this way, the tag transmits the baggage owner information to the reader. Then, the reader transforms the reflected waves sent by the tag into digital data for computer processing. Once the data is processed, the database system sends applicable messages to the baggage owner.

GPS

The Global Positioning System (GPS) comprises three segments: 1)The space segment (all functional satellites). 2) The control segment (all ground stations occupied in the monitoring of the system master control station, Monitor stations, and ground control stations). 3) The client segment (all civil and military GPS users).

GPS Was developed by the U.S. Department of Defense (DOD) and it was used by both the civilians and military Personnel. The civil signal SPS (Standard Positioning Service) can be used generously by the general public, whilst the Military signal PPS (Precise Positioning Service)only it is used by authorized government agencies. The first Satellite was positioned in orbit on 22 nd February 1978, and they are currently 28 operational satellites orbiting the Earth at a height of 20,180 km on 6 different orbital planes. Their orbits are liable at 55° to the equator, ensuring that at least 4 satellites are in radio announcement with any point on the planet. During the growth of the GPS system, exacting the emphasis was placed on the following three aspects:

a) It had to give the users with the ability of determining position, speed and time, whether in motion at rest.

b) It had to have a continuous, global, 3-dimensional positioning capability with a high degree of accuracy, Irrespective of the weather.

c) It had to recommend the potential for civilian use

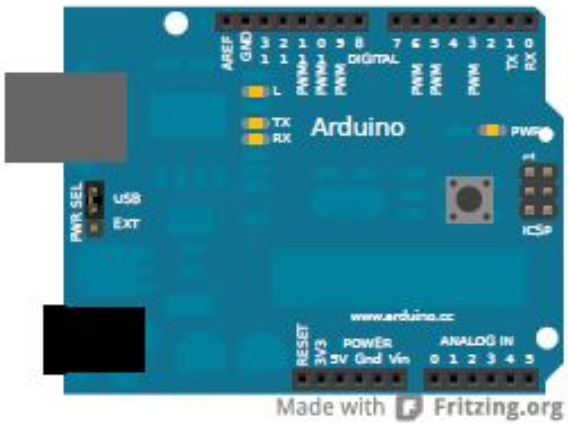
LCD MODULE

Dot matrix LCD modules is mainly used for demonstrate the parameters and fault condition. In the 16 characters 2 lines show is used. It has controller which will interface data's and LCD panel. Liquid crystal displays (LCD's) contain the materials, which combine the properties of both liquids and crystals. It's having a melting point, and it contain a temperature range within which the molecules are almost as mobile as they would be in a liquid, they are grouped jointly in an ordered form similar to a crystal. An LCD contain the two glass panels, the liquid crystal material sandwiched in between them. The inside surface of the glass plates are coated with transparent electrodes which define the character, symbols or patterns to be displayed polymeric layers are at hand in between the electrodes and the liquid crystal molecules to sustain a defined orientation angle.

ARDUINO

Microcontroller

A micro-controller is a tiny computer on a single integrated circuit containing a processor core, memory, and programmable input/ output peripherals. The main part is that a micro-controller contains the processor (which all computers have) and memory, and some of the input/output pins that you can control.

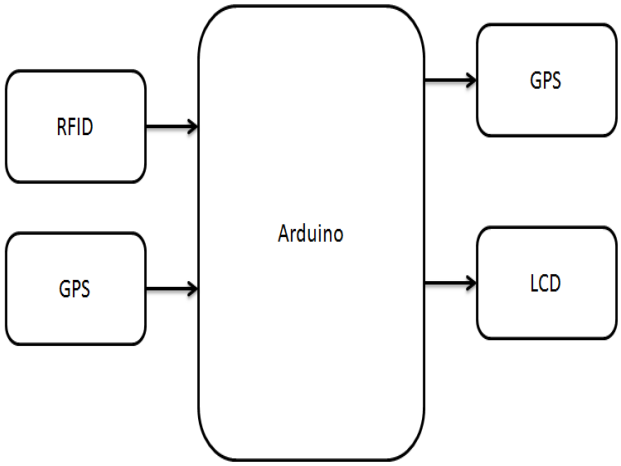


The Arduino Uno board will combines a micro-controller along with all of the extras to make it simple to build and to debug the work. The Uno is a microcontroller board is based on the ATmega328P. It contain 14 digital input/output pins (of which 6 can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz crystal, a USB connection, a power jack, an ICSP header and a reset button. It needed to support the microcontroller, it just connect to a computer with a USB cable or power it with a AC-to-DC adapter or battery.

ISSN 2394 - 7780

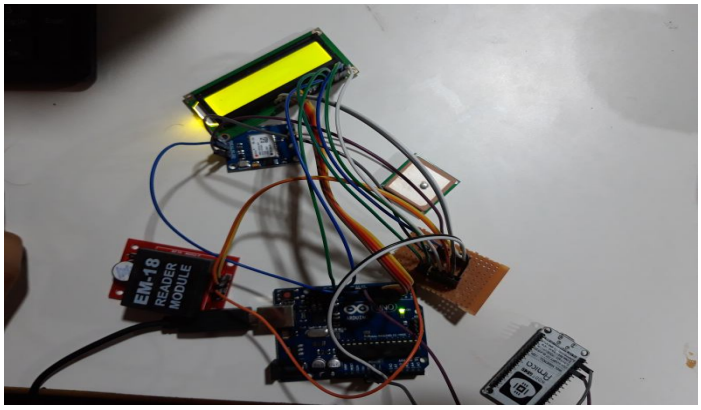
IV. IMPLEMENTATION& TESTING

The proposed method will allows to track your bags throughout the journey directly on your smartphone using WiFi, GPS technology



- RFID technology used for identified the safety of products which are present in the Bags.
- When ever you takes from are place a products to the baggage. that information displayed in LCD.
- GPS used for continuously monitoring a baggage position through the internet

The main aim of this paper is that to map out and ensure the Baggage at different location and inform to the owner about the status of his/her baggage, every time the baggage passes each step. Every baggage has been attached with an RFID card with unique number. That number is given to the owners. If this RFID tag make in communication with the RFID reader at the each stage, the data passes to the PC through the RS 232 cable and checks for any prohibited items like metals contained in the baggage. This checking of metals in the baggage was done by the metal sensor. If the metal detected, the system gives alarm and inform the user through the message using GSM modem and the same information was passed to the database. In this prototype proposed system we are using a single RFID reader and four switches. If we press the first switch, the system goes to the first phase of the security system. If the baggage was not there at the security node for some occasion, the owners will get the message that your baggage checking was under processing. The system waits for some more time, the system send the message to the owners that please contact the person authorities to enquire about your baggage.



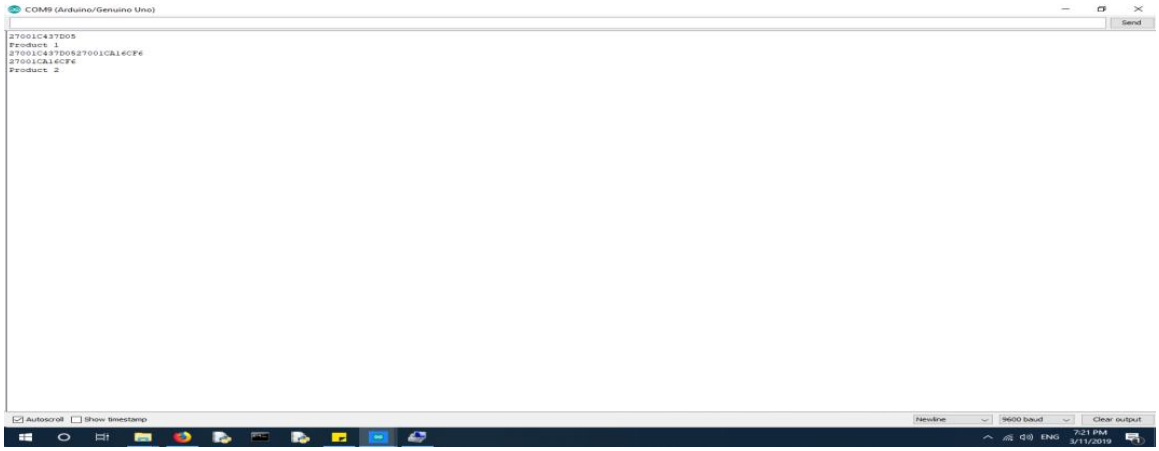
Conforming Baggage and handing it over to owners using IoT

When the baggage owner reaches the bag they have to enter the unique identification number received by him on his mobile. Now, the identification number is read by the reader they will try to match the data related to the Identification number on the RFID tag and entered by the baggage owner, which was already uploaded on the main cloud server by the admin. As soon as the entered identification number is read by the reader. The baggage tracking device may receive signals from GPS satellites on a constant or periodic basis to determine the current location of the baggage tracking device. The signals may be processed by the GPS unit of the baggage tracking device to conclude the longitude and latitude information and the resulting physical address, or a portion or all of the data may be transmitted to the controller for such processing. The longitude and latitude information may be used by the GPS unit and/or the processor to decide actual street locations and/or airport

ISSN 2394 - 7780

codes which are transmitted to the user, or the longitude and latitude information may be transmit instead or in combination with the street address information. Upon determining the current location information, the controller of the baggage tracking device may transmit the current location information through a transmitter provided to the baggage tracking device.

The information about the baggage unique number and the no of the products inside the bag it will scan and stored in cloud. After dispatch to the user it will display the details of products and baggage unique no to the user.



V. CONCLUSION

This Proposed work shows the implementation of tracking the baggage which are either missing or stolen using IoT. Certain actions and techniques have been made and projected in order to accomplish the same. Experimentation has been done and through gps in order to track the location of the bags which are misplaced and lost. Experiment results further concludes that the bags can be easily tracked based upon the google map for tracking the route, directions and location of the bag

REFERENCE

[1]. Tanvir Ahmed, “A Data Warehouse Solution for Analysing RFID-Based Baggage Tracking Data” in IEEE 14th International Conference on Mobile Data Management 2013, Page: 283-292

[2]. L. Riley. IATA Introduces RFID Standard for Baggage Tags Annual Industry Savings Projected at US$760 Million[Online].

[3]. International Air Transport Association, RFID Business Case for Baggage Tagging, 2007, [Online] Available: http://www.iata.org

[4]. IRS Global.: Overall Analysis for 2015 Creative Economy for Trying to New Business Strategy related IoT, In: Market Report 2014-9(2014)

.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

BLOCKADE OF MALEVOLENT TWITTER APPLICATIONS

Lavanyaa M[1], Nandhini P. S[1], Nitin karthik S[2] and P. Sugantha Priyadharshini[3]
Student[1] and Assistant Professor[3], Department of CSE, Sri Ramakrishna Engineering College, Tamilnadu

ABSTRACT
Twitter is one of the most popular and addictive social media used by people all over the world.Twitter is prone to malicious tweets containing URLs for spam, phishing, and malware distribution. With more than millions of installs per day, applications are the important cause for attractiveness and popularity ofTwitter or any social media.This systemrealizes that at least 13% of Twitter apps in dataset are usually malicious. Nowadays faux application links have grown drastically.Unfortunately, hackers have accomplished the potential of exploitation apps for spreading malware and spam. During this project, we tend to come up with aframework which will automatically detect the malicious applications. Our key contribution in developing TRAPPE which is the primary tool targeted on detecting the malicious application on Twitter. First we identify a set of features that help us to analyze malicious from benign ones. Second, leveraging these distinguishing features,where we show that our tool can detect malicious apps with accuracy. Finally, we explore the ecosystems of malicious Twitter application links and identify mechanism that these links use to spread.

Keywords: Malevolent Application,Twitter Application, Social Network,Spam.

I. INTRODUCTION
A social networking website may be a web site wherever every user contains a profile and might keep contact with friends, share their updates, meet new people that have a same interests. . Moving beyond spam email, the spread of malware on OSNs takes the form of postings and communications between friends. We use the term social malware to describe damaging behaviour including identity theft, distribution of malicious URLs, spam, and malicious apps that utilizes OSNs. These Online social networks (OSN) enable third party apps to enhance the user experience on the platforms. Such enrichment includes interesting or entertaining ways of communicating among online friends and different activities such as playing games, listening songs.

Recently, hackers have started taking advantage of the recognition of this third-party apps platform and deploying malicious applications. There are many ways that hacker can benefit from a malicious apps. Some of the ways are: the app can reach large numbers of users and their friends to spread spam, the app can obtain users' personal information such as email address, home town, and gender, and the app can "re-produce" by making other malicious apps popular. Therefore, it is becoming increasingly important to understand social malware better and build better defences to protect users from the crime underlying this social malware. The URL blacklists are designed to detect phishing and malware on the web do not suffice, e.g., because a large fraction of social malware (21% in our dataset) points to malicious applications hosted on Twitter. Although such malicious apps are widespread in Twitter, as we show later, currently there is no commercial service, publicly-available information, or research-based tool to advise a user about the risks of an app.

In this paper we develop TRAPPE, a suite of efficient classification techniques for identifying whether an app is malicious or not. This is arguably the first comprehensive study focusing on malicious Twitter apps that focuses on quantifying, profiling, and understanding malicious apps, and synthesizes this information into an effective detection approach. The basis of our study is a dataset. We classify url as social spam if it points to a web page that spread malware, attempts to phish, request to carry a task, false promises etc. We systematically profile apps and show that malicious app profiles are significantly different than those of benign apps. A striking observation is the laziness" of hackers; many malicious apps have the same name, as 8% of unique names of malicious apps are each used by more than 10 different apps (as defined by their app IDs). Overall, we profile apps based on two classes of features: (a) those that can be obtained on-demand given an application's identifier (e.g., the permissions required by the app and the posts in the application's profile page), and (b) others that require a cross-user view to aggregate information across time and across apps. We develop TRAPPE(Twitter's Application Evaluator) to identify malicious apps either using only features that can be obtained on-demand or using both on-demand and aggregation-based app information. This paper is mainly for detecting and blocking malicious application on twitter, currently there is no commercial service, publicly-available information, or research-based tool toadvise a user about the risks of an app.

II. EXISTING SYSTEM
Social networking sites have becomeone of the main ways for users to keep track and communicate with their friends. Twitter plays a major role in the social media. Hackers have started to take the benefits of third party

ISSN 2394 - 7780

applications in Twitter. The existing system focuses mainly on detecting the suspicious URL in Twitter. The URL is collected from the twitter and it notifies the user that this application is suspicious through a pop-up message. The existing system detects the correlation of URL redirect chains extracted from several tweets.

The existing system uses the Frequent Pattern Mining Algorithm (FPMA).

Disadvantages of existing system

1) It only detects the suspicious applications. When the user logs in to the same application next time, again it will notify the user.
2) The work focused only on finding the accounts created by spammers. Finally, the existing system gives an overview about the threat on Twitter.

III.PROPOSED SYSTEM:

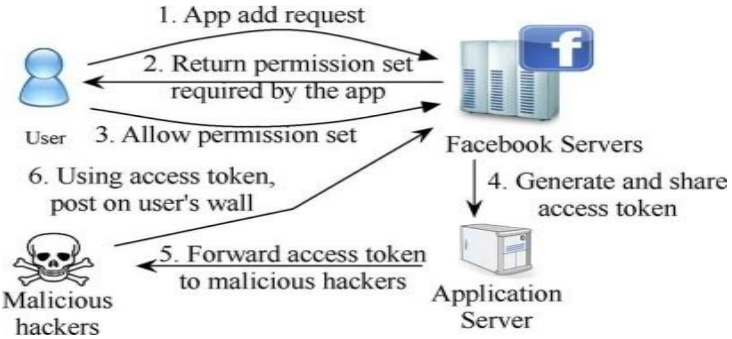
In the proposed system,we can detect and block malicious applications in the twitter before using it. This is done by the help of TRAPPE.TRAPPE, a suite of efficient classification techniques for identifying whether an app is malicious or not. We notice that malicious applications considerably take issue from benign applications with respect to two categories of features: On-Demand Features and Aggregation-Based Features. The main merit of the proposed system is, the work is arguably the first comprehensive study focusing on malicious Twitter apps that focuses on quantifying, profiling, and understanding malicious apps and synthesizes this information into an effective detection and blockade approach. The features used by TRAPPE, such as the reputation of redirect URIs, the number of required permissions, and the use of different client IDs in app installation URLs, are robust to the evolution of hackers. Not using different client IDs in app installation URLs would limit the ability of hackers to instrument their applications to spread each other.If it is a malevolent application a notification is sent to the user, and then it is blocked at the first instance.

- Data Collection
- Feature Extraction
- Training
- Classification and Detection

Thebasisofourstudystartswiththecollectionof data. This module has subcomponents such as the collection of all Twitter application with URLs and crawling for URLs redirections.Whenever this component obtains a Twitter utility with a URL, it executes a crawling thread that follows all redirections of the URL and looks up the corresponding IP addresses. The crawling thread merge these retrieved URL and IP chains to the tweet records and pushes it into a queue. Ourcrawlercannotreachmalicious landing URLs when they use conditional redirections to evadecrawlers. However, because our detection system does not rely on the features of landing URLs, it works independently of such crawlerevasions.

IV. FEATURE EXTRACTION

The feature extraction component has three subcomponents: grouping of identical domains, finding entry point URLs, and extracting feature vectors. This component monitors the tweet queue to determine whether a sufficient number of tweets have been collected. When more than the expected tweets are collected it pops the tweets from the tweet queue. First, for all URLs in the tweets, this component checks whether they share the same IP addresses. If several URLs share at least one IP address, it replaces their domain names with a list of domains with which they are grouped. Next, this component tries to find the entry point URL for each of the tweets. If two or more URLs share the highest frequency in a URL chain, this component selects the URL nearest to the beginning of the chain as the entry point URL. Finally, for each entry point URL, the component finds URL redirect chains that contain the entry point URL, and extracts various features from these URL redirect chains along with the related tweet information.



ISSN 2394 - 7780

V. TRAINING

The training part includes two subcomponents: accessing the account statuses and training of the classifier.Becauseweuse anofflinesupervisedlearningalgorithm,thefeaturevectors for training are relatively older than feature vectors for classification. To label the training vectors, we use the account status; URLs from suspended accounts are consideredmaliciouswhereasURLsfromactiveaccountsare consideredbenign. Werepeatedlyupdateourclassifierusing trainingvectors.Theclassificationcomponentstartsourclassifierusinginput featurevectorstoclassifysuspiciousposts using Machine Learning Algorithm. Theclassification moduleacceptsthe URLandtherelatedsocialcontextfeatures extracted in the previous step. These URLs, detected as suspicious, will be delivered to security experts or more sophisticateddynamicanalysisenvironmentsforanin-depth investigation.

VI. CONCLUSION AND FUTURE WORKS:

This system proposes a new malevolent URL detection system for Twitter, called TRAPPE. Unlike the other systems, TRAPPE is robust when protecting against conditional redirection, because it does not rely on the features of malicious landing pages that may not be reachable. Instead, it focuses on the correlations of multiple redirection of URLs. This project introduces new features on the basis of these real-time classification system using these features, and evaluated the systems accuracy and performance. The evaluation results show that our system is highly accurate and can be a deployed system to classify large samples of tweets from the Twitter public timeline. Using Support Vector Machine algorithm to detect the malicious URLs in Twitter stream then immediately block that URLs and provide high accuracy. Our main future objective is to extend these ideas to develop a real time classification system software for all attributes and every social medias.

REFERENCES

[1]. T. Lakshmi, S. Parthiban “Warning Bird Mail Alert Based Malicious URLs Blocker System in Twitter”, International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, Special Issue 3, March 2014.

[2]. UmaMaheswari, S.K.Srivatsa “Detection of Suspecious URLs Using Real Time System on Social Networks”, International Journal of Scientific & Engineering Research, Volume 5, Issue 6, June-2014.

[3]. Y. Chen, H. Gao, J. Hu, C. Wilson, Z. Li, and B. Y. Zhao “Detectingandcharacterizingsocial spamcampaigns”,inIMC, 2010.

[4]. Y. Chen, A. Choudhary, H. Gao, K. Lee, and D. Palsetia “Towards online spam filtering in social networks” in NDSS, 2012.

[5]. Juan Martenaz- Romo, Lourdes Araujo “Detecting malicious tweets in trending topics using a statistical analysis of language” Expert Systems with Applications, Volume 40, Issue 8, 15 June 2013.

[6]. MD. Sabeeha, SK. Karimullah, P. Babu “Detection of Malicious URLs by Correlating the Chains of Redirection in an Online Social Network (Twitter)” International Journal of Research Studies in Computer Science and Engineering (IJRSCSE), Volume 1, Issue 3, July 2014

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

REVIEW ON OPEN SOURCE TECHNOLOGIES AND PROSPECTS

Selvamohan Thangavel[1] and P. Menaka[2]
Student[1] and Academic Guide[2], Dr. N. G. P. Arts and Science, Covai

ABSTRACT
The DevOps phenomenon is gaining popularity through its ability to support continuous value delivery and ready accommodation of change. However, given the relative immaturity and general confusion about DevOps, a common view of expectations from a DevOps role is lacking. Through investigation of online job advertisements, combined with interviews, we identified key Knowledge Areas, Skills and Capabilities for a DevOps role and their relative importance in Indian job market. In this paper we explore various aspects of DevOps.We look at key success attributes, main processes, tools and frameworks that play an elementary role in DevOps.

Keywords: DevOps;Indian market, Continuous Integration; Continuous Deployment; Education; Empirical; SAE, Analysis; Content Analysis' Cloud; AWS.

I. INTRODUCTION
A DevOps has recently gained popularity as a philosophy that synergizes the operational silos of Software Development (Dev) and IT Operations (Ops) [1]. The three main catalysts that propel its rapid adoption include: a) higher quality expectations from software as it is increasingly offered as a service in the cloud b) demands for rapid delivery of change with growing acceptance of agile and its change embracing attitude, and c) the availability of on-demand powerful and plentiful hardware on the cloud [2]. The uptake of the DevOps trend has been global [1]. Some large organizations claim to have successfully applied its practices in their distributed teams and achieved smooth team collaboration, shortened feedback loops and better customer collaboration [3].

A DevOps strategy supports a globally scalable, rapid and incremental service delivery strategy within a cloud computing infrastructure. Thus it offers potential for software and services companies to operate and compete successfully beyond the traditional centres of technology innovation. For many 'Small Advanced Economies (SAEs). Many believe that DevOps is here to stay, at least in many IT sectors to help organizations deliver quality service with efficiency [2]. However, given the relative recency and emergent nature of the DevOps phenomenon, an inadequate body of knowledge, and general confusion surround DevOps concepts and definitions [3]. A recent study has compared responsibilities of a DevOps engineer role in four countries (India, USA, UK and Canada) and has shown that the responsibilities and skills expected from DevOps roles significantly vary from country to country [4].. The questions this research tries to address are:

What knowledge areas, skills and capabilities are in demand for a DevOps role in IT market?

This study will identify implications and chart directions for research and practice in the DevOps area, which may have wider applicability to other small advanced economies. This paper proceeds as follows. Section II briefly situates the study in the literature to provide the background and related work in this area. Section. III. Some issues arising for researchers, educators and practitioners in this area are also discussed in Section IV, Section V.concludes the paper.

II. LITERATURE REVIEW
A. Background
Traditionally, a disconnect has existed between software development and operations [9], frustrating organizational desires for continuous value delivery. It was apparent that the '*wall of confusion*' caused by independent departments working separately could not achieve the levels of productivity and quality demanded by modern day software [10]. A systems thinking approach was therefore needed, one that emphasized organization-wide collaboration to address the lack of cohesion between these departments [11]. The DevOps approach tries to address this problem by continuously integrating software development with operational deployment [12]. It envisions software development work as one activity that flows across functions instead of viewing it as individual actions that remain "lurking in silos" [11]. This is how DevOps as a strategy aims to break down the functional silos and improve collaboration as well as productivity [10]. The DevOps movement gained momentum as more and more professionals began to realize its potential benefits in the world of building, deploying, and maintaining environments [11]. With maturing technology and on-demand plentiful resources in the cloud, the possibilities of a wider industrial application of DevOps was increased. By putting DevOps philosophy into practice, the 'unicorns' of DevOps such as Amazon, Google, Netflix and Snapchat are observed to be achieving significant performance improvements and success [14]. Furthermore, these

ISSN 2394 - 7780

companies substantially invested into DevOps and have innovatively advanced the release engineering techniques and technologies which can now reduce release cycle times to days or even hours [12]. Several equally successful DevOps model variants such as NoOps, ChatOps, and SmartOps are brought to the fore by these organizations [11, 12]. DevOps is 'trendy' as tempting success stories of DevOps 'Unicorns', SMEs, and startups are echoed from websites, reports, books, blogs, social and broadcast media [8]. Similarly, slogans like "*Enterprise DevOps adoption Isn't Mandatory - but Neither is Survival*" [21] are enticing everyone to jump upon the DevOps bandwagon [1] without fully understanding what it is. As a result, confusion prevails in the industry as to what DevOps actually means or entails when it comes to engaging people with this strategy [6, 8].

B. Related Work

Investigation into what employers want from their potential employees could be carried out in a number of ways such as interviews, surveys from employers and job seekers or unobtrusively through online job ads [23]. Several studies have been conducted using these methods in the field of IS using job ads to assess the employer requirements often as an attempt to reconcile the gaps between industry needs and academia's offerings.

The second major area of the desired competency in students was more technical in nature requiring skill and competence in Architecture and Infrastructure, Operating Systems, Network and Security. They analyzed 211 randomly selected online job postings of five different countries and for three particular roles; DevOps Engineer, Build and Release Engineers. They identified common themes of activities these roles have to perform. They argue that companies do not fully understand what skills to look for when they advertise to hire people in these roles. This, according to them, was due to a lack of common vocabulary and the body of knowledge in the DevOps area; a finding that resonates well with the existing literature especially regarding the opaqueness in the definition of the DevOps concept [28]. Secondly, using Summative Content Analysis (SCA), a quantification of words appearing in the job advertisement was carried out using a data analysis tool, *Nvivo*[10]. The purpose was to understand the contextual use of an individual word occurrence and ascertain its relative importance in comparison with the other concepts appearing in the advertisements. More representative abstract theme. For example, Build Automation, Build Environment, Build Process were grouped into a *Software Build Process* theme. Similarly, Network Infrastructure (REST, Web services, Firewalls), Network Issues (Trouble Shooting), Network Management (Practice & Procedure, LAN/WAN) were unified under a more abstract and boarder concept *Networking*

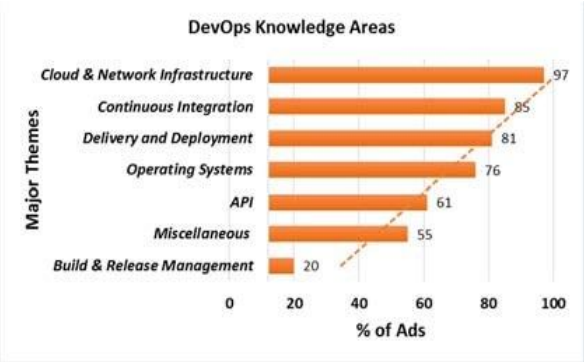


Figure-1: DevOps Knowledge Areas and Major Themes

Continuous Integration and *Delivery and Deployment* with a significantly high percentage of 85 and 81 percent respectively. These figures reflect a general view in the literature that DevOps initiatives are almost inseparable from the drive to gain speed in production and delivery through cloud technologies & CI and CD practices (See Figure 1).

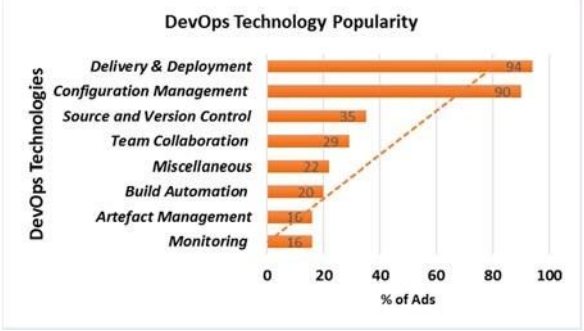


Figure-2: DevOps Technology Popularity

ISSN 2394 - 7780

Example [1] that it was surprising to see a lack of focus on Testing Automation (8%) in the advertisements analyzed in this study.

B. DevOps Technologies

In DevOps technologies, experience with Delivery and Deployment (D& D) tools were the most sought after skill in potential candidates. Hands on experience with tools such as *Docker, Jenkins, Bamboo* and *Octopus* were highly desirable as shown from the very high percentage (94 %) for D&D category in Figure 2. Experience with Configuration Management tools were the second most sought after skill job seekers. Tools such as *Puppet, Chef, Ansible,* and *BitBucket* were repeatedly mentioned. This means that tools like Puppet and Chef that support CM have maintained their popularity over the last few years in the literature and industry as reported in [39] and [40]. Source and version control tools such as *Git* and *Subversion* were apparently less significant compared to Deployment and CM tools with only 35 percent of ads reporting them. As seen in Figure 2, technological enablers of DevOps such as Build Automation, Artefact management and Monitoring did not appear frequently scoring 20, 16 and 16 percent respectively. Again, this lack of emphasis on Build Automation and Artefact management tools such as (Ant, Gradle, Maven, Artifactory etc.), could be due to the belief that these tools are mainly for supporting developers rather than Ops people and hence not required in many of the DevOps engineering jobs.

C. Languages and Frameworks

In programming languages, experience with Java, C# and Ruby were commonly desired with 71 percent of the ads requiring competency in these languages (Figure 3). Some form of scripting skills were demanded from the candidates in all advertisements (100%).

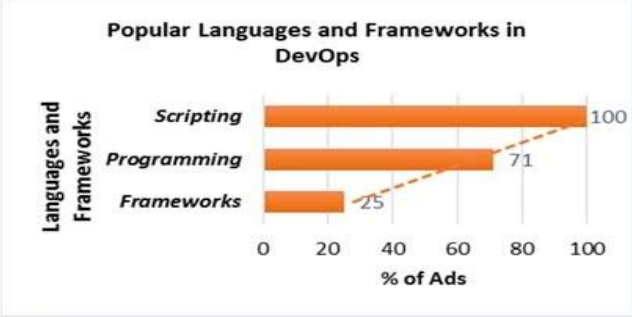


Figure-3: DevOps Languages and Frameworks

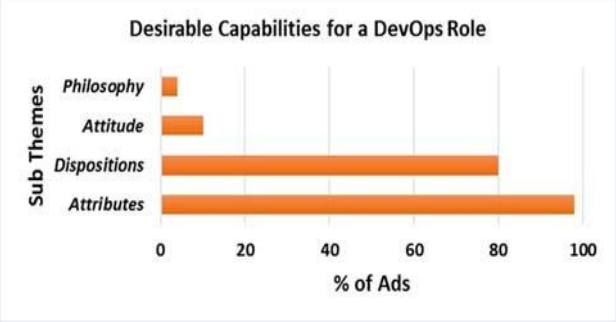


Figure-4: Capabilities Desired for a DevOps Role

The analysis revealed that Python, PHP, PowerShell, JavaScript, Bash and Angular were in high demand (See Appendix 1 for details). Our results confirm scripting related findings by Kerzazi and Adam [8], who also identified scripting tasks to be the most important theme across DevOps roles they evaluated. The commonly cited frameworks of choice for the employers included .NET and Spring however they were specified only in 25 percent of the ads (See Figure 3).

D. Capabilities

Complementing the required knowledge and skills, job ads also showed a desire for recruits who had specific (Attributes, Dispositions, Attitude & Philosophy) detailed in Appendix 1. Schussler observes that *"dispositions are different from knowledge and skills"* and *"concerns not what abilities people have, but how people are disposed to use those abilities" [12].* The dispositions and attributes sought were typically human and team centric, demanding flexibility and adaptability, a wider mindset including customer/business awareness, relationship management, communication, general business acumen and respect in collaborative relationships (Figure 4).

ISSN 2394 - 7780

E. Job Titles and Roles
From our analysis of Job listings, we see a diversity of job titles were advertised to join organizations in various DevOps roles (See Appendix 1). Furthermore, job titles whether emphasizing a Dev or Ops aspect, demanded skills extending from Dev to Ops and vice versa. For example, 20% of the job ads sought Full Stack Developers in C#, Java PHP and .NET but also required experience in CI / CD, Build & Release, Cloud technologies and infrastructure management in Linux or Unix. Similarly, 70% of the job emphasizing Ops elements required the candidates to have strong scripting skills and knowledge and experience of DevOps tools as well as awareness of CI and CD practices. This is an indicator of the industry trend where the DevOps philosophy has started to take its roots where the departmental silos are being challenged. Dev and Ops people are increasingly joining teams and sharing responsibilities from development to deployment of code.

IV. DISCUSSION
The results from our analysis of job advertisement data raised several interesting points for further discussion from which we can draw a set of conclusions. We discuss our main findings below.

State of DevOps
From our analysis we see DevOps occupying an intermediate role in today's software companies. We are seeing differing constellations of teams situated within wider groupings or "tribes"[09], with a typical formation having multiple teams interfacing to a single DevOps release team, often with a Release Manager role who acts as a boundary spanner between the development activities and the production release. So while we are seeing continuous integration we are not seeing continuous deployment yet.

C. Knowledge Areas
Knowledge areas demanded were a mix of traditional development and cloud computing knowledge and skills, based within an infrastructure and technology context. Build, release CI & CD automation practices were sought as critical skillsets. Operating systems and system administration know-how were important, as were APIs and Packaged or high level products supporting web interoperability and enabling productivity, and component and services composition.

During the interviews the DevOps team lead identified a general lack of skillset in networking and infrastructure concepts in people seeking DevOps roles in their organization.

"We have very hard time hiring for people because the skillset does not exist. Like people with good

fundamentals of networking and data centre engineering."

D. Tools and Technologies
In addition to the broader issues associated with DevOps and GSE we identified some major thematic areas which represent the context and needs of employers for DevOps personnel.

In the technology area we saw very rich and complex constellations of technologies being demanded. The picture presented was one of a sophisticated repertoire of tools to be orchestrated in order to perform DevOps functions. This richness and complexity brought its own significant learning overhead.

One of the Developers reported that getting to grips with complexity of DevOps technologies in combination with DevOps practices during the software development lifecycle was quite challenging. The team lead of this developer confirmed the challenges and added that:

"Her learning curve was like 90 degrees"

We saw specialists, typically senior technical leads, joining teams for periods of time to select or recommend, install, configure and establish working practices around specific tools sets. In a sense we could term the experts in these roles as 'Tribal Nomads'.

E. Languages and Frameworks
Again with the languages and frameworks, we saw a diverse set of technologies being employed. In the development roles we saw traditional development languages (3GL's etc.), sometimes within wider vendor frameworks. Web oriented languages were common and from a more operational focus we saw the dominance of scripting languages enabling DevOps personnel to perform system administration and infrastructure management/tuning roles/tasks.

For employers, programming language skills such as those were required in combination with the underlying computing and networking knowledge. In the interviews, the training manager mentioned the absence of this combination in the fresh graduates seeking a DevOps role:

ISSN 2394 - 7780

F. Capabilities

A broader theme that came through from analyzing the data related to the attributes and dispositions demanded of DevOps roles, was that leadership attributes were actively sought. The diagram below illustrates Quinn's leadership model, identifying four quadrants with broad profiles of activity. From our data we saw the strong emphasis on 'Transformational Leadership' roles such as Mentor, Facilitator, Innovator and Broker. These stood in contrast to the more traditionally viewed expectations of technical employees engaged in projects and task related activities, better fitting a 'Transactional Leadership' style. Expectations of taking responsibility for other team members through training and mentoring them to develop new KSCs were very evident in the job ads.

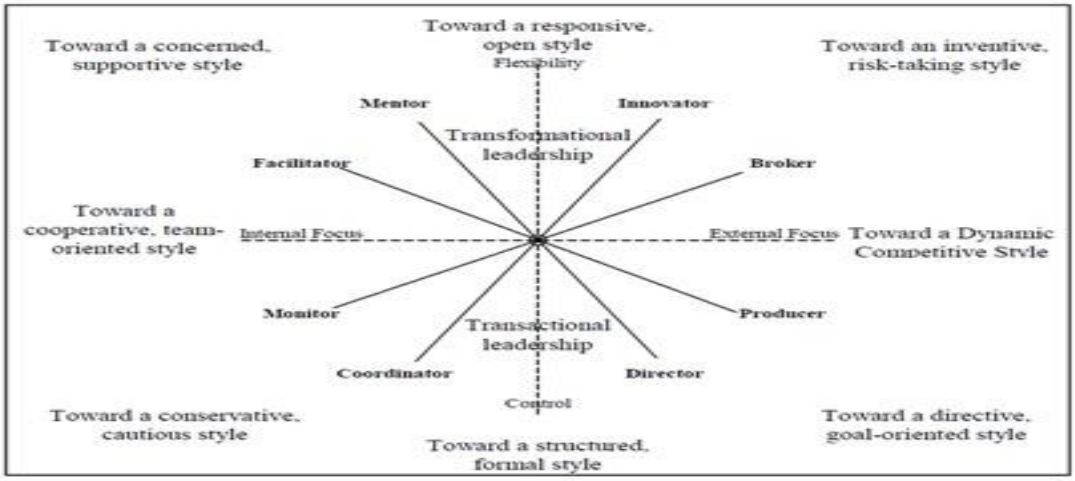


Figure-5: Competing Values Framework of Leadership Roles [43]

V. CONCLUSIONS

This investigation has provided a snapshot of Knowledge areas, Skills and Capabilities (KSCs) to gain a reasonably comprehensive overview of employers' expectations from DevOps roles. Findings from this study reveal that DevOps is being adopted as a philosophy whereby responsibilities of individual members are shared across increasingly joint Development and Operations teams. As a result, extended capabilities are desired from DevOps roles that go beyond their usual Dev or Ops strengths. This we believe will make more traditional roles such as dedicated Release Engineers fade away.

In summary, we believe that DevOps is a key trend, underpinned by business drivers of continuous value delivery, and globally scalable technology platforms. However, the demands of the roles required, the inherent organizational tensions, and the ideal global configurations of such "tribes" of DevOps personnel are still emerging.Yet, DevOps can definitely be seen as a global phenomenon in software engineering, the implications of which are still becoming apparent.

REFERENCES

[1] A. Ravichandran, K. Taylor, and P. Waterhouse, "DevOps in the Ascendency," in DevOps for Digital Leaders, ed: Springer, 2016, pp. 314.

[2] D. Spinellis, "Being a DevOps Developer," IEEE Software, vol. 33, pp. 4-5, 2016.

[3] R. Britto, D. Smite, and L.-O. Damm, "Software Architects in Large-Scale Distributed Projects: An Ericsson Case Study," IEEE Software, vol. 33, pp. 48-55, 2016.

[4] K. Harland and H. O'Connor, "Broadening the Scope of Impact," 1 March 2015.

[5] NZTech, "DIGITAL NATION NEW ZEALAND: An Analysis of the Impact of the Tech Sector and Technology on the New Zealand Economy - From Tech Sector to Digital Nation," New Zealand Technology Industry Association, Wellington2016 2016.

[6] T. Kanij, R. Merkel, and J. Grundy, "An empirical study to review and revise job responsibilities of software testers," in 2014 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC), 2014, pp. 89-92.

[7] E. Diel, S. Marczak, and D. S. Cruzes, "Communication Challenges and Strategies in Distributed DevOps," in 2016 IEEE 11th International Conference on Global Software Engineering (ICGSE), 2016, pp. 24-28.

ISSN 2394 - 7780

[8] F. Calefato and F. Lanubile, "A Hub-and-Spoke Model for Tool Integration in Distributed Development," in 2016 IEEE 11th International Conference on Global Software Engineering (ICGSE), 2016, pp. 129-133.

[9] Analysis," Qualitative health research, vol. 15, pp. 1277-1288, 2005.

[10] S. K. Bang, S. Chung, Y. Choh, and M. Dupuis, "A grounded theory analysis of modern web applications: knowledge, skills, and abilities for DevOps," in Proceedings of the 2nd annual conference on Research in information technology, 2013, pp. 61-62.

[11] S. T. Acuña and N. Juristo, "Assigning people to roles in software projects," Software: Practice and Experience, vol. 34, pp. 675-696, 2004.

[12] V. Braun, V. Clarke, G. Terry, P. Rohleder, and A. Lyons, "Thematic analysis," Qualitative Research in Clinical and Health Psychology, p. 95

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

AN INTERACTIVE STUDY OF BIG DATA TECHNOLOGIES IN HEALTH CARE WITH MACHINE LEARNING ALGORITHMS

Parimala S[1] and Dr. P. Senthil Vadivu[2]
Assistant Professor[1], Department of Computer Science, SRM Institute of Science and Technology, Chennai
Head[2], Department of Computer Applications, Coimbatore

ABSTRACT
The aim of this study is to create a collaborative Big Data Platform Analytics (BDA) platform with the Machine Learning Algorithms. This paper is going to elucidate the significance of big data analytics and Machine Learning in healthcare, we also exhibit the abstract framework of big data analytics for healthcare which involves the data collection in different divisions, the database of the genome, with appropriate electronic health records, text images, and clinical records and decision support system

Keywords: Big Data Platform Analytics (BDA), Machine Learning, Health care.

I. INTRODUCTION

Implementation of computer programming is the only factor that makes the huge difference between conventional Health care analytics and the modern health care analytics. In 2011, the US stored roughly 150 Exabyte (1018) of health data, and this number is expected to increase to more than a yottabyte (1024) over the next few years [1].

Nowadays, the healthcare industry is facing different challenges in handling the developing health care data. The field of big data analytics is emergent and has the impending to deliver valuable visions for the healthcare system. The Big data Analytics as noted above, most of the massive amounts of data generated by this system is saved in hard copies, which must then be digitized [2].

Those electronic data are used to enhance the quality of the health care and also simultaneously reduce the costs and potentially promise to support the functions of healthcare and medical applications. It also offers the personalized care to improve the care of the patients and eliminates the unnecessary data. A McKinsey Global Institute study suggests, "If US healthcare were to use Big Data creatively and effectively to drive efficiency and quality, the sector could create more than $300 billion in value every year" [3]. Even though, many experimentations takes place, both the machine learning and the big data analytics technologies plays an important role to identify the appropriate patterns to work on it. Machine Learning and Data mining are somewhat similar in concept. Both the technologies are used to identify the patterns, based on the human intervene Data mining applications and machine learning are used to improve the understanding the program rather than extracting the data.

II. ALGORITHMIC TECHNIQUES:

Machine learning provides various algorithms. Jason Brownlee [5] illustrates different machine learning strategies. The hierarchal structure of various algorithms is given below.

There are different classifications methods propose by researchers. The widely used methods are described by Han et al. [7].Meanwhile Patil et al .Pursued a hybrid way pairing the two genetic algorithm and decision tree to make an advanced decision tree to improve performance and efficiency of computation. [6].

The Concept of Big Data is defined by Gartner [4] as high volume, high velocity, and /or high variety data that require new processing paradigms to enable insight discovery, improved decision making and process optimization. Many number of technologies are being developed to acclimate the machine learning algorithms to work with massive sat of data sets. Map Reduce and Hadoop are such distributing frameworks of processing.

The implementations of Machine learning in health care industry has generated greater results. But it vastly focuses on diagnosing the diseases and the health condition of the patient's not obviously on treatment. But it assist in diagnosing the disease as it is the initial step to be taken form any treatment of the chronic diseases. Central-Line associated blood stream infections in one of the very serious condition that affects the patients. Through the central line when the germs and bacteria pass in to the blood stream they indicate that the patients are in great risk. At this time Machine Learning comes into play it can predict which patients can under high risk to CLBSIs and the chance is given to the physicians to take extra care to that patients and take necessary steps for the treatment".

ISSN 2394 - 7780

III. MACHINE LEARNING CHALLENGES INITIATING FROM BIG DATA CHARACTERIZATION

Big Data are often described by its dimensions, which are referred to as its Vs. Earlier definitions of Big Data focused on three Vs. [8] (volume, velocity, and variety); however, a more commonly accepted definition now relies upon the following four Vs. [9]: volume, velocity, variety, and veracity. It is important to note that other Vs. can also be found in the literature. For example, value is often added as a 5th V [12], [10]. However, value is often added as the desired outcome of Big Data processing [11] and not as defining characteristics of Big Data itself.

IV. EXTRAPOLATIONS ON HEALTH CARE TECHNOLOGY

A. Analytics will be the backbone enhancing internal clinical Facts.

Data analytics was the number one funding in the health care systems. We anticipate that even this year 2019 will guide in a diversity of progressive analytics protests. Many will be fresh and different in the output generated, but the ambiguity of practical clinical significance will endure. So an affirmation of the computational competences will be most momentous since that would open the number of opportunities.

B. AI beyond the hype

The most considerable AI applications in real-world will be in image processing through the initial stage in machine learning for areas like radiology and skin related dermatological abrasions. The Secondary stage will be self-monitoring of radiology applications for dermatology.

C. Role of CDS Tools

Clinical decision support (CDS) provides clinicians, staff, patients or other individuals with knowledge and person-specific information, intelligently filtered or presented at appropriate times, to enhance health and health care. CDS encompasses a variety of tools to enhance decision-making in the clinical workflow. This is prediction is expected by many of them and is considered to be forthcoming. The price of the genome sequencing suddenly decreased and stooped running at one stage. There are obstacles to wide implementation and frugalities of balance since the consumers still have some privacy issues and are uncertain to relieve already existing conditions. The other concept is that, healthcare providers don't have enough tools to infer the complex results. Because there thought was rare diseases are more common. The value of AI will increase and cost of gene sequencing will reduce.

V. CONCLUSION

Health care industry that uses machine learning gets the benefits to enhance the efficiency and also quality treatment to the patients. At the same time it also lowers the cost of the treatment. Still there is a need for more improved and more information to health care providers since they can make healthier diagnosis and treatment. The approach of Machine Learning appears to be increasing in the field of Health care in diagnosing the images and diseases also. Any further research can effortlessly extend the system to progress the amenities and services.

REFERENCES

1. R. Fang, S. Pouyanfar, Y. Yang, C. Chen Computational health informatics in the big data age: a survey ACM Computer Survey, 49 (1) (2016), pp. 1-6, 10.1145/2932707 CrossRef Scopus, Google
2. X. Wu, X. Zhu, G. Q. Wu, and W. Ding, Data mining with big data, IEEE transactions on Knowledge and Data Engineering, vol. 26, no. 1, pp. 97–107, 2014
3. Shah NH, Tenenbaum JD. The coming age of data-driven medicine: translational bioinformatics' next frontier. Journal of the American Medical Informatics Association. 2012; 19: e2-e4.
4. M.A. Beyar and D.Laney, "The importance of 'big data': A definition ", Gartner Research, Stamford, CT,USA,Tech. Rep.G00235055,2012
5. Jason Brownlee, "Machine Learning Foundations, Master the definitions and concepts", Machine Learning Mastery, 2011.
6. Patil D.V, Prof. Dr. R. S. Bichkar, "A Hybrid Evolutionary Approach To Construct Optimal Decision Trees with Large Data Sets", IEEE, 2006
7. Jawei Han and Micheline Kamber," Data Mining: Concepts and Techniques," Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2000 "
8. R. Narasimhan and T. Bhuvaneshwari, ``Big data_A brief study," Int.J.Sci. Eng. Res., vol. 5, no. 9, pp. 350_353, 2014.

ISSN 2394 - 7780

9. F. J. Ohlhorst, Big Data Analytics: Turning Big Data into Big Money, vol. 15. Hoboken, NJ: Wiley, 2012.

10. Y. Demchenko, P. Grosso, C. De Laat, and P. Membrey, ``Addressing big data issues in scientific data infrastructure," in Proc. Int. Conf. Collabo- ration Technol. Syst. (CTS), May 2013, pp. 48_55.

11. M. Ali-ud-din Khan, M. F. Uddin, N. Gupta, and N. Gupta, ``Seven V's of big data understanding big data to extract value," in Proc. Zone Conf. Amer. Soc. Eng. Edu., Apr. 2014, pp. 1_5.

12. W. Fan and A. Bifet, ``Mining big data: Current status, and forecast to the future," SIGKDD Explorations Newslett., vol. 14, no. 2, pp. 1_5, Dec. 2012.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

SCHOOL AND COLLEGE FAILURE STUDENTS DROPOUT SYSTEM PREDICTION BASED ON ANN AND MKNN ALGORITHM USING DATA MINING TECHNIQUES

T. Kavipriya[1] and N. Kumar[2]
Assistant Professor[1], Department of Computer Technology, Hindusthan College of Arts and Science, Coimbatore
Assistant Professor[2], Department of Computer Science, Dr. N. G. P Arts and Science College , Coimbatore

ABSTRACT
Data mining techniques are applied to predict school and college failure and dropout of the student. This method used a real data on middle-school students for prediction of failure and drop out. It implements white-box classification strategies, like induction rules and decision trees or call trees. This paper represents the K-Nearest Neighborhood (KNN) classification is one of the most fundamental and simple classification methods. The main Idea is to use robust neighbors in training data. This modified KNN is better from traditional KNN in both terms: robustness and performance. The proposed KNN classification is called Modified K-Nearest Neighborhood (ANN & MKNN). ANN & MKNN can be considered a kind of weighted KNN, so that the query label is approximated by weighting the neighbors of the query. The proposed method is evaluated on a variety of several standard data sets.

I. INTRODUCTION

Generally, data mining (sometimes called data or knowledge discovery) is the process of analyzing data from different perspectives and summarizing it into useful information that can be used to increase revenue, cuts costs, or both. Data mining software is one of a number of analytical tools for analyzing data. It allows users to analyze data from many different dimensions or angles, categorize it, and summarize the relationships identified. Technically, data mining is the process of finding correlations or patterns among dozens of fields in large relational databases.

Although data mining is a relatively new term, the technology is not. Companies have used pitiful computers to shift through volumes of supermarket scanner data and analyze market research reports for years. However, continuous innovations in computer processing power, disk storage, and statistical software are dramatically increasing the accuracy of analysis while driving down the cost. Dramatic advances in data capture, processing power, data transmission, and storage capabilities are enabling organizations to integrate their various databases into *data warehouses*. Data warehousing is defined as a process of centralized data management and retrieval. Data warehousing like data mining, is a relatively new term although the concept itself has been around for years. Data warehousing represents an ideal vision of maintaining a central repository of all organizational data. Centralization of data is needed to maximize user access and analysis. Dramatic technological advances are making this vision a reality for many companies. And, equally dramatic advances in data analysis software are allowing users to access this data freely.

II. LITERATURE REVIEW

Although, using data mining in higher education is a recent research field, there are many works in this area. That is because of its potentials to educational institutes. Romero and Ventura have a survey on educational data mining between in the 1995 and 2005. They concluded that educational data mining is a promising area of research and it has a specific requirements not presented in other domains. Thus, work should be oriented towards educational domain of data mining. El-Halees gave a case study that used educational data mining to analyze students' learning behavior. The goal of study is to show that how useful data mining can be used in higher education to improve student' performance. It used students' data from database course and collected all available data including personal records and academic records of students, course records and data came from e-learning system. Then, it applied data mining techniques to discover many kinds of knowledge such as association rules and classification rules using decision tree. Also he clustered the student into groups using EMclustering, and detected all outliers in the data using outlier analysis. Finally, it presented how can it benefited from the discovered knowledge to improve the performance of student.

Al-Radiate et al applied the data mining techniques, particularly classification to help in improving the quality of the higher educational system by evaluating student data to study the main attributes that may affect the student performance in courses. The extracted classification rules are based on the decision tree as a classification method; the extracted classification rules are studied and evaluated. It allows students to predict the final grade in a course under study.

ISSN 2394 - 7780

Bradawl and Pal applied the classification as data mining technique to evaluate student' performance, they used decision tree method for classification. The goal of their study is to extract knowledge that describes students' performance in end semester examination. They used students' data from the student' previous database including Attendance, Class test, Seminar and Assignment marks. This study helps earlier in identifying the dropouts and students who need special attention and allow the teacher to provide appropriate advising. Shannaq et al. [11], applied the classification as data mining technique to predict the numbers of enrolled students by evaluating academic data from enrolled students to study the main attributes that may affect the students' loyalty (number of enrolled students). The extracted classification rules are based on the decision tree as a classification method, the extracted classification rules are studied and evaluated using different evaluation methods. It allows the University management to prepare necessary resources for the new enrolled students and indicates at an early stage which type of students will potentially be enrolled and what areas to concentrate upon in higher education systems for support.

III. RESEARCH METHODOLOGY

K-means Clustering

The k-means algorithm is one of the most widely used clustering algorithms and has been applied in many fields of science and technology. One of the major problems of the k-means algorithm is that it may produce empty clusters depending on initial center vectors. For static execution of the k-means, this problem is considered insignificant and can be solved by executing the algorithm for a number of times. In situations, where the k-means is used as an integral part of some higher level application, this empty cluster problem may produce anomalous behavior of the system and may lead to significant performance degradation. This paper presents a modified version of the k-means algorithm that efficiently eliminates this empty cluster problem. In cluster analysis, the k-means algorithm can be used to partition the input data set into k partitions (clusters).

The process iterates through the following steps:

- Assignment of data to representative centers upon minimum distance, and

1. Computation of the new cluster centers.

- The process stops when cluster centers (or the metric M) become stable for two consecutive iterations. The basic k-means algorithm is greedy in nature.
- K-means is the most popular and easy-to-understand clustering algorithm. The main idea of K-means is summarized in the following steps:
- Arbitrarily choose k objects to be the initial cluster centers/centroids;
- Assign each object to the cluster associated with the closest centroid;
- Compute the new position of each centroid by the mean value of the objects in a cluster; and
- Repeat Steps 2 and 3 until the means are fixed.

FUZZY C- MEANS CLUSTERING

Fuzzy c-means (FCM) is a method of clustering which allows one piece of data to belong to two or more clusters. This method frequently used in pattern recognition. It is based on minimization of the following objective function:

$$J_m = \sum_{i=1}^{N}\sum_{j=1}^{C} u_{ij}^{m}\left\|x_i - c_j\right\|^2 \quad , \quad 1 \le m < \infty$$

where m is any real number greater than 1, u_{ij} is the degree of membership of x_i in the cluster j, x_i is the ith of d-dimensional measured data, c_j is the d-dimension center of the cluster, and ||*|| is any norm expressing the similarity betiten any measured data and the center. Fuzzy partitioning is carried out through an iterative optimization of the objective function shown above, with the update of membership u_{ij} and the cluster centers c_j by:

$$u_{ij} = \frac{1}{\sum_{k=1}^{C}\left(\frac{\left\|x_i - c_j\right\|}{\left\|x_i - c_k\right\|}\right)^{\frac{2}{m-1}}} \quad , \quad c_j = \frac{\sum_{i=1}^{N} u_{ij}^{m} \cdot x_i}{\sum_{i=1}^{N} u_{ij}^{m}}$$

ISSN 2394 - 7780

This iteration will stop when $\max_{ij}\left\{\left|u_{ij}^{(k+1)} - u_{ij}^{(k)}\right|\right\} < \varepsilon$, where ε is a termination criterion betiten 0 and 1, whereas k is the iteration steps.

This procedure converges to a local minimum or a saddle point of J_m. The algorithm is composed of the following steps:

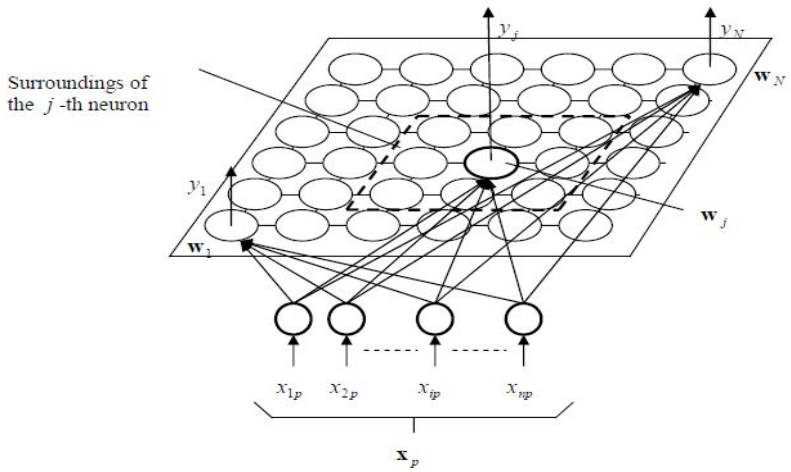
Neural networks

It is possible to use the neural network with so called unsupervised learning for cluster analysis That is based on evaluation of the difference (distance) of the itighted vector w of the neural Network from the vector of input pattern x and search of neuron, whose itighted coefficient have the minimum distance of w from x . This neuron, which won among the neurons of the network, has the right to adjust its itights and the tights of neurons in its surroundings and thus the response on submitted learning pattern to better value. After submitting of a further learning pattern it can win another neuron of the net that can adjust its itights and the itights of neurons in its surroundings and thus to increase better assert etc. The clusters are thus created in the net that in certain places of the network optimally respond to certain symptoms of submitted patterns, as itll as unknown patterns.

The "map" of patterns is created. This network was presented by Kohonen in 1982 and it is called Kohonenself organizing map. The schema of this network is presented in the Figure 1.

The input vector (for the p -th input pattern) has the form ( ) Tp p pnpx , x , , x 1 2

x = K.



It is calculated for each neuron its distance j D (of the vector j w from the vector p x) as an

Euclidean distance (j p) j p D w ,x = w – xor as a spherical distance( ) j j p j p D w , x = 1− w _ x .For the evaluation of j D is used the formula

Where j = 1,K, N .

The surroundings c NE of the winning neuron is a set of neurons inside the bounded area (for Example of a square or (because the circle is an ideal area) the hexagon is used that approximate the circle) around the winning neuron. See Figure 2 or Figure 3, respectively

The final step in the algorithm is to update the itights, this occurs as follows:

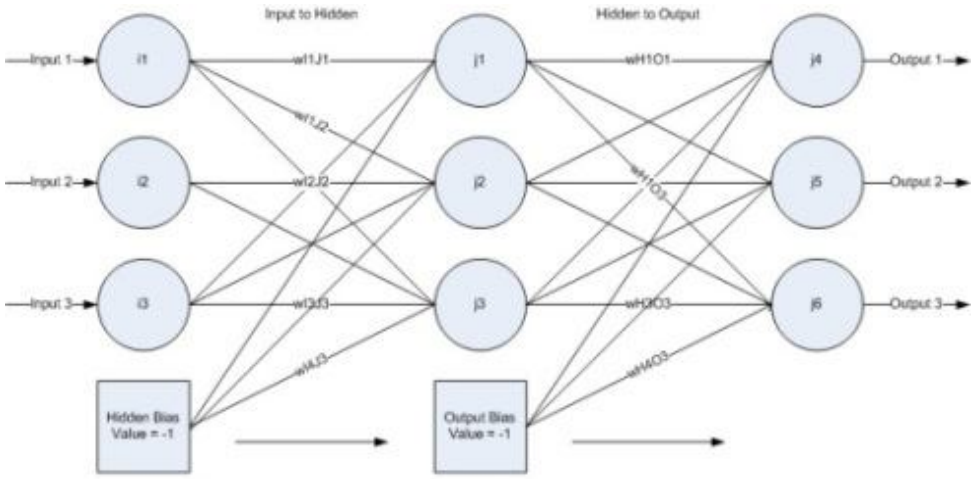
$$w_{ij} = w_{ij} + \Delta w_{ij} \; and \; w_{jk} = w_{jk} + \Delta w_{jk}$$

where $\Delta w_{ij}(t) = \alpha . inputNeuron_i . \delta_j$
$and \; \Delta w_{jk}(t) = \alpha . hiddenNeuron_j . \delta_k$

$\alpha - learning\ rate$
$\delta - error\ gradient$

The alpha value you see above is the learning rate; this is usually a value betiten 0 and 1. It affects how large the itight adjustments are and so also affects the learning speed of the network. This value need to be careful selected to provide the best results, too low and it will take ages to learn, too high and the adjustments might be too large and the accuracy will suffer as the network will constantly jump over a better solution and generally get stuck at some sub-optimal accuracy.

ISSN 2394 - 7780



Standard Architecture for a Back Propagation Neural Network

Above is a basic multilayer neural network, the inputs are shard and so are the outputs, note that each of these links have separate itights. Now what are those square blocks in the neural network? They are our thresholds (bias) values, instead of having to store and update separate thresholds for each neuron (remember each neuron's activation function took an itighted sum minus a threshold as input), it simply create 2 extra neurons with a constant value of -1. These neurons are then hooked up to the rest of the network and have their own itights (these are technically the threshold values).

The only control over this architecture you have is over the number of hidden neurons since your inputs and desired outputs are already known, so deciding on how many hidden neurons you need is often a tricky matter, too many is never good, and neither is too little, some careful experimentation will often be required to find out an optimal amount of hidden neurons.I'm not going to go over feeding the input forward as its really simple: all you do is calculate the output (the value of the activation function for the itighted sum of inputs) at a neuron and use it as the input for the next layer.

Predicting is making claims about something that will happen, often based on information from past and from current state. Everyone solves the problem of prediction every day with various degrees of success. For example irater, harvest, energy consumption, movements of (foreign exchange) currency pairs or of shares of stocks, earthquakes, and a lot of other stuff needs to be predicted. In technical domain predictable parameters of a system can be often expressed and evaluated using equations - prediction is then simply evaluation or solution of such equations. Hoitver, practically it faces problems where such a description would be too complicated or not possible at all. In addition, the solution by this method could be very complicated computationally, and sometimes it would get the solution after the event to be predicted happened.

It is possible to use various approximations, for example regression of the dependency of the predicted variable on other events that is then extrapolated to the future. Finding such approximation can be also difficult. This approach generally means creating the model of the predicted event.

Neural networks can be used for prediction with various levels of success. The advantage of then includes automatic learning of dependencies only from measured data without any need to add further information (such as type of dependency like with the regression). The neural network is trained from the historical data with the hope that it will discover hidden dependencies and that it will be able to use them for predicting into future. In other words, neural network is not represented by an explicitly given model. It is more a black box that is able to learn something.

It is possible to predict various types of data, hoitver in the rest of this text it will focus on predicting of time series Time series shows the development of a value in time. Of course, the value can be influenced by also other factors than just time. Time series represents discrete history of a value and from a continuous function it can be obtained using sampling.

It propose that Data mining techniques are applied to Engineering colleges and once students irater found at risk, they would be assigned to a tutor in order to provide them with both academic support and guidance for motivating and trying to prevent student failure. It has shown that classification algorithms can be used successfully in order to predict a student's academic performance and, in particular, to model the difference betiten Fail and Pass students.

ISSN 2394 - 7780

Enhanced k means algorithm

The aim of the proposed algorithm is to improve the computational efficiency of the K Means algorithm. The algorithm involves initial centroid selection, which is done randomly in existing Algorithm. Hence it proposes an algorithm which selects initial centroids based on the distances calculated from the origin. One of the most popular clustering algorithms is k-means clustering algorithm, but in this method the quality of the final clusters relies heavily on the initial centroids, which are selected randomly. Moreover, the k-means algorithm is computationally very expensive also. The proposed algorithm is found to be more accurate and efficient compared to the original k-means algorithm. This proposed method finding the better initial centroids and provides an efficient way of assigning the data points to the suitable clusters. This method ensures the total mechanism of clustering in O(nlogn) time without loss the correctness of clusters. This approach does not require any additional inputs like threshold values. The proposed algorithm produces the more accurate unique clustering results. The value of k, desired number of clusters is still required.

Steps

1: In the given data set D, if the data points contain the both positive and negative.

2: Find the minimum attribute value in the given data set D.

3: For each data point attribute, subtract with the minimum attribute value.

4: For each data point calculate the distance from origin.

5: Sort the distances obtained in step 4. Sort the data point's accordance with the distances.

6: Partition the sorted data points into k equal sets.

7: In each set, take the middle point as the initial centroid.

8: Compute the distance betiten each data point di (1 <= i<= n) to all the initial centroids cj (1 <= j <= k).

9: Repeat 10: For each data point di, find the closest centroid cj and assign di to cluster j.

11: Set Clustered[i]=j. // j:Id of the closest cluster.

12: Set Nearest_Dist[i]= d(di, cj).

13: For each cluster j (1 <= j <= k), recalculate the centroids.

14: For each data point di,

14.1 Compute its distance from the centroid of the present nearest cluster.

In the rest of this section the MKNN method is described in detail, ansitring the questions, how to compute the validity of the points and how to determine the final class label of test samples.

A. Validity of the Train Samples

In the MKNN algorithm, every sample in train set must be validated at the first step. The validity of each point is computed according to its neighbors. The validation process is performed for all train samples once. After assigning the validity of each train sample, it is used as more information about the points.

To validate a sample point in the train set, the H nearest neighbors of the point is considered. Among the H nearest neighbors of a train sample x, validity(x) counts the number of points with the same label to the label of x. The formula which is proposed to compute the validity of every point in train set is (1).

$$Validity(x) = \frac{1}{H}\sum_{i=1}^{H} S(lbl(x), lbl(N_i(x)))$$

Where H is the number of considered neighbors and lbl(x) returns the true class label of the sample x. also, Ni(x) stands for the ith nearest neighbor of the point x. The function S

Takes into account the similarity betiten the point x and the ith nearest neighbor. The (2), defines this function

$$S(a,b) = \begin{cases} 1 & a = b \\ 0 & a \neq b \end{cases}$$

ISSN 2394 - 7780

B. Applying Itighted KNN

KNN is one of the variations of KNN method which uses the K nearest neighbors, regardless of their classes, but then uses itighted votes from each sample rather than a simple majority or plurality voting rule. Each of the K samples is given a itighted vote that is usually equal to some decreasing function of its distance from the unknown sample.

For example, the vote might set be equal to 1/(de+1), where de is Euclidian distance. These itighted votes are then summed for each class, and the class with the largest total vote is chosen. This distance itighted KNN technique is very similar to the window technique for estimating density functions. For example, using a itighted of 1/(de+1) is equivalent to the window technique with a window function of 1/(de+1) if K is chosen equal to the total number of training samples [19].

In the MKNN method, first the itight of each neighbor is computed using the 1/(de+0.5). Then, the validity of that training sample is multiplied on its raw itight which is based on the Euclidian distance. In the MKNN method, the itight of each neighbor sample is derived according to,

$$W(i) = Validity(i) \times \frac{1}{d_e + 0.5}$$

Where W (i) and Validity (i) stand for the itight and the validity of the ith nearest sample in the train set. This technique has the effect of giving greater importance to the reference samples that have greater validity and closeness to the test sample. So, the decision is less affected by reference samples which are not very stable in the feature space in comparison with other samples. In other hand, the multiplication of the validity measure on distance based measure can overcome the it kness of any distance based itights which have many problems in the case of outliers. So, the proposed MKNN algorithm is significantly stronger than the traditional KNN method which is based just on distance.

ADVANTAGES

Data mining is a broad process that consists of several stages and includes many techniques.This knowledge discovery process comprises the steps of pre-processing, the application of DM Techniques and the evaluation and reading of the results. DM is aimed at working with very large amounts of data (millions and billions). The statistics does not usually work till in large databases with high dimensionality. Benefits of effective implementation of appropriate data classification can significantly improve ILM process and save data centre storage resources. If implemented systemically it can generate improvements in data centre performance and utilization. Data classification can also reduce costs and administration overhead. "Good enough" data classification can produce these results:

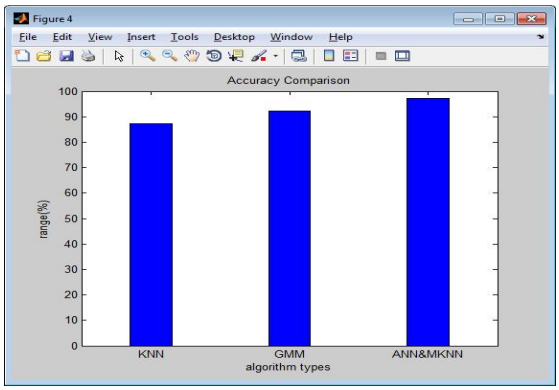
- Data compliance and easier risk management. Data are located where expected on predefined storage tier and "point in time"
- Simplification of data encryption because all data need not be encrypted. This saves valuable processor cycles and all related consecutiveness.
- Data indexing to improve user access times
- Data protection is redefined where RTO (Recovery Time Objective) is improved.

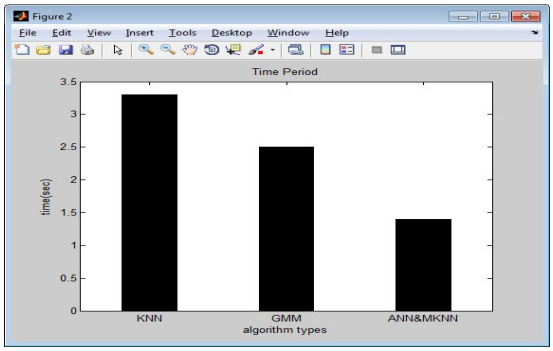
RESULT

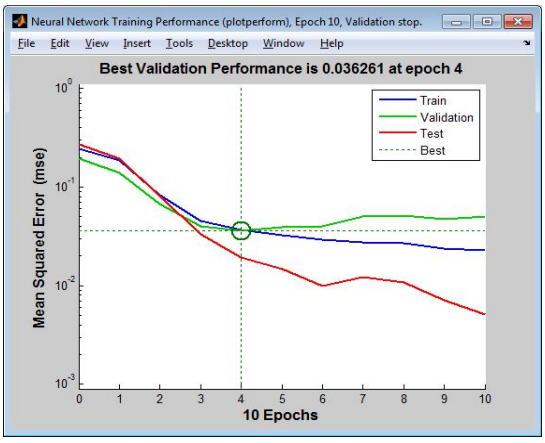
This mknn method is used the classified the resion of student prediction using neural network approach and modified knn algorithm is used and give high classification and less time period result for our data set here below show the result tables and plots .

S . N o	Algorithm	Accuracy	Time period
1	K N N	8 7 . 2	3 . 5 7
2	G M M	9 2 . 3	2 . 6 4
3	ANN&MKNN	9 7 . 2	1 . 8 5 3

ISSN 2394 - 7780







IV. CONCLUSION

By observing above results it can conclude that, the envisage student stoppage at college can be a complicated task not merely because it is a multifactor difficulty but also because the available data is usually imbalanced. It proposed effective technique in this paper for to predict educational performance of a student failure and dropout from the colleges based on attribute is nothing but real data of student that collected from college in middle or educational activity. A path from root to leaf is represents classification rules and it consists of 3 forms of nodes, which includes decision node, probability node and finish node. It can be used in verdict examination. Using this method, try to boost their correctness for computing the students may not pass or dropout by first; with all accessible characteristics next and then choosing best attributes. Attribute selection is done by Java programming language.

Hence the data processing tool mainly works in prediction and classification of knowledge. Matlab programming language supports much normal data processing task information pre-processing, clustering, classification and have choice of information is rebalanced victimization price responsive classification that is Naïve Bayes rule. Our proposed approach works efficiently when compared to other previously approached schemes. As its seen, predicting student failure in a class is a troublesome task, not solely as a result of it's a multifactor drawback (in that there is plenty of private, family, social, and economic factors which will be influential). To resolve these issues, it's shown the utilization of various DM algorithms and approaches for predicting student failure. It's applied totally different classification approaches for predicting the educational status or final student performance at the end of the course. Moreover it's shown that some approaches like choosing the most effective attributes, cost sensitive classification, and information equalization can even be very helpful for improving accuracy.

ISSN 2394 - 7780

BIBLIOGRAPHY

1. Tinto, V., "Research and practice of student retention: What next, College Student Retention: Research", Theory, and Practice, 8(1), pp. 1-20, 2006.
2. Tinto, V., "Leaving College: Rethinking the cause and cure of student attrition". Chicago: University of Chicago Press, 1993.
3. Tinto, V., "Dropout from Higher Education: A theatrical synthesis of recent research". Review of Education Research, 45, 89-125, 1975.
4. J. Han and M. Kamber, "Data Mining: Concepts and Techniques," Morgan Kaufmann, 2000.
5. Witten, I. H., Frank, E., Hall, M. A., "Data Mining: Practical Machine Learning Tools and Techniques", 3rd Ed. Morgan Kaufmann, 2011.
6. J. R. Quinlan, "Introduction of decision tree", Journal of Machine learning", pp. 81-106, 1986.
7. Yoav Freund and Llew Mason, "The Alternating Decision Tree Algorithm". Proceedings of the 16th International Conference on Machine Learning, pp. 124-133, 1999.
8. Bernhard Pfahringer, Geoffrey Holmes and Richard Kirkby. "Optimizing the Induction of Alternating Decision Trees".Proceedings of the Fifth Pacific-Asia Conference on Advances in Knowledge Discovery and Data Mining, pp. 477-487, 2001.
9. Kember, D., "Open Learning Courses for Adults: A model of student progress". Englewood Cliffs, NJ.: Educational Technology Publications, 1995.
10. Ashby, A., "Monitoring Student Retention in the Open University: Detritions, measurement, interpretation and action". Open Learning, 19(1), pp. 65-78, 2004.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

MESSAGE TRANSFER CARRIED OUT THROUGH DIGITAL WATERMARKING IN DEFENCE

Dr. N. Revathy[1], T. Guhan[2] and M. Sherlyn Sandhya[3]
Associate Professor[1], PG and Research Department of Computer Applications, Hindusthan College of Arts and Science, Coimbatore
Assistant Professor[2], Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore
Student[3], Department of Computer Science and Engineering, Coimbatore

ABSTRACT
Military communications or military signals involve all aspects of communications, or conveyance of information, by armed forces. Military communications span from pre-history to the present. The earliest military communications were delivered by humans on foot. Later, communications progressed to visual and audible signals, and then advanced into the electronic age. This project was held on using such software to use transfer the message and receive the message via network. So that it is so fast and speedy growing. Examples from Jane's Military Communications include text, audio, facsimile, tactical ground-based communications, terrestrial microwave, tropospheric scatter, naval, satellite communications systems and equipment, surveillance and signal analysis, encryption and security and direction-finding and jamming. We aim to become a indian in the military industry by completely focusing on army people, our employees, growth, innovation and efficiency. All of these elements will drive us towards success and show us as all indian army that can perform and give value for money.

Keywords: Terrestrial microwave; Tropospheric scatter; Satellite communications systems; Encryption; Security; Direction-finding; Jamming

I. INTRODUCTION

Military communications or military signals involve all aspects of communications, or conveyance of information, by armed forces. Military communications span from pre-history to the present. The earliest military communications were delivered by humans on foot. Later, communications progressed to visual and audible signals, and then advanced into the electronic age. Examples from Jane's Military Communications include text, audio, facsimile, tactical ground-based communications, terrestrial microwave, tropospheric scatter, naval, satellite communications systems and equipment, surveillance and signal analysis, encryption and security and direction-finding and jamming

We aim to become a pioneer in the vehicle rental industry by completely focusing on customers, our employees, growth, innovation and efficiency. All of these elements will drive us towards success and show us as all company that can perform and give value for money.

TextMark - Protect your texts with digital watermarks!
Objectives: Only method for inserting a digital watermark in texts (TextMark). The method for digital marking of information that's most difficult to remove: For removing an attacker would need to also model the complete language correctly in a computer.

Scanning, speech recognition, internet downloading, intelligent text processing systems: Text processing becomes increasingly simple, writing good texts remains difficult. With TextMark you protect your intellectual property. This innovation distinguishes itself by its broad applicability to all kinds of textual documents and its tamper proof characteristic.

The Internet is a two-edged sword: It offers authors the chance to publish their works worldwide, on the other hand, it brings about the risks of unauthorized publishing and copying. Nobody loses copyright when publishing works in the Internet. But most of the time, the right alone isn’t sufficient to protect intellectual property. Hence the need for technical tools that protect against web piracy.

The digital watermark for proving authorship
The principle of digital watermarking is known from bank notes. Insignificant characteristics suffice to prove originality and identify counterfeits. Today, the modern digital watermark is a widespread method that makes a published work unique so that it can be identified automatically. In this way author rights can be proved in case of unauthorized publication or copying. For images and music several known methods exist which imprint video- and audio-files with an unsuspicious mark. With the help of this mark authorship identification is simple and thus pirates can easily and inexpensively be caught and sentenced.

ISSN 2394 - 7780

The problem: How is watermarking possible in simple text?
A commonly known method changes the word distances slightly and operates with similar concepts as watermarking tools for images. Unfortunately, it is extremely simple to remove such a watermark in images and text completely. Currently existing pirate tools enable every school boy to remove such watermarks. The text, the image or the song by itself will still remain allowing the work to be copied and resold or published unauthorized on another web site. In such cases, chances of proving authorship are slim.

The solution: directly integrate the digital watermark into the text!
With TextMark it is possible to integrate a digital Watermark (e.g. the name of the author or the name of the publishing house) directly into a text! It will be encoded into the text by rephrasing it minimally (e.g. choice of synonyms, word order, positions of additional blanks for block justification etc.). The meaning of the text will be retained fully because the program is able to understand language. Sections that could not be completely understood remain unchanged. This second version can safely be published (as printed work, on CD-ROM, on the Internet) as it is protected by TextMark.

The watermark can be hidden as often as possible in the text. The upper boundary depends on the length of the text. In the standard version there will be a relationship of ca. 1:40 between encoded information and the text to protect (e.g. for every 40 letters of text one letter of watermark can be hidden).

Inconspicous and tamper resistant
By using linguistic rephrasing techniques, the changes remain inconspicuous and the work is practically tamper resistant. Hackers use existing weaknesses. But they have never gone to the extent of constructing synonym dictionaries and a grammar. Furthermore, a watermark can be encoded in absolutely files containing text - from Word documents to PDF files.

Not every text is of the same kind...
Of course it isn’t possible to use this method in the same way for any text. The more important a special mode of expression (i.e. "lyric quality of language") is for the value of the text (e.g. works of fiction and poetry), the more it can be lost by rephrasing it. For this reason , TextMark has a mode to obtain highest levels of relatedness to the original meaning or not to change arbitrary aspects at all. TextMark users can select one or several aspects among choosing only exact synonyms (e.g.: car --> automobile), inserting spaces in justified text or at the end of lines, or only by changing the position of words within a sentence. To still hide the same watermark with minimal changes, a significantly larger part of text will be needed in comparison to having all features activated.

No plaintiff, no judge!
Additionally, a search engine will be availed to search the internet automatically for copies of all texts with a TextMark mark and report all unauthorized publications to the author or publisher. In the standard case that the identity number or the e-mail address of the author or copyright holder is hidden within the text as a watermark, the search engine will automatically send an informative e-mail message to the person specified by the watermark. TextMark calculates the probability of a coincidental similarity of texts. This will also be mentioned within the e-mail to the pirate. He will presumably adjust his conduct quickly when he notices that his chances in court are minimal. In the occasional case of a lawsuit we will assist in providing the technical proof of authorship with its probability.

What happens if a net pirate wants to use TextMark for his own purposes?
All Compris Intelligence GmbH text rephrasing products - among them TextHide - can detect the digital watermarks and refuse to eliminate them! For identifying an improper use, the original is not required - therefore making the search more simple and cost-efficient.

The invisible seal with TextMark
TextMark can seal a text to assure that the content is not modified during transmission. This is achieved by hiding a checksum which TextMark will generate by using the text itself. Only the sender and the recipient will know of the existence of a seal. In combination with encryption, only the intended recipient will be able to test the seal.

Different problems demand different solutions
Each watermarking technology has to make small modifications to the original in a unique manner. You can still place your original into our search engine www.placens.com. Furthermore, you can sell and deliver your online publications over the internet against clearly defined usage restrictions, enforced by our displaying software. For each of these topics, individual data sheets are available.

ISSN 2394 - 7780

II. EXISTING SYSTEM

Defensive behavior is defined as that behavior which occurs when an individual perceives threat or anticipates threat in the group. The person who behaves defensively, even though he or she also gives some attention to the common task, devotes an appreciable portion of energy to defending himself or herself. Besides talking about the topic, he thinks about how he appears to others, how he may be seen more favorably, how he may win, dominate, impress or escape punishment, and/or how he may avoid or mitigate a perceived attack.

Such inner feelings and outward acts tend to create similarly defensive postures in others; and, if unchecked, the ensuing circular response becomes increasingly destructive. Defensive behavior, in short, engenders defensive listening, and this in turn produces postural, facial and verbal cues which raise the defense level of the original communicator Disadvantages of existing system:-

- The existing system is not on-line
- No direct information for the user in the System
- Tracking of goods are done manually
- Time wasting due to lack of proper planning
- Repetition of work: if there are any changes to be made, the data will have to be entered again.
- More manpower will be wasted
- Processing delays.

III. PROPOSED SYSTEM

Military communications or military signals involve all aspects of communications, or conveyance of information, by armed forces. Military communications span from pre-history to the present. The earliest military communications were delivered by humans on foot. Later, communications progressed to visual and audible signals, and then advanced into the electronic age. Examples from Jane's Military Communications include text, audio, facsimile, tactical ground-based communications, terrestrial microwave, tropospheric scatter, naval, satellite communications systems and equipment, surveillance and signal analysis, encryption and security and direction-finding and jamming

We aim to become a pioneer in the vehicle rental industry by completely focusing on customers, our employees, growth, innovation and efficiency. All of these elements will drive us towards success and show us as all company that can perform and give value for money.

The advantages of proposed system are:

- Data is centralized which has overcome the Sharing problem in previous system.
- As data is maintained electronically, it’s easy for a person to update the details, which has overcome the tedious updating in previous system.
- Maintenance is easy and performance is good

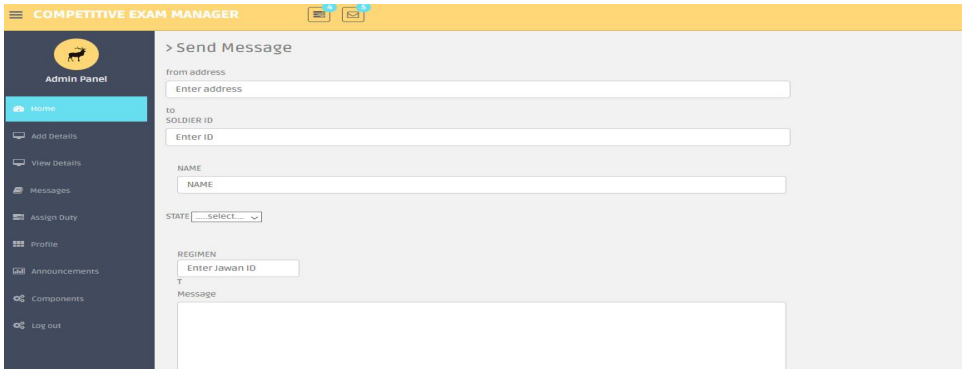
IV. INPUT & OUTPUT DESIGN

Main Home

ISSN 2394 - 7780

Inside Home

Send Message



V. CONCLUSION

With TextMark it is possible to integrate a digital Watermark (e.g. the name of the author or the name of the publishing house) directly into a text! It will be encoded into the text by rephrasing it minimally (e.g. choice of synonyms, word order, positions of additional blanks for block justification etc.). The meaning of the text will be retained fully because the program is able to understand language. Sections that could not be completely understood remain unchanged. This second version can safely be published (as printed work, on CD-ROM, on the Internet) as it is protected by TextMark.

The watermark can be hidden as often as possible in the text. The upper boundary depends on the length of the text. In the standard version there will be a relationship of ca. 1:40 between encoded information and the text to protect (e.g. for every 40 letters of text one letter of watermark can be hidden).

SCOPE FOR FUTURE ENHANCEMENT

To survive from the competition each system has to produce some modifications to it in the future. New features will provide the system a new fresh look, by which it can attract a lot of users. Due to this reason it's necessary that the system need to be modified.

The principle of digital watermarking is known from bank notes. Insignificant characteristics suffice to prove originality and identify counterfeits. Today, the modern digital watermark is a widespread method that makes a published work unique so that it can be identified automatically. In this way author rights can be proved in case of unauthorized publication or copying. For images and music several known methods exist which imprint video- and audio-files with an unsuspicious mark. With the help of this mark authorship identification is simple and thus pirates can easily and inexpensively be caught and sentenced.

A commonly known method changes the word distances slightly and operates with similar concepts as watermarking tools for images. Unfortunately, it is extremely simple to remove such a watermark in images and text completely. Currently existing pirate tools enable every school boy to remove such watermarks. The text, the image or the song by itself will still remain allowing the work to be copied and resold or published unauthorized on another web site. In such cases, chances of proving authorship are slim.

ISSN 2394 - 7780

REFERENCES

[1]. Everything You Want to Know About Watermarking: From Paper Marks to Hardware Protection. By Saraju P. Mohanty, Anirban Sengupta, Parthasarathy Guturu, and Elias Kougianos, Proceedings of the Springer, Vol. 52.

[2]. G. Voyatzis, Ioannis Pitas "The Use of Watermarks in the Protection of Digital Multimedia Products", Proceedings of the IEEE, Vol. 87, No. 7, July 1999, pp. 1197 – 1207.

[3]. C. H. Lu, Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, 1st Ed.: Idea Group Publishing, 2005

[4]. R. Chandramouli, Nasir Memon, Majid Rabbani "Digital Watermarking", Encyclopedia of Imaging Science and Technology, JAN 2002, DOI: 10.1002/0471443395.img010

[5]. Digital Image Watermark Key Extraction with Encryption and Decryption Scheme in MATLAB, Isha Garg, Anchit Bijalwan, International Journal of Computer Applications (0975 – 8887) Volume 105 – No. 10, November 2014. Pp. 07 – 11

[6]. An Upgraded Approach for Robust Video Watermarking Technique Using Stephens Algorithm Paramjit Kaur M.Tech, Dr. Vijay Laxmi CSE &Guru Kashi University, Talwandi Sabo, Bathinda, Punjab India, , International Journal of Computer Science and Mobile Computing, Vol.3 Issue.11, November- 2014, pg. 612-622

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

HYBRID ALGORITHM BASED ON WOA AND CSA FOR SOLVING DATA CLUSTERING

M. Amalmary[1] and Dr. A. Prakash[2]
Assistant Professor[1], Department of Computer Technology, Hindusthan College of Arts and Science, Coimbatore
Associate Professor[2], Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore

ABSTRACT
Data clustering is a well-known data mining approach that usually used to minimizes the intra distance but maximizes inter distance of each data center. The cluster problem has been proved to be an NP-hard problem. In this paper, a hybrid algorithm based on Whole optimization algorithm (WOA) and Crow search algorithm (CSA) is proposed, namely HWCA. The HWCA algorithm has the advantages of the search strategy of the WOA and CSA. In addition to, there are two operators used to improve the quality of solution, namely hybrid individual operator and enhance diversity operator. The hybrid individual operator is used to exchanges individuals from the WOA and CSA systems by using the roulette wheel approach. In other hand, the HWCA performs enhance diversity operator to improve the quality of each system. Moreover, the HWCA is incorporated with center optimization strategy to enhance diversity of each system. In the performance evaluation, the proposed MPGO algorithm was comparison WOA and CSA algorithm with six well-known UCI benchmarks. The results show that the proposed algorithm has a higher measure of accuracy rate with comparison algorithms.

Keywords: Data Clustering, Whole optimization algorithm, Crow search algorithm, Hybrid approach

I. INTRODUCTION
In real-word applications, data clustering is a popular analysis tool for bioinformatics, data mining, geographical information systems, image processing, and pattern recognition. Typically, data clustering is used to organize data into sensible clusters based on similarity criteria to find out each groupging exists minimizes the intra distance and maximizes inter distance. Each cluster comprises data that are similar to each other but dissimilar to the data from other clusters and the clustering problem has been proven to be an NP- hard problem [15].Recentl, metaheuristic partitional clustering models, such as the differential evolution [2], firefly algorithm [12], gravitation search algorithm [4] and particle swarm optimization [14] have attracted considerable attention from researchers. WOA is modeled after the intelligent behavior of whales. The WOA has an effective searching strategy for solving optimization problems and can perform better than well-known metaheuristic algorithm such as grivational searching algorithm (GSA) [11], and particle swarm optimization (PSO) [5]. In addition to, the CSA has an efficient search strategy for solving optimization problems and is better and faster than the GSA and PSO algorithm too. In this paper, a hybrid clustering algorithm based on WOA and the CSA is proposed, namely HWCA. The HWCA algorithm has the advantages of the search strategy of the WOA and CSA. In addition to, there are two operators used to improve the quality of solution, namely hybrid individual operator and enhance diversity operator. The hybrid individual operator is used to exchanges individuals from the WOA and CSA systems by using the roulette wheel approach. In other hand, the HWCA performs enhance diversity operator to improve the diversity of each sub-system. The performance of the proposed MPGO algorithm was compared with the performance of the WOA algorithm [8], and CSA [1] with six UCI benchmarks. The results indicated that better accuracy rate of proposed HWCA algorithm is obtained. The rest of this paper is organized as follows. The background knowledge is discussed in Section 2. The description of the proposed HWCA algorithm is presented in Section 3. In Section 4, the performance evaluation is provided. Finally, the conclusions and future works are stated in Section 5.

II. BACKGROUND KNOWLEDGE
A. Whale Optimization Algorithm
The Whale optimization algorithm (WOA) was first proposed by Mirjalili and Lewis [7]. It is a novel meta-heuristic algorithm inspired by the social behavior of humpback whales while chasing their prey. WOA implements searching strategies such as encircling prey, bubble-net attacking and search for prey. Given N agents in which the position is represented as potential positions, the solution agent i in iteration t can be defined as shown in Eq. (1).

$$x^t i = \{x^t i,1, x^t i,2, x^t i,j, \ldots, x^t i,d\} \text{ for } \quad i = 1, 2, 3 \ldots, N. \qquad (1)$$

where d is the number of dimensions of the searching space, and $x^t i$, j is the position of agent i in dimension j. Some notations of WOA are described as follows.

w^t: Best search agent in iteration t

ISSN 2394 - 7780

D : Distance between the current search agent i and the best agent

a : Decreasing value from 2 to 0

b : Shape of the logarithmic spiral

A : Random variable in interval [-a, a]

l : Random variable in interval [-1, 1]

r : Random variable in interval [-1, 0]

$x^t ra$: Random searching agent ra in iteration t

1) Encircling prey: The current best solution is the target prey; Other search agents update their positions to be closer

to the best search agent. This behaviour is modelled using the following Eq. (2):

$$x^{t}i^{+1} = w^{t} - (A \times D) \quad (2a)$$

$$A = 2a \times r - a \quad (2b)$$

$$C = 2 \times r \quad (2c)$$

$$D = C \times w^{t} - x^{t}i \quad (2d)$$

2) Bubble-net attacking:In order to model of the bubble net behaviour of whales, there are two approaches, The first approach involves the shrinking encircling mechanism, as shown in (2), The second approach is spirally updating position. The spiral-shaped path is represented by the following Eq. (3)

$$x^{t}i^{+1} = D \times e^{bl} \times \cos(2\pi l) + w^{t} \quad (3a)$$

$$D = wt - x^{t}i \quad (3b)$$

The WOA implements two behaviors (the shrinking encircling model or spiral model) to update the position of whales. There is approximately 50% to choose a model to update, as shown in the following Eq. (4)

$$x^{t}i^{+1} = {}^{w} \quad t - (A \times D) \quad \text{if } p < 0.5, \quad (4)$$

$$D \times e^{(}bl) \times \cos(2\pi l) + w^{t} \text{if } p \geq 0.5.$$

3) Search for prey: The whale searches randomly according to the position of other whales. Thus, in WOA, a random search agent is chosen from the current population, called $x^{t}ra$. Searching for prey can be modelled using the following Eq. (5)

$$D = C \times x^{t}rand - x^{t}i \quad (5a)$$

$$x^{t}i^{+1} = x^{t}rand - A \times D \quad (5b)$$

B. Crow Search Algorithm (CSA)

In the natural world, the crows are one of the most intelligent birds, their behaviour proves their high-level skill of cognitive ability, which is only slightly lower than that of humans. They have shown self-awareness in mirror tests and tool-making [10]. In fact, each crow owns its hiding space for storing their food, and taking precautions to protect food from potential followers that will steal their food. The CSA,

which was introduced by Askazadeh [1], is a novel swarm based intelligence algorithm was designed to solve mathmetics optimizations problems. The concepts used in the CSA are mentioned in the following statements:

1) Crows which live in flocks.

2) Crows can memorize the location of their hiding spaces.

3) Crows will follow one another to steal food.

4) Crows will protect their hiding spaces from attackers with a probability of interval [0,1]

In the CSA, individual aggregates are described as crows.There are two main parameters of crows called flight length fL and awareness probability AP, respectively. The value of fLis used for a local search (small value) or global search (large value), and the values of AP are used to control the intensity (small value) and diversity (large value) of crows. These crows is randomly generated with a position by the CSA. The following search

ISSN 2394 - 7780

equation can be used to compute the fitness values and update the position of each crow in the current population. Then, the position of crows i in iteration t, which indicates a potential solution for N crows, is defined as follows Eq. (6):

$X_i t = \{x^t i,1, x^t i,2, x^t i,j , \ldots , x^t i,d\}$ for i = 1, 2, 3 . . . , N. (6)

where $x^t i,j$ is the potential position solution of crow i in dimension j, and d denotes the dimensions of the searching space. Each crow updates its current solution in two cases: in the first case, assume crow c does not know that crow i is following it, and on the second case, assume crow c knows that crow i is following it. The detailed equations for the computation are shown in Eq. (7):

t

$x^t i,j^{+1} = x_i,j + randi \times fl \times (m^i c,j - x^i i,j)$ if randi ≥ AP,

random position if randi < AP. (7)

where $x^t i,j$ denotes the position of crow i in dimension j at iteration t, $m^t i,j$ denotes the position of the hiding place of crow i in dimension j at iteration t. Further, fL denotes the flight length of crow i at iteration t, AP denotes the awareness probability of crow c at iteration t, and randi is a random variable in interval [0, 1].

C. Center Optimization Strategy

The CPSO algorithm proposed by Liu et al. [6] erves as an improved PSO approach. The CPSO algorithm can be referred to as a population of N particles, with their positions representing potential solutions. After the positions of N – 1 particles have been updated, a central individual ci is added to the population as follows Eq. (8):

$x^t ci,j^{+1} = i=1 \quad x_{i,j} N - 1 \quad$ f or $\quad j= 1,2 \ldots , d.$ (8)

where $x^t ci,j^{+1}$ is the position of the center particle in dimension j in iteration t + 1.

III. PROPOSED ALGORITHM

A. Fitness Function

The Euclidean distance is the most general measure of the similarity between two patterns, and the distance between two patterns i, j is given by Eq. (9).

$x^t i,j^{+1} = x^t i,j$ if if $f(x^t i,j) < f(x^t i,j^{+1})$ (14)

$x^t i,j^{+1}$: otherwise

IV. EXPERIMENTAL RESULTS

All the simulation results were performed on a computer with a Xeon(R) E3-1225 3.30 GHz Intel CPU comprising 16GB main memory running on Windows 7, all programming are implemented by using Java language.

A. Parameter Setting

The basic parameter settings of each algorithms are listed in Table I. All experimental results were collected from 20 in- dependent runs, each of 1000 iterations. The benchmarks of is supported by UCI (http://archive.ics.uci.edu/ml/datasets.html). These comprise four benchmarks with pattern numbers ranging from 150 to 6435, as presented in Table II.

TABLE I

PARAMETER SETTINGS FOR THE PROPOSED ALGORITHM

Algorithm	Parameter	Value
WOA		
	Number of agents	20
	Value of Spiral b	0.306
CSA		
	Number of crows	20
	Flight Length F L	10
	Awareness probability AP	0.25
HWCA	Number of individual of each sub-system	20
	c1, c2	1.4

ISSN 2394 - 7780

B. Comparison Results

The performance of the HWCA algorithm was verified with WOA [8], and original CSA [1] by using six UCI datasets (Iris, Wine, Breast Cancer, Car evaluation).

The experiments results are shown in Table III, The ΔAccuracy values of the HWCA algorithm is better than WOA algorithm (from 0.2% to 18%, respectively), and CSA algorithm (from 0.5% to 8%, respectively).

C. Hybrid Individual Strategy

The hybrid operator is used at specific iterations. Certain individuals are selected and exchanged from two swarm-based systems (PSO and GSA) using the roulette wheel approach that developed by Goldberg [3] with probabilities that depend on their fitness values. The roulette wheel approach is represented by Eq. (13)

$$pni = N^{fit} ii = 1 \; f \; iti \qquad (13)$$

where pni represents the probability of each individual will be selected, and fiti is the fitness value of particle/agent i

D. Diversity Enhance Strategy

In this paper, the diversity enhancement operator is proposed, which is similar to the crossover operator of the DE algorithm [13]. In the process of recombination, the diversity enhancement operator arranges the original particle (agent)

$x^{t}i$ and new trial particle (agent) $x^{t,+1}i$ in each dimension as follows Eq. (14)

V. CONCLUSION

In this paper, the data clustering problems is be solved by using proposed HWCA. First, the HWCA algorithm simultaneously executes the WOA and CSA systems. Second, the HWCA algorithm uses CPSO to increase the quality of the solution. Third, the HWCA algorithm enhances the diversity of the WOA and CSA systems using the crossover operator.Finally, some individuals from the WOA and CSA systems are selected for exchange to improve the qualify of solution using the roulette wheel approach. The results indicated that the proposed HWCA algorithm could get better solution with six UCI datasets in measure of accuracy value. In our future study, we aim to investigate two aspects:(1) application of the HWCA algorithm in medical image clustering, (2) To decrease the computation time by using some pattern reduction approaches.

REFERENCES

1. A. Askarzadeh, “A novel metaheuristic method for solving constrained engineering optimization problems: Crow search algorithm,” Computers & Structures, vol. 169, pp.1–12, 2016.
2. S. Das, A. Abraham, and A. Konar, “Automatic clustering using an improved differential evolution algorithm,”Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, vol. 38, no. 1, pp. 218–237, Jan 2008.
3. D. E. Goldberg, Genetic Algorithms in Search, Optimization and Machine Learning, 1st ed. Boston, MA, USA:Addison-Wesley Longman Publishing Co., Inc., 1989.
4. K. W. Huang, J. L. Chen, C. S. Yang, and C. W. Tsai, “Amemetic gravitation search algorithm for solving clustering problems,” in 2015 IEEE Congress on Evolutionary Computation (CEC), May 2015, pp. 751–757.
5. J. Kennedy and R. Eberhart, “Particle swarm optimization,” in IEEE International Conference on Neural Networks, vol. 4, 1995, pp. 1942–1948.
6. Y. Liu, Z. Qin, Z. Shi, and J. Lu, “Center particle swarm optimization,” Neurocomputing, vol. 70, no. 46, pp. 672– 679, 2007.
7. S. Mirjalili and A. Lewis, “The whale optimization algorithm,” Advances in Engineering Software, vol. 95, pp. 51–67, 2016.
8. J. Nasiri and F. M. Khiyabani, “A whale optimization algorithm (woa) approach for clustering,” Cogent Mathematics & Statistics, p. 1483565, 2018.
9. M. OMRAN, A. P. ENGELBRECHT, and A. SALMAN, “Particle swarm optimization method for image clustering,”International Journal of Pattern Recognition and Artificial Intelligence, vol. 19, no. 03, pp. 297–321, 2005.
10. H. Prior, A. Schwarz, and O. Gntrkn, “Mirror-induced behaviour in the magpie (pica pica): Evidence of selfrecognition,” PLOS Biology, vol. 6, no. 8, pp. 1–9, 2008.

ISSN 2394 - 7780

11. E. Rashedi, H. Nezamabadi-pour, and S. Saryazdi, "Gsa: A gravitational search algorithm," Information Sciences, vol. 179, no. 13, pp. 2232 – 2248, 2009.
12. J. Senthilnath, S. Omkar, and V. Mani, "Clustering using firefly algorithm: Performance study,"Swarm and Evolutionary Computation, vol. 1, no. 3, pp. 164–171, 2011.
13. R. Storn and K. Price, "Differential evolution - a simple and efficient heuristic for global optimization over continuous spaces," Journal of Global Optimization, vol. 11,no. 4, pp. 341–359, 1997.
14. D. W. van der Merwe and A. P. Engelbrecht, "Data clustering using particle swarm optimization," in IEEE Congress on Evolutionary Computation, vol. 1, Dec2003, pp. 215–220.
15. R. Xu and D. Wunsch, II, "Survey of clustering algorithms," IEEE Transactions on Neural Networks, vol. 16,no. 3, pp. 645–678, 2005.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

A BAT OPTIMIZATION BASED QoS ROUTING FOR WIRELESS SENSOR NETWORKs (WSNs)

N. Senthil Kumar[1] and Dr. N. Revathy[2]
Professor[1], S. N. M. V College of Arts and Science
Associate Professor[2], Hindusthan College of Arts and Science

ABSTRACT
With the increasing demand for real time applications in the Wireless Senor Network (WSN), real time critical events anticipate an efficient Quality-of-Service (QoS) based routing for data delivery from the network infrastructure. Designing such QoS based routing protocol to meet the reliability and delay guarantee of critical events while preserving the energy efficiency is a challenging task. Considerable research has been focused on developing robust energy efficient QoS based routing protocols. Existing routing algorithms are not effective in supporting the dynamic characteristics of WSNs and cannot ensure sufficient quality of service in WSN applications. This research work proposes a novel agent-assisted QoS-based routing algorithm for wireless sensor networks. Optimization approaches have also been used as agents to carry out QoS related tasks such as routing, in WSNs. In order to improve the performance of the optimization algorithm, Bat optimization Algorithm (BA) is used in this research to solve the QoS based routing of WSNs is a Non-deterministic Polynomial (NP) hard and finite problem. Bat algorithm is a metaheuristic algorithm for global optimization. It was inspired by the echolocation behaviour of microbats, with varying pulse rates of emission and loudness. In the proposed algorithm, the QoS of WSNs is chosen as the adaptive value of effective optimization to improve the overall performance of network. Intelligent software agents are used to monitor changes in network topology, network communication flow, and each node's routing state. These agents can then participate in network routing and network maintenance.

Index terms: Wireless Sensor Networks (WSNs), QoS, Routing, Bat Algorithm (BA), Non-deterministic Polynomial (NP), and protocol

1. INTRODUCTION
Wireless Sensor Networks (WSNs) have become one of the developing research field, as they are envisioned to have wide applications with different phenomenon related to environmental tracking, response, security monitoring in manned or unmanned missions [1]. Recent advances in wireless technology with networking capabilities have generated a lot of interest to design routing protocols for WSNs with Quality of Service (QoS) based real-time applications [2].

In WSN, the routing protocol ensures that the data reaches the sink possibly across multi-hops. The best routing protocol should have the following characteristics namely routing without loops, minimal routing overheads, automatic load balancing, recovery from link failures, congestion avoidance mechanism, energy efficiency as well as QoS.

The QoS routing requires not only to find a route from a source to a destination, but a route that satisfies the end-to-end QoS requirement, often given in terms of bandwidth, delay or loss probability [3]. Transmission of video and imaging data requires both energy and QoS aware routing in order to ensure efficient usage of the sensors and effective access to the gathered measurements [4]. The advantage of QoS routing protocol becomes apparent when traffic gets heavy. A major criticism of such QoS routing protocol is that it is designed without considering the situation when multiple QoS routes are being setup simultaneously.

Bat optimization Algorithm (BA) is used in this research to solve the QoS based routing of WSNs is a Non-deterministic Polynomial (NP) hard and finite problem. Bat algorithm is a metaheuristic algorithm for global optimization. It was inspired by the echolocation behaviour of microbats, with varying pulse rates of emission and loudness. In the proposed algorithm, the QoS of WSNs is chosen as the adaptive value of effective optimization to improve the overall performance of network.

2. LITERATURE REVIEW
Jeon et al. [5] proposed an energy-efficient routing protocol that tries to manage both delay and energy concerns. Based on AntNet protocol, this algorithm uses the concept of ant pheromone to produce two prioritized queues, which are used to send differentiated traffic. However, such approach can be infeasible in current sensor nodes due to the memory required to save both queues. This can be even more problematic if the sensor network is very populated, since the routing table on each device depends on the number of neighbors.

ISSN 2394 - 7780

Zhang et al. [6], study three distinct Ant-based algorithms for WSN. However, the authors only focus on the building of an initial pheromone distribution, good at system start-up. Saleem et al [7] have surveyed some existing SI algorithms proposed for wireless sensor networks, discussed the general principles of SI and its application to routing, and introduced a novel taxonomy for routing protocols in wireless sensor networks and use it to classify the surveyed protocols.

Zhang et al. [10] developed three ant-based routing algorithms for WSNs—sensor-driven and cost-aware ant routing (SC), flooded for-ward ant routing (FF), and flooded piggybacked ant routing (FP). These algorithms, with initial pheromone settings, have a good system start-up, but the SC and FF algorithms are not quite effective in latency. Besides, the FP algorithm, while providing high success rates of data delivery, consumes much higher energy.

Cobo[11] presented an ant-based routing for Wireless Multimedia Sensor Networks (WMSN) using multiple QoS metrics; this approach built a hierarchical structure on the network before choosing suitable paths to meet various QoS requirements from different kinds of traffic, thus it could maximized network utilization.

Liang et al. [32] proposed a cluster-based algorithm, which used PSO to optimize clustering process under the condition of location and energy reserved about candidates and their neighbors. This algorithm may settle the existing algorithms' problems of dying early due to ignoring the state of neighbors in the process of cluster-heads decision.

3. PROPOSED METHODOLOGY

Novel agent-assisted QoS-based routing algorithm is proposed for wireless sensor networks. Optimization approaches have also been used as agents to carry out QoS related tasks such as routing, in WSNs. In order to improve the performance of the optimization algorithm, Bat optimization Algorithm (BA) is used in this research to solve the QoS based routing of WSNs is a Non-deterministic Polynomial (NP) hard and finite problem. Bat algorithm is a metaheuristic algorithm for global optimization. It was inspired by the echolocation behaviour of microbats, with varying pulse rates of emission and loudness. In the proposed algorithm, the QoS of WSNs is chosen as the adaptive value of effective optimization to improve the overall performance of network. Intelligent software agents are used to monitor changes in network topology, network communication flow, and each node's routing state.

3.1 Reverse agent

The task of the reverse agent is to return to the source node v_s along the path of the forward agent, and to implement the corresponding routing algorithm. When a forward agent arrives at the destination node v_d, the node v_d will initialize the forward agent into a reverse agent through changing some signs, and the reverse agent inherits the travel records of the forward agent. Considering the reverse agent needs to follow its predecessor (the forward agent) to return to the source node; the reverse agent will no longer transmit message in flooding mode. In order to quickly adjust the routing table information along the travel path, the reverse agent is given a higher priority, and the adjustment to the routing table by the reverse agent is decided by the different routing algorithms. The synthetic QoS is taken into consideration for this research work. An Agent model for QoS routing is used for this research work which uses forward and reverse agent.

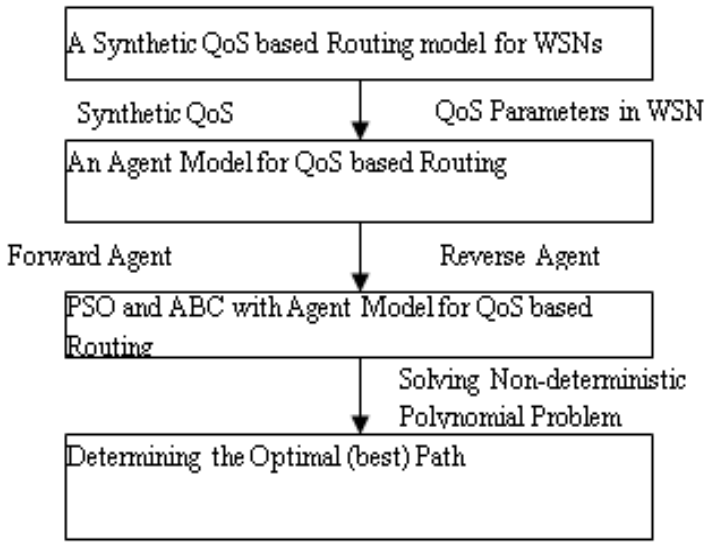


Figure-1: Dataflow diagram of the Overall Methodology

ISSN 2394 - 7780

3.2 A Synthetic QoS based Routing model for WSNs

In WSNs, a QoS based routing protocol needs to perform the following features: (1) Path determining—to determine the optimal routing path meeting the demand of the QoS from the numerous paths. (2) Resource reliability—to use network resource even without the ability of pre-reserving network resources. Usually, we can design some resource reservation mechanisms in high-level protocol to control the QoS, such as Resource Reservation Protocol (RSVP), etc. (3) Path keeping—to prevent the sudden dropping of the QoS routing performance.

3.3 Quality of service (QoS) parameters in WSNs

Different network applications will have their own QoS demands. Therefore, only one QoS parameter is not enough to optimize routing path in a wireless sensor network, and a synthetic QoS (multi-parameters) is necessary. The purpose of the synthetic QoS based routing is to get the optimal path, departing from the source node, ending in destination node, and meeting all the QoS constraints, such as delay, jitter, bandwidth, etc

Delay: also called latency, it is the transmission delay between the two reference points. In the cable network, delay is mainly caused by congestion. While in the wireless sensor networks some other events may trigger data packet delay, including cohort delay, propagation delay, data flow competition, queue delay, etc.

Bandwidth: bandwidth is one of the most important metrics of QoS routing protocol; it is specifically the available bandwidth of path from the source node to the destination node. However, the bandwidth will change with the movement of nodes. Many routing protocols are trying to search the largest bandwidth, but the least delay path should be chosen when several paths are synchronously available.

Jitter: also called alterable delay; it is the time it is the time difference between packets in a group of data flows sent by the same routing. Usually, the application impacted by delay will also be impacted by jitter.

Packet Delivery Ratio and Loss: namely the highest rate of packet loss in the network. Packet loss is usually caused by the network congestion and the node's mobility in wireless sensor networks.

Power Control and Conservation: in most cases, the sensor network nodes are powered by capacity-limited batteries, which restrict the lifetime of the nodes. When the energy of a node gets exhausted, the topology of network must be changed and the routing needs to be re-established.

In this work, mainly consider the synthetic effect of QoS parameters, including delay, bandwidth and packet loss. The WSNs can be expressed as a weighted directed graph $G(V, E)$, where V is a set of sensor nodes with a wireless connection. If there are $n+1$ nodes V, $V = \{v_0, v_1, v_2, v_3, \ldots, v_n\}$ the communication radius of each node is r_i its communication area is A_{vi} and the edge $e = (v_i, v_j) \in E$ denotes the two-way wireless connection between two nodes (v_i, v_j). The path $P(v_1, v_n)$ in G is an orderly compositing sequence of edges:

$$P(v_1, v_n) = ((v_1, v_2), (v_2, v_3) \ldots (v_{i-1}, v_i) \ldots (v_{n-1}, v_n)), V_i \in V, 2 \le n \le |V| \quad (1)$$

$P(v_1, v_n)$ is a is a multi-hop path, the number of edges in $P(v_1, v_n)$ represents the hop distance between node v_1 and node v_n Each node in the path can be regarded as an independent router. The first node of the path is the source node, and the final node is the destination node, respectively called as v_s and v_d. Each node has its adjacent nodes. Each edge $e = (v_i, v_j) \in E$ denotes that v_i and v_j are the mutual adjacent nodes. $N_{vi} = \{v_j | e = (v_i, v_j) \in E, i \neq j$ is a set of adjacent nodes of v_i; it is found by the discovery mechanism of the adjacent nodes, which is also called HELLO information exchange. After exchanging HELLO message, the node adds its QoS parameters to HELLO information. Given a path $P(v_s, v_d)$ its synthetic QoS metrics can be defined by the delay, bandwidth, and packet loss, and can be reflected on the node v and the link e. for every node $v \in V$ the metrics are delay function—$Delay(v)$, band width function—$Bandwidth(v)$, packet loss function—$Packet\ loss(v)$, and energy function—$Energy(v)$. Accordingly, in the network, every link $e = (v_i, v_j) \in E$ has its corresponding QoS metrics. After defining the QoS metrics of the node and the link, the QoS metrics of the path $P(v_s, v_d)$ can be calculated. Given the source node $v_s \in V$ and the destination node $v_d \in V$, the corresponding QoS metrics of path $P(v_s, v_d)$ are computed as the following:

$$Delay(p(v_s, v_d)) = \sum_{v \in P(v_s, v_d)} Delay(v) + \sum_{e \in P(v_s, v_d)} Delay(e) \quad (2)$$

$$Bandwidth(p(v_s, v_d)) = \min_{e \in P(v_s, v_d)} \{Bandwidth(e)\} \quad (3)$$

$$Packet_{loss(p(v_s, v_d))} = 1 - \prod_{e \in P(v_s, v_d)} (1 - packet_{loss(e)}) \quad (4)$$

ISSN 2394 - 7780

If the path$P\ (v_s, v_d)$is a path satisfying all the QoS metrics, it must meet the following requirements:

$$Delay\left(p(v_s, v_d)\right) = \sum_{v \in P\,(v_s v_d)} Delay\,(v) + \sum_{e \in P\,(v_s v_d)} Delay(e) < D \quad (5)$$

$$Bandwidth\left(p(v_s, v_d)\right) = \min_{e \in P\,(v_s v_d)} \{Bandwidth(e)\} > B \quad (6)$$

$$Packet_{loss(p\,(v_s v_d))} = 1 - \prod_{e \in P\,(v_s v_d)} \left(1 - packet_{loss\,(e)}\right) < PL \quad (7)$$

where D, B, and PL are the QoS guarantees of the WSN network. After defining every QoS function of the routing model, we can establish the synthetic QoS model for every path. In the synthetic QoS model, in which every QoS indicator must satisfy the QoS constrain, any inconformity will greatly cut down the metrics' contribution and bring the negative and punitive influence to the synthetic QoS. For example, if$Delay\left(p(v_s, v_d)\right) < D$,the delay of the path may satisfy the constraint conditions, then

$$f_{delay} = 1 - \frac{(1-k)Delay\,(p(v_s v_d))}{D} \rightarrow (8)$$

Take k close to1,suchas0.9,thenthevalueoff_{delay} will be between 0.9 and 1.

If $Delay\left(p(v_s, v_d)\right) > D$, it denotes that the delay indicator of path cannot satisfy the constraint demands for delay application, then

$$f_{delay} = (1 - k) - \frac{Delay\,(p(v_s v_d))}{D} \rightarrow (9)$$

Algorithm, these agents can then participate in network routing and network maintenance. Thus, algorithm performance can be obviously improved in delay, packet loss, and the synthetic QoS, respectively, with little energy consumption.

An agent model for QoS based routing: In QoS based routing, the synthetic QoS metrics are added into the data structure of agent. Therefore, the data structure of the agent consists of the agent ID and its type, the source node ID, the destination node ID, the current node ID, the hop distance of agent, the start time and reach time, etc., and also includes the mobile records of the agent. In the structure of the mobile records, the QoS metrics are defined, such as delay, bandwidth, packet loss, energy, etc. In the QoS based routing algorithm, the forward agent and the reverse agent are adopted to establish the routing strategy of WSN nodes. Routing tables are updated as the forward agent sends a packet from the source node to the destination node. Once it reaches its destination, each forward agent tells the traveling time information and other QoS parameter to the reverse agent, which updates the routing tables as it traces the path of the forward agent in reverse.

Routing Table: Routing table is a table stored in router, and plays the role of path discovery in node routing . In QoS based routing, the synthetic QoS metrics are added into the data structure of agent. Therefore, the data structure of the agent consists of the agent ID and its type, the source node ID, the destination node ID, the current node ID, the hop distance of agent, the start time and reach time, etc., and also includes the mobile records of the agent. In the structure of the mobile records, the QoS metrics are defined, such as delay, bandwidth, packet loss, energy, etc. In the QoS based routing algorithm, the forward agent and the reverse agent are adopted to establish the routing strategy of WSN nodes. Routing tables are updated as the forward agent sends a packet from the source node to the destination node. Once it reaches its destination, each forward agent tells the traveling time information and other QoS parameter to the reverse agent, which updates the routing tables as it traces the path of the forward agent in reverse.

Forward agent: If node s hopes to establish routing with other nodes, the node s creates a forward agent in the creation time of the forward agent message and writes into its own address, and then continuously sends the forward agent to each adjacent node in flooding mode. When node v_k receives a forward agent, it implements the following tasks. At the outset, the forward agent checks whether there exist some visited nodes in its travel records. If exists, it shows that circulation appears in agent travel, and deletes it from the stacks. If the travel information of the forward agent is stored by a stack, the delete operation can be done by simple stack pop-up operation. Then, the forward agent adds a new data item into the mobile records, which point to a dynamically increasing list. Data item includes the identification and relative information of the node v_k according to the algorithm requirements.

Next, if the node$v_k$is not the destination node, the value of the routing counter in the forward agent adds 1. Every source node address and its serial number contained in the forward agent are only certain, and every

ISSN 2394 - 7780

intermediate node will record the source node address and the maximum serial number. If the serial number received by the current node is not bigger than the maximum serial number from the same source node, the forward agent will be discarded. Since the forward agent and the data message have the same priority and follow the First-In First-Out (FIFO), the forward agent will experience the same delay and congestion as the data message, by which the QoS based routing can be built.

If broadcasting the forward agent, all of the adjacent nodes of the node $v_k$will receive the message from the forward agent. Finally, the forward agent will arrive at the destination node. The forward agent may be deleted when the value of the routing hop counter is beyond the setting value. By the flooding communication, the intermediate nodes can copy and broadcast the forward agent. Thus, the destination node may indirectly receive more than one forward agent from the source node $v_s$which forms the different routing paths between the source nodes $v_s$and the destination nodev_d.

BAT ALGORITHM (BA): Bat algorithm is a new population based metaheuristic algorithm exploits the so-called echolocation of the bats. Echolocation is typical sonar which bats use to detect prey and to avoid obstacles. It is generally known that sound pulses are transformed into a frequency which reflects from obstacles. The bats navigate by using the time delay from emission to reflection. The pulse rate can be simply determined in the range from 0 to 1, where 0 means that there is no emission and 1 means that the bat's emitting is at their maximum. In order to transform these behaviors of bats to algorithm, Yang used three generalized rules:

- All bats use echolocation to sense distance, and they also 'know' the surroundings in some magical way;
- Bats fly randomly with velocity v_i at position x_i with a fixed frequency f_{min}, varying wavelength λ and loudnessA0 to search for prey. They can automatically adjust the wavelength of their emitted pulses and adjust the rate of pulse emission r from [0,1], depending on the proximity of their target;
- Although the loudness can vary in many ways, it is assumed that the loudness varies from a positive large value A_0 to a minimum constant value A_{min}.

In BA algorithm, initialization of the bat population is performed randomly and each bat is defined by its locations x_i^t, velocity v_i^t,, frequency fit loudness A_i^t, and the emission pulse rate r_i^t in a D-dimensional search space. The new solutions x_i^t are performed by moving virtual bats according to the following equations

$$f_i = f_{min} + (f_{max} - f_{min})\beta \quad (10)$$

$$v_i^t = v_i^{t-1} + (x_i^t - x_*)f_i \quad (11)$$

$$x_i^t = x_i^{t-1} + v_i^t \quad (12)$$

where β from the closed interval [0,1] is a random vector drawn generated by a uniform distribution. Here x* is the current global best location (solution) which is located after comparing all the solutions among all the bats. Initially, each bat is randomly assigned a frequency which is drawn uniformly from the interval [f_{min}, f_{max}].

The local search is launched with the proximity depending on the rate $r_i$of pulse emission for the i^{th} bat. As the loudness usually decreases once a bat has found its pray, while the rate of pulse emission increases, the loudness can be chosen as any value of convenience. Mathematically, these characteristics are captured with the following equations:

$$A_i^{t+1} = \alpha A_i^t \quad (13)$$

$$r_i^{t+1} = r_i^0(1 - e^{-\gamma t}) \quad (14)$$

where α and γ are constants. Adopting the routing-choose method to select the next node of the forward agent, the routing table of the node $v_k$will determine the next node, to which the forward agent will go. The source node Sproduces a forward agent, and establishes the initial travel record in node$S$. Through the routing table of the node$S$, it transfers the forward agent to node $A$and then adds the travel record in. In the same way, the forward agent can arrive at the node $B$and finally arrive at the destination node$D$ .The travel record only lists the node identification.

4. SIMULATION RESULTS

This section mainly focuses on providing an efficient QoS based routing through Agent assisted system. This paper is simulated using Network Simulator (NS2). The system is installed with Red hat Linux version. Then

ISSN 2394 - 7780

the TCL files for existing Particle Swarm Optimization (PSO) algorithm and the proposed algorithms are imported and evaluated. The performance of the proposed BA approach is compared with the PSO approach based on the parameters such as throughput and Power delay. The corresponding graphs are obtained and the performance is evaluated with following table.

Table-1: NS2 Simulation Parameter

Simulation Parameter	Value
Number of nodes	50
Area size	500 x 500 m
Mac	802.11
Traffic Source	CBR
Transmit Power	0.02w
Receiving Power	0.01w
Active Power	240w
Inactive Power	2.4w
Transmission Range	50m
Initial Energy	1J
Packet Size	512 bytes
Antenna	Omni Antenna
Radio propagation	Two ray Ground
Interface Queue	Drop tail
Queue Length	50
Channel Type	Channel/Wireless channel

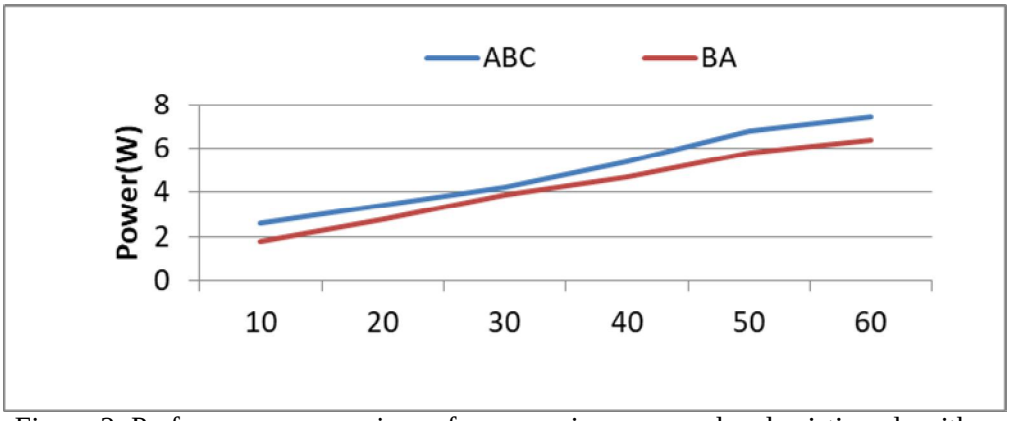


Figure-2: Performance comparison of power using proposed and existing algorithm

From the figure .2.it is noted that the proposed BAT algorithm consumes less power when compared with the existing Artificial Bee Colony (ABC) technique. It is clearly observed that, at the initial stage of the iteration, the difference between two algorithms is very less but when the number of iterations increases, the proposed BAT algorithm consumes lesser power when compared with the existing Artificial Bee Colony (ABC) algorithm.

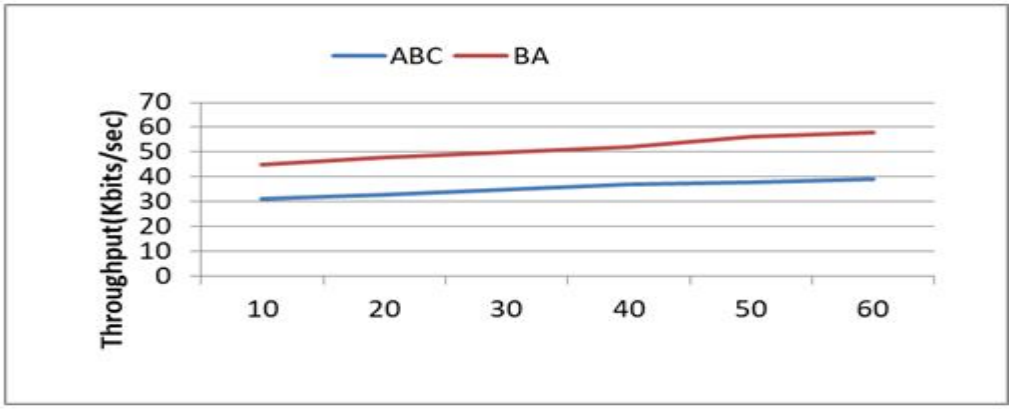


Figure-3: performance comparison of throughput using proposed and existing algorithm

ISSN 2394 - 7780

The figure .3.shows the throughput comparison of the proposed BAT approach and the existing ABC approach. It is noted that the proposed BAT algorithm attains higher throughput when compared with the existing ABC technique. It is clearly observed that, the proposed BAT algorithm attains higher throughput when compared with the existing ABC algorithm at all the stages of iterations.

5. CONCLUSION AND FUTURE WORK

This work mainly focuses on the effective optimization algorithm to improve the overall performance of the network. QoS- BA algorithm for the synthetic QoS routing model has been presented to increase the QoS level of WSN. In the proposed research work, Bat optimization Algorithm (BA) has been introduced to solve the QoS based routing of WSNs and to increase the overall performance of the system. Intelligent software agents are used to monitor changes in network topology, network communication flow, and each node's routing state. The problem proposal has been studied thoroughly. Finally, compared with the existing approach, the QoS-ABC algorithm obviously shows its improvement in the quality of service of WSN including delay, packet loss and the synthetic QoS. The future enhancements of the present research work are to improve the overall performance of the system. Advanced and Hybrid Optimization algorithms can be used as the agents in the future enhancement. Other QoS parameters can be taken for consideration in this present research work.

REFERENCES

1. K. Akkaya and M. Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", Elsevier Ad Hoc Network Journal, Vol. 3, No. 3, pp. 325-349, 2005.
2. P. Toldan and A. Ahamd Kumar, "Design Issues and various Routing Protocols for Wireless Sensor Networks", In: Proc. of National Conf. On New Horizons in IT, ISBN: 978-93-82338- 79-6, pp. 65-67, 2013.
3. L. J. G. Villalba, L.S. Orozco Ana, A. T. Cabrera and C. J. B. Abbas, "Routing Protocols in Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, pp. 919- 931, 2007.
4. Hakim Badis, Ignacy Gaw˛edzki and Khaldoun Al Agha, "QoS Routing in Ad Hoc Networks Using QOLSR With no Need of Explicit Reservation" IEEE 60th conference on Vehicular Technology Conference, 2004, Page(s): 2654 – 2658, 2004.
5. M. K. Jeya Kumar, "Evaluation of Energy-Aware QoS Routing Protocol for Ad Hoc Wireless Sensor Networks", International Journal of Electrical and Electronics Engineering, vol. 4, 2010.
6. Bonabeau E, Dorigo M, Theraulaz. G. Swarm intelligence: from natural to artificial systems. New York, USA: Oxford University Press; 1999.
7. Jeon, P., Rao, R., Kesidis, G., Two-Priority Routing in Sensor MANETs Using Both Energy and Delay Metrics in preparation, 2004
8. Zhang, Y., Kuhn, L., Fromherz, Improvements on Ant Routing for Sensor Networks".In: Ants 2004, Int. Workshop on Ant Colony Optimization and Swarm Intelligence, Sept.2004
9. Saleem M, Caro GAD, Farooq. M. Swarm intelligence based routing protocol for wireless sensor networks: survey and future directions. Information Sciences 2010. doi:10.1016/j.ins.2010.07.005.
10. Zhang Y, Kuhn L, Fromherz M. Improvements on Ant Routing for Sensor Networks. In: Ants 2004, workshop on Ant Colony Optimization and Swarm Intelligence. p. 154–65.
11. Cobo L, Quintero A, Pierre. S. Ant-based routing for wireless multimedia sensor networks using multiple QoS metrics. Computer networks 2010;54(17): 2991–3010.
12. Liang Y, Yu HB, Zeng P. Optimization of cluster-based routing protocols in wireless sensor network using PSO. Control and Decision 2006;21:453–6. [in Chinese].

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

THE SECURE DISTRIBUTED CLOUD STORAGE

P. Deepika[2], S. Saranya[2] and Richard Benjamin M[3]
Assistant Professor[1] and Student[2], PG and Research Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore
Assistant Professor[3], Department of Computer Applications, Hindusthan College of Arts and Science, Coimbatore

ABSTRACT
The main objective of this paper is to minimize the energy cost for Internet Data Centres in deregulated electricity markets. Load balancing is one of the effective methodology which distribute workload across several computers, or other resources over the network links to achieve optimal resource utilization, minimum data processing time, minimum average response time, and avoid overload. In this paper we will use approximately three different servers, which are partitioned into small clouds called balancers, each balancer will have some servers called sub servers. Cloud Service Provider (CSP) is used to handle a Main cloud (which is made up of small Clouds) called Main Server. Client interacts with cloud using a web application called client Site.First a job arrives at the system. The main server decides which cloud partition should receive the job. The way in which a job has to be assigned to the nodes is decided by the balancer. When client uploads file it will be stored in the server. The cloud will take care that it will be loaded into the server which has minimum load.

I. INTRODUCTION
Distributed Cloud is the application of Cloud Computing Technologies to inter connect data and applications served from multiple geographic locations. Distributed means that something is shared among multiple systems which may also be in different locations. Distributed clouds speeds the communications for global services and enable more responsive communications for specific regions. Distributed Storage is an attempt to offer the advantages of centralized storage with the scalability and cost base of local storage. A distributed object store is made up of many individual object stores, normally consisting of one or a small number of physical device.

II. LITERATURE REVIEW
Efficient Anchor Point Selection Based Data Gathering In Cluster Wireless Sensor Networks
The sensor nodes near to the fixed sink node suffer from the quickly tired energy. For this, many Existing methods have been researched to distribute the energy consumption into all wireless sensor nodes using a rechargeable mobile sink. Since the mobile sink changes its location in the network continuously, it has limited time to communicate with the sensor nodes and needs the time to move to each sensor node. Therefore, before the mobile sink approaches the sensor node, the node can collect huge data by event occurrence. It causes the memory overflow of the sensor node and then the data loss. The proposed solution works by cluster the network based on LEACH protocol such that the depth of each partition is bounded by k no of cluster Head. Then, in each cluster head, the minimum number of required caching anchor point's selection algorithm is identified. The proposed experimental results show that our proposed scheme minimizes the data loss and has similar network lifetime over the existing scheme based on a mobile sink.

III. METHODOLOGY
LEACH Protocol Cluster Head Selection.

Constructing Maximum-Lifetime Data Gathering Forests In Sensor Networks
Energy efficiency is critical for wireless sensor networks. The data gathering process must be carefully designed to conserve energy and extend network lifetime. For applications where each sensor continuously monitors the environment and periodically reports to a base station, a tree-based topology is often used to collect data from sensor nodes. In this work, we first study the construction of a data gathering tree when there is a single base station in the network. The objective is to maximize the network lifetime, which is defined as the time until the first node depletes its energy. The problem is shown to be NP complete. We design an algorithm which starts from an arbitrary tree and iteratively reduces the load on bottleneck nodes (nodes likely to soon deplete their energy due to high degree or low remaining energy). We then extend our work to the case when there are multiple base stations, and study the construction of a maximum lifetime data gathering forest. We show that both the tree and forest construction algorithms terminate in polynomial time and are provably near optimal. We then verify the efficacy of our algorithms via numerical comparisons.

METHODOLOGY
Tree Based Construction

ISSN 2394 - 7780

An Energy-Efficient Clustering Algorithm For Multi Hop Data Gathering In Wireless Sensor Networks
Wireless sensor networks afford a new opportunity to observe and interact with physical phenomena at an unprecedented fidelity. To fully realize this vision, these networks have to be self-organizing, self healing, economical and energy-efficient simultaneously. Since the communication task is a significant power consumer, there are various attempts to introduce energy awareness within the communication stack. Node clustering, to reduce direct transmission to the base station, is one such attempt to control energy dissipation for sensor data gathering. In this work, we propose an efficient dynamic clustering algorithm to achieve a network-wide energy reduction in a multi hop context. We also present a realistic Energy dissipation model based on the results from stochastic geometry to accurately quantify energy consumption employing the proposed clustering algorithm for various sensor node densities, network areas and transceiver properties.

METHODOLOGY
Time Controlling Clustering Algorithm
An Application-Specific Protocol Architecture For Wireless Microsensor Networks
Networking together hundreds or thousands of cheap micro sensor nodes allows users to accurately monitor a remote environment by intelligently combining the data from the individual nodes. These networks require robust wireless communication protocols that are energy efficient and provide low latency. In this paper, we develop and analyze low-energy adaptive clustering hierarchy (LEACH), a protocol architecture for micro sensor networks that combines the ideas of energy-efficient cluster-based routing and media access together with application-specific data aggregation to achieve good performance in terms of system lifetime, latency, and application-perceived quality. LEACH includes a new, distributed cluster formation technique that enables self-organization of large numbers of nodes, algorithms for adapting clusters and rotating cluster head positions to evenly distribute the energy load among all the nodes, and techniques to enable distributed signal processing to save communication resources. Our results show that LEACH can improve system lifetime by an order of magnitude Compared with general-purpose multi hop approaches.

METHODOLOGY
Leach Protocol Architecture
Mobile Sink Based Data Gathering And Forwarding
IN WSN
Environment monitoring is performed using the sensor devices. Wireless Sensor Network (WSN) is constructed with a set of data collection units. Base station, sinks and sensor devices are used in the WSN. Power resources, bandwidth and storages are the limitations of the sensor devices. Sink nodes are used to collect data from a group of sensor devices. Many to one traffic pattern based data collection model increases the transmission load to a set of nodes. The traffic pattern based network load problem is referred as hotspot problem. Energy efficient communication protocols and multi-sink systems are used to handle hotspot problems. Static and mobility based sink placement schemes are used to handle data collection process. Mobile sinks are used to increase the network lifetime with delay constraints. Random mobility and controlled mobility models are used in the mobile sinks. In random mobility the sinks are moved randomly within the network. The sinks are deterministically moved across the network is referred as controlled mobility. The network lifetime is managed with the number of nodes and delay values. The Delay bounded Sink Mobility problem is initiated under sensor node allocation to sinks. A polynomial-time optimal algorithm is used for the origin problem. Extended Sink Scheduling Data Routing algorithm is used to schedule sink nodes. The mobile sink scheduling scheme is enhanced to support large size networks. Distributed scheduling algorithm is applied to schedule nodes with high scalability. The scheduling scheme is tuned for multiple sink based environment. Delay and energy parameters are integrated in the sink scheduling process. The decentralized scheduling mechanism achieves high data collection efficiency with low latency values. Region based sink movement is used to manage data collection risk levels.

METHODOLOGY
Distributed Scheduling Algorithm

PROPOSED METHODOLOGY
In this method we proposed 6 modules
1. Authentication module
2. IP Address Representation
3. Sub server
4. Load balancer

ISSN 2394 - 7780

5. Security
6. Response time

Authentication Module
The authentication module is to register the new users and previously registered users can enter into our paper. The admin only can enter and do the uploading files into the servers. After login by every user and the admin the sql server checks the login id and password is valid or not. If the login is not valid it displays that the login is not correct.

IP Address Representation Module
The IP Address Representation module is to give the IP addresses which we are going to assign those as servers. We can enter and view IP addresses from this module. In load balancing system we can connect the three servers [system]. The connection has to be represented by the IP Address representation only.

SUB SERVER
The main server divided in to three sub servers. IP addresses are assigning to those sub servers. We can enter IP address, from the load balancing system we can connect the three sub servers [system]. The connection has to be represented by the IP Address representation only. Manager upload files in the system, those files are also in three sub servers.

LOAD BALANCER
In this load balancing get benefits of distributing the workload includes increased resource utilization ratio which further leads to enhancing the overall performance thereby achieving maximum client satisfaction. The Authentication users can enter into the upload page and can view the file name which the manager stored into the servers. The user can select the file from the list and can download from the server which is in idle state. We will get the response time and from which server we are getting the file. Finally we can get the decrypted file through using key pairs.

SECURITY
For Authentication, Admin store the files in encrypted format using RSA algorithm. User can view the files after decryption only. Only Admin allow, user can view the encrypted files.

RESPONSE TIME
Response time is the total time it takes from when a user makes a request until they receive a response. Here, user can calculate the response time for the whole system .Latency+ processing time=response time. In our paper amount of time takes for downloading files from system.

IV.CONCLUSION
Our proposal strives to balance the loads of nodes and reduce the demanded movement cost as much as possible, while taking advantage of physical network locality and node heterogeneity. In the absence of representative real workloads (the distributions of file chunks in a large scale storage system) in the public domain, we have investigated the performance of our proposal and compared it against competing algorithms through synthesized Probabilistic distributions of file chunks.

V.FUTURE ENHANCEMENT
In future we have got increase latency and effectiveness of our style additional valid by analytical models and a true implementation with a small-scale cluster setting.

REFERENCES
1. B. Krishnamachari, Networking Wireless Sensors. Cambridge, U.K.: Cambridge Univ. Press, Dec. 2005.
2. R. Shorey, A. Ananda, M. C. Chan, and W. T. Ooi, Mobile, Wireless, Sensor Networks. Piscataway, NJ, USA: IEEE Press, Mar. 2006.
3. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “A survey on sensor networks,” IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114, Aug. 2002.
4. W. C. Cheng, C. Chou, L. Golubchik, S. Khuller, and Y. C. Wan, “A coordinated data collection approach: Design, evaluation, and comparison,” IEEE J. Sel. Areas Commun., vol. 22, no. 10, pp. 2004– 2018, Dec. 2004.
5. K. Xu, H. Hassanein, G. Takahara, and Q. Wang, “Relay node deployment strategies in heterogeneous wireless sensor networks,” IEEE Trans. Mobile Comput., vol. 9, no. 2, pp. 145–159, Feb. 2010.

ISSN 2394 - 7780

6. O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis, "Collection tree protocol," in Proc. 7th ACM Conf. Embedded Netw. Sensor Syst., 2009, pp. 1–14.
7. E. Lee, S. Park, F. Yu, and S.-H. Kim, "Data gathering mechanism with local sink in geographic routing for wireless sensor networks," IEEE Trans. Consum.Electron., vol. 56, no. 3, pp. 1433– 1441, Aug. 2010.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

SECURE AUDITING AND DEDUPLICATING DATA IN CLOUD

Anithaa Dheve S[1] and Geethamani G. S[2]
Student[1] and Associate Professor[2], Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore

ABSTRACT
As the cloud computing technology develops during the last decade, outsourcing data to cloud service for storage becomes an attractive trend, which benefits in sparing efforts on heavy data maintenance and management. Nevertheless, since the outsourced cloud storage is not fully trustworthy, it raises security concerns on how to realize data deduplication in cloud while achieving integrity auditing. In this work, the problem of integrity auditing and secure deduplication on cloud data is studied. Specifically, aiming at achieving both data integrity and deduplication in cloud, propose two secure systems, namely SecCloud and SecCloud. SecCloud introduces an auditing entity with a maintenance of a MapReduce cloud, which helps clients generate data tags before uploading as well as audit the integrity of data having been stored in cloud. Compared with previous work, the computation by user in SecCloud is greatly reduced during the file uploading and auditing phases. SecCloud+ is designed motivated by the fact that customers always want to encrypt their data before uploading, and enables integrity auditing and secure deduplication on encrypted data.

Keywords: servers, protocal, cloud computing, encryption, maintainance engineering.

I. INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

A. PROBLEM STATEMENT

The main objectives of the proposed system is to reduce the hacking of data, reduce data deduplication and to make the system more secure for data storage, more accurate and fast processing. In this section the developer develops a model for not accepting the duplicate files in the cloud. It also developed by encrypting and decrypting the file by using the private key.

Finally, if the user uploads the file which is already present in the cloud, the file will not be able to upload, the auditor will sent a acknowledgement that the file is already exist in the cloud.The cloud will not accept the duplicate file. It approve the files and check the graph status like duplicate, non duplicate files, mapped files ratio in cloud storage.

B. EXISTING SYSTEM

Even though cloud storage system has been widely adopted, it fails to accommodate some important emerging needs such as the abilities of auditing integrity of cloud files by cloud clients and detecting duplicated files by cloud servers.The first problem is integrity auditing. The cloud server is able to relieve clients from the heavy burden of storage management and maintenance.The second problem is secure deduplication. The rapid adoption of cloud services is accompanied by increasing volumes of data stored at remote cloud servers.

C. DISADVANTAGES OF EXISTING SYSTEM

- The first problem is generalized as how can the client efficiently perform periodical integrity verifications even without the local copy of data files.
- The second problem is generalized as how can the cloud servers efficiently confirm that the client (with a certain degree assurance) owns the uploaded file (or block) before creating a link to this file (or block) for the user.

D. PROPOSED SYSTEM

The advantage is the idea of convergent encryption to make the deterministic and “content identified” encryption, in which each “content” (file or sector) is encrypted using the session key derived from itself. In this way, different “contents” would result in different cipher texts, and deduplication works.

Convergent encryption suffers from dictionary attack, which allows the adversary to recover the whole content with a number of guesses. To prevent such attack, as with, a “seed” (i.e., convergent key seed) is used for

ISSN 2394 - 7780

controlling and generating all the convergent keys to avoid the fact that adversary could guess or derive the convergent key just from the content itself.It generate convergent keys on sector-level (i.e., generate convergent keys for each sector in file F), to enable integrity auditing. Specifically, since convergent encryption is deterministic, it allows to compute homomorphic signatures on (convergent) encrypted data as with on plain data, and thus the sector-level integrity auditing is preserved.

II. DESIGNING GOALS

A. USER

In this module the User has to Login. Upload the required files in the cloud like drop box. Whatever file is uploaded the file has been encrypted in background and store in to cloud storage. Download the encrypted file and it can be decrypted easily with the secret key.

B. AUDITOR

Auditor verifies all the files already uploaded in cloud storage. Approve the files and check the graph status like duplicate, non duplicate files, mapp ed files ratio in cloud storage.

C. ENCRYPTION/DECRYPTION ALGORITHM

Blowfish is a symmetric block cipher algorithm for encryption/decryption. Blowfish is accepted as a fast and strong encryption algorithm because it has not been cracked. Blowfish is fixed 64 bit block cipher and a takes key length from 32-448bits. Total 16 processing rounds of data encryption is performed in Blowfish. This algorithm is divided into two parts- (i) Key expansion and (ii) Data encryption. In key expansion process 448 bits key is converted into 4168 bytes. The advantages of blowfish algorithm are that it is secure and easy to implement and best for hardware implementation, but the disadvantage is it require more space for the ciphertext because of difference between key size and block size.

III. SYSTEM TESTING

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

A. White Box Testing

White Box Testing is a testing in which in which the software tester has knowledge of the inner workings, structure and language of the software, or at least its purpose. It is purpose. It is used to test areas that cannot be reached from a black box level.

ISSN 2394 - 7780

B. Black Box Testing
Black Box Testing is testing the software without any knowledge of the inner workings, structure or language of the module being tested. Black box tests, as most other kinds of tests, must be written from a definitive source document, such as specification or requirements document, such as specification or requirements document. It is a testing in which the software under test is treated, as a black box .you cannot "see" into it. The test provides inputs and responds to outputs without considering how the software works.

C. Unit Testing
Unit testing is usually conducted as part of a combined code and unit test phase of the software lifecycle, although it is not uncommon for coding and unit testing to be conducted as two distinct phases.

Test strategy and approach
Field testing will be performed manually and functional tests will be written in detail.

Test objectives
- All field entries must work properly.
- Pages must be activated from the identified link.
- The entry screen, messages and responses must not be delayed.

Features to be tested
- Verify that the entries are of the correct format
- No duplicate entries should be allowed
- All links should take the user to the correct page.

INTEGRATION TESTING
Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

Acceptance Testing
User Acceptance Testing is a critical phase of any paper and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

Test Results: All the test cases mentioned above passed successfully. No defects encountered.

IV. SYSTEM IMPLEMENTATION
Implementation is the stage of the paper when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods. The implementation concern about two steps,

- Conversion
- Post implementation review

Initially as a first step the executable form of the application is to be created and loaded in the common server machine which is accessible to all the user and the server is to be connected to a network. The final stage is to document the entire system which provides components and the operating procedures of the system.

V. SYSTEM MAINTENANCE
Maintenance is actually implementation of the review plan as important as it is programmers and analyst is to perform or identify with user with the maintenance. There are psychologically personality and professional reasons for this. Analyst and programmers spend fair more time maintaining programmer then they do writing them Maintenance account for 50-80% of total system development. Maintenance is expensive .One way to reduce the maintenance costs are through maintenance mgt and software modification audits Types of maintenance are

ISSN 2394 - 7780

1. Perfective maintenance
2. Preventive maintenance
3. Adaptive maintenance

A. Perfective maintenance
Changes made to the system to add features or to improve the performance.

B. Preventive maintenance
Changes made to the system to avoid future problems. Any changes can be made in the future and our paper can adopt the changes.

C. Adaptive maintenance
Changes made to system for making the software to run on a new version.

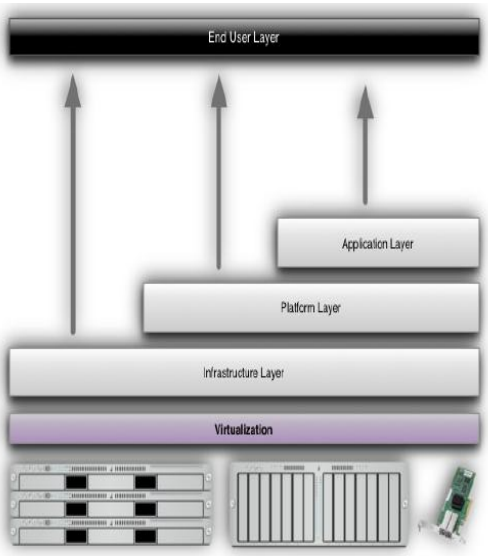


Fig-4: Structure Of Service Models

VI. CONCLUSION
Aiming at achieving both data integrity and deduplication in cloud, we propose SecCloud and SecCloud+. SecCloud introduces an auditing entity with maintenance of a MapReduce cloud, which helps clients generate data tags before uploading as well as audit the integrity of data having been stored in cloud. In addition, SecCoud enables secure deduplication through introducing a Proof of Ownership protocol and preventing the leakage of side channel information in data deduplication. Compared with previous work, the computation by user in SecCloud is greatly reduced during the file uploading and auditing phases. SecCloud+ is an advanced construction motivated by the fact that customers always want to encrypt their data before uploading, and allows for integrity auditing and secure deduplication directly on encrypted data.

VII. FUTURE ENHANCEMENT
Furthermore, Compared with previous work, the computation by user in SecCloud is greatly reduced during the file uploading and auditing phases. SecCloud+ is an advanced construction motivated by the fact that customers always want to encrypt their data before uploading, and allows for integrity auditing and secure deduplication directly on encrypted data.

REFFERENCE
1. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A view of cloud computing,” Communication of the ACM, vol. 53, no. 4, pp. 50–58, 2010.
2. J. Yuan and S. Yu, “Secure and constant cost public cloud storage auditing with deduplication,” in IEEE Conference on Communications and Network Security (CNS), 2013, pp. 145–153.
3. S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, “Proofs of ownership in remote storage systems,” in Proceedings of the 18th ACM Conference on Computer and Communications Security. ACM, 2011, pp. 491–500.

ISSN 2394 - 7780

4. S. Keelveedhi, M. Bellare, and T. Ristenpart, "Dupless: Serveraided encryption for deduplicated storage," in Proceedings of the 22Nd USENIX Conference on Security, ser. SEC'13. Washington, D.C.: USENIX Association, 2013, pp. 179–194. [Online]. Available: https://www.usenix.org/conference/usenixsecurity13/ technicalsessions/ presentation/bellare
5. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 598– 609.
6. G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, "Remote data checking using provable data possession," ACM Trans. Inf. Syst. Secur., vol. 14, no. 1, pp. 12:1–12:34, 2011.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

OPTIMIZATION OF ENERGY CONSUMPTION USING LOAD SHARING IN CLUSTERED NETWORKS

G. Priyanka
Department of Computer Technology, Hindusthan College of Arts and Science

ABSTRACT
In Adhoc networks, Clustering concept provides a tree structure in which certain nodes are assigned the additional tasks such as routing of the networks. Ordinary nodes doesn't involve in routing but they rely on the cluster heads for Packet delivery. The formation overhead may happen if a suitable tap is not applied to number of nodes that joins as cluster head. The efficiency of the network may get affected due to overhead. This paper proposes a cluster formation algorithm which defines the cluster division in case of members of cluster heads exceeds the threshold value. This frees the cluster heads from the burden. The results of Proposed algorithm reveals the improvement in performance in terms of E2E delay, PDF and Throughput.

Keywords: Mobile Adhoc Network, Cluster head, Mobility, Energy.

1. INTRODUCTION
A mobile spontaneous network could be aredistributedstyle of network shaped by assortment of autonomous mobile nodes connected by wireless links.Constraints likerestrictedinformation measure, energy inadequacy, mobility, non-deterministic topology and physically insecure settingmakes routing a difficultspace of analysis. During amassivespontaneous network, clustercould be aresolution to limit the number of routing data that propagates within the network. During a cluster formation, one node works as a clusterhead and coordinates all the activities like routing. The choice of the clusterheads could be acrucial issue, since the performance of the network depends informed the qualityof these nodes as cluster heads. This analysis work is administered to develop a framework for load sharing in mobile spontaneous networks. The choice of clusterhead is performed by considering variety of performance parameters associated with load-balancing, energy consumption and stability of the nodes. The load equalisation is achieved by incorporating a threshold worth on the amount of nodes that maybe part of a clusterhead as its members. If a clusterhead becomes fullbecause of migration of nodes in its section than cluster cacophonic is performed to makea brand new cluster. Energy consumption throughout the communication among a cluster is additionally taken into account at the time of clusterhead choice. Finally, a simulation of the papered work is performed on NS2. Comparisons and analysis are created between the papered approach and therefore the weighted clusteralgorithmic rule to demonstrate the effectiveness of the theme. The rest of the paper is organized as follows: Sect. twooffersa quick note on the state of the art of the analysis efforts within thespace of cluster approaches. The papered model is in brief introduced in Sect. 3. Sect. fouranalyses the results of the papered model and final conclusions are given in Sect. 5.

II. LITERATUREREVIEW
A number of cluster approaches arebestowed time to time by known authors. In Lowest ID cluster algorithmic rule (LIC) [1] a node with the minimum id is chosen as a cluster head. Thus, the ids of the neighbours of the cluster headare going to beon top of that of the clusterhead. Every node is allotteda definite id. Sporadically, the node broadcasts the list of nodes that it will hear. A node thatsolely hears nodes with id on top of itself could be a clusterhead. Otherwise, a node is a normal node. Downside of lowest ID algorithmic rule is that sure nodes are at risk of power emptying [2] because of serving as clusterheads for extended periods of your time. In Highest propertyclusteralgorithmic rule (HCC) [1] the degree of a node is computed by its distance from others. Every node broadcasts its id to the nodes that are among its transmission vary. The node with mostrange of neighbors (i.e., most degree) is chosen as a clusterhead. This methodfeatures a low rate of clusterhead modification. Typically, every cluster is allotted some resources thatis shared among the members of that cluster. Because therange of nodes during a cluster is inflated, the output drops. K-CONID [3] combines 2cluster algorithms: the Lowest-ID and therefore the Highest-degree heuristics. so asto pick outclusterheadspropertyis taken into account as a primary criterion and lower ID as a secondary criterion.

In HCC clustertheme, one cluster head is exhausted once it serves too many mobile hosts. It's not fascinatingand therefore the CH becomes a bottleneck. Thereforea brand new approach [4] is given during which a CH's salutation message shows its dominated nodes' range exceeds a threshold (the mostbest CH will manage), no new node can participate during this cluster. Adjustive multihop cluster [5] sets higher and lower bounds (U and L) on the amount of clustermembers among a cluster that a clusterhead will handle. Oncethe amount of clustermembers during a cluster is a smaller amount than the edge, the cluster must merge with one amongst the neighboring clusters. On the contrary, if the amount of clustermembers during aclustering is larger than the edge, the cluster is split into 2 clusters.Mobility based d-hop clustering algorithm partitions network into d-hop

ISSN 2394 - 7780

clusters based onquality metric. The target of forming d-hop clusters is to form the cluster diameter additionallyversatile. Native stability is computed so asto pick some nodes as clusterheads. A node could become a clusterhead if it's found to be the foremost stable node among its neighbourhood. Thus, the clusterhead are the node with rock bottomprice of native stability among its neighbours. In qualitybased mostlyMetric for agglomeration [7] a timer is employedto cut back the clusterhead amendment rate by avoiding re-clustering for incidental contacts of 2 passing clusterheads. Mobility-based Frame Work for accommodativeagglomeration [8] partitionsvariety of mobile nodes into multi-hop clusters supported (a, t) criteria. The (a, t) criteria indicate that each mobile node in a cluster encompasses a path to eachalternative node that may be out there over a whileamount 't' with a likelihood 'a',no matter the hop distance between them. Most of protocols executes the agglomeration procedure sporadically, and re-cluster the nodes from time to time so as to satisfy some specific characteristic of clusterheads.

In LCC [9] the agglomerationalgorithmic ruleis split into 2 steps: cluster formation and cluster maintenance. The cluster formation merely follows LIC, i.e. at first mobile nodes with rock bottom ID in their neighbourhood's are chosen as clusterheads. Re-clustering is event-driven and invoked if 2 clusterheads get into the reach varyof everyalternative and once a mobile node cannot access any clusterhead. Accommodativeagglomeration for mobile wireless network [10] ensures tiny communication overhead for building clusters as a result ofevery mobile node broadcasts just one message for the cluster construction. 3-hop between adjacent clusterheads (3-hBAC) [11] algorithmic rule introduce a replacement node standing, "clusterguest", which suggests this node isn'tinside the transmission range of clustermembers. Once a mobile node finds out that it cannot function a clusterhead or be part of a cluster as a clustermember, however some neighborcould be a clustermember of some cluster, it joins the corresponding cluster as a clusterguest.

Aagglomeration protocol that doesn't use dedicated management packets or signals for clustering specific call is Passive agglomeration [12]. During thistheme, oncea possible clusterhead with "initial" state has one thing to send, like a flood search, it declares itself as a clusterhead by piggybacking its state within the packet. Load levellingagglomeration (LBC) [13] offera close-by balance of load on the elective clusterheads. Once a node is elected asa clusterhead it'sfascinating for it to remain as a clusterhead up to some mostsuchquantityof your time, or budget. Initially, mobile nodes with the very best IDs in their nativespace win the clusterhead role. LBC limits the most time units that a node willfunction a clusterhead endlessly, thereforeonce a clusterhead exhausts its lengthbudget, it resets its VID to zero and becomes a non-clusterhead node.

Power-aware connected dominant set [14] is associate energy-efficient agglomerationthemethat decreases the dimensions of a dominating set (DS) . The inessential mobile nodes are excluded from the dominating set saving their energy consumed for serving as clusterheads. Mobile nodes within a DS consume additional battery energy than those outside a DS as a result of mobile nodes inside the DS bear further tasks, together with routing dataupdate and information packet relay. Hence, it's necessary to reduce the energy consumption of a DS. agglomeration for energy conservation [15] assumes 2 node types: master and slave. The aim of this theme is to reduce the transmission energy consumption summed by all master-slave pairs and to functionseveral slaves as attainableso asto work the network with longer time period and higher performance.

Weighted agglomerationalgorithmic rule (WCA) [16] selects a clusterhead in keeping withthe amount of nodes it will handle, mobility, transmission power and battery power. To avoid communications overhead, this algorithmic ruleisn't periodic and therefore the clusterhead election procedure is simply invoked supported node quality and oncethe present dominant set is incapable to hide all the nodes. The clusterhead election algorithmic rule finishes once all the nodes become either a clusterhead or a member of a clusterhead. The gap between members of a clusterhead, should be less or adequate to the transmission vary between them. No 2clusterheadswill be immediate neighbors. In WCA high quality of nodes results in high frequency of affiliationthat increase the network overhead. Higher affiliation frequency results inadditional recalculations of the cluster assignment leading to increase in communication overhead.

Entropy based agglomeration [17] overcomes the downside of WCA and forms anadditional stable network. It uses associate entropy-based model for evaluating the route stability in unintentional networks and electing clusterhead. Entropy presents uncertainty and could be alive of the disorder in every system. Thereforeit'sa stronger indicator of the steadiness and quality of the unintentional network. The agglomeration approach bestowed in WBACA [18] relies on the provision of position data via a world Positioning System (GPS). The WBACA considers following parameters of a node for clusterhead selection: transmission power, transmission rate, mobility, battery power and degree. In property, energy &quality driven weighted agglomerationalgorithmic rule (CEMCA) [19] the election of the cluster head relies on the mixture of

ISSN 2394 - 7780

manyimportant metrics such as: rock bottom node mobility, the very best node degree, the very best battery energy and therefore the best transmission vary.

III. PROPOSED METHODOLOGY

CLUSTERING FRAMEWORK

Clustering naturally facilitates energy economical technique wherever nodes forwards data to a cluster head for process. The Choice of clusterhead is one amongthe keyproblems in style of mobile unintentional networks. The choice of clusterhead is performed once considering variety of performance parameters together with degree distinction, distance with neighbors, quality of nodes and remaining battery power. Figure 1 shows the clustering framework

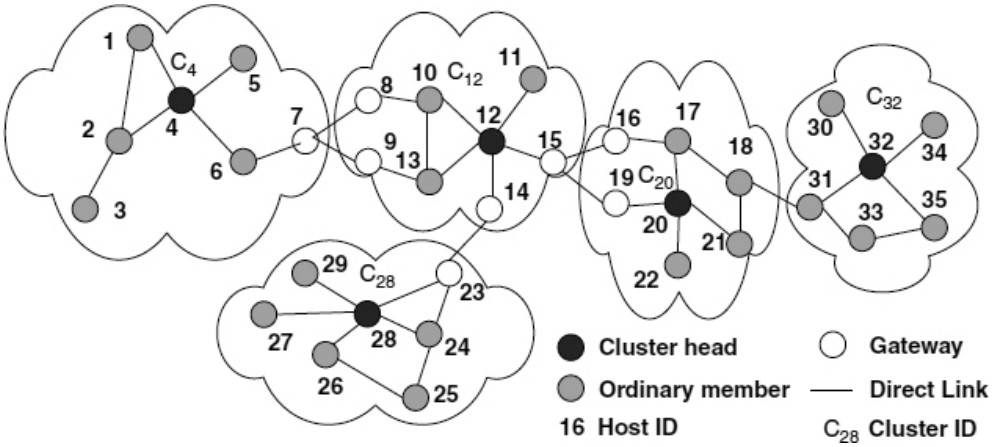


Figure-1: Clustering Framework

Degree distinction

In cluster-based structure, a performance parameter for load levellingwill be introduced as degree distinction (Δv), for every node v that is outlinedbecause thedistinction of ideal node degree (δ) and actual degree (connectivity) of that node. Degree of node (dv) is that thevariety of neighbors of node v that are within the transmission vary. Ideal degree is that thevariety of neighbors that a clusterhead will handle effectively.

Energy Consumption

Clusterhead has got to perform further task for routing and forwarding the packets, there fore it's additionally liable to energy drain. Additional power is required for human action long distant neighbours. In mobile unintended network nodes communicate with one another through the wireless channel. neighbors. Sum of distance to all or anyneighbors (Sdv) is found

Mobility

Mobility or stability is a very importantfactor for deciding the clusterheads. To avoid frequent clusterhead changes, it'sfascinating to elect a clusterhead that doesn't move terribly quickly. Once the clusterhead moves quick, the nodes is also detached from the clusterhead and as a result, anaffiliationhappens. An affiliationwill increase Energy consumption.

Power

A clusterhead consumes a lot of battery than a standard node as a result ofit'sadditional responsibilities. We are able to estimate the remaining battery power by the numberof your time spent by the node as a clusterhead. The parameter Pvis that theaccumulative time of a node being a clusterhead. Pvis employedto notifywhat proportionof battery power has been consumed by the node. Higher the worth of Pv, lower the remaining battery power.Advisement factors are chosen in such way that totalof those factors should be adequate to one. Each node calculates its weight and broadcasts it sporadicallyin an exceedinglygreeting packet to all or any nodes in its transmission. Once a node receives the weights of its 1-hop neighbors, it inserts them within theattainable CH set, which has all potential cluster-heads

Cluster formation with load sharing

At the system initiation every node assumed to be holding a standing “undecided”. Periodic broadcast of greeting message allows a node to collecthelpfuldataregarding its neighbourhood. Primarily based upon the data obtained from the greeting messages every node computes the combined weight worth. This data is changed by neighbours and nodes store this neighbourhood information as well as combined weight in neighbor tables. If a node determines that it'sall-time lowworth of combined weight among its neighbors, it changes its standing as “CH” and sends “join_cluster” messages to its neighbors. Every neighbouring node receiving this be a part of

ISSN 2394 - 7780

request, check its own status and if it's still “undecided” , it respond with “accept_join” and become a member of that clusterhead and alter its standing as “member”. This method runs in parallel and continuingtill all the nodes of the network either become clusterheads or members.

Algorithm 1: Cluster formation algorithmic rule

1. Calculate the combined weight stateof every node v
2. Broadcast weight stateto all or any immediate neighbors
3. Record the information received from immediate neighbors and record the Wx
4. If Node v choose itself as clusterhead
5. Start a timer Tclusterhead and Send “join_cluster” message to all or anynodes x within theneighbor table
6. If
7. Node x settle for “Join_cluster”, reply with “accept_join” to v else
8. doesn'tanswerbe a part of request else
9. node v isn't a CH, wait for join_cluster from alternative CH
10. visit step four if there's any node with standing “undecided”

In unintendedsurroundings there might exist some thingswherever some regions of the network become overcrowded (for example location close to the speaker in an exceedingly conference) and therefore the clusterheads lay during this regions is alsooverladen. A clusterhead is termedoverladen if it's serving quite threshold members. The overladen clusterheads will adversely have an effect on the performance of the network.

Algorithm 2: Cluster division rule

1. Every CH (A) endlesslyMonitors the number of members in its cluster
2. If (No. of members of the cluster > threshold)
3. A sends CLUSTER_DIV message to all or any of its members
4. A knows the member that is farthest from it and sends a CH_APPOINT message
5. Node (E) received CH_APPOINT message changes its standing as “CH”
6. Node E then sends Join_cluster message to all neighbors
7. All members of divided cluster calculate their distances to A and E, let these are DAx and DEx
8. If (DEx<DAx)
9. Nodes send accept_join message to E and become its members else
10. nodeskeepbelow the cluster of A else
11. No members would like of cluster division.

Simulation and Result Analysis

Proposed work is simulated using Omnet++ and the performance is compared in terms of PDF, Throughput and E2E delay. In this Experiment 100 nodes are taken for analysis.

Packet delivery Fraction (PDF)

Packet delivery quantitative relation is outlinedbecause the ratio of total packets transmitted to total packets received at the destination. In WCA a number of the packets could drop because of congestion and buffer overflow at the clusterheads, this leads to the drop of PDF whereas within theplanned work we've performed load levelling and this improves PDF. Fig 2 PDF with packet interval.

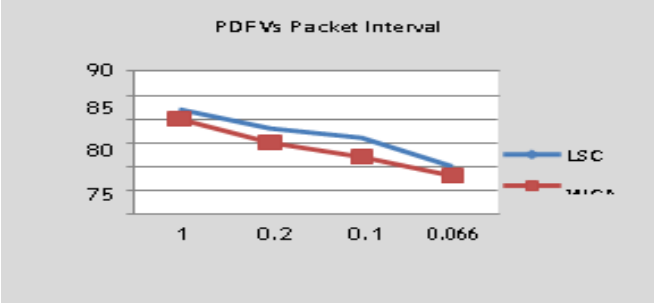


Fig-2: PDF with Packet Interval

ISSN 2394 - 7780

Throughput

Throughput measures the effective utilization of the channel and is measured in kbps. The papered work shows higherturnout than the WCA. In WCA, packets need tostay up for their f lipas a result ofa number of the clusterheads could also befull and engorged. The papered work uniformly distributes the load on the chosen cluster heads and therefore smart turnout is maintained. Fig 3 shows Throughput with packet interval.

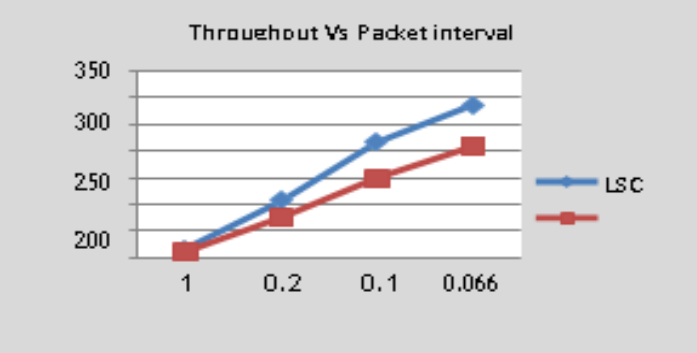


Fig-3: Throughput with packet interval

E2E Delay

This metric includes all double delay which will be caused by: buffering throughout route discovery, queuing at the interface queue, retransmission delay at the mac layer, propagation and transfer time. As the traffic within the network will increase, the clusterheads need to bear the multipliedload of routing the packetssupply to destination. If clusterheads are serving an outsized number of members, there's a modification that a number of the clusterheads could become bottleneck. This results larger end to finish delay of routed packets.The Dominantamount of members of a clusterhead,ends up in improved performance at the time of routing in significant traffic conditions. WCA doesn't limit the member of a clusterhead and so, because the packet interval is attenuate, additional packets are transmitted by the supply nodes within the unit time and this ends up in the more e2e delay. In papered work a threshold is about on number of members, thus clusterheads don't seem to beoverladen. The e2e delay within thepaperedalgorithmic ruleis a smaller amount than that of WCA as shown by experimental results. Fig 4 shows E2E delay with packet interval

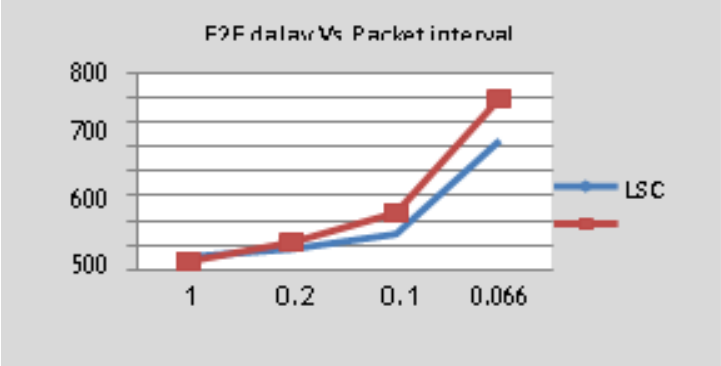


Fig-4: E2E delay with packet interval

V. CONCLUSION

In conclusion, this work provides a framework for load sharing inclusters. The papered LSC subdivide the overladen cluster in 2 clusters and therefore the head of the new born cluster is chosen by considering the facility consumption throughout communication and weight values of the nodes. Since additional power is requiredto speak at giant distance, the farthest away node with appropriate weight is assigned because of the new clusterhead. Members that are nearer to new clusterhead as compared to previous clusterhead, be part of new clusterhead as its members. Uniform distribution of the load on the chosen clusterheads will improve the performance in terms of PDF, throughput, E2E delay.

REFERENCES

1. M. Gerla and J. T. Tsai, “Multiuser, Mobile, Multimedia RadioNetwork” Wireless Networks, 1995, vol. 1, pp. 255–65.
2. A.D. Amis, R. Prakash, T.H.P Vuong, D.T. Huynh. "Max-Min D-Cluster Formation in Wireless Ad Hoc Networks" In proceedings of IEEE Conference on Computer Communications (INFOCOM) 2000, Vol. 1. pp. 32-41.

ISSN 2394 - 7780

3. G. Chen, F. Nocetti, J. Gonzalez, and I. Stojmenovic, "Connectivity based k-hop clustering in wireless networks" proceedings of the 35th Annual Hawaii International Conference on System Sciences, 2002, Vol. 7, pp. 188.3.
4. F. Li, S. Zhang, X. Wang, X. Xue, H. Shen, "Vote- Based Clustering Algorithm in Mobile Ad Hoc Networks", In proceedings of International Conference on Networking Technologies, 2004.
5. T. Ohta, S. Inoue, and Y. Kakuda, "An Adaptive Multihop Clustering Scheme for Highly Mobile Ad Hoc Networks," in proceedings of 6th ISADS, 2003.
6. I. Er and W. Seah. "Mobility-based d-hop clustering algorithm for mobile ad hoc networks" IEEE Wireless Communications and Networking Conference, 2004, Vol. 4, pp. 2359-2364.
7. P. Basu, N. Khan, and T. D. C. Little, "A Mobility Based Metric for Clustering in Mobile Ad Hoc Networks" in proceedings of IEEE ICDCSW' 2001, pp. 413–18.
8. A. B. MaDonald and T. F. Znati, "A Mobility-based Frame Work for Adaptive Clustering in Wireless Ad Hoc Networks" IEEE JSAC, 1999, vol. 17, pp. 1466–87.
9. C.-C. Chiang, "Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel" in proceedings of IEEE SICON'1997.
10. C. R. Lin and M. Gerla, "Adaptive Clustering for Mobile Wireless Networks" IEEE JSAC, vol. 15, pp. 1265–75.
11. J. Y. Yu and P. H. J. Chong, "3hBAC (3-hop between Adjacent Clusterheads): a Novel Non-overlapping Clustering Algorithm for Mobile Ad Hoc Networks" in proceedings of IEEE Pacrim'2003, vol. 1, pp. 318–21.
12. T. J. Kwon et al., "Efficient Flooding with Passive Clustering an Overhead-Free Selective Forward Mechanism for Ad Hoc/Sensor Networks" in proceedings of IEEE, 2003, vol. 91, no. 8, pp. 1210–20.
13. A. D. Amis and R. Prakash, "Load-Balancing Clusters in Wireless Ad Hoc Networks" in proceedings of 3rd IEEE ASSET'2000, pp. 25–32.
14. J. Wu et al., "On Calculating Power-Aware Connected Dominating Sets for Efficient Routing in Ad Hoc Wireless Networks" J. Commun. and Networks, 2002, vol. 4, no. 1, pp. 59–70.
15. J.-H. Ryu, S. Song, and D.-H. Cho, "New Clustering Schemes for Energy Conservation in Two-Tiered Mobile Ad-Hoc Networks," in proceedings of IEEE ICC'2001, vo1. 3, pp. 862–66.
16. M. Chatterjee, S. Das, and D. Turgut. WCA: A weighted clustering algorithm for mobile ad hoc networks, Cluster computing Journal, 2002, vol. 5(2), pp. 193–204.
17. Yu-Xuan Wang, Forrest Sheng Bao, "An Entropy-Based Weighted Clustering Algorithm and Its Optimization for Ad Hoc Networks" Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2007.
18. S.K. Dhurandher and G.V. Singh" Weight-based adaptive clustering in wireless ad hoc networks" IEEE, 2005.
19. F.D.Tolba, D. Magoni and P. Lorenz " Connectivity, energy & mobility driven Weighted clustering algorithm " in proceedings of IEEE GLOBECOM, 2007.
20. Ivan Stojmenovic and Jie Wu, 'Broadcasting and Activity Scheduling in Ad Hoc Networks", in Mobile Ad hoc networking, S. Basagni, M. Conti, S. Giordano, I. Stojmenovic (Editors), IEEE Press and John Wiley and Sons, Inc., New York, 2003.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

A DYNAMIC POPULARITY AWARE REPLICATION STRATEGY WITH PARALLEL DOWNLOAD SCHEME IN CLOUD ENVIRONMENTS

V. Jansirani[1] and G. S. Geethamani[2]
Department of Information Technology
HOD &Professor, Department of Information Technology, Hindustan College of Arts and Science, Coimbatore

ABSTRACT
Cloud computing has emerged as a main approach for managing huge distributed data in different areas such as scientific operations and engineering experiments. In this regard, data replication in Cloud environments is a key strategy that reduces response time and improves reliability. One of the main features of a distributed environment is to replicate data in various sites such that popular data would be more available. If the site does not have a data file what user have searched, it will have to fetch it from other locations. Then, the Simultaneouslydownload approach is applied to reduce download time. It enables a user to get different parts of a file from several sites simultaneously. In this work, we present a data replication strategy, named the Dynamic Popularity aware Replication Strategy (DPRS). DPRS replicates only a small amount of frequently requested data file based on 80/20 idea. It determines to which site the file is replicated based on number of requests, free storage space, and site centrality. We introduce a parallel downloading approach that replicates data segments and parallel downloads replicated data fragments, to enhance the overall performance, total number of replications and percentage of storage filled by using the CloudSim simulator. Extensive experimentations demonstrate the effectiveness of DPRS under most of access patterns

Keywords: Android Device, Location Tracking, Alert System, GPS.

I. INTRODUCTION

High-speed computing and storage elements are needed for new applications like astrophysics, astronomy. Since these applications perform with the huge amount of datasets and computing. Though a mainframecomputer can execute the tasks, it is more cost and difficult to use.Distributed systems integrate different dispersed storage and computation elements. Distributed system decreases cost of system and utilizes the idled bandwidth and CPUs. Cloud computing has role on Information Technology (IT) solutions for both engineering and business applications. Cloud computing system has attractive characteristics that are important for both science purposes. Clouds also provide solutions to computationally intensive applications similar to HPC (High Performance Computing) environments like supercomputing centers.Cloud computing presents aindividual computing ecosystem where providers and application owners can set up elastic relationship driven by application performance features (e.g. availability, execution time, monetary budget, etc.).Cloud application owners, on the other hand, need services/resources that meet high performance requirements. Due to their data intensive nature, new scientific applications can be appropriate if Cloud schedulers use data reuse and replication strategies in executing their workflows. Data replication technique is a common idea to achieve these aims. Nowadays, different fields such as the Internet, P2P systems, and distributed databases use data replication approach to improve the overall performance. An effective data replication strategy should be able to find a suitable time to copy files, determine which data should be copied, and place copies in the best site. The key phase in proposing appropriate dynamic data replication algorithms is the analyses of data access patterns. Different models of data access patterns introduced as the distribution of access counts of data in distributed environment.

II EXISTING SYSTEM

In An existing system the data which have searched by the user they are stored in storage but it not stored in priority wise that another user search the relevant data again,its shows the data before what have searched .so the user cannot get the data fast and response by slow because of its takes the from the database where its stored

A. Advantage

User can able to search the data what they need,

Display the data based on the user search

B. Disadvantage

Waste of time for the user.

Response time is slow

ISSN 2394 - 7780

III. PROPOSED SYSTEM

n Proposed system the user can get the data fast in high response, DPRS Algorithm have been used for the data to retrieve fast and avoid duplication replication data, its gives the data more fast and user not to waste their time ,user have login to the system is they are exited ,if they were new user they can able to login and show the recently used or searched data, it displayed based on the given number of data display in the cluster and they user can view the replication data in the cluster and the cluster contain the data searched which are mostly searched .

Retrieve data fast without delay of showing the result for the user.

No waste of time for the user to wait for the result.

A. Motivations

Cloud computing environment is one of the hottest core technical issues in the modern period of time,"the Cloud computing is a model for enabling convenient, resource pooling, lead access which can be easily delivered with more types of service provider interaction"One of the main advantages of pay as you go model is that we can decrease cost by provisioning a certain amount of resources. The customer can choose processor, memory, hard disk, operating system, networking, access control and any additional new software as needed to their environment. The resources presented on-demand to the users. It provides the great advantages to industry and home users and attracts the attention of the scientific societies. On the other hand, small part of data is an important and critical part of shared resources in different research communities. The volume of data is measured in terabytes or petabytes in most of categories. Large amount of data is normally kept in data centers of Cloud environment. Therefore,dataduplicates is used to manage big data by storing several replicas of data files in distributed locations. Data replication is necessary to enhance data accessibility, availability, and fault tolerance, while improving data access time and load of network

IV. MODEL DESCRIPTION

A.Cloudsim initialization

The cloud computing concept can be enhanced by cloudsim tool. These tool has to initialized before stating the cloud application.

B.Registration

In this module user must register himself by filling some personal details.

C.Login

After registration user will get user ID and password through which user can login to access the system

D.Clustering

The clustering process has to be performed in order to simplify the replication process

Perform Replication

The replication is performed in this model. Initially the population of the files are computed and based on the populated files replication is performed

Inttotaitem=popularitem.size();Int weight =sum/totalitem;E.View replicated file

The replicated file can be viewed in this model after all the data's have searched.

V. CONCLUSION

The large scale of data in cluster, grid or Cloud environments increase the needed of data management, significantly. Data replication is an important approach to decrease user-waiting time and improve data access by creating several replicas of the same service. In Dynamic Popularity aware Replication Strategy (DPRS) is proposed based on the data access popularity and parallel download as criteria. DPRS determines the number of replication as well as the appropriate sites for placement based on the number of requests, free storage space.CloudSim simulator performs the performance evaluation of DPRS and other replication methods. DPRS is compared with five previous algorithms, i.e., SWORD, D2RS, DRSP, MORM, and ADRS strategies. Accordingly, DPRS improve the mean response time, effective network usage, replication frequency, storage usage, and hit ratio with respect to the others. The average response time of DPRS is lower by 36% compared to MORM strategy for 1000 tasks. DPRS can save storage space for distributed system while the available and performance QoS requirements are ensured.

ISSN 2394 - 7780

```
// File popularity calculation and Determination of files
for each cluster c, c= 1, 2, …Nc;  // Nc is the number of clusters in the system
Aggregate NR^n_c(f_i), i= 1, 2, …Nk;
Sort all files according to NR^n_c(f_i) in a descending order;
Store the sorting result into Set1;
Calculate FPV^r_c (f_i) and FPV^n_avg (f_i)  i= 1, 2, …Nk;   // Eq. (1) and (2)
Sort the set Set1 according to FPV^n_avg (f_i)  in a descending order;
Set the value x=0.8,   0<x<1;
Calculate  Num_i;      //Eq. (3)
Select the first Num_i file from Set1 and put them into Set2;    //Set2 is the set of replication candidate

//Replica placement step
for each file f_j in Set2
{       check LRC_c to see whether cluster c has f_j.
        if cluster c does not have f_j
                Calculate M^n_j for each site n in cluster c;    // Eq. (4)
                Sort all sites in cluster c according to suitability (M^n_i) in a descending order;
                Store the sorting result into  Set3.

        Select the first N site from Set3 and put them into Set4;
        Divide f_j into N fragments;
        Calculate P_n for each site n in Set4; // P_n shows the portion of the file to be replicated on node n
        Replicate the N fragments across the N sites in Set4;
}
```

VII. FUTHURE ENHANCEMENT

Further, this system makes more effective in response time more than MORM Strategy and the user can also view the cluster details what they have searched.

REFERENCE

1. http://www.intel.com/technology/mooreslaw/index.htm.
2. ChipWalter,Kryder'sLaw,ScientificAmerican,August2005.
3. N. Mansouri, G.H. Dastghaibyfard, E. Mansouri, Combination of data replication and scheduling algorithm for improving data availability in Data Grids, J. Netw. Comput. Appl. 36 (2013) 711–722.
4. L. Breslau, P. Cao, L. Fan, G. Phillips, S. Shenker, Web caching and Zipf-like distributions: evidence and implications, in: Proceedings of IEEE INFOCOM'99, no.1, New York, USA, 1999, pp. 126–134.
5. D.G. Cameron, R. Carvajal-Schiaffino, A. Paul Millar, C. Nicholson, K. Stockinger, F. Zini, Evaluating scheduling and replica optimisation strategies in OptorSim, The International Workshop on Grid Computing, Phoenix, Arizona, November 17, IEEE Computer SocietyPress,2003.
6. K. Ranganathan, I. Foster, Decoupling computation and data scheduling in distributed data intensive applications, International Symposium for High Performance Distributed Computing, HPDC-11, 2002.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

PRIVACY-PRESERVING PUBLIC AUDITING FOR SECURE CLOUD STORAGE

Raj Dharaniya V[1] and Marrynal S Eastaff[2]
Student[1] and Assistant Professor[2], Department of Information Technology, Hindusthan College of Arts and Science

ABSTRACT
In this paper, The privacy-preserving public auditing system for data storage security in cloud computing. Knowledge about the data content stored on the cloud server during the efficient auditing logs process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task. In the cloud storage, users data can be remotely stored, most needed high-quality applications and it allows services from a shared pool of configurable computing resources, without the subtances of local data storage and maintenance. In cloud computing and cloud garage environment, audit logs are required to be encrypted and outsourced on far off servers to protect the confidentiality of statistics and the privacy of users. The searchable encrypted audit logs support a seek at the encrypted audit .In this paper, we advocate a privacy- preserving and unforgivable searchable encrypted audit log scheme based In this paper, first in our scheme only the information proprietor can generate legitimate searchable encrypted audit logs. The customers and servers cannot forge or tamper searchable encrypted audit log even though they collude with every different. And finally, the scheme lets in a high-quality-grained conjunctive key phrases question in a searchable encryption way.

Keywords: Data storage, privacy-preserving, public auditability, cloud computing, delegation, batch verification.

I. INTRODUCTION
Cloud computing services will offer the users with efficient and scalable data storage , with a much lower marginal cost than traditional approaches. It is routine for users to leverage cloud storage services to share data with others in a group, as data sharing becomes a standard feature in most cloud storage offerings, including Drop box, iCloud and Google Drive[1]. In cloud integrity of data in cloud storage is subject to skepticism and scrutiny, since data stored in the cloud can be easily lost or corrupted due to the inevitable hardware software failures and human errors, To make this matter even worse, cloud service providers may be reluctant to inform users about these data errors in order to maintain the reputation of their services and avoid losing profits. Therefore, the integrity of cloud data should be verified before any data utilization, such as search or computation over cloud data.

The traditional perspective for checking data correctness is to retrieve the entire data from the cloud, and then verify data integrity by checking the correctness of signatures (e.g., RSA) or hash values (e.g., MD5) of the entire data. Certainly, this conventional approach is able to successfully check the correctness of cloud data. It have been proposed to allow not only a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data. In this mechanisms, data is splited into number of small blocks, where each block is independently signed by the owner; and a random combination of all the blocks instead during integrity checking the full data is gained. A public verifier could be a data user (e.g., researcher) who would like to utilize the owner's data via the cloud or a third-party auditor (TPA) who can provide expert integrity checking services. So that during public auditing on cloud data, the content of private data belonging to a personal user is not disclosed to any public verifiers.

II. SYSTEM DESIGN
EXISTING SYSTEM
The data owner outsources her data on cloud servers in the cloud storage system. When data user logs in the system using his identity and password[4], he must apply to data owner for data access first. Data owner creates a searchable encrypted audit log, and then authorizes it to user. The audit log contains a log ticket which is consists of an access ticket and the cipher text of the audit log. If the cloud provider cannot authenticate users before downloading, like in many existing CP-ABE cloud storage systems the cloud has to allow everyone to download to ensure availability.Cloud users will not have the strong belief that the cloud server is doing a best job in terms of confidentiality.

DISADVANTAGES OF EXISITNG SYTEM
- Accuracy of the data in the cloud is being at risk.
- Then we can every time create searchable encrypted audit log

ISSN 2394 - 7780

- Not correct data integrity.
- Based on the number of decryption keys the cost and complexity increases.

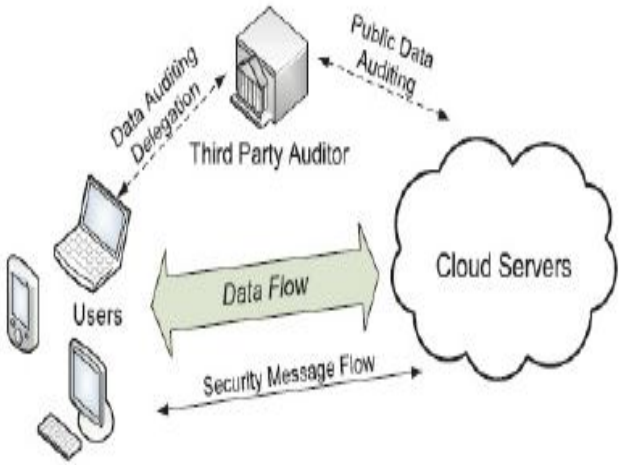


Fig-1: The architecture of cloud data storage service.

III. PROPOSED SYSTEM

In this paper, we keen on how to reduce the damage of the clients' key exposure in cloud storage auditing. Our goal is to design a cloud storage auditing protocol with built-in key-exposure resilience[2]. Below we have addressed, How to do it efficiently with all kind of new challenges in this new problem setting. First of all, applying the traditional solution of key revocation to cloud storage auditing is not practical We are introducing a public-key encryption which we call key-aggregate cryptosystem (KAC). Users used to encrypt a message not only under a public-key, but also under an identifier of cipher text called class. It means the cipher texts are further classified into different classes. The master-secret called master-secret key which is hold by the key owner, which can be used to extract secret keys for different classes. Security not only involved cipher text policy involved High level security using key aggregation. All files can be uploaded in encrypted format and downloading by decryption files using AES algorithm. So cloud server can by encrypted format hackers will be unawareness about data.

ADVANTAGES OF PROPOSED SYSTEM

The delegation of decryption can be efficiently implemented with the aggregate key, which is only of fixed size.Public audit ability

- Privacy preserving
- Storage correctness
- Batch auditing
- Lightweight

A. Public auditability

The public auditability is used to verify the correctness of the cloud data on needed without retrieving a copy of the whole data or introducing additional online subtance to the cloud users[13].

B. Storage correctness

The storage correctness is to ensure that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users' data intact.

C. Privacy-preserving

Privacy preserving ensure that the TPA cannot derive users' data content from the information collected during the auditing process.

D. Batch auditing

It has capabilities of multiple auditing from large number of different users simultaneously with security and efficiency using TPA in batch auditing[13].

E. Lightweight

Lightweight allows TPA to perform auditing with minimum communication and computation overhead.

ISSN 2394 - 7780

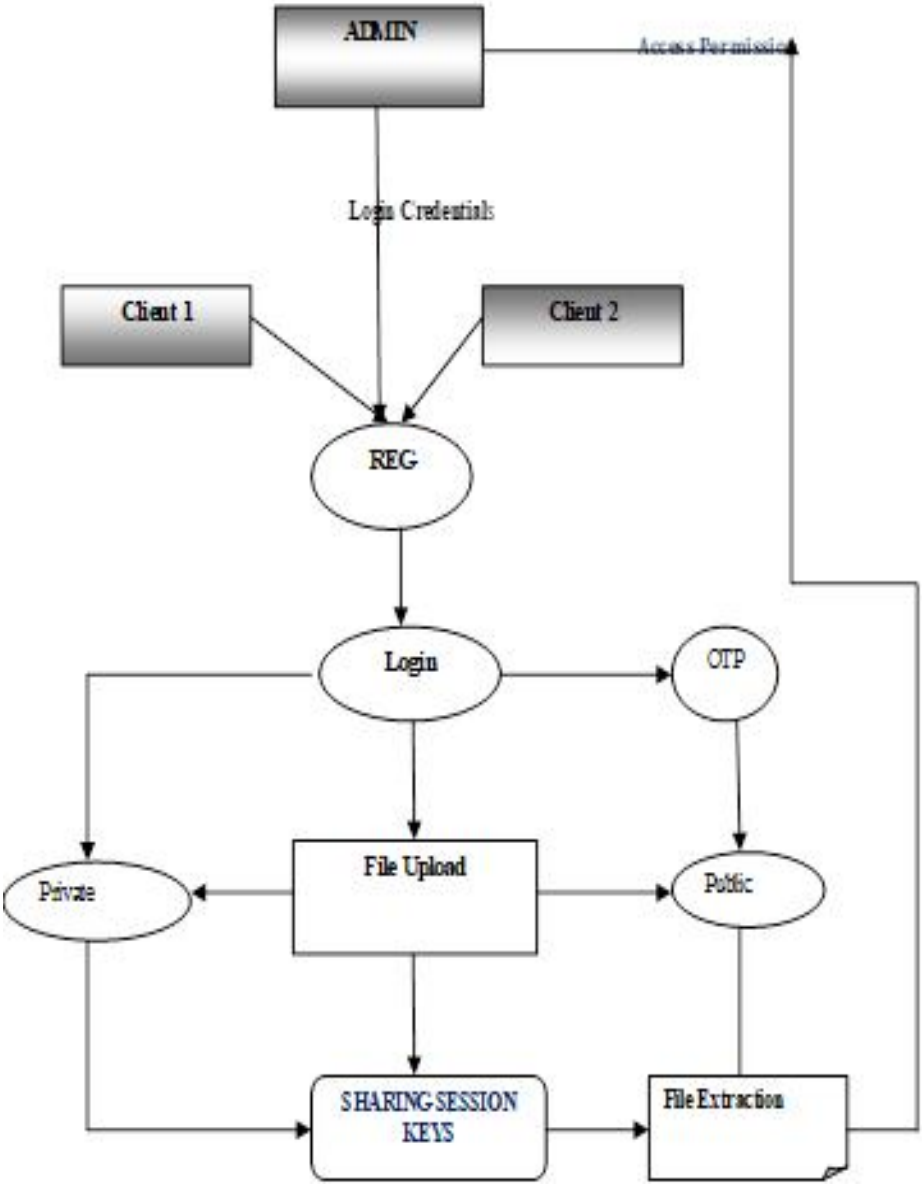


Fig-2: Architecture Diagram

IV. MODULES

A. Encryption / Decryption

We used RSA algorithm for encryption/Decryption. This algorithm mechanism is used for secure transaction. we are using the RSA algorithm of key size of 2048 bits. Then splitting up of keys takes place and stored in four non-identical places. If a user wants to access the file he/she may need to provide the four set of data to produce the single private key to manage encryption/decryption[10].

B. File Upload / Download

1) File Upload

The client will request to the key manager for the public key, which will be generated according to the policy associated with the file. Different policies for files, public key also differs. But for same policy are provided for same public key. Then a private key is generated by client by combining authentication details like the username, password and security credentials. Then the file is encrypted with the public key and private key and forwarded to the cloud[14].

2) File Download

After completion of the authentication process the client can download the file. As the public key maintained by the key manager, the client request the key manager for public key[14]. Only the authenticated client can get the public key. Then the client user can decrypt the file with the public key and the private key. Checks whether the user is authorized to download the file. But the main thing is cloud doesn't have any attributes or the authentication details of the user.

ISSN 2394 - 7780

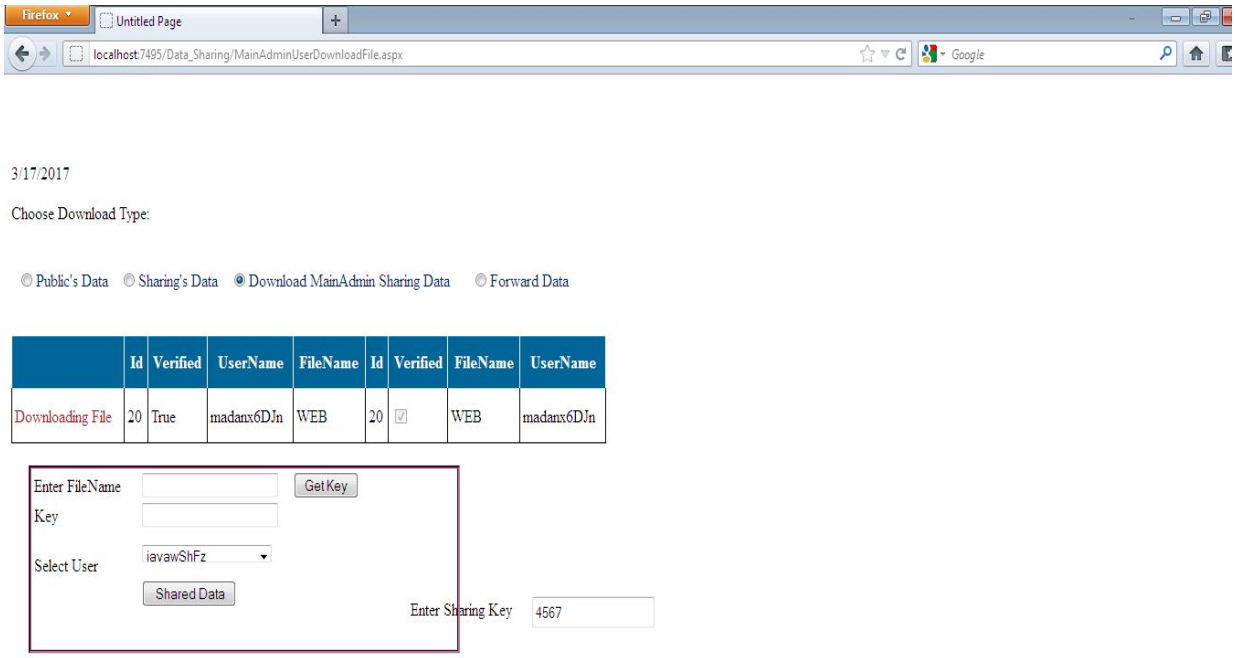


Fig-3: file download

F. Encryption Process

*I*n this module, the information and data's shared by the user in the cloud is encrypted by using AES algorithm. All of the information shared by every user is encrypted and stored in the cloud[10].

G. Integrity Checking

Integrity checking is the process of comparing the encrypted information with altered cipher text. If there is any change in detection a message will send to the user that the encryption process is not done properly. If there is no change in detection means then it will allow doing the next process. Integrity checking is mainly used for anti-malware controls.

H. Data Forwarding

In this module, the encrypted data or information stored in the cloud is forwarded to another user account by using that user's private key. If any user wants to share their information with their friends or someone they can directly forward the encrypted data to them. Without downloading the data the user can forward the information to another user.

I. Data Extraction

In this module, the encrypted data is decrypted by the user using the private key of owner of the data. Decryption is the process of converting cipher text into plain text[14]. AES algorithm is used for encrypting and decrypting the information. The user can view the data and also can download the data with high security once after getting the permission from admin.

V. SYSTEM IMPLEMENTATION

System Implementationcan be as follows: To a prepared set of users to available new system (the deployment), and positioning on-going support and maintenance of the system within the Performing Organization (the transition). Detail level of finer, deploying the system consists of executing all steps necessary to educate the Consumers on the use of the new system, placing the newly developed system into production, confirming the data required at the start of operations is available and accurate, and validating that business functions that interact with the system are functioning properly. Responsibilities involves changing from a system *development* to a system *support and maintenance* mode of operation, with ownership of the new system moving from the Paper Team to the Performing Organization. System implementation is the important stage of paper when the theoretical design is tuned into practical system. The stages in the implementation are:

- Planning
- Training
- System testing and
- Changeover Planning

ISSN 2394 - 7780

VI. CONCLUSIONS

Cloud Computing is gaining popularity and advancement day-by-day. But still the security threat hinders the success of Cloud Computing. In this paper, some of the privacy threats are addressed and the techniques to overcome them are surveyed. While some perspective utilized traditional cryptographic methods to achieve privacy, some other approaches kept them away and focused on alternate methodologies in achieving privacy. Also, approaches to preserve privacy at the time of public auditing are also discussed. Thus, to conclude that it is necessary that every cloud client user must be promises that his data is stored, processed, accessed and audited in a secured manner at any time.

VII. FUTURE ENHANCEMENT

Third party notification with time. Third party included within the cloud with less overhead. The client user must be given full access control over the published data. Also, muscular security mechanisms must always accomplish every cloud application. Gaining all these would end up in achieving the prolonged dreamt vision of secured Cloud Computing in the nearest future.

REFERENCES

1. http://www.rroij.com/open-access/shared-data-based-privacy-preservingauthentication-in-cloud-for-publicauditing.php?aid=56300
2. VARADAN"Enabling Cloud Storage Auditing With Key-Exposure Resistance"https://www.jpinfotech.org/enabling-cloud-storage-auditing-key-exposure-resistance/ ,29 SEPTEMBER 2015
3. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing,"Technical Report UCB-EECS-2009-28, Univ. of California,Berkeley, Feb. 2009.
4. Cloud Security Alliance, "Top Threats to Cloud Computing, "http://www.cloudsecurityalliance.org, 2010.
5. M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions,"http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof-mass-email-deletions/, 2006.
6. J. Kincaid, "MediaMax/TheLinkup Closes Its Doors,"http://www.techcrunch.com/2008/07/10/ mediamaxthelinkup-closesits-doors/, July 2008.
7. Amazon.com, "Amazon s3 Availability Event: July 20, 2008,"http://status.aws.amazon.com/s3-20080720.html, July 2008.
8. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling PublicAuditability and Data Dynamics for Storage Security in CloudComputing," IEEE Trans. Parallel and Distributed Systems, vol. 22,no. 5, pp. 847-859, May 2011.
9. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, "Provable Data Possession at UntrustedStores," Proc. 14th ACM Conf. Computer and Comm. Security(CCS '07), pp. 598-609, 2007.
10. M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-PreservingAudit andExtraction of Digital Contents," Cryptology ePrintArchive, Report 2008/186, 2008.
11. A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievabilityfor Large Files," Proc. ACM Conf. Computer and Comm. Security(CCS '07), pp. 584-597, Oct. 2007.
12. Cloud Security Alliance, "Security Guidance for Critical Areas ofFocus in Cloud Computing," http://www.cloudsecurityalliance.org, 2009.
13. VARADAN "https://www.jpinfotech.org/privacy-preserving-public-auditing-for-secure-cloud-storage/"IEEE PAPERS IN PONDICHERRY on 20 JUNE 2013
14. A Handbook of Applied Cryptography by Alfred J. Menezes,Paul C. Van Oorschot and Scott A. Vanstone, CRC Press Series on Discrete Mathematics and Its Applications

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

CLOUD COMPUTING: SECURITY ISSUES

N. Sanooj[1] and G. Sivabrindha[2]
Student[1] and HOD & Professor[2], Department of Information Technology, Hindustan College of Arts and Science, Coimbatore

ABSTRACT
Distributed computing is the act of utilizing a system of remote servers facilitated on web to store, oversee and process information on interest and pay according to utilize. It gives access to a pool of shared assets rather than nearby servers or PCs. As it don't gain the things physically, it spares overseeing cost and time for associations. Distributed computing is a totally web subordinate innovation where customer information is put away and keep up in the server farm of a cloud supplier like Google, Amazon, Microsoft and so on. Distributed computing is a rising space and is acclaimed all through the world. There are some security issues sneaking in while utilizing administrations over the cloud. This exploration paper shows a survey on the distributed computing ideas just as security issues innate inside the setting of distributed computing and cloud foundation. This paper additionally breaks down the key research and difficulties that presents in distributed computing and offers best practices to specialist organizations just as endeavors wanting to use cloud administration to improve their main concern in this extreme monetary atmosphere and lift up its use. The primary accentuation of our investigation dependent on existing writing and to comprehend the idea of multi-occupancy security issue.

I. INTRODUCTION
Distributed computing is a circulated engineering that brings together server assets on an adaptable stage to give on interest figuring assets and administrations. Cloud Service Providers (CSP's) offer cloud stages for their clients to utilize and make their web administrations, much like Internet Service Providers (ISP's) offer costumers fast broadband to get to the web. CSPs and ISPs both offer administrations. Distributed computing is a model that empowers advantageous, on-request arrange access to a common pool of configurable processing assets, for example, systems, servers, stockpiling, applications that can be quickly provisioned and discharged with insignificant administration exertion or specialist organization's connection.

Mists are the new pattern in the development of the dispersed frameworks. Prior to Cloud we utilized Grid. In Cloud Computing, the client does not require learning or skill to control the framework of mists; it gives just reflection. It very well may be used as an administration of the Internet with high versatility, higher throughput, nature of administration and high processing force. Distributed computing suppliers convey normal online business applications which are gotten to from servers through internet browser. Late advancements in the field of Cloud figuring have gigantically changed the method for processing just as the idea of registering assets. In a cloud based registering foundation, the assets are typically in another person's reason or organize and got to remotely by the cloud clients. Now and again, it may be required or if nothing else workable for an individual to store information on remote cloud servers. These gives the accompanying three touchy states or situations that are of specific worry inside the operational setting of distributed computing:

• The transmission of individual delicate information to the cloud server.

• The transmission of information from the cloud server to customers' PCs.

• The capacity of customers' close to home information in cloud servers which are remote servers not possessed by the customers. All the over three conditions of distributed computing are seriously inclined to security break that makes the exploration and examination inside the security parts of distributed computing practice a basic one. The viewpoints exhibited in this paper are sorted out so as to talk about and indentify the way to deal with distributed computing just as the security issues and worries that must be considered in the sending towards a cloud based registering framework. Dialog on the innovative ideas and ways to deal with distributed computing including the structural representation has been mulled over inside the setting of exchange in this paper. Security issues inborn in distributed computing approach have been talked about a short time later. The investigation in the mechanical and security worries of distributed computing has prompted the finishing up acknowledgment on the general parts of distributed computing.

II. CLOUDCOMPUTING
Broadly speaking cloud providers offer three types of services:

- Software as a Service (SaaS)
- Platform as a service (PaaS)

ISSN 2394 - 7780

- Infrastructure as a service (IaaS)

Software as a Service (SaaS): It is likewise called a conveyance display where the product and the information which is related with is facilitated over the cloud condition by outsider called cloud specialist organization, much the same as your Gmail account, you utilize that application on another person's framework

Platform as a Service (PaaS): In this administration, you can utilize Online apparatuses to create applications so they keep running on frameworks programming which is given by another organization, similar to Google Application Motor.

Infrastructure as a Service (IaaS): In this administration, you can utilize Online devices to create applications so they keep running on frameworks programming which is given by another organization, similar to Google Application Motor.

2.2 Deployment models

There are three Deployment Models and are described below:

- Public Model
- Private Model
- Hybrid Model

Public Model: foundation is accessible to the overall population. As the name proposes, open cloud is a model in which assets are commonly accessible to everybody and anyplace.

Private Model: This model is created for the private associations like one house and an association and they can utilize it for their very own motivation. This sort of an administration isn't gotten to by everybody.

Hybrid Model: Cross breed Mists are blend of open and private cloud in an equivalent system. This should be possible if private cloud need some essential administrations from the open cloud like Private cloud can store some data on their private cloud and we can utilize that data on open cloud.

III. SECURITY ISSUES IN CLOUD COMPUTING

Distributed computing comprises of utilizations, stages and framework fragments. Each section performs distinctive activities and offers diverse items for organizations and people the world over. There are various security issues for distributed computing as it envelops numerous innovations which incorporates systems, databases, working frameworks, virtualization, asset planning, exchange the board, simultaneousness control and memory the executives. Accordingly, security issues for a considerable lot of these frameworks and advancements are material to distributed computing. Information security includes scrambling the information just as guaranteeing that proper arrangements are upheld for information sharing. The given beneath are the different security worries in a distributed computing condition.

• Access to Servers & Applications

• Data Transmission

• Virtual Machine Security

• Network Security

• Data Security

• Data Privacy

• Data Integrity

• Data Location

• Data Availability

• Data Segregation

• Security Policy and Compliance

3.1 Data Transmission

It is the way toward sending advanced or simple information over a correspondence medium to at least one processing system. In Cloud condition the vast majority of the information isn't encoded in the preparing time. To process information for any application that information must be decoded. In homomorphism encryption

ISSN 2394 - 7780

which enables the information to be prepared without being unscrambled. The assault is completed when the aggressors place themselves in the correspondences way between the clients. Here there is the likelihood that they can hinder and change interchanges.

3.2 Virtual Machine Security
The term Virtual Machine (VM) portrays sharing the assets of one single physical PC into different PCs inside itself. VM's give readiness, adaptability and versatility to the cloud assets by enabling the merchants to duplicate, move and control their VM's. Remembering this, noxious programmers are discovering approaches to get their hands on significant information by controlling protections and breaking the security layers of cloud conditions. The distributed computing situation isn't as straightforward as it professes to be. The administration client has no clue about how the information is handled and put away and can't specifically control the stream of information stockpiling and preparing. Having VM's would by implication permits anybody access to the host plate of the VM to take an illicit duplicate of the entire framework.

3.3 Data Integrity
Debasement of information can occur at any dimension of capacity. So Honesty observing is should in distributed storage. Information Honesty in a framework is kept up through database imperatives and exchanges. Exchanges ought to pursue Corrosive (atomicity, consistency, detachment, solidness). Information created by distributed computing administrations are kept in the mists. Keeping information in the mists, clients may lose control of their information and depend on cloud administrators to implement get to control.

3.4 Data Location
Cloud clients don't know about the definite area of the datacenter and furthermore they don't have any authority over the physical access to that information. A large portion of the cloud suppliers have datacenters around the globe. In numerous nations specific sorts of information can't leave the nation in view of conceivably delicate data. Next in the multifaceted nature chain there are dispersed frameworks in which there are different databases and various applications. In view of the investigation, we found that there are numerous issues in distributed computing yet security is the serious issue which is related with distributed computing. Top seven security issues in distributed computing condition as found by "Cloud Security Collusion" CSA are:

• Misuse and reprehensible use of Cloud Computing.

• Insecure API.

• Wicked Insiders.

• Shared Technology issues / multi-tenancy nature.

• Data Crash.

• Account, Service & Traffic Hijacking.

• Unidentified risk report.

3.5 Misuse and reprehensible Use of Cloud Computing
Programmers, spammers and different lawbreakers exploit the appropriate enlistment, basic methodology and similarly unspecified access to cloud administrations to dispatch different assaults, for example, key breaking, secret phrase and so forth.

3.6 Insecure Application Programming Interfaces (API)
Clients handle and interface with cloud benefits through API's. Suppliers must guarantee that security is coordinated into their administration models, while clients must know about security dangers.

3.7 Wicked Insiders
Malignant insiders make a gigantic danger in distributed computing condition, since shoppers don't have an unmistakable sight of supplier arrangements and strategies. Vindictive insiders can increase unapproved access into association and their benefits.

3.8 Shared Technology issues/multi-tenancy nature
This is essentially founded on shared framework, which isn't intended to oblige a multi-occupant design.

3.9 Data Crash
Involved information may incorporate erased or adjusted information without making a reinforcement, unlinking a record from an immense domain, loss of an encoding key and illicit access of touchy information.

ISSN 2394 - 7780

3.10 Account, Service & Traffic Hijacking
Record or administration commandeering is generally completed with stolen certifications. Such assaults incorporate phishing, extortion and abuse of programming vulnerabilities. Assailants can get to basic regions of distributed computing administrations like classification, honesty and accessibility of administrations.

3.11 Unidentified Risk Report
Cloud administrations implies that associations are less required with programming and equipment, so associations ought not know with these issues, for example, inward security, security consistence, reviewing and logging might be ignored.

IV. RESEARCHCHALLENGES
Distributed computing research tends to the difficulties of meeting the prerequisites of cutting edge private, open and crossover distributed computing designs and furthermore the difficulties of enabling applications and improvement stages to exploit the advantages of distributed computing. Many existing issues have not been completely tended to, while new difficulties continue rising up out of industry applications. A portion of the testing research issues in distributed computing are given underneath.• Service Level Agreements (SLA's)

• Cloud Data Management & Security

• Interoperability

• Multi-tenancy

• Server Consolidation

• Common Cloud Standards

• Platform Management

4.1 Service Level Agreements (SLA's)
Cloud is administrated by administration level understandings that enable a few occasions of one application to be copied on different servers if need emerges; subject to a need plot, the cloud may limit or close down a lower level application. A major test for the cloud clients is to assess SLA's of cloud sellers. The greater part of the cloud merchants make SLA's to make a protective shield against lawful activity while offering confirmations to clients. So there are a few issues, for example, information security, blackouts and value structures that must be considered by the clients before marking an agreement with the merchant. And furthermore is there any SLA related with reinforcement, document, or protection of information? On the off chance that the administration account ends up idle, at that point do they keep client information? On the off chance that indeed, at that point to what extent? So it's a critical research territory in distributed computing.

4.2 Cloud Data Management
Cloud information can be enormous, unstructured and regularly annex just with uncommon updates. As administration sellers don't approach the physical security arrangement of server farms, they should depend on the framework supplier to accomplish full information security. In a virtualized situation like the mists, VMs can powerfully move starting with one area then onto the next; consequently straightforwardly utilizing remote verification isn't adequate. In such case, it is basic to manufacture trust components at each structural layer of the cloud. Programming structures, for example, MapReduce and its different usage, for example, Hadoop are intended for dispersed handling of information concentrated assignments, these systems commonly work on Web scale record framework.

4.3 Interoperability
It is the capacity of a PC framework to run application programs from various sellers and to collaborate with different PCs crosswise over LAN or WAN autonomous of their physical design and working frameworks. Numerous open cloud systems are arranged as shut frameworks and are not intended to associate with one another. To beat this test, industry benchmarks must be created to help cloud specialist organizations plan interoperable stages and empower information convenientce. Associations need to naturally arrangement administrations, oversee VM examples, and work with both cloud-based and endeavor based applications utilizing a solitary device set that can work crosswise over existing papers and different cloud suppliers.

4.4 MULTI-TENANCY
Multi-tenure is a noteworthy worry in distributed computing. Multi-occupancy happens when various customers utilizes a similar cloud, same working framework, on a similar equipment, with similar information stockpiling framework to share the data and information or keeps running on a solitary server. There are different kinds of

ISSN 2394 - 7780

cloud applications that clients can access through the Web, from little Web based gadgets to substantial undertaking programming applications that have expanded security prerequisites dependent on the sort of information being put away on the product merchant's framework. These application demands require multi-occupancy for some reasons, the most critical is cost. Various clients getting to a similar equipment, application servers, and databases may influence reaction times and execution for different clients. For application-layer multi-tenure explicitly, assets are shared at every framework layer and have substantial security and execution concerns. For instance, different administration demands getting to assets in the meantime increment hold up times yet not really CPU time, or the quantity of associations with a HTTP server has been depleted, and the administration must hold up until it can utilize an accessible association or in a most dire outcome imaginable drops the administration ask.

4.4.1 Architecture

This architecture fully separates your information from other customer's information, while allowing us to roll out rapidly the latest functionality to each, all at once. This approach offers the most configurability and allows you to extract deep insight from your information Oracle delivers a latest Multitenant architecture that allows a multitenant container database to grasp numerous pluggable databases. An existing database can simply be adopted with no application changes necessary

V. CONCLUSION AND FUTURE WORK

Distributed computing has gigantic prospects, yet with equivalent number of security dangers. One of the greatest security stresses with the distributed computing model is the multi-occupancy. In this paper, we previously examined different models of distributed computing, security issues and research difficulties in distributed computing. Multi-occupancy is serious issue for Distributed computing Security. There are a few other security challenges that incorporate security parts of system and virtualization. The boundless potential outcomes of distributed computing can't be concealed just for the security issues - the unending examination and research for vigorous, standard and coordinated security models for distributed computing may be the main way of motivation. In view of this reality that the effect of security issues in distributed computing can be diminished by multi-tenure design. Notwithstanding the idea of security issues, it tends to be without a doubt inferred that the organization of any type of distributed computing should manage the security concerns comparing to those of the wellbeing basic frameworks. We trust that because of the multifaceted nature of the cloud, it will be hard to accomplish start to finish security. New security systems should be created and more seasoned security methods are should have been profoundly changed to most likely work with the mists design. We trust our work will give a superior comprehension of the structure difficulties of distributed computing, and clear the way for further research around there.

REFERENCE

[1] Abbadi, I.M. and Martin, A., "Trust in the Cloud", Information Security Technical Report,

[2] Casola, V., Cuomo, A., Rak, M. and Villano, U., "The Cloud Grid approach: Security analysis and performance evaluation", Future Generation Computer Systems.

[3] Zissis, D and Lekkas, D., "Addressing cloud computing security issues", Future Generation Computer Systems.

[4] Teneyuca, D, "Internet cloud security: The illusion of inclusion", Information Security Technical Report.

[5] R. L Grossman, "The Case for Cloud Computing".

[6] Tim Mather, Subra Kumaraswamy, Shahed Latif, "Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance".

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

INTERNET USAGE CONTROL USING ACCESS CONTROL TECHNIQUES

Sabatini Judis Nivya[1] and Marrynal S Eastaff[2]
Student[1] and Assistant Professor[2], Department of Information Technology, Hindusthan College of Arts and Science

ABSTRACT
The access list is a group of statements that defines each pattern that would be found in an IP packet. The packet comes through an e interface with an associated access list, the list is scanned from top to bottom--in the exact order that it was entered--for a pattern that matches the incoming packet. The source address of the traffic in access list criteria could be the destination address of the traffic, the upper-layer protocol, or other information the access control lists provides basic traffic filtering capabilities cisco (also referred to as access lists). All routed network protocols can be configured an access lists (IP, AppleTalk, and so on) to filter the packets of those protocols as the packets pass through a router. In access lists you define typical criteria are packet source addresses, packet destination addresses, and upper-layer protocol of the packet. Set of criteria that can be defined has its own specific each protocol. You can define multiple criteria in multiple for a single access list, separate access list statements. The same identifying name or number, to tie the statements to the same access list are reference of these statements. The available memory statement has a limited criterion. The traffic flow is important to understand up front before you configure an ACL on a router interface the placement and understanding [1].

Keywords: Network Traffic, Network Security, Protocols, Standard ACL, Extended ACL

I. INTRODUCTION

To filter traffic as it either comes into or leaves an interface ACLs, known for their ability, can also be used for other purposes, including restricting remote access (virtual type terminal, or VTY) to an IOS device, filtering routing information, prioritizing traffic with queuing, triggering phone calls with dial-on-demand routing(DDR), changing the administrative distance of routes, and specifying traffic to be protected by an IPSec VPN, among many others. Basically, a set of commands of ACLs are, grouped together by a number or name, that are used to filter traffic entering or leaving an interface. Define commands specifically which traffic is permitted and denied in ACL. Global Configuration mode are created in ACLs.

A default Switches break up collision domains and routers break up broadcast domains. A creating virtual local area network (VLAN), broadcast domains break up in a pure switched internetwork. A logical group of network users and resources connected administratively defined ports on switches with a VLAN. VLANS created, when it will be the ability to create smaller broadcast domains within a layer 2 switched internetworks by assigning different ports on the switch to different sub networks. A swtich VLAN is treated like its own subnet or broadcast domain, meaning that frames broadcast onto the network are only switched between the ports logically grouped within the same VLAN[6].

II. SYSTEM DESIGN

A. EXISTING SYSTEM

A set of end stations and the switch ports that connect them with a VLAN. We could have different reasons for the logical division, such as department or paper membership. The end station and the port to which it is connected both belong to the same VLAN physical requirement. Support to a Layer 2 switch offers some of the benefits of both bridging and routing by Adding virtual LAN (VLAN) . Switch forwards traffic based on the Layer 2 header like a bridge, which is fast like a VLAN. It partitions the network into logical segments like a router, which provides better administration, security, and management of multicast traffic. A network has an associated VLAN ID, which appears in the IEEE 802.1Q tag in the Layer 2 header of packets transmitted on each VLAN. Might omit an end station tag, or the VLAN portion of the tag, in which case the first switch port to receive the packet can either reject it or insert a tag using its default VLAN ID. Can handle traffic for more than one VLAN port, but it can support only one default VLAN ID. An easy way to comply with IJRASET paper formatting requirements is to use this document as a template and simply type your text into it.[12]

1. DISADVANTAGES OF EXISITNG SYTEM

A. Communication Problem: As we know VLAN is giving high security. But there is a communication problem. For example, if any user in VLAN1 wants to communicate with another user in VLAN2 but they can't communicate. First communication they have to configure the data of the user in the switch. As we can say that for communication every time, we have to do configuration.

ISSN 2394 - 7780

B. Complexity: complexity in the sense of expansion of the network. It means if we expand the network and something goes wrong with that network then maintenance of the network's costs too much.

C. Capacity: routing of the VLAN does by router. A network is too large than router can't be handle the load of the work by single router. Network should be small to handle the workload.

D. Infection: In VLAN network every user relates to each other so if one user is infected by any virus or any worms then whole network will be affected by that viruses[7].

B. PROPOSED SYSTEM

"Administrators enable the scope of VLANs broadcast traffic and network-wide flooding, to reduce network overhead and enhance both privacy and security."

Limiting the Broadcast/Flooding Overhead — End hosts broadcast Dynamic Host Configuration Protocol (DHCP) traffic when joining the LAN, and routinely broadcast Address Resolution Protocol (ARP) requests to learn the medium access control (MAC) addresses in the same IP subnet. For example, cam- pus 2 has one IP subnet with up to 4000 hosts with around 300 packets/s of broadcast traffic; this broadcast traffic is dominated by ARP, iTunes broadcast messages, and NetBios. It not only consumes network bandwidth, but also consumes bandwidth and energy resources on the end hosts (particularly for mobile devices). A switch also floods packets to a destination MAC address they have not yet learned how to reach. A scope of broadcast traffic and network-wide flooding, to reduce network overhead and enhance both privacy and security."

Limiting the Broadcast/Flooding Overhead — End hosts broadcast Dynamic Host Configuration Protocol (DHCP) traffic when joining the LAN, and routinely broadcast Address Resolution Protocol (ARP) requests to learn the medium access control (MAC) addresses in the same IP subnet. For example, cam- pus 2 has one IP subnet with up to 4000 hosts with around 300 packets/s of broadcast traffic; this broadcast traffic is dominated by ARP, iTunes broadcast messages, and NetBios. It not only consumes network bandwidth, but also consumes bandwidth and energy resources on the end hosts (particularly for mobile devices). A switch also floods packets to a destination MAC address they have not yet learned how to reach[5].

1. ADVANTAGES OF PROPOSED SYSTEM

1. *Protecting Security and Privacy*

AN broadcast and flooding traffic also raise security and privacy concerns. Broadcast traffic is an effective of sending denial-of-service attack on the network. In addition, a malicious host can intentionally overload switch forwarding tables (e.g., by spoofing many source MAC addresses), forcing switches to flood legitimate traffic that can be easily monitored by the attacking host. ARP is vulnerable to man-in-the-middle attacks, where a malicious host sends unsolicited ARP responses to impersonate another host on the LAN, thereby intercepting all traffic sent to the victim. A network administrator can reduce these risks by constraining which users can belong to the same VLAN. A campus has separate subnets for faculty, graduate students, and undergraduate students, and assigns each subnet to one VLAN registered on basic MAC addresses of the user machines Ensures students cannot intercept faculty traffic (e.g., a midterm exam end route to the printer), and the graduate-student experiments research on VLAN do not inadvertently overload the faculty VLAN[3].

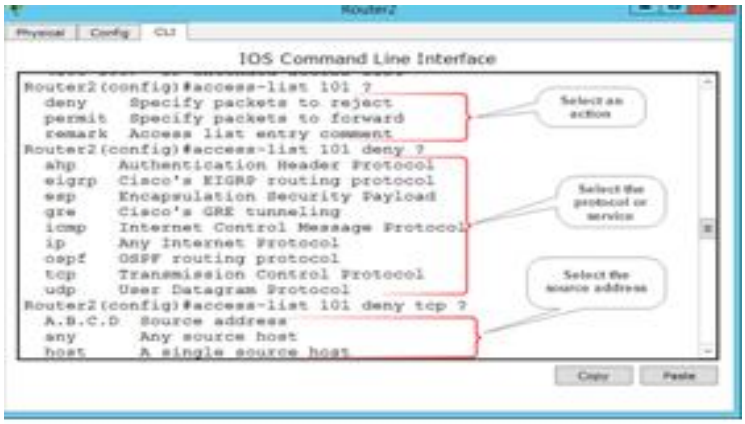


Figure-1: Identifying Sources

2. DE-CENTRALIZING NETWORK MANAGEMENT

Allow administrators VLANs to delegate some management tasks to individual departments. A network simplifies troubleshooting by allowing an administrator to observe connectivity from any part of the campus simply by trunking a port to a VLAN.

ISSN 2394 - 7780

I. MODULES

A. NETWORK PROTOCOLS

i. Ethernet

Built the current standards around the use of twisted pair wire. Common twisted pair standards are 10BaseT, 100BaseT, and 1000BaseT. The number (10, 100, 1000) and the speed of transmission (10/100/1000 megabits per second); “base” stands for the "baseband" and “T” stands for the "twisted pair" cable .10BaseFL can also be used at this level in fiber cable.[13]

B. Fast Ethernet

The protocol supports fast Ethernet transmission up to 100 Mbps. It requires the use of different, more expensive network concentrators/hubs and network interface cards. In category 5 twisted pair or fiber optic cable is necessary

C. TCP and SPX (Transport Layer)

The concerned with transport layer is efficient and reliable transportation of the data packets from one network to another. E-mail message or other piece of information is not sent as one unit in most cases of document. Small data packets is broken with each header information that identifies its correct sequence and document.[14]

D. VLAN

A, workstations are connected to each other by means of a hub or a repeater traditional LAN. Any incoming data throughout the network is propagate in these device. Attempt to send information by two people at the same time collision will occur and all the transmitted data will be lost. Collision will continue to be propagated throughout the network by hubs and repeaters. The original information will therefore need to be resent after waiting for the collision to be resolved, thereby incurring a significant wastage of time and resources. A collisions will prevent from traveling through all the workstations in the network, a bridge or a switch can be used. Forward collisions will not allow these devices but will allow broadcasts (to every user in the network) and multicasts (to a pre-specified group of users) to pass through. A router may be used to prevent broadcasts and multicasts from traveling through the network[2].

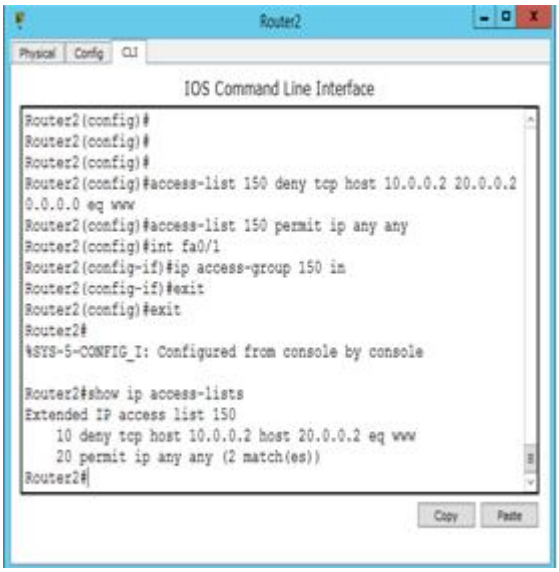


Figure-2: IOS Interface

E. ROUTING PROTOCOL SECURITY

Has received varying levels of attention in routing security over the past several years and has recently began to attract more attention specifically around BGP on the public Internet. Most area are open to attack is often not the Internet's BGP tables but the routing systems within your own enterprise network. An routing infrastructure can easily be attacked with MITM and other attacks designed to corrupt or change the routing tables with the following results:

- Traffic redirection—The adversary is able to redirect traffic in this attack, enabling the attacker to modify traffic in transit or simply sniff packets[11].
- Traffic sent to a routing black hole—Here to send specific routes to null0 the attacker is effectively kicking IP addresses of the network

ISSN 2394 - 7780

- Router DOS—Attacking the routing process can result in a crash of the router or a severe degradation of service.
- Routing protocol DOS—Attack is previously like the described against a whole router, a routing protocol attack could be launched to stop the routing process from functioning properly

Unauthorized route prefix origination— Attack aims to introduce a new prefix into the route table that shouldn't be there. To attack network to be routable throughout the victim network[8].

F. 3.1.6 ACCESS CONTROL LIST

A list of access control entries (ACE) is an access control list (ACL). A trustee and specifies the access rights allowed, denied, or audited for that trustee in each ACE in an ACL. The descriptor security for a securable object can contain two types of ACLs: a DACL and a SACL.

Identifies the trustees that are allowed or denied access to a securable object in discretionary access control list (DACL). Access a securable object tries process, the system checks the ACEs in the object's DACL to determine whether to grant access to it. The system grants object does not have a DACL access to everyone. If ACEs has no object's DACL, the system denies all attempts to access the object because the DACL does not allow any access rights.

In sequence Checks the until it finds one or more ACEs that allow all the requested access rights, or until any of the requested access rights are denied. You more information, see How DACLs Control Access to an Object. An information about how to properly create a DACL, see Creating a DACL[4].

II. SYSTEM IMPLEMENTATION

System Implementation can be as follows: To a prepared set of users to available new system (the deployment), and positioning on-going support and maintenance of the system within the Performing Organization (the transition). Detail level of finer, deploying the system consists of executing all steps necessary to educate the Consumers on the use of the new system, placing the newly developed system into production, confirming the data required at the start of operations is available and accurate, and validating that business functions that interact with the system are functioning properly. Responsibilities involves changing from a system development to a system support and maintenance mode of operation, with ownership of the new system moving from the Paper Team to the Performing Organization. System implementation is the important stage of paper when the theoretical design is tuned into practical system. The main stages in the implementation are as follows:

- Planning
- Training
- System testing and
- Changeover Planning

Any system people may implement the time from different departments and system analysis involve. To practical problem of controlling various activities of people outside their own data processing departments to confirmed. An implementation coordinating committee to control the line manager

- The implication of system environment
- Self-selection and allocation form implementation tasks
- Consultation with unions and resources available
- Standby facilities and channels of communication

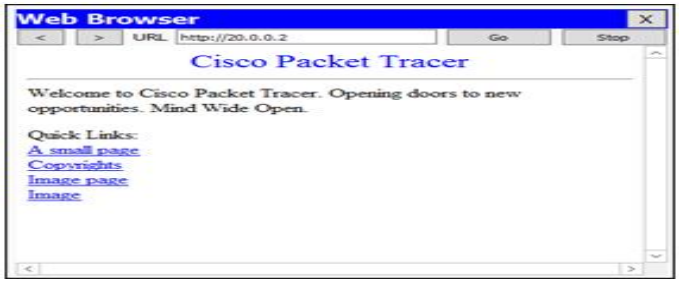


Figure-3: Verification of Router

ISSN 2394 - 7780

II. CONCLUSIONS

To filter traffic within a routed network is a critical network security practice the use of access control lists. To monitor ACLs vulnerable ports and block known malicious traffic at key points within a network to provide a network administrator. A network is a key part of the first line of defense to access control lists in place at the ingress and egress point. The network edges reduce many of the risks associated with direct network attacks to filtering strategy in place.

Access control lists in place at the WAN and LAN level against compromised or infected systems from attacking vulnerable systems on other subnets or at other sites.

There should be several access control lists in the router's configuration for use on a daily basis, or waiting to be used to block infected hosts or malicious traffic.

Network security administrators should be aware of the current vulnerabilities so that ACL's can be updated and waiting in a router's configuration before an actual attack begins. This practice can help isolate an attack quickly and save hundreds of man hours that would be required to battle a full scale outbreak[9] [10].

REFERENCES

1. T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing of Encrypted wireless ad hoc networks. In Proceedings of MobiHoc, pages 120–130, 2006.
2. M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormholebased antijamming Techniques in sensor networks. IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.
3. A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In Proceedings of ISIT, 2007.
4. T. Dempsey, G. Sahin, Y. Morton, and C. Hopper. Intelligent sensing and classification in ad hoc networks: a case study. Aerospace and Electronic Systems Magazine, IEEE, 24(8):23–30, August 2009.
5. Y. Desmedt. Broadcast anti-jamming systems. Computer Networks, 35(2-3):223–236, February 2001.
6. K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES. Cryptographic Engineering, pages 235–294, 2009.
7. O. Goldreich. Foundations of cryptography: Basic applications. Cambridge University Press, 2004.
8. B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In Proceedings of MobiSys, 2008.
9. IEEE. IEEE 802.11 standard. http://standards.ieee.org/getieee802/ download/802.11-2007.pdf, 2007.
10. A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In Proceedings of NDSS, pages 151–165, 1999.
11. Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer jamming attacks against WSN MAC protocols. ACMTransactions on Sensors Networks, 5(1):1–38, 2009.
12. L. Lazos, S. Liu, and M. Krunz. Mitigating controlchannel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2nd ACM conference on wireless network security, pages 169– 180, 2009.
13. G. Lin and G. Noubir. On link layer denial of service in data wireless LANs. Wireless Communications and Mobile Computing, 5(3):273–284, May 2004.
14. X.Liu, G. Noubir, and R. Sundaram. Spread: Foiling smart jammers

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

STUDENT'S FEEDBACK SYSTEM

Dr. V. Kavitha[1], P. Hemashree[2] and Ram Kumar[3]
Associate Professor[1], Assistant Professor[2] and Student[3], PG & Research Department of Computer Applications, Hindusthan College of Arts and Science, Coimbatore

ABSTRACT
Nowadays, educational Institutions are paying increasing attention to the views of Student's on the involvement in learning and teaching through reviews or feedback. Online Feedback System is a web application which provides base for the schools/colleges to conduct student's feedback online. The goal of the study was to develop an all in one feedback system serving both students and teachers. The system comprises of generation and analysis of teacher's feedback pages, summary, and a delivery of feedback. The system is developed for the all college students and staff members Also Students can give opinion about their faculty members. The student has to choose from excellent, very good, good, satisfactory, and poor. Then after attempting every question has to submit his feedback with the system. This online feedback system is the perfect place to find feedback evaluated according to the requirements and it is the efficient one to get feedback analysis of students and staffs.

Keywords: Feed back, Admin Login, Time Saver

I. INTRODUCTION

In today's world of online interaction, electronic education is becoming an important, of the academic domain. Faced with the strong growth of popularity of online courses, a need arises for a flexible, strengthened & easily integrated online academic feedback delivery system The 'Feedback management System' Approaches all about institutional and educational practices and processes that are taken into consideration, the student's concerns of the level of the knowledge they receive. This procedure explains that there is a good relationship between the students learning environment and teachers.The system developed faculty feedback system to provide feedback in an easy and consistent manner to the college HOD or principal. The system is referred as faculty feedback system which delivers via student and staffs interface as online system which is acting as Service Provider.The 'Feedback System' Approaches all about institutional practices and processes that are taken into consideration, the student's concerns of the level of the knowledge they receive. The College Feedback System is a management information system for education establishments to manage student data. An Online Student Feedback System is an automatic feedback generation system that provides the proper feedback to the teachers as per the categories like always, poor, usually, very often, sometimes.

ADVANTAGES

The key features and advantages of online feedback system are listed below:

1) Cost-efficiency: using this system reduces the cost of paper and in person surveys which are conducted also the administration cost is reduced.

2) Time saver: feedback software saves a lot of time and effort. Through this system, you can quickly generate, collect and examine surveys. Performing all of these functions in one integrated web system saves you a extensive amount of time.

3) Convenience: It is very convenient for users to complete online surveys. Participants can fill out forms when they choose to and start and stop a survey at their ease.

4) Accessibility: Administering your surveys through an online system increases accessibility. Link of the survey can be sent via Gmail or any other social networking platform. Respondents then have a variety of ways to access the forms including mobile phones, laptops, tablets, computers, etc.

5) Reach & Scalability: One of the greatest advantages of using online surveys is the reach and scalability. You can send surveys to thousands of people at the same time you take to send survey to single person. Also you can send surveys across the world and create forms in different languages.

6) Flexibility: Online surveys provide more flexibility in the design. in manual system participants can skip question but here this is not possible since every field is mandatory therefore the form will not get submitted till each and every questions are attempted.

7) Anonymity: here admin also cannot view that which feedback was submitted by which student. With this feature student can give honest feedback without disclosing their identity.

ISSN 2394 - 7780

8) More Accurate: Since it is computer generated report the calculation error which generally comes in manual is reduced and hence providing you with more accurate reports.

9) Results: As soon as student has completed the form, principal can view and analyze the reports. Through an online feedback management system, data can be presented in formats like percentage, graphs, pie charts, etc.

II. MODULES

- STUDENT MODULE
- FACULTY MODULE
- ADMIN MODULE

MODULES DESCRIPTION

STUDENT MODULE

First, the student has to register. Only registered Student will log in by his username and password. . In the dashboard all the contents of the student's feedback forms will be displayed. There would be an option student feedback in this there would be questions related to how students can make the teaching quality better. Student can tell his likes and dislikes about the teachers by attending every questions.

FACULTY MODULE

Here faculty will first login in this section. The faculty will enter their user name and password if the faculties do not have an account they have to sign up in order to create an account. As the details are filled the faculty dashboard appears in which they can fill self appraisal, peer appraisal. The faculty should firstly fill the self appraisal in which they Have to rate themselves on some criteria. The peer faculty has to click onto the peer appraisal in order to fill the form as they click onto peer appraisal.

- **ADMIN MODULE**

The user cannot sign up for the feedback system since she is the only one to access the feature the login is predefined in code itself. Once the admin login into her portal she can perform various tasks like Giving authority appraisals also reviewing form no one which is duly filled by faculty after verifying that only then the HOD can further proceed with the summary form. In summary, the total of all marks will be calculated and according to it percentage is calculated also the grades are calculated on this percentage basis also the user can take print out of the summary list and keep a backup of it.

III. INPUT & OUTPUT DESIGN

HOME PAGE

The home page of student feedback system is shown below which includes the Login and Registration form. Moreover the details of feedback system is explained in this form.

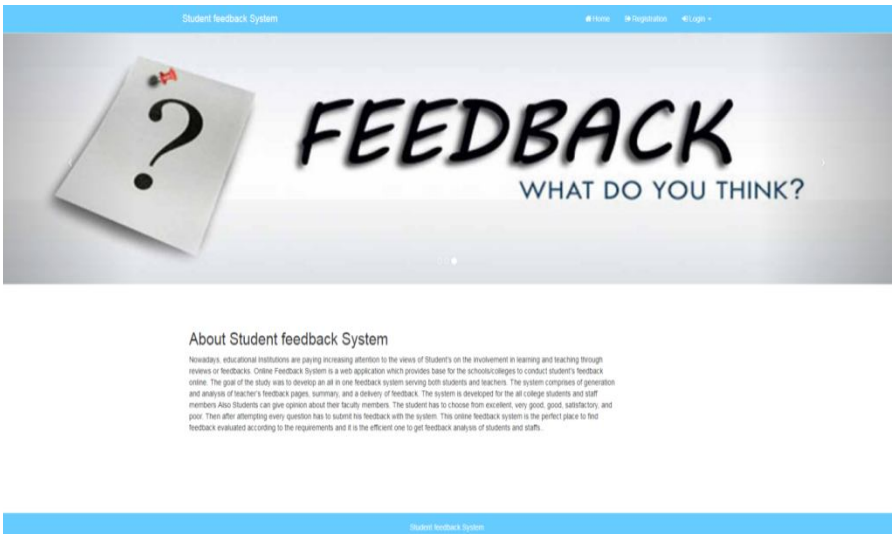


Fig-1: HomePage

REGISTERATION

In registration form have some of the queries about student like name of the student, Email id, password, Mobile number, Class, Semester, Gender, Hobbies, Date of birth and Image of the student. After feeding all the details of the students then that data should be stored in the student database.

ISSN 2394 - 7780

Fig-2: Registration Form

STUDENT LOGIN

In student Login form required to details of student Login id, Password, Captcha and Forgot password.

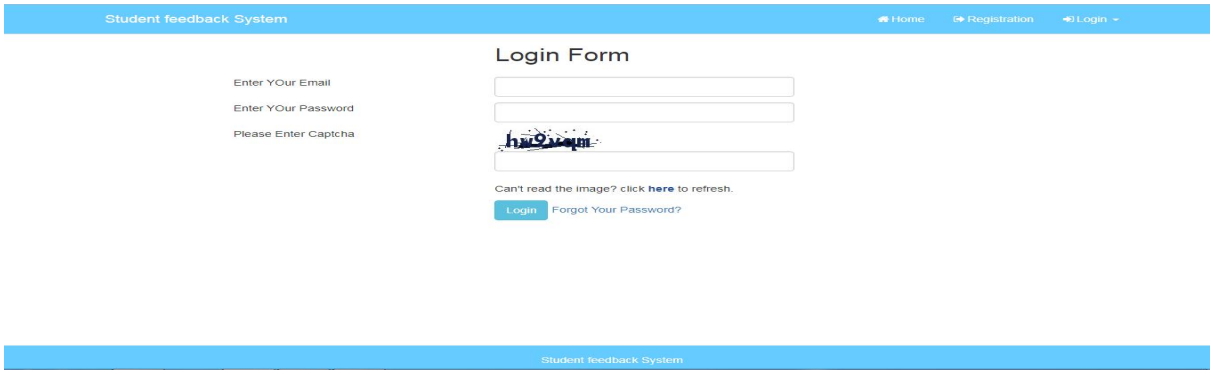


Fig-3: Student Registration Form

Student Feedback Form

In student feedback form having five options respectively

- Strongly Agree
- Agree
- Neutral
- Disagree
- Strongly Disagree

The student should select the faculty name and any one of the above option. The student should give the feedback by three major parts respectively

1. Course Material
2. Class Teaching
3. Class Assessment

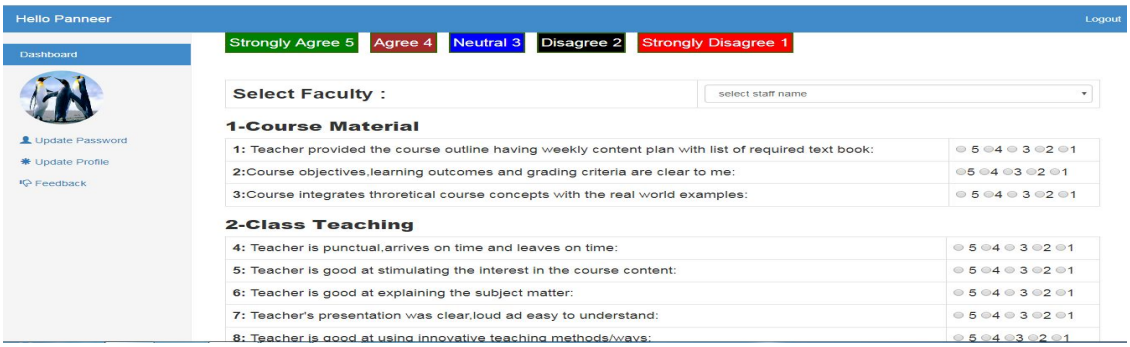


Fig-4: Students Feedback Form

ISSN 2394 - 7780

Faculty Feedback View

Using Faculty Feedback View form, the faculty can view their performance according to the above said students feedback queries. Hence the staff member can measure themselves moreover the name of the student must be hidden from the faculty view point.

Sr.No	Teacher	Quest1	Quest2	Quest3	Quest4	Quest5	Quest6	Quest7	Quest8	Quest9	Quest10	Quest11	Quest12	Quest13
1	rav@gmail.com	5	5	5	5	5	5	5	5	5	5	5	5	ddddddddddddd
2	rav@gmail.com	5	3	1	5	5	3	3	3	3	5	5	5	
3	rav@gmail.com	5	5	5	2	1	5	5	4	5	5	5	5	dfdfdfdfdfd
4	rav@gmail.com	5	5	3	5	5	5	5	5	5	5	5	5	test

Fig-5: Faculty Feedback View

Admin Login

In Admin Login form required to details of student Login id, Password, Captcha.

Admin Dashboard

Using admin dashboard, the admin can take report of the entire student feedback system. The Admin Dashboard contains the following

- Total Number of Faculty
- Total Number of Students
- The number of feedback given by the students

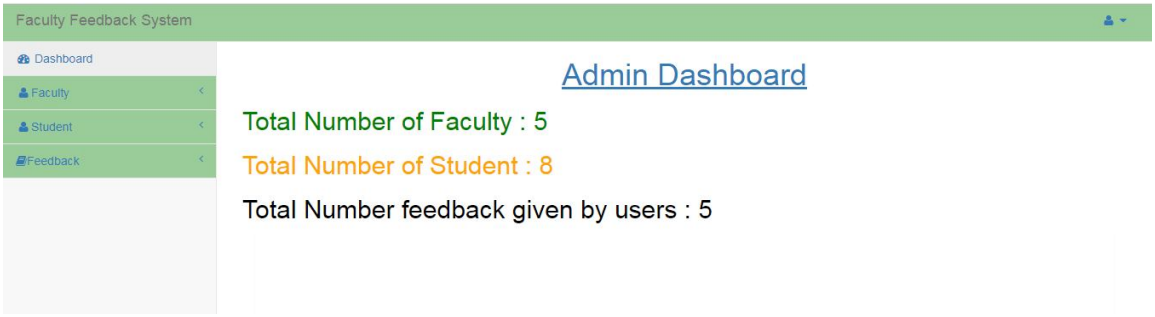


Fig-6: Admin Dash Board

Add Faculty

Using add faculty form can able to include the details of the staff members Name, Designation, Mail id, Password, Program and Semester. After collecting the details from the faculty member that will stored in the faculty database table.

Fig-7: Add faculty form

View Faculty

Using this view faculty form, the details of the faculty members report will be generated

S.No	Name	Designation	Programme	Semester	User Name	Email	Mobile	Password	Update	Delete	Status
1	ravi	Associate Professior	B.Tech	vi	ravm5454	rav@gmail.com	9015501897	ravi			
2	sanjeev kumar	Developer	B.tech	ii	sanj9015	sanjeevtech2@gmail.com	9015501897	2ddea1			
3	sanjeev kuma	aaaa	B.tec	i	sanj9015	sanjeevtechh2@gmail.com	901550189	dfdfd			

Fig-8: View Faculty Form

ISSN 2394 - 7780

View Student

Using this view student form, the details of the student's report will be generated.

Fig-9: View Student Form

View Feed Back

Using this view Feedback form, the details of the overall feedback report will be generated.

Fig-10: View Feedback Form

Feed Back Average

Student feedback average report will produce the overall performance of the concern staff members like the feedback matrices of Strongly Agree, Agree, Neutral, Disagree, Strongly disagree

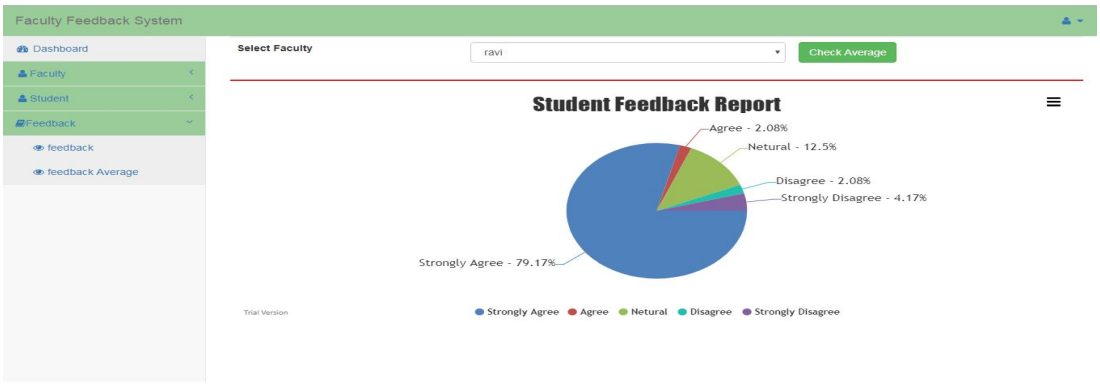


Fig-11: Student's Feedback Report

IV. CONCLUSIONS

In today's world where education has become a basic necessity for every child/adult so to ensure that proper education Is being delivered or not their lefts only one way 'by taking feedback' so as to reduce the manpower the software is build which automatically takes the feedback turn by turn so as to not skip any of the member.

The 'Feedback System' Approaches all about educational and institutional practices, the student's concerns about the knowledge they are being given.

REFERENCES

1. https://www.scribd.com/document/35586210/Eproperty-Paper-Report
2. http://www.waikato.ac.nz/tdu/pdf/booklets/6_AssessmentFeedback

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

REVIEW ON ANALYSIS OF ROUTING ALGORITHMS FOR WIRELESS SENSOR NETWORKS

M. Prakasam and M. Jhanani
Assistant Professor, Department of Computer Science (PG), K. S. Rangasamy College of Arts and Science (Autonomous), Tiruchengode, Tamilnadu

ABSTRACT
Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. The major challenge of the WSN seems to be the energy utilization and as a consequence the decline of the lifetime of the sensor nodes. This survey paper addresses the problem of the energy drain in the sensor nodes lifetime, which as a result it ends up in the nodes death. Wireless sensor networks are deployed widely in sensitive applications like health care, surveillance and e-commerce domains. In computer science and telecommunications, wireless sensor networks are an active research area with numerous workshops and conferences arranged each year, for example IPSN, SenSys, and EWSN. Providing such a low-energy, ad hoc, distributed protocol will help pave the way for imminent micro sensor networks.It improves the efficiency of the energy consumption along with the improvement of the node lifetime values. The proposed strategy helps in improving the dynamic updating of the routing table, which may overcome the problem of the dead node sensing and cluster head value updating.

Keywords: Wireless Sensor Network, Routing Algorithm

I. INTRODUCTION

Wireless network set up is done by using radio signal frequency to communicate between computers and other network devices. A wireless network enables people to link and access applications and information without wires. It provides freedom of movement and the ability to spread applications to different parts of office block, city, or nearly anywhere in the world. Wireless networks allow people to interact with e-mail or look through the Internet from a location that they prefer [9].

Many types of wireless communication systems are also available here, but a unique attribute communication takes place among computer devices. Computer devices have PCs, memory, and a means of interfacing with a specific type of network. Old-style cell phones don't fall within the meaning of a computer device; however, fresher phones and even audio headphones are beginning to join computing power and network adapters. Eventually, most electronics will suggest wireless network connections.

A computer network is a group of computer systems and other computing hardware devices that are linked together through the communication channels to ease of communication and resource-sharing and file sharing among a wide range of users. Networks are commonly categorized based on their characteristics. A Wireless sensor network can be defined as a network of devices that can communicate the information gathered from a monitored field through the wireless links. The data is forward through multiple nodes, and with a gateway, the data is connected to other networks like wireless Ethernet. Commonly monitored parameters and temperature, pressure, humidity, wind direction and speed, illumination intensity, vibration intensity, sound intensity,, chemical, power-line voltage, concentrations, pollutant levels and vital body functions[10].

II. LITERATURE REVIEW

Radio Sleep Mode Raja Jurdak et.al [1]: Energy efficiency is a middle challenge in sensor networks, and the radio is a major contributor to over all energy node utilization. Current energy efficient for MAC protocols used for sensor networks use a set low power radio mode for putting the radio to sleep. This paperproposes adaptive radio low-power sleep mode based on current traffic conditions inside the network. It first introduces a comprehensive node energy model, which includes energy components for radio switching, transmission, response, listening, and sleeping, as well as the often disregarded microcontroller energy component for determining the optimal sleep mode along with MAC protocols to use for specified traffic scenarios. This paperhas proposed adaptive radio sleep modes as an energy optimization system for wireless sensor networks.

Mobile Data Gathering MiaoZhao et.al [2]: Recent advances have shown a great potential of mobile data gathering in wireless sensor networks, where one or more mobile collectors are employed to collect the data from sensors using short-range of communications. Among several of data gathering approaches, one typical scheme is called anchor-based mobile data gathering. In this paper, we focus on such adata gathering method and provide distributed algorithms to achieve its optimal performance. We consider

ISSN 2394 - 7780

two different cases depending on whether themobile collect or has fixedor variable stay timeateachanchor point. Finally, we provide extensive numerical results to demonstrate the usage and efficiency of the proposed algorithms and set off our theoretical analysis.

RoutingDesigninWirelessSensorNetworks Peng Guo, XuefengLiu et.al [3]:In many domain-specific monitoring applications of wireless sensor networks (WSNs), such as structural health monitoring, volcanotomo graphy, and machine diagnosis, the raw datain WSN sarerequired to be listlessly gathered to the sink, where a focused centralized algorithm is then executed to extract some global features or model parameters. We present a series of novel routing schemes customized for different cases of computation results. The work in this paper can also serve as a guideline for distributed computing of big data, where the data spreads in a large network.

Ant Colony Optimization Yongjun Sun et.al [4]:In order to find the optimal path of data transmission in the WSNs, anewrouting algorithm based on antcolony algorithm is proposed. Using the improved heuristic function and considering the node communication transmission distance, transmission direction, and residual energy, an optimal path from the source node to the destination node can be found Simulation results show that newant algorithm can effectively save the energy of node sandprolong the network lifetime. The simulation results indicate with the purpose of bycomparing with EEABR, Leach-Antand OARA, the method proposed in the paper obviously minimizes the average energy consumption and extends the life cycle of the wireless sensor network.

Network-on-Chip Liang Wang et.al [5]: Technology scaling leads to the reliability issue since a primary concernin Network-on-Chip (NoC) design. We observe that due to routin galgorithmroutersage much faster than others which become a bottleneck for NoC life time. In this paper, network on chip paper lifetime is model edasaresourceconsumed overtime. Ametric lifetime budget is associated with each router, indicating the maximum allowed workload for current period. Since the heterogeneityinrouter life time reliability has strong correlation with the routingalgorithm, we define aproblemtooptimize the lifetime by routing packets along the path with maximum lifetime budgets.

Flexibility: Froehle et.al [6] gives plan concerning analysis on WBAN for area that provides safety of future astronaut throughout area Exploration, advance health industry and technology. In the spacesuit health watching system, Bluetooth module and sensors should be enforced on the interior aspect of the pressure suit to with efficiency live important signal and to shield instrumentation from worst surroundings and antenna must be connected to the Bluetooth. In the simulation Perfect Electric Conductor (PEC) was used because the ground plane material that improves the antenna output however having air gap is downside in pressure suit therefore to decrease this gap a folded ground style was enforced.

Smart BAN: Tuomas Paso et.al [7] proposed a plan concerning the European level customary idea for rational wireless body area networks. Smart BAN idea is mainly based on the heterogeneous multi-radio approach and Smart BAN hub act as a connection between devices operative with totally dissimilar radio standards. The planned knowledge model is divided into 3 main parts: BAN, Nodes, Process and Measurements. A Smart BAN is acknowledged with the aid of its BANID that ought to be typical and available by any licensed user. The Smart BAN is using 2 entirely different channels: a control channel, a data channel. At last we could say that Smart BAN is employed for monitoring specific phenomena[9].

Decrease of Transmission Delay: Kim *et.al* [8] a MAC protocol that apply on the delay restriction to MAC Protocol in medical hint observation to scale reverse the packet loss and time delay in TDMA primarily based on the CSMA/CA background. The papered MAC Protocol's inspector frame has similar sort and constitution as Bio MAC protocol super frame. The proposed Method's aim is to lessen delay as a result it is named DTD-MAC (Decrease of Transmission Delay). The paper WBSN environment is established as star and computer simulation is conducted in static atmosphere inside which assortment of knob devices doesn't have an improvement. DTD-MAC Protocol is efficient additional than Bio-MAC.

Table-I: Summary of Literature Review

S. No	Title	Author Publisher and Year	Working Platform	Objective	Future Scope
1	Radio Sleep ModeOptimization inWireless SensorNetworks	Raja Jurdak,Member, IEEE,[2010]	Wireless SensorNetworks	radioisamajorcontributor tooverallenergy node consumption	Thispaperhasproposedadaptiveradio sleep modesasan energy optimization systemfor wireless sensor networks

2	Optimization-Based Distributed Algorithms for Mobile Data Gathering in Wireless Sensor Networks	Miao Zhao, Member, IEEE, [2012]	Mobile Data Gathering	Among a variety of data gathering approaches, one typical scheme is called anchor-based mobile data gathering	Finally, we provide extensive numerical results to express the usage and efficiency of the proposed algorithms.
3	Lossless In-Network Processing and Its Routing Design in Wireless Sensor Networks	Peng Guo, IEEE [2017]	Wireless sensor network (WSN), in-network processing, matrix computation, routing scheme.	many domain-specific monitoring applications of wireless sensor networks (WSNs), such as structural health monitoring,	The work in this paper can also serve as a guideline for distributed computing of big data, where the data spread is a nalarge network.
4	An Improved Routing Algorithm Based on Ant Colony Optimization in Wireless Sensor Networks	Yongjun Sun, IEEE, [2017]	Wireless sensor networks, routing algorithms, ant colony optimization, energy consumption, network lifetime	Data routing in energy constrained wireless sensor networks (WSNs) is one of the key points.	Proposed in the paper obviously minimizes the average and energy consumption and extends the life cycle of the wireless sensor network.
5	Adaptive Routing Algorithms for Lifetime Reliability Optimization in Network-on-Chip	Liang Wang, IEEE, [2016]	Routing algorithm, network-on-chip, lifetime reliability, dynamic programming	Technology scaling leads to the reliability issue as a primary distress in Network-on-Chip (NoC) design.	In this paper, we proposed dynamic programming-based lifetime aware routing algorithms for NoC reliability management
6	Flexible Antenna for Wireless Body Area Network	Froehle et.al [6] IEEE [2015]	Flexible Antenna	Next generation spacesuit 2 (NDX-2).	Decrease the air gap between the substrate and ground plane.
7	Etsi Tc Smartban	Tuomas Paso et.al [7] IEEE [2015]	PHY and MAC layers	SmartBAN	Wearable or implantable SmartBAN devices are expected to operate more frequently in specific types of environment.
8	An Effect of Delay Reduced Mac Protocol for WBAN Based Medical Signal Monitoring	Kim et.al [8] IEEE [2015]	MAC protocol	DTD-MAC(Decrease of Transmission Delay)	It is necessary to derive the improved approach to guarantee the stable QoS in a dynamic environment where bio sensor nodes are added and more tight performance requirement.

VI. SUMMARY

In this paper, novel constellation based wan clustering protocol is proposed for the wireless sensor networks. It improves the efficiency of the energy consumption along with the improvement of the node lifetime values. The proposed strategy helps in improving the dynamic updating of the routing table, which may overcome the problem of the dead node sensing and cluster head value updating.

VII. CONCLUSION

Compared with communication protocols, in terms of energy indulgence, ease of formation, and system epoch/quality of the network. Providing such a low-energy, ad hoc, distributed protocol will help pave the way for imminent micro sensor networks. It is evident from the MATLAB simulation that the proposed system works well efficient to cope up with energy efficient and novel clustering. In this research, novel constellation based wsn clustering protocol is proposed for the wireless sensor networks. It improves the efficiency of the energy consumption along with the improvement of the node lifetime values. The proposed strategy helps in improving the dynamic updating of the routing table, which may overcome the problem of the dead node sensing and cluster head value updating. It is evident from the simulation that the proposed system works well

ISSN 2394 - 7780

efficient to cope up with energy efficient and novel clustering. It is concluded that the proposed system performs well in terms of the metrics considered

REFERENCES

1. AhmedE.A.A.Abdulla."Hymn:ANovelHybridMulti-HopRouting AlgorithmToImproveTheLongevityOf Wsns"IEEETransactions OnWirelessCommunications,Vol.11,No.7,July2012.
2. MiaoZhao,"Optimization-BasedDistributedAlgorithmsForMobileData Gathering InWireless SensorNetworks" IEEETransactionsOnMobileComputing, Vol.11, No.10, October 2012.
3. PengGuo,"LosslessIn-NetworkProcessingandItsRoutingDesignInWirelessSensorNetworks"IEEE Transactions OnWirelessCommunications,Vol.16,No.10,October2017.
4. [4] YongjunSun,"AnImprovedRoutingAlgorithmBasedOnAntColonyOptimizationinWirelessSensor Networks" IEEECommunicationsLetters,Vol.21,No.6,June2017.
5. Liang Wang, Xiaohang Wang "AdaptiveRoutingAlgorithmsForLifetimeReliability OptimizationInNetwork-On-Chip" IEEETransactionsOnComputers, Vol.65, No.9, September2016.
6. Froehle, Patrick, Tyler Przybylski, Christopher McDonald, Milad Mirzaee, Sima Noghanian, and Reza Fazel-Rezai. "Flexible Antenna for Wireless Body Area Network." In Antennas and Propagation & USNC/URSI National Radio Science Meeting, 2015 IEEE International Symposium on, pp. 1214-1215. IEEE, 2015.
7. Hamalainen, Matti, Tuomas Paso, Lorenzo Mucchi, Marc Girod-Genet, John Farserotu, Hirokazu Tanaka, Woon Hau Chin, and Lina Nachabe Ismail. "ETSI TC SmartBAN: Overview of the wireless body area network standard." In Medical Information and Communication Technology (ISMICT), 2015 9th International Symposium on, pp. 1-5. IEEE, 2015.
8. Kim, Rae Hyun, Pyung Soo Kim, and Jeong Gon Kim. "An effect of delay reduced MAC protocol for WBAN based medical signal monitoring." In Communications, Computers and Signal Processing (PACRIM), 2015 IEEE Pacific Rim Conference on, pp. 434-437. IEEE, 2015.
9. Dr.S.Prema., Anisha M D,2017, "Enhanced Unwavering Routing for Optimized Throughput Algorithm (Eurota) In Wireless Body Area", International Advanced Research Journal in Science, Engineering and Technology, ISSN (Online) 2393-8021, ISSN (Print) 2394-1588, Vol. 4, Issue 10, October2017.
10. Dr.S.Prema, Arunkumar.A, "A Comprehensive Evaluation and Analysis of Routing Algorithms for Wireless Sensor Networks", International Journal of Advanced Research in Computer and Communication Engineering (IJARCCE), ISSN (Online) 2278-1021, ISSN (Print) 2319-5940, Vol. 7, Issue 11, November 2018

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

24/7 LIVE PATIENT HEALTH TRACKING SYSTEM USING IOT PROTOCOL

S. Lakshmipriya
Assistant Professor, PG and Research Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore

ABSTRACT
This paper will help to understand the developments of research on IOT to eradicate or minimize the Medical detection errors. IOT is a recent communication Technology, in which the objects of everyday life will be equipped with arduino family of microcontrollers, transceivers for digital communication and suitable protocol stacks, that will make them able to communicate with one another and with the users.In the recent development of, internet of things (iot) makes all objects interconnected and it has been recognized as the next technical revolution. One such application is in healthcare to monitor the patient health status internet of things makes medical equipments more efficient by allowing real time monitoring of patient health, in which sensor acquire data of patient's and reduces the human error.

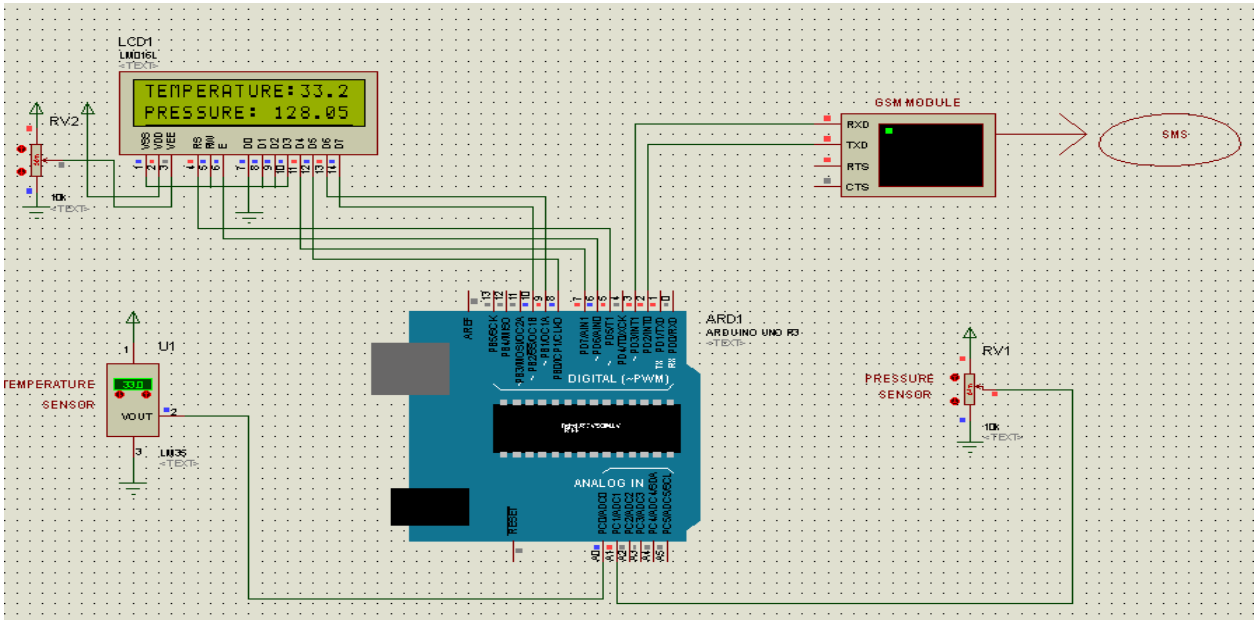
I. INTRODUCTION
In internet of things patient's parameters get transmitted through medical devices via a gateway, where it is stored and analyzed. The significant challenges in the implementation of internet of things for healthcare applications are monitoring all patient's from various places. Thus internet o things in the medical field brings out the solution for effective patient monitoring at reduced cost and also reduces the trade-off between patient outcome and disease management. In our paper we have taken parameters like, monitoring patient's body temperature, heart beat and body pressure using arduino microcontroller.The 24 hours health monitoring operation is achieved with the experimental results.

II. EXISTING METHODOLOGY
Internet of Things (IoT) is a new technological paradigm that can connect things from various fields through the Internet. For the IoT connected healthcare applications, the wireless body area network (WBAN) is gaining popularity as wearable devices spring into the market. This paper proposes a wearable sensor node with solar energy harvesting and Bluetooth low energy (BLE) transmission that enables the implementation of an autonomous WBAN. Multiple sensor nodes can be deployed on different positions of the body to measure the subject’s body temperature distribution, heartbeat and detect falls. A webbased smartphone application is also developed for displaying the sensor data and fall notification. To extend the lifetime of the wearable sensor node, a flexible solar energy harvester with an output based maximum power point tracking (MPPT) technique is used to power the sensor node. Experimental results show that the wearable sensor node works well when powered by the solar energy harvester. The autonomous 24 hours operation is achieved with the experimental results. The proposed system with solar energy harvesting demonstrates that long-term continuous medical monitoring based on WBAN is possible provided that the subject stays outside for a short period of time in a day. Index Terms—Internet of things, wireless body area network,energy harvesting, maximum power point tracking, Bluetooth.

III PROPOSED SYSTEM
In this PAPER, we are going to make an “24/7 LIVE PATIENT HEALTH TRACKING SYSTEM USING IOT PROTOCOL” which will tell us about the health status of the patient who age above 40 year and are suffering from high blood pressure or hyperthyroidism. Through the web server we can know the status of your patient anywhere in the world over the internet .Here pressure sensor is used for detecting Blood pressure of the patient.temperature sensor is used for detecting body temperture of the patient. Here we are using Arduino uno R3 which consists of master and slave unit. The sensor will check the level of Body Temperature/Blood Pressure and send it to slave unit and further send the data to master unit which at last send a message to the doctor.

ISSN 2394 - 7780

RESULT



CONCLUSION

IoT changes the way the facilities are delivered to the healthcare industry. These technologies improve the product, causing a larger effect by bringing together minor changes. Healthcare devices are becoming popular in various fields from sport and fitness to health monitoring. In particular, due to the increasing elderly population throughout the world, wearable devices are becoming important for long-term health monitoring. The main aim of this work was to give a comprehensive overview of this area of research and to report the full range of tools in area of wearable health monitoring devices. In this review paper, we have reported both research works and commercial devices to study and investigate the currently available technology. In preparing this paper, we studied the literature from various points of view. Based on consultation with expert scientists in environmental engineering and medicine, we believe that, motion trackers, gas detectors, and vital signs are the most important elements in health monitoring; therefore, to achieve the full range of health monitoring, all these parameters were studied. In each field, a variety of methodologies are employed, but not all are efficient and effective. The most important criteria in this study was the possibility of using the device in the real world, performance, efficiency, and power consumption. In addition, we considered the price of each device. Finally, the most challenging bottleneck and some conclusions regarding the promising future in the IoT is presented.

REFERENCES

1. https://www.ida.gov.sg/~/media/Files/Infocomm%20Landscape/Technology/TechnologyRoadmap/InternetOfThings.pdf
2. Dr. OvidiuVermesan SINTEF, Norway, Dr. Peter FriessEU, Belgium, “Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems”, river publishers’ series in communications, 2013
3. Dr. OvidiuVermesan SINTEF, Norway, Dr. Peter FriessEU, Belgium, “Internet of Things–From Research and Innovation to Market Deployment”, river publishers’ series in communications, 2014.
4. O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, et al., “Internet of Things Strategic Research Agenda”, Chapter 2 in Internet of Things -Global Technological and Societal Trends, River Publishers, 2011.
5. Martin Serrano, Insight Centre for Data Analytics, Ireland ,Omar Elloumi, Alcatel Lucent, France, Paul Murdock, Landis+Gyr, Switzerland, “ALLIANCE FOR INTERNET OF THINGS INNOVATION, Semantic Interoperability” , Release 2.0, AIOTI WG03 –loT Standardisation,2015.
6. Dave Evans. April 2011. *The Internet of Things:How the NextEvolution of the Internet Is Changing Everything,* Cisco.
7. G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "*Smartobjects as building blocks for the internet of things,*"InternetComputing, IEEE, vol. 14, pp. 44-51, 2010.
8. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wirelesssensor networks: a survey, Computer Networks 38 (2002) 393–422.Tavel, P. 2007 Modeling and Simulation Design. AK Peters Ltd.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

PREDICTION OF STUDENT PERFORMANCE IN INTERVIEW USING KNOWLEDGE DISCOVERY TECHNIQUE

S. Balaji[1], B. Saranya[2] and S. Suhashine[3]
Assistant Professor[1], in CSE
[2,3]Mahendra Engineering College

ABSTRACT
Educational Data Mining is an emerging discipline, concerned with developing methods for exploring the unique and increasingly large-scale data that come from educational settings and using those methods to better understand students, and the settings which they learn in Whether educational data is taken from students' use of interactive learning environments, computer-supported collaborative learning, or administrative data from schools and universities, it often has multiple levels of meaningful hierarchy, which often need to be determined by properties of the data itself, rather than in advance. Issues of time, sequence, and context also play important roles in the study of educational data. The basic paper idea is to design a software that allows us to extract the student data from a large database. The database contains all the information about the students regarding educational details, personal information and skills. There are various categories to distinguish student's results. The data in educational institute is growing significantly. So there is a need for a model for extracting meaningful data from the student's database which helps for future predictions. This paper deals in predicting the student performance in interview and help them to improve their skills. This helps the instructors to monitor and assess the student's based on their capability. With this the student's recruitment level increases which helps the trainers to look after the students. With this the performance and ability of the students can be easily predicted and they can be analyzed in the earlier stages and can lead to further development.

Keywords: Data, Mining, Academics

I. INTRODUCTION
The data in educational system is growing significantly. It is very difficult to maintain these huge amount of data and to extract the necessary data. There is a model for educational database to extract the student's details to avoid any drop out from the school. The problem arises when the students and trainers did not know the cause for the low recruitment. This model helps the trainers to provide excellent way of teaching the students who are not able get placed in the company. This is the major problem nowadays and should be resolved in early and intervene. This helps the trainers and students to know their ability and performance as early as possible. Thus knowing these details can help the recruitment rate of the institution to increase in a certain rate which will be the main motive of the organization. This paper helps to analyze the current ability of the students and also provides ways to improve their performance in early stages.

II. SYSTEM ANALYSIS
The main objective of this paper titled "Prediction of student's performance in interview using knowledge discovery technique" is to enhance the student recruitment rates. It helps the students as well as the trainers to know their drawbacks and the ways to correct it. It also helps the trainers to know the student's weakness early and intervene. By knowing the student's level, the trainers can easily find a way to educate them without wasting time on other works. The model provides only the necessary training to be given to the students. It establishes ways to provide teaching based on students abilities. It helps the trainers and students to concentrate more on the weakness. By knowing the weakness, the trainers can easily find a way to rectify it and to make them bold to get placed in the company. This model is very efficient because it provides reliable outcomes that satisfies both the students and the trainers. There is a huge amount of data available in the Information Industry. This data is of no use until it is converted into useful information. It is necessary to analyze this huge amount of data and extract useful information from it. Data mining is the process of sorting through large data sets to identify patterns and establish relationships to solve problems through data analysis. Data mining tools allow enterprises to predict future trends.

III. SYSTEM STUDY
Currently using model is a data mining on prediction of student's performance based on their academics. This involves techniques that forecast student's progression status by analyzing student's data. The data from the learning system is a substantial indicator for monitoring of the potential student failure in the school. This helps in reducing the rate of student drop out from the school. The disadvantages of the existing system as follows:

- It is limited only with the school level.

ISSN 2394 - 7780

- Covers the students only based on the academics level.
- Does not concern about personal skills.

IV. PROPOSED SYSTEM

- This paper involves collection of data from the institution and storing it in a warehouse.
- The data which contains null or invalid values are preprocessed and cleaned.
- The classification algorithms are used to classify the data into appropriate classes.
- These classes are used to predict the ability of the student's recruitment in interviews.
- Then appropriate clustering algorithms are used to cluster the students based on their educational stuff.

V. SYSTEM ARCHITECTURE

Implementation is the stage of the paper when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The import of data is the automated or semi-automated input and output of data sets between different software applications. It involves "translating" from the format used in one application into that used by another, where such translation is accomplished automatically via machine processes, such as transcoding, data transformation, and others. True exports of data often contain data in raw formats otherwise unreadable to end-users without the user interface that was designed to render it.

VI.IMPORTING DATA SETS

The import of data is the automated or semi-automated input and output of data sets between different software applications. It involves "translating" from the format used in one application into that used by another, where such translation is accomplished automatically via machine processes, such as transcoding, data transformation, and others. True exports of data often contain data in raw formats otherwise unreadable to end-users without the user interface that was designed to render it.

VII.PREPROCESSING THE DATA

Data preprocessing is an important step in the data mining process. The phrase "garbage in, garbage out" is particularly applicable to data mining and machine learning papers. Data gathering methods are often loosely controlled, resulting in out-of-range values impossible data combinations (e.g., Sex: Male, Pregnant: Yes), missing values, etc. Analyzing data that has not been carefully screened for such problems can produce misleading results. Thus, the representation and quality of data is first and foremost before running an analysis. Often, data preprocessing is the most important phase of a machine learning paper, especially in computational biology.

VIII.CLASSIFYING DATA

A classification task begins with a data set in which the class assignments are known. For example, a classification model that predicts credit risk could be developed based on observed data for many loan applicants over a period of time. In addition to the historical credit rating, the data might track employment history, home ownership or rental, years of residence, number and type of investments, and so on. Credit rating would be the target, the other attributes would be the predictors, and the data for each customer would constitute a case. The simplest type of classification problem is binary classification. In binary classification, the target attribute has only two possible values: for example, high credit rating or low credit rating. Multi-class targets have more than two values: for example, low, medium, high, or unknown credit rating.

IX.CLASSIFICATION ALGORITHM:DECISION TREES

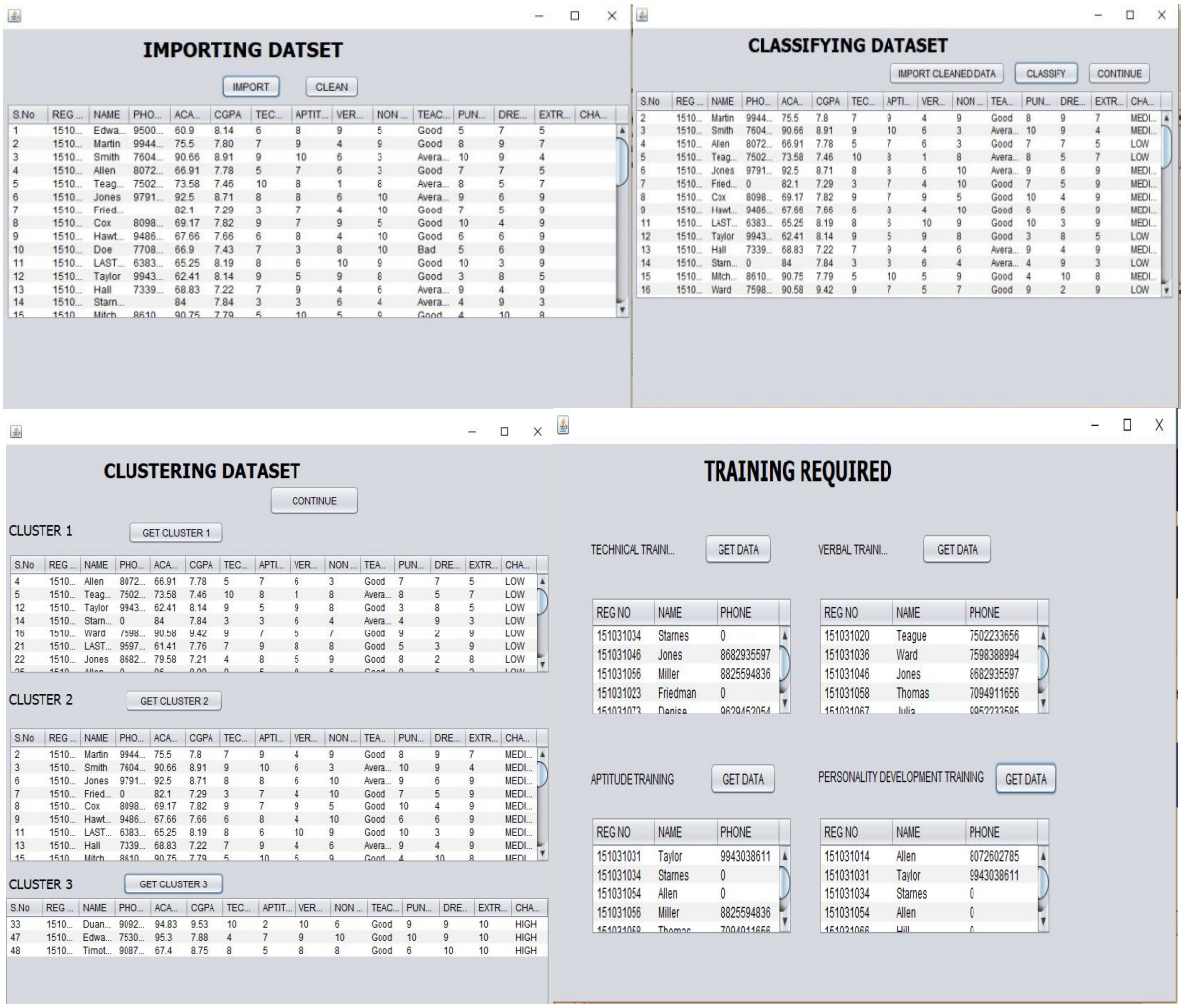
A decision tree is a decision support tool that uses a tree-like model of decisions and their possible consequences, including chance event outcomes, resource costs, and utility. It is one way to display an algorithm that only contains conditional control statements. A decision tree is a flowchart-like structure in which each internal node represents a "test" on an attribute (e.g. whether a coin flip comes up heads or tails), each branch represents the outcome of the test, and each leaf node represents a class label (decision taken after computing all attributes). The paths from root to leaf represent classification rules. Decision trees are commonly used in operations research and operations management. The decisions have to be taken online with no recall under incomplete knowledge, a decision tree should be paralleled by a probability model as a best choice model or online selection model algorithm. Another use of decision trees is as a descriptive means for calculating conditional probabilities.

ISSN 2394 - 7780

X.ANALYSING DATA SETS

Data Analysis is a process of collecting, transforming, cleaning, and modeling data with the goal of discovering the required information. The results so obtained are communicated, suggesting conclusions, and supporting decision-making. Data analysis is a process of applying statistical to organize, represent, describe, evaluate, and interpret data. The process of evaluating data using analytical and logical reasoning to examine each component of the data provided. Following data collection, the data needs to be critically analysed.

IMPLEMENTATION



XII.CONCLUSION

The data in educational institute is growing significantly. So there is a need for a model for extracting meaningful data from the student's database which helps for future predictions. This paper deals in predicting the student performance in interview and help them to improve their skills. This helps the instructors to monitor and assess the student's based on their capability. With this the student's recruitment level increases which helps the trainers to look after the students. With this the performance and ability of the students can be easily predicted and they can be analyzed in the earlier stages and can lead to further development.

REFERENCES

[1] Z. Ibrahim, D. Rusli, Predicting students academic performance: comparing artificial neural network, in: 21st Annual SAS Malaysia Forum, 5th September, 2014.

[2] U. bin Mat, N. Buniyamin, P.M. Arsad, R. Kassim, An overview of using academic analytics to predict students' achievement: 2013 IEEE 5th Conference on, IEEE, 2016, pp. 126-130.

[3] M. of Education Malaysia, National higher education strategic plan (2015).

[4] URL http://www.moe.gov.my/v/pelan-pembangunan-pendidikan-malaysia-2013-2025.

[5] Kalles D., Pierrakeas C., Analyzing student performance in distance learning with algorithms and decision trees, Hellenic Open University, Patras, Greece,2016.

ISSN 2394 - 7780

[6] Woodman, R. (2016). Investigation of factors that influence student retention and success rate on Open University courses in the East Anglia region. M.Sc. Dissertation, Sheffield Hallam University, UK.

[7] C. Romero S. Ventura "Educational data mining: A review of the state of the art" IEEE Trans. Syst. Man Cybern. C Appl. Rev. Vol. 40 pp. 601-618 Nov. 2017.

[8] International Educational Data Mining Society Jul. 2011[online] Available: http://www.educationaldatamining.org/.

[9] J. Ranjan K. Malik "Effective educational process: A data-mining approach" Vine vol.37 no.4 pp. 502-515 2017.

[10] J. Luan "Data mining applications in higher education" Proc. /spss Executive vol. 7 pp. 1-20 2018.

[11] S.H. Lin "Data mining for student retention management" J. Comput. Sci. Colleges vol.27 no. 4 pp. 92-99 Apr. 2018.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

EMPOWERING BIG DATA ANALYTICS FOR INDUSTRIAL TYPE–TELECOMTOWER UTLIZATION SCRUTINY

Teklay Teklu[1], S. Balaji[2] and Dr. S. Sasikala[3]
Head, Department of Information Technology, Adigrat University, Ethiopia
Assistant Professor, CSE, Mahendra Engineering College
Associate Professor, Department of Computer Applications, Hinduathn College of Arts and Science

ABSTRACT
This paper facilitates the analysis on Tower Utilization performance to support the transaction for updating and downloaded data, we are using Hadoop technology to fine tune the data for analysis. Tower utilization holds key to GIL earnings. The acquisition of tower utilization business has catapulted GTL Infrastructure (GIL) to the top slot in the domestic telecom infrastructure space. However, the key to its success is how effectively GIL increases utilization of its telecom towers.

The GIL management has indicated that the valuation of the all cash deal worth Rs 8,400 core to purchase 17,500 towers is among the cheapest in the sector. Its enterprise value stands at Rs 48 lakh per tower. For Tata Teleservices' tower business that was merged with Quippo Telecom earlier last year, EV/tower hovers at Rs 52 lakh, whereas for Bharti Infratel, it is close to Rs 2 crore. Another key parameter is tenancy ratio or the average number of tenants per tower

Keywords- Big Data, Industry, R, Hive

I. INTRODUCTION
Existing system for 'Tower Utilization Analysis' analysis is being managed with Excel tool. Every day data is being captured using excel sheet and prepared the quick analysis using Excel capabilities, Sort, Chart and Graphs. Now the proposed is to automate the data gathering from Remote Website and organize the data by suitable cleansing using PIG component and upload the fine-tuned data in HIVE for Adhoc reports and R for Prediction and decision making.**Os:Linux**

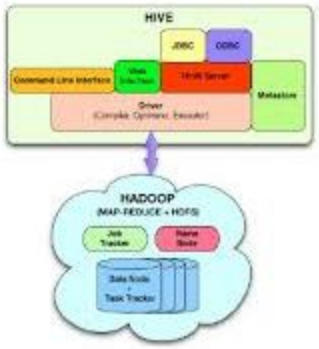
Hadoop
Apache Hadoop is a framework that allows for the distributed processing for the large datasets across clusters of commodity computers using a simple programming model. It is an open source Data management with scale-out storage and distributed processing

Apache Sqoop
Apache Sqoop is a tool for transferring data between Hadoop and relational databases. For example, you can use Sqoop to import data from a MySQL or Oracle database into HDFS.

ISSN 2394 - 7780

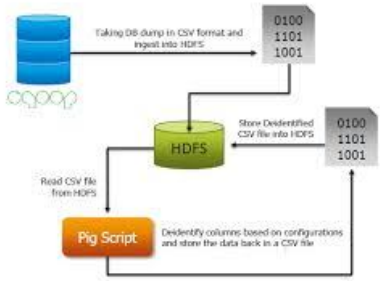
Hive

Hive is a tool that structures data in Hadoop into the form of relational-like tables and allows queries using a subset of SQL. Hive is a good tool for performing queries on large datasets, especially datasets that require full table scans. Hive can be used to support a tester who is interested in doing arbitrary queries to confirm values of calculated statistics or to run reasonableness tests across large swaths of data.



Pig

Apache Pig provides an alternative language to SQL, called Pig Latin, for querying data stored in HDFS. Pig does not require the data to be structured as tables, however, and can be more efficient than SQL if the queries involved require reuse of intermediate results. Pig comes with standard functions for common tasks like averaging data, working with dates, or finding differences between strings.

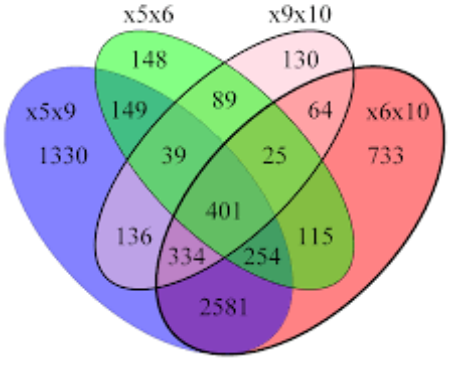


NoSQL

Not all Hadoop clusters use HBase or HDFS. Some integrate with NoSQL data stores that come with their own mechanisms for storing data across a cluster of nodes. This enables them to store and retrieve data with all the features of the NoSQL database, then use Hadoop to schedule data analysis jobs on the same cluster. Most commonly this means Cassandra, Riak or MongoDB, and users are actively exploring the best way to integrate the two technologies. 10Gen, one of the main supporters of MongoDB, for instance, suggests that Hadoop can be used for offline analyticswhile MongoDB can gather statistics from the Web inreal time.

R

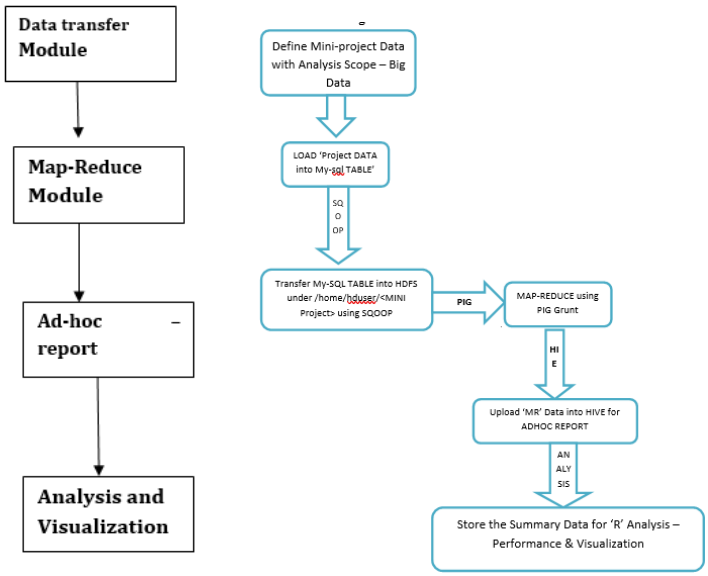
R is a programming language and software environment for statistical computing and graphics supported by the R foundation for statistical computing. The R language is widely used among statisticians



ISSN 2394 - 7780

II. SYSTEM ANALYSIS

System flow Diagram



System having 4 components:

- Data transfer Module
- Map-Reduce Module
- Adhoc – report Generation module
- Analysis and Visualization Module

Data copy using sqoop from my-sql into Hadoop

Data profile & Data Cleansing using Pig: Data profile table, 2 DC activities

Adhoc Reports using HIVE: 4 Reports

1. High & Low of Each stock
2. Monthly , weekly and yearly stock reports
3. Stock Trends using Plot(v, type="o", col-"blue")
4. Top performing Stock among 5
5. Analysis and Visualization using R: summary and charts.

III. SYSTEM IMPLEMENTATION

Pig Unit can help bring agility to your Hadoop practice; the same agility that JUnit, Testing and Respec bring to Java and Ruby communities. PigUnit tests offer assurance that your Pig scripts will run when the scripts change or when Pig's version changes in your environment. Imagine knowing, in a few minutes, how your entire portfolio of Pig papers will fare in a different Pig version or Hadoop distribution.

Unit testing is the Engineering rigor of software development and, for more than a decade, modern software development teams have been employing unit testing to ensure the quality of their products. Unit tests are the pieces of the code that execute individual units of the software under controlled conditions and verify the outcome against the expected results. If you run a Hadoop shop, Pig Unit can help you have that same Test Driven Development using Pig. The Pig Unit framework uses JUnit to run a Pig script or its parts under specified data conditions. The framework provides Pig with a 'data sandbox' created from the tuples specified in the test.This gives us two immediate advantages:

Rapid development: Pig scripts can run without needing a real cluster which speeds up the development cycle tremendously.

Identification of data conditions: Since Pig Unit tests can run under a narrow set of data conditions, developers become more cognizant about the nature of the data to expect in their Pig scripts.

ISSN 2394 - 7780

Development cost:

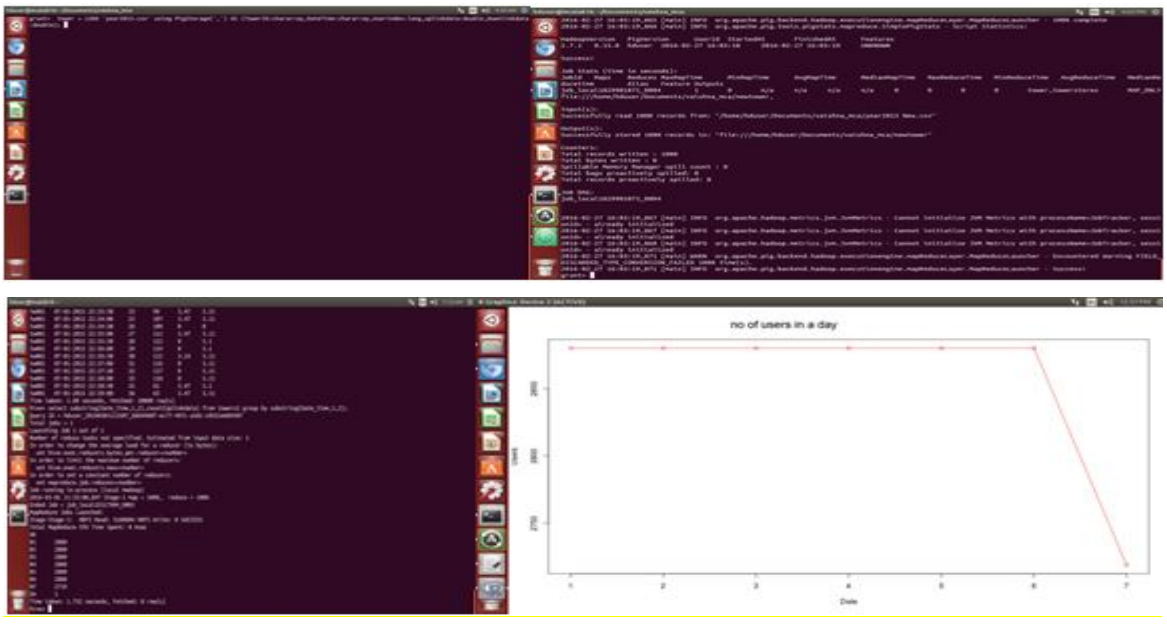
Item	Analysis & Design	Development	Testing	Implementation	Total Hrs	Cost (23$/Hr)
Data Gathering-sqoop	2	2	1	2	7	9660
Data Profiling /Cleansing – PIG	2	4	2	2	10	13800
Adhoc reports – Hive	4	8	2	2	16	22080
Analysis - R	1	2	1	2	6	8280

IV. CONCLUSION

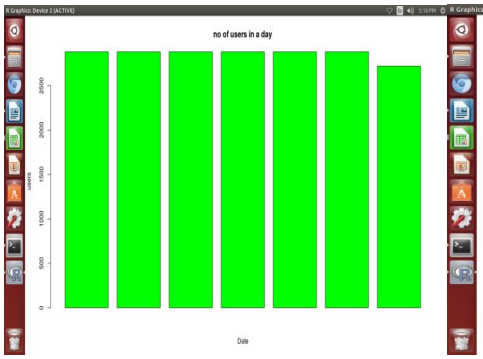
Big data is the reality and is going to stay there for a long time. It is important to note that the enterprises and telecom are taking big data seriously as the tower haven cognizance of the fact that tower utilization today is not more done in a protected environment and have to face the stiff competition not only from the public towers but also from the private and towers. The towers needs to continuously adopt new technologies and system to remain ahead of the competition and big data is going to be a boon for this. Big data, no matter how big is the buzz word, but has its own set of limitations when it comes to the ground realities. Each tower will have to analyze its own policy for adaptation of the same weaving the organizational culture together as it is one of the most important of the whole process. The example taken here clearly demonstrates the monetary benefits which could be achieved by adapting the big data and the investment in that would be a good move. Moreover, there would be a strong need for data driven decision making rather than intuitive decision making, which is the bottom line of the big data.

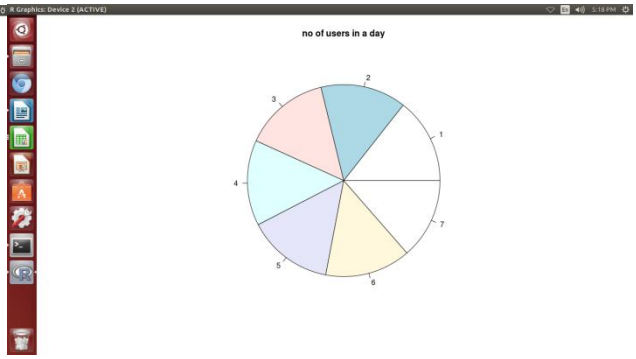
REFERENCES

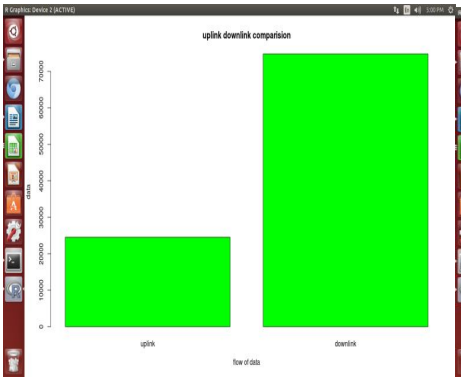
1. A Revolution That Will Transform How We Live, Work, and Think Author: Viktor Mayer-Schonberger 242 pages March 5th 2013 by Houghton Mifflin Harcoutr
2. Big Data (ebook) Author: Nathan Marz 425 pages,1st edition Published September 2012
3. Hadoop:The definitive guide Author: Tom White 1st edition ,528 pages June 12th 2009 by O'Reilly Media
4. www.dataversity.net/top-10-big-data-website/
5. SmartData Collective www.smartdatacollective.com/all/8731?ref=navbar)
6. BigData startup(http://www.dbigdata-startups.com)

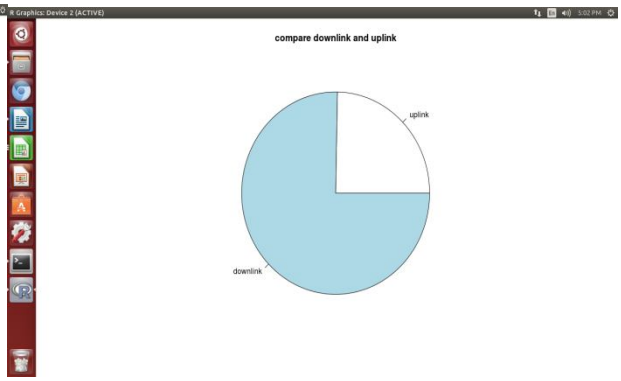


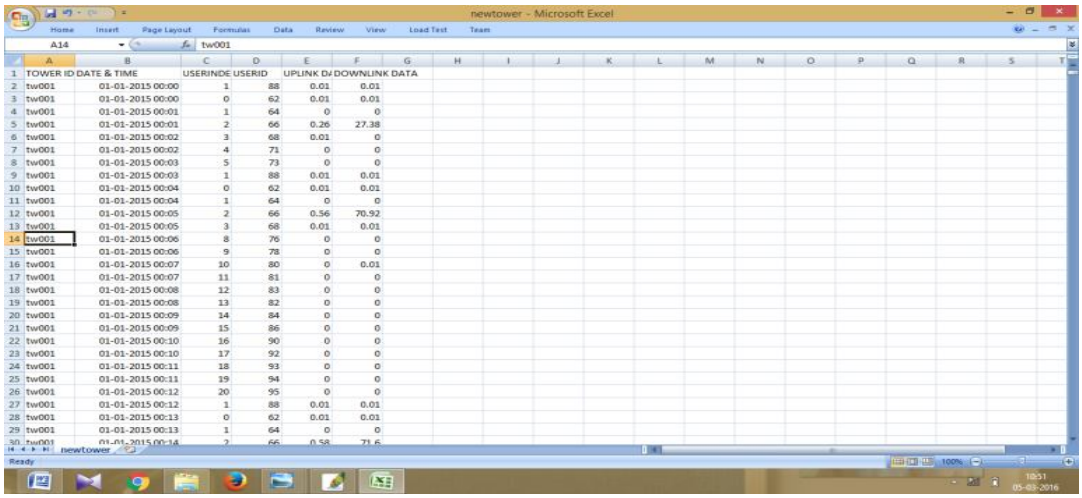
ISSN 2394 - 7780











International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

AUTOMATIC LICENSE PLATE REGONITION FOR TOLL -E COLLECTION

P. Lalitha[1], S. Aravind[2], S. Ramya[3] and V. Rajkumar[4]
Associate Professor[1]and Assistant Professor[2], Department of Computer Applications, Hindusthan College Of Arts and Science, Coimbatore, TamilNadu

ABSTRACT
ElectronicS Toll Collection system developed in India to save the time by collecting the toll electronically instead of manually. In order to provide zero delay toll collection system, so many modern toll collection systems are used like RF Tags based toll collection system, Barcode Scanner based toll collection system, and number plate As all the aforesaid systems are reliable, but still it's not defined as system without human Interaction . E . cognition based toll collection. The paper presents Fast toll collection system using Raspberry pi.The main objective of this paper is designing of Fast toll collection system using open cv with Raspberry pi. ETC system can be reduced the man power and save time.They can use existing closed circuit television or road-rule enforcement cameras, or ones specifically designed for the task. Automatic license plate recognition is a Computer Vision technique which is able to recognize a license plate number. This system is useful in many field likes parking lots, private and public entrances, theft control. In this paper I designed such a system. First capture the image from camera then load into system after that we used OpenCV library tools. Then we make the training set of different characters of different sizes. On the basis of these training set we extracted the character from images. When the license plate is detected, its digits are recognized and displayed in the GUI. In this mainly focuses on Neural Network and proprietary tools OpenCV using python.

Keywords: IOT, sensors, camera, automatic recognition, electronic toll

I. INTRODUCTION
Nowadays generally all highways toll system are manually operated, where an employee/worker collects cash from the driver and provides a receipt. This procedure can be slow, and encounter traffic jams at the toll plazas on busy highways. Our system will save time, effort, and man power because we are avoiding the manual task of collecting cash. In this work propose a low cost and efficient technique called Electronic Toll Collection[2] using RFID modules that automatically collects the toll from moving vehicles when they cross the toll. We also assume that an owner maintains a bank account, so that toll tax is deducted automatically from that account at toll plaza. If the account balance is low or if the vehicle is not supplied with an RF system, the toll gate restrict to vehicle. In such a case vehicle owner will have to pay the toll tax in cash and collect the receipt.The novelty of transport has become one of the essential signs of the urban modernization level, but it also causes serious problems concerning transport system. Due to automation, minimum human interference is required and this provides the facility so that the time and energy can be saved and efficiency can be improved.With the revolution in communication and embedded systems Electronic Toll Collection(ETC),[4] the new era of intelligent transportation systems(ITS)has been started. Many toll authorities have searched for ways to improve the toll collection process. Considering current scenario the number of vehicles passing through a specific toll booth are substantially high, hence there is a need for alternate solution for the highway toll collection method which should be more opportune, cost effective and more efficient than traditional methods. The proposed ALPR system will provide the better solutions to the toll collection and will deal with the problems arising due to traditional toll collection methods. When vehicle passes through toll automatically, it also sends notification to the registered user via SMS and E-mail which provides best security.

II. PROPOSED SYSYTEM
Automatic number plate recognition[1,6] is a mass surveillance method that uses optical character recognition on images to read vehicle registration plates. They can use existing closed circuit television or road-rule enforcement cameras, or ones specifically designed for the task. They are used by various police forces as a method of ETC system on pay-per-use roads and to catalogue the movements of traffic or individuals.

ISSN 2394 - 7780

WEB CAMERA

A **webcam** [3]is a video camera that feeds or streams its image in real time to or through a computer to a computer network. When "captured" by the computer, the video stream may be saved, viewed or sent on to other networks via systems such as the internet, and emailed as an attachment. When sent to a remote location, the video stream may be saved, viewed or on sent there. Unlike an IP camera (which connects using Ethernet or Wi-Fi), a webcam is generally connected by a USB cable, or similar cable, or built into computer hardware, such as laptops.

Technology

Webcams typically include a lens, an image sensor, support electronics, and may also include a microphone for sound. As a camera system's depth of field is greater for small image formats and is greater for lenses with a large f-number (small aperture), the systems used in webcams have a sufficiently large depth of field that the use of a fixed-focus lens does not impact image sharpness to a great extent.

BUZZER

A buzzer or beeper is a signaling device, usually electronic, typically used in automobiles, household appliances such as a microwave oven, or game shows. Initially this device was based on an electromechanical system which was identical to an electric bell without the metal gong (which makes the ringing noise).

LCD MODULE

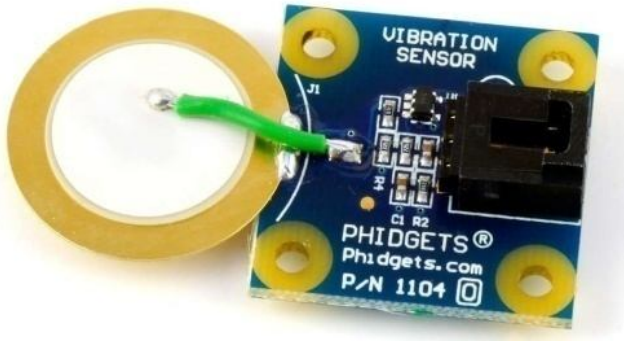
Dot matrix LCD modules is used for display the parameters and fault condition.16 characters 2 lines display is used. It has controller which interface data's and LCD panel. Liquid crystal displays (LCD's) have materials, which combine the properties of both liquids and crystals. Rather than having a melting point, they have a temperature range within which the molecules are almost as mobile as they would be in a liquid, but are grouped together in an ordered form similar to a crystal. An LCD consists of two glass panels, with the liquid crystal material sandwiched in between them. The inner surface of the glass plates are coated with transparent electrodes which define the character, symbols or patterns to be displayed polymeric layers are present in between the electrodes and the liquid crystal molecules to maintain a defined orientation angle.

ISSN 2394 - 7780

VIBRATION SENSORS

Vibration sensors detect the vibration of the ground soil in case of a debris flow. Prior to installing a vibration sensor, it is extremely important to determine what level of vibration is appropriate to activate the sensor in case of a debris flow. It is also important to keep in mind the risk of unintentional activation caused by earthquakes, as well as areas in which there is construction traffic and other vibration causes that may activate the sensor.

- Machinery damage and costly production delays caused by unforeseen machinery failure can be prevented.
- When pending problems are discovered early, the plant engineer has the opportunity to schedule maintenance and reduce downtime in a cost effective manner.
- Vibration analysis is used as a tool to determine machine condition and the specific cause and location of machinery problems.
- This expedites repairs and minimizes costs

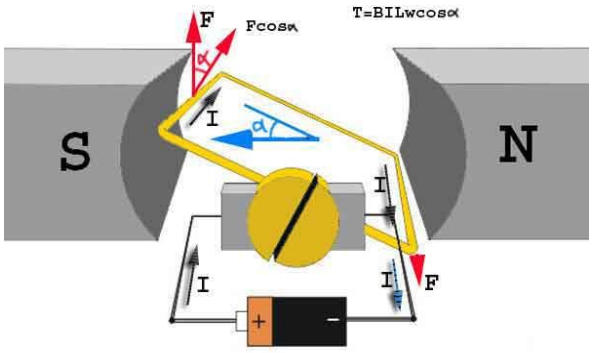


DC MOTOR

A **DC motor** is any of a class of rotary electrical machines that converts direct current electrical energy into mechanical energy. The most common types rely on the forces produced by magnetic fields. Nearly all types of DC motors have some internal mechanism, either electromechanical or electronic; to periodically change the direction of current flow in part of the motor.DC motors were the first type widely used, since they could be powered from existing direct-current lighting power distribution systems. A DC motor's speed can be controlled over a wide range, using either a variable supply voltage or by changing the strength of current in its field windings. Small DC motors are used in tools, toys, and appliances.

Electromagnetic Motor

A coil of wire with a current running through it generates an electromagnetic field aligned with the center of the coil. The direction and magnitude of the magnetic field produced by the coil can be changed with the direction and magnitude of the current flowing through it.



WORKING PROPOSED SYSTEM

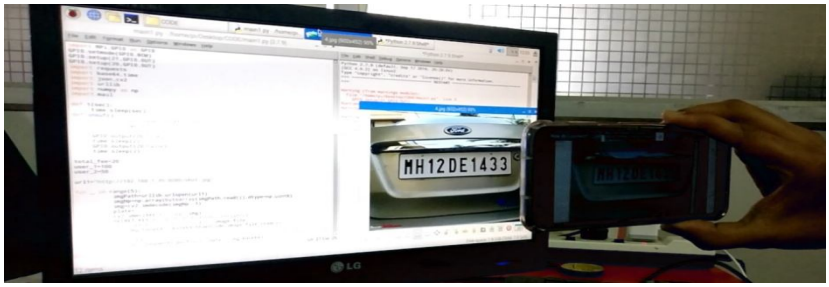
Step1: With the help of a camera, the number plate of the vehicle will be captured.[5]

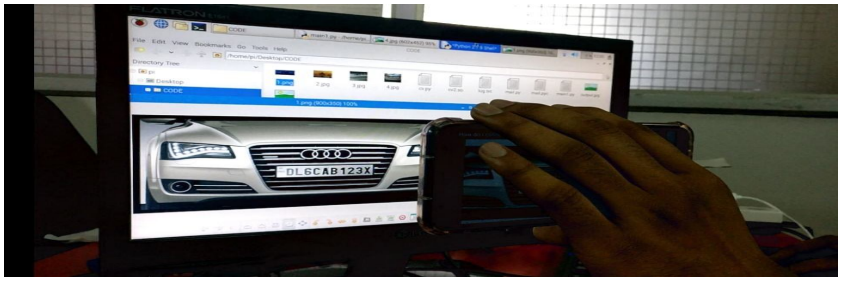
Step2: Once the license number is extracted from the overall image, it will be compared and searched in the centralize database and the respective vehicle owner's details will be fetched.[7]

Step3: Once the image is matched amount will be automatically detected from the vehicle owner.

Step4: If the image is not matched to the centralized database, then the security alert will be done and the siren will be belled, gate will not open and the image of the vehicle number will be sent to nearby police station.

ISSN 2394 - 7780





ADVANTAGES

- No special tag for vehicle is needed.
- License plates are not likely to be duplicated.
- No chance of interference between adjacent lanes.
- Reduce the man power
- Minimize the fuel consumption
- And totally avoided a waiting time in toll plaza.

III. CONCLUSION

An efficient less time consuming vehicle number plate detection method is papered which performed on multifaceted image. By using, Sobel edge detection method here detects edges and fills the holes less than 8 pixels only. To removing the license plate we remove connected components less than 1000 pixels. Our anticipated algorithm is mainly based on Indian automobile number plate system. Extraction of number plate accuracy may be increased for low ambient light image.

REFERENCES

1. IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 12, NO. 3, SEPTEMBER 2011 An Algorithm for License Plate Recognition Applied to Intelligent Transportation System. Ying Wen, Yue Lu, Member, IEEE, Jingqi Yan, Zhenyu Zhou, Karen M. von Deneen, and Pengfei Shi, Senior Member, IEEE
2. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014 Study of Different Electronic toll Collection Systems and Proposed toll Snapping and Processing System. Apurva Hemant Kulkarni M.E Department of Computer Science & Engineering, G.H.R.I.E.M jalgaon North Maharashtra university,INDIA
3. Rafael C. Gonzalez and Richard E. Woods, "Digital Image Processing"3rd edition, Pearson/Prentice Hall, 2008 (variance) pp. 96 97,(Mathematical Morphology) pp. 628-635, (Segmentation) pp.700-725, (Thresholding) pp.738-742, (Object Recognition - Correlation) pp. 866-872.
4. KHADIJAH KAMARULAZIZI ,DR.WIDID ISMAIL electronic toll collection system using rfid technologies Journal of Theoretical and Applied information technology © 2005 - 2010 JATIT & LLS..
5. Zhigang Xu, Honglei Zhu, "An Efficient Method of Locating Vehicle Licence Plate", 3rd International conference on Natural Computetion, IEEE, 0-7695-2875-9/07, 2007.
6. Prathamesh Kulkarni (Student Member, IEEE), Ashish Khatri, Prateek Banga, Kushal Shah, "Automatic Number Plate Recognition (ANPR) System for Indian conditions", IEEE Transactions, 2009.
7. International Journal of Scientific Engineering Research Volume 3, Issue 8, August -2012 1. Still Image Recognition Of License Plate System. N.Kanagaraj1, G.Baskaran2,S.Saravanan3,A.Ramachandran4 1,2,3,4

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

SECURITY AND ANTI-THEFT APPLICATION

Jenaker R[1] and Dr. Rangaraj R[2]
Student[1] and Head & Professor[2], PG and Research Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore

ABSTRACT
The main theme of my paper is to connect an android application to cloud database and its data can be viewed by website. Platform is android studio 3.1. APPLICATION: This is designed and developed in android studio using XML,java and APIs. This needs user request to activate this application. After user requested this app sends the location information and voice information(.mp3) to the cloud. Firebase acts as the intermediate between application and the website. This application has the never ending background process. WEBSITE: To provide the user to get access and retrieve the data from any where a website is created. Which is connected to the cloud. Application and website are synchronized to the cloud with the API key for the firebase

Keywords: Security, Android

I. INTRODUCTION

The android application has the live monitoring . It get the access location, mic and storage for the device. And it can store those information in the cloud. The user can see the recorded information anywhere by using a website. This application can be used in many ways like anti-theft application, child monitoring and women security. In system not only give live monitoring and also can record all the records of the monitoring. This system never ending background process. It is actually like creating a friend when you feel alone and not secure, your friend can see you , hear you and know where are you you right now.

II. EXISTING SYSTEM

With the new generation of wireless mobile computing many are trying to provide security not only to the data but also user and the device. The role of the anti-theft applications is when the theft is happened to the device it must act against and helps the user to find the device. But the problem and difficulty in understanding the situation by the device. Our technology was well developed , we can just need our hand to unlock our mobile phone with out touching it and facial recognition was developed to 3-D monitoring and 180 degree processing. And our technological development is not enough to identify the difference between user's friend and anonymous person.There are many systems there user needs to initiate the process . The process includes location, alarm, emergency message.

The application gets terminated when the device is turned off. When the device is turned on again the application won't start its process.

- They also do not contain any media files like photos and .mp3 files.
- They get access only location service and that too does not run on background.
- The success rate is very low.

III. PROPOSED SYSTEM

The android application has the live monitoring . It get the access location,mic and storage for the device. And it can store those information in the cloud. The user can see the recorded information anywhere by using a website.This application can be used in many ways like anti-theft application,child monitoring and women security.In system not only give live monitoring and also can record all the records of the monitoring.

* User initiation and stop process form

* AUTHENDICATITION form

* User data retrieval and refresh form

User initiation and stop process form

This process contains two button one is start button this button request to the system to start the process.The process contains two activities one is recording the inputs from the mic and another one is recording the inputs from the GPS(global possition system).The another button is stop buttton ,this button will teriminate the never ending background process. This never ending background process can not be terminated by killing the application , it can be stopped only but the stop button.

ISSN 2394 - 7780

IV. CONCLUSION

As said before this system can be used in different ways like anti-theft,child monitoring and women security.Anti-theft,the technology was not well developed to identify the difference between the user's friend and anonymous person, but this system help to find the device easily as it get access of mic,GPS and camera, camera will take image in the time distance of 5sec. But is camera is not added to this system currently due to it won't work on background and shortage of time.Women security, if a girl or women is facing any situation only physical power can help her, what the technology can do is helps the police to finish the case easily is system works perfect in the way.

REFERNCE

[1]. https://www.javatpoint.com/android-tutorial

[2]. https://www.raywenderlich.com/category/android

[3]. https://hackr.io/tutorials/learn-android-development

[4]. https://www.androidauthority.com/android-studio-tutorial-beginners-637572/

[5]. https://stackoverflow.com/users/878126/android-developer

[6]. https://www.tutorialspoint.com/android/index.htm

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

AUGMENTING BIG DATA ANALYTICS IN MOVIE RATING SCRUTINY

Dr. S. Sasikala[1], D.Vijayakumar[2], S. Aravind[3], A. S. Aghilan[4] and P. Kiruthik Roshan[5]
Associate Professor[1], Assistant Professor[2,3] and Student[4,5], Hindusthan College of Arts and Science

ABSTRACT
This paper intended to gather" movie rating analysis" details from different users with different movies and conduct the analysis to measure the top 5 movies and bottom 5 movies, year wise movie count details, and rating wise movie count details based on the movie rating details. Data volume for each block is around 2500 transactions (Low,High, and close values) based on year wise,and rating..Then organize the customers history using Hadoop components Pig,Hive and R, Pig will be used to build the data profile and cleanse the given data for Adhoc reports using HIVE and final analysis with statistical measures using R and finally present the predictions using 'R' charts and graphs.

Keywords- Big Data, Movie Rating, R, Hive

I. INTRODUCTION

Big data is an evolving term that describes any voluminous amount of structured, semi-structured and unstructured data that has the potential to be mined for information. the term 'Big Data' is used for collections of large datasets that include huge volume, high velocity, and a variety of data that is increasing day by day. Using traditional data management systems, it is difficult to process Big Data. Therefore, the Apache Software Foundation introduced a framework called Hadoop to solve Big Data management and processing challenges. Hadoop is an open-source framework to store and process Big Data in a distributed environment. It contains two modules, one is MapReduce and another is Hadoop Distributed File System (HDFS). MapReduce is a parallel programming model for processing large amounts of structured, semi-structured, and unstructured data on large clusters of commodity hardware. HDFS is a part of Hadoop framework, used to store and process the datasets. It provides a fault-tolerant file system to run on commodity hardware. The Hadoop ecosystem contains different sub-papers (tools) such as Sqoop, Pig, and Hive that are used to help Hadoop modules.

- Sqoop is used to import and export data to and from between HDFS and RDBMS.
- Pig is a procedural language platform used to develop a script for MapReduce operations.
- Hive is a platform used to develop SQL type scripts to do MapReduce operations.
- R is a programming language and software environment for statistical analysis, graphics representation and reporting.

The customer shopping can be analysed using the Bigdata hadoop components like Sqoop,Pig, Hive and R. The log file from each customer shopping is stored into mySql and it is imported into Hadoop Distributed File System (HDFS) using Sqoop. The customer shopping file may contain some data in an unstructured format. These unstructured data are cleansed using Pig shell. The fined tuned data after cleansing is taken into Hive for taking the Adhoc reports. The reports are given into R for further analysis and easy visualization of the report using charts and graphs for better understanding. The analysed customer shopping report can be used to know about the total amount of data transferred in each customer shopping in a particular time.

II. SYSTEM ANALYSIS

An Existing system for 'movie rating' analysis is being managed with Excel tool. Every day data is being captured using excel sheet and prepared the quick analysis using Excel capabilities, Sort, Chart and Graphs. Now the proposed system is to automate the data gathering from customer shopping. The Hadoop technology is open source which is highly available to build the analysis model. The Hadoop components can be used to obtain useful insights from the huge volume of data. The event log files from ten different towers are taken for analysis. The data contain details about the Customer-id, time, customer-name, Extended_price, Country, and product_id in customer shopping.The collected data is stored in mysql and the data is imported into HDFS using Sqoop. The unstructured data in the log file is organized by suitable cleansing using PIG component and upload the fine-tuned data in to HIVE for preparing Adhoc reports and R for Prediction and decision making.

The software requirements for the development of this paper are not many and are available as free as open source. The work for the paper is done with the current equipment and Hadoop software technology. The analysis of customer shopping by using the Hadoop components saves lot of time. The report can be taken based on year wise and the also the total amount of data transferred from each shopping can be also obtained easily for further analysis and the for the improvement steps to be taken based on the reports.

ISSN 2394 - 7780

SYSTEM REQUIREMENTS

Hardware:

PROCESSOR	:	i7 Intel core
HARD DISK CAPACITY	:	1 TB
MONITOR	:	19”HP Monitor
PRINTER	:	HP Laser Jet
KEYBOARD	:	DELL
MOUSE	:	HP MOUSE

Software:

MYSQL

HADOOP

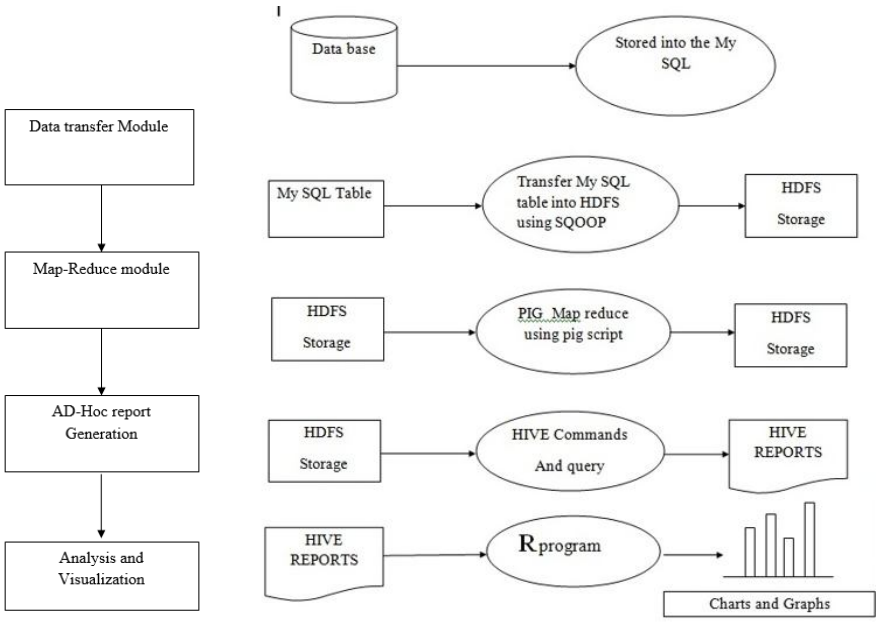
SQOOP

PIG

HIVE

R

III. SYSTEM DESIGN



Input design features can ensure the reliability of the system and produce result from accurate data or they can result in the production of erroneous information.

MySql

The data containing the details of movie are copied to mySql. A single linear table is created in mySql and the data are copied for quick process and data evalution using my-sql capabilities.

Sqoop

The evaluated data from mysql is being imported using Sqoop into Hadoop environment for further tuning and analysis. The sqoop import command is used to bring the table from mySql to HDFS.

Pig

The imported data from sqoop is given as input to the Pig grunt shell. The logdata is loaded in to pig shell using load command. The loaded log data may contain some of the text data in an unstructured format. These unstructured data are cleansed using pig filter commands. This fine tuned data are stored as comma separated csv file for further analysis using pigstorage.

ISSN 2394 - 7780

Hive
The fine tuned data which is in csv format is loaded into a database inside hive. A table with suitable data type is created inside the database using hql create query, after analyzing the data. The data in the csv file is loaded in to the table created for taking adhoc reports using select query.

The result values are stored in to HDFS as csv file for further analysis in R.

R
The resultant values stored as csv file from Hive based on the query is taken as an input to R using read command. The loaded data is used to create summary of the data for analysis,and for creation of the Chart or Graphs for Visualization and easy understanding about the analysis.

Data transfer module
Data transfer module transfers the datas from one component to another Hadoop component. Un-structured movie rating data is being captured from movie data management system. The log file containing the movie rating details of different movies copied into mySql. A single linear table is created in mySql and the data are copied for quick process and data evalution using my-sql capabilities. The evaluated data from mysql is being imported using Sqoop into Hadoop environment for further tuning and analysis. The sqoop import command is used to bring the table from mySql to HDFS.

Map-Reduce Module
MapReduce, are designed for batch-oriented processing of big data sets. MapReduce is a processing technique and a program model for distributed computing. The MapReduce algorithm contains two important tasks, namely Map and Reduce. Map takes a set of data and converts it into another set of data, where individual elements are broken down into tuples (key/value pairs). Secondly, reduce task, which takes the output from a map as an input and combines those data tuples into a smaller set of tuples. As the sequence of the name MapReduce implies, the reduce task is always performed after the map job.The major advantage of MapReduce is that it is easy to scale data processing over multiple computing nodes.

The data from sqoop is given as input to the Pig grunt shell. The loaded log data may contain some of the text data in an unstructured format. These unstructured data are cleansed using pig filter commands. This fine tuned data are stored as comma separated csv file for analysis .

Ad-hoc- report Generation module.
Ad hoc analytics is the discipline of analyzing data on an as-needed or requested basis. Ad Hoc Reporting allows end users to easily build their own reports and modify existing ones with little to no training. Ad hoc reporting generates reports that meet individual information requirements quickly and easily, allowing end users to dynamically modify and drill through report data for powerful information analysis. This type of flexibility frees up valuable IT resources and gets information to end users immediately, empowering them to interact with the data.

Apache Hive is a data warehousing system for large volumes of data stored in Hadoop. It's considered one of the de-facto tools for Hadoop since it provides a SQL-based query language that makes it easy to query big data sets. However, queries performed with Hive are usually very slow because of its reliance on MapReduce.

The fine tuned data which is in csv format is loaded into a database inside hive. A table with suitable data type is created inside the database using hql create query, after analyzing the data. The data in the csv file is loaded in to the table created for taking adhoc reports using select query.

Analysis and visualization module
R is a programming language and software environment for statistical analysis, graphics representation and reporting. R provides graphical facilities for data analysis and display either directly at the computer or printing at the papers. R Programming language has numerous libraries to create charts and graphs. A pie-chart is a representation of values as slices of a circle with different colors. The slices are labeled and the numbers corresponding to each slice is also represented in the chart. A bar chart represents data in rectangular bars with length of the bar proportional to the value of the variable. R uses the function barplot() to create bar charts. R can draw both vertical and horizontal bars in the bar chart. In bar chart each of the bars can be given different colors.

The resultant values stored as csv file from Hive based on the query is taken as an input to R using read command. The loaded data is used to create summary of the data for analysis, the summary of the data are taken for analysis of maximum tower utilization and the corresponding chart are drawn for easy visualization of the

ISSN 2394 - 7780

data for easy understanding and to take further steps of improvements for effective utilization of the tower.

PigUnit can help bring agility to your Hadoop practice; the same agility that JUnit, TestNG and Respec bring to Java and Ruby communities. PigUnit tests offer assurance that your Pig scripts will run when the scripts change or when Pig's version changes in your environment. Imagine knowing, in a few minutes, how your entire portfolio of Pig papers will fare in a different Pig version or Hadoop distribution.

Unit testing is the Engineering rigor of software development and, for more than a decade, modern software development teams have been employing unit testing to ensure the quality of their products. Unit tests are the pieces of the code that execute individual units of the software under controlled conditions and verify the outcome against the expected results. If you run a Hadoop shop, PigUnit can help you have that same Test Driven Development using Pig. The PigUnit framework uses JUnit to run a Pig script or its parts under specified data conditions. The framework provides Pig with a 'data sandbox' created from the tuples specified in the test.

This gives us two immediate advantages:
Rapid development: Pig scripts can run without needing a real cluster which speeds up the development cycle tremendously.

Identification of data conditions: Since PigUnit tests can run under a narrow set of data conditions, developers become more cognizant about the nature of the data to expect in their Pig scripts.

Example

Here's a "word count" solution implemented in Pig:

```
A = load 'input' using PigStorage() as (a:chararray);
B = foreach A generate flatten(TOKENIZE((a))) as word:chararray;
C = group B by word;
D = foreach C generate COUNT(B), group;
store D into 'output/wordcount' using PigStorage();
```

Example with multiple inputs

Many complex Pig scripts have multiple inputs. PigUnit allows a way to specify multiple inputs rather non-intuitively. Here at MetaScale, we have developed a base test class (PigTestBase) and a data mocking utility (MockPigFeed) to assist with sending multiple inputs to the script under test. To understand this, let's extend the previous example to have multiple inputs:

```
A1 = load 'input1' using PigStorage() as (a:chararray);
A2 = load 'input2' using PigStorage() as (a:chararray);
A = union A1,A2;
B = foreach A generate flatten(TOKENIZE((a))) as word:chararray;
C = group B by word;
D = foreach C generate COUNT(B), group;
store D into 'output/wordcount' using PigStorage();
```

Delimiters

When mocking data elements, note that PigUnit expects tab ("\t") delimiter for input aliases and will change the output aliases to have comma (",") delimiter.

Item	Analysis & Design	Development	Testing	Implementation	Total Hrs	Cost (23$/Hr)
Data Gathering-sqoop	2	2	1	2	7	9660
Data Profiling /Cleansing – PIG	2	4	2	2	10	13800
Adhoc reports – Hive	4	8	2	2	16	22080
Analysis - R	1	2	1	2	6	8280

Due to the number of paper participants in this phase of the SDLC, many of the necessary conditions and activities may be beyond the direct control of the Paper Manager. Consequently, all Paper Team members with

ISSN 2394 - 7780

roles in the implementation efforts must understand the plan, acknowledge their responsibilities, recognize the extent to which other implementation efforts are dependent upon them, and confirm their commitment.

Developed “Movie Rating Analysis” application can be implemented to any Telecom entertainment sector. The movie rating analyst can use this analysis to identify the performance of the movies, so that to take a decision on movie rating for the improvements of effective data transfer.

CONCLUSION

In recent entertainment sector the issue and concern of users satisfaction is becoming important for the purpose of achieving organizational goals and objectives through providing quality products and services to the users. users satisfaction is the expression of happiness or positive feelings about particular service from the sector.In this “movie rating analysis” paper also analyzing different movie rating data, and finally finding the Top five movies details, Least five movie details,Year wise cmovierating details, and rate wise movie details. In this report a user can easily find the complete detais regarding movies. The data of the each movies is taken for analysis. Movie rating data is analysed using the Bigdata hadoop components like Sqoop,Pig, Hive and the results are shown as charts using R.

REFERENCES

[1] A Revolution That Will Transform How We Live, Work, and Think Author: Viktor Mayer-Schonberger 242 pages March 5th 2013 by Houghton Mifflin Harcoutr

[2] Big Data (ebook) Author: Nathan Marz 425 pages,1st edition Published September 2012

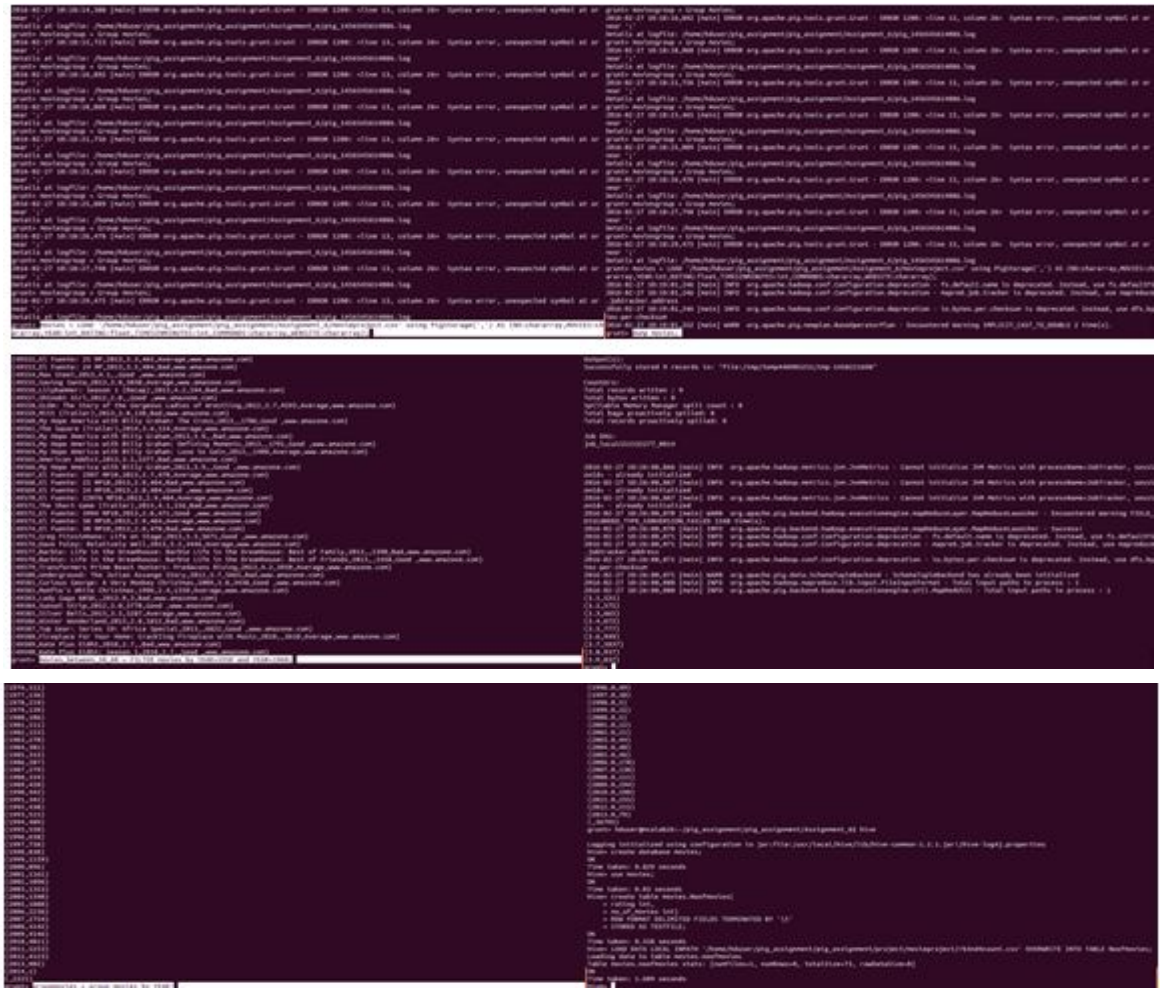
[3] Hadoop:The definitive guide Author: Tom White 1st edition ,528 pages June 12th 2009 by O’Reilly Media

[4] www.dataversity.net/top-10-big-data-website/

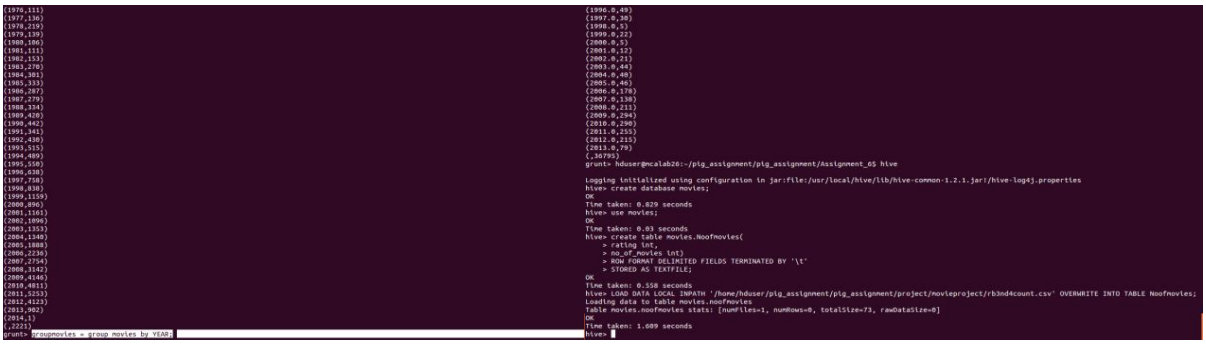
[5] SmartData Collective www.smartdatacollective.com/all/8731?ref=navbar)

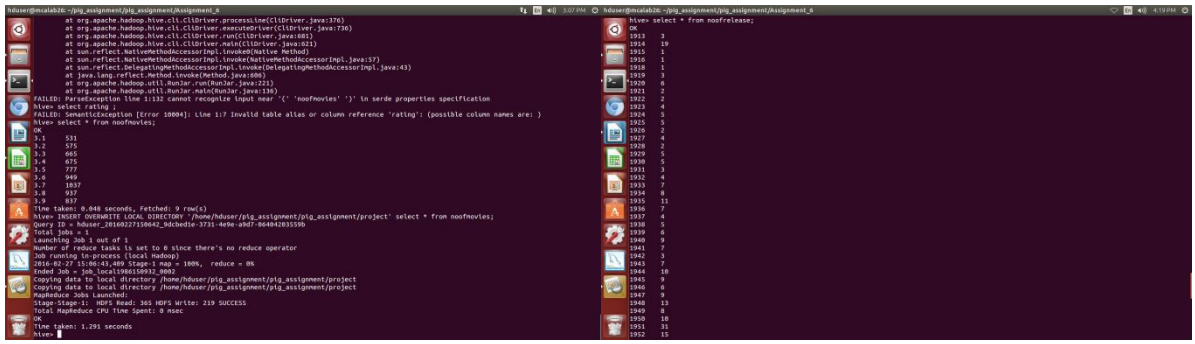
[6] BigData startup(http://www.dbigdata-startups.com)

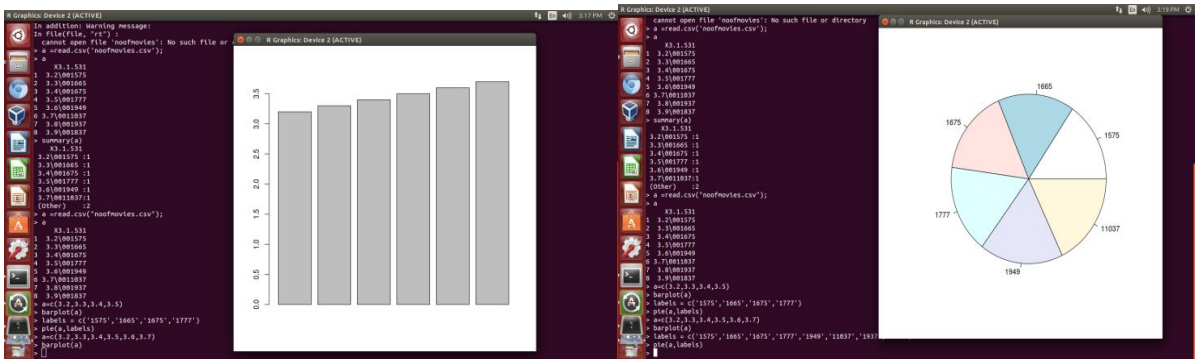
Pig Script

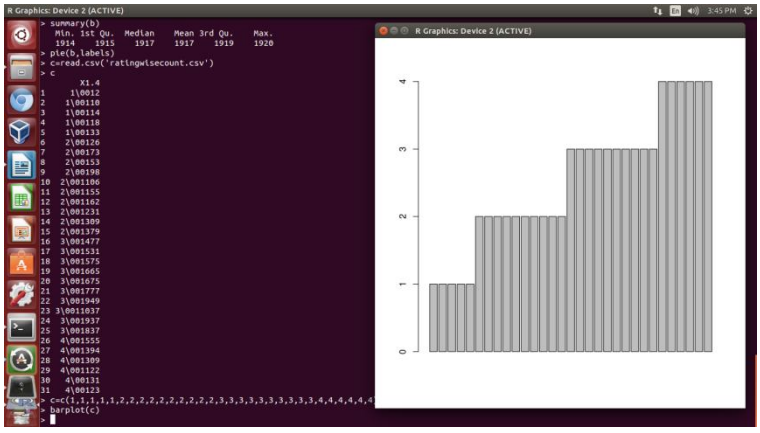


ISSN 2394 - 7780









International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

A REVIEW ON ASSORTMENT OF DATA MINING APPLICATIONS

R. Subalakshmi
Assistant Professor, Department Of Computer Science, P. S. G College Of Arts & Science

ABSTRAC*T*
Data mining bustle of extracting some practical knowledge from a large data base, via any of its techniques. Data mining is used to discover knowledge out of data and presenting it in a form that is tacit to humans. Data mining perception of all methods and techniques which allow analyzing very large data sets to extract and discover previously unknown structures and relations out of such huge heaps of details. This paper studies the techniques on the foundation of algorithms.

Keywords: Data mining Techniques, Data mining algorithms, Data mining applications.

I INTRODUCTION

Development of information technology has generated huge amount of data-base and vast amount of data in diverse research fields. To research in knowledge mining has give increase to store data and manipulate formerly stored data for further decision making process.

II LITERATURE REVIEW

Shankar et al presented paper on Employee Attrition using classification methods such as Decision tree, Logistic Regression, SVM, KNN, Random Forest, Naive bayes methods on the human resource data. Feature Selection Method was used to implement on the data and the analysis the result to prevent employee attrition. In this paper the analysis was done on the past and existing employee information to estimate the future attritioners and study the turnover made by the employee. The results of data extraction algorithms can be utilized to construct reliable and accurate predictive methods for employee attrition. This data study and data extraction methods can depict attrition probability for each one employee and provide them score to build the retention techniques.

Antonio Pratelli et al research is done in collaboration with the Department of Road Planning and paper of Tuscany Region. In this study the author brings out the traffic and its elements about the main regional street corridor linking Florence with Pisa and Leghorn. It integrates three different data sources, Bluetooth sensors data, traffic counts data and transport modeling results to study travel time, Origin/Destination and other information about this road. The Data Mining Algorithm called Predictive Association Rules to predict Origin/Destination matrix and integrates the transport model results to validate the algorithm and classification model elaborated. This research brings out the interaction of data mining and transport modeling and data sources big data from ITS sensors, data from transport models and others) allows to build innovative models useful for infrastructure management and road planning.It automates through platforms such as Knime. This model can be further developed joining it with accident or weather data so to figure out intervention scenarios to improve traffic flow

Md.Mahamud Hasan and Sadia Zaman Mishu suggested that mining of frequent item set using various support levels and an adaptive method which is applied on Apriori and FP growth algorithm to mine efficient frequent itemset. This paper defines minimum support (threshold) to mine frequent itemsets on Apriori and FP Growth algorithm. If minimum support is set to low, too many frequent itemsets will be generated which may cause the Apriori and FP Growth algorithm to become inefficient or even loss of memory. On the other hand, if minimum support is set to too high, less frequent itemsets are found .To avoid this problem Average Binomial Distribution (ABD) to find appropriate minimum support adaptively. It has been helped to mine optimal frequent itemsets so that our proposed method performs better than existing benchmark. This method can be added to different clustering techniques can be applied to extend the research and to mine the associations for large database.

Carlos Teixeira, José Braga de Vasconcelo and Gabriel Pestana in their research focuses on knowledge management and Engineering in organizations and a related architecture of a software tool for corporate log file analysis. The intention of log file analysis is to provide information about how the client uses an app (software application) and to detect anomalies that are not identify by the user so those anomalies can be corrected before the rise of a problem. The result of this research aims to describe architecture and to find software flows and apply datamining techniques to calculate and obtain knowledge to be recorded in KMS.

ISSN 2394 - 7780

Suhartina Hajrahnur et al bring out the Traffic congestion seems to be a daily routine of people in the Capital Jakarta. The information on traffic is very useful to rider. The information can be gathered from social networks has not been categorized. A congestion classification system was recognized in Jakarta with a datamining technique, a classification method using the decision tree technique, C4.5. C4.5 method transforms a large fact into a decision tree presenting the rules. Locations obtained will be plotted by geocoding and the classification process will be tested using a data partition with a confusion matrix. The results in this study show average accuracy rate 99.08%, precision 99.46%, and Recall 97.99% and it is visualized it into map

Johannes De Smedt et al in this paper presents the interesting Behavioral Constraint Miner (iBCM), a sequence classification technique that discovers patterns using behavioral constraint templates. The templates comprise a mixture of constraints and can express patterns ranging from simple occurrence, to looping and position-based behavior over a sequence. iBCM also captures negative constraints, i.e. absence of particular behavior. The constraints can be exposed by using simple string operations in an efficient way. Lastly deriving the constraints with a window-based approach allows to identify where the constraints hold in a string, and to identify patterns that are subject to concept drift. During empirical evaluation, it is shown that iBCM is better capable of classifying sequences more accurately and concisely in a scalable manner.

Sakti Pramanik ,AKM Tauhidul Islam and Shamik Sural in this paper proposed a predicted Edit distance based clustering to significantly lower clustering time. Existing clustering methods for sequence fragments, such as, k-mer based VSEARCH and Locality Sensitive Hash based LSH-Div attain much reduced clustering time but at the cost of significantly lower cluster quality. Through extensive performance analysis, clustering based on this predicted Edit distance provides more than 99% accurate clusters while providing an order of magnitude faster clustering time than actual Edit distance based clustering.

Ji Feng , Yan Wei, and Qingsheng Zhu proposes a novel parameter free classification algorithm called NNBCA, and the problem of parameter k selection in the training and testing stages is solved perfectly by using the NaN(Natural Neighborhood) method. A new supervised classification algorithm, Natural Neighborhood Based Classification Algorithm (NNBCA) was introduced and it resulted a good classification method without artificially selecting the neighborhood parameter. Disparate the original KNN-based method, which needs a prior k, NNBCA predicts different k for different samples. This algorithm NNBCA is more flexible neighbor information both in the training and testing stages. N This article introduces a new supervised classification algorithm, Natural Neighborhood Based Classification Algorithm (NNBCA). Findings indicate that this new algorithm provides a good classification result without artificially selecting the neighborhood parameter. Unlike the original KNN-based method, which needs a prior k, NNBCA predicts different k for different samples. Therefore, NNBCA is able to learn more from flexible neighbor information both in the training and testing stages. NBCA provides a better classification result than other methods.

Mingfeng Ye suggested the method of attribute reduction based on knowledge dependence with rough set theory and this method can find the more effective attributes for decision support. The datamining algorithm on knowledge dependence can yield a decision tree which puts forward more effective decision support information. This algorithm is useful for a single decision information system and the correct prediction rate is high.

Ohoud Almadani & Riyad Alshammari proposed a system to detect the stroke that occurs when a brain cells die and it helps to prevent the patients from complications. The attributes are patient age, gender, lipid disorder, lab test abnormalities, hypertension medications, diabetes medications, and other medications are included, which resulted of data set that contains 147 attributes. The data is divided into training data set to set to build the model and the test to evaluate the model. J48 (C4.5), JRip, and Neural Network (multilayer perceptron [MLP]) algorithms were applied on the stroke training data set to build a model. All Data mining algorithms have been applied using Weka Software. It then works to build decision tree branches from that attribute values and distribute instances into its corresponding branch .The third algorithm is a Neural Network called Multilayer perceptron (MLP). MLP is a forward feed neural network. It uses one direction feed of input through one or more layers to produce output layer. To train this algorithm a back-propagation learning algorithm is used, and it helps to solve non-linearity problem. C4.5 and Jrip are the highest classifiers in name of accuracy after PCA on the test data set.

III CONCLUSIONS

This paper presents a depiction of data mining techniques and algorithms. Data Mining is the process of discovering interesting knowledge from large amounts of data stored either in databases, data warehouses, or other information repositories. The various algorithms used for the mining of data are précised. The future

ISSN 2394 - 7780

scope provides augmentation and effectiveness of data in the system. It will provide faster and qualitative exaction of data with better tools and techniques.

IV REFERENCES

1. R Shiva Shankar, J Rajanikanth, V.V.Sivaramaraju and K VSSR Murthy , PREDICTION OF EMPLOYEE ATTRITION USING DATAMINING,2018.
2. Antonio Pratelli, Massimiliano Petri and Marco Ierpi, Michela di Matteo , Integration of Bluetooth, Vehicle Count Data and Trasport Model Results by Means of Datamining Techniques, IEEE International Conference on Environment and Electrical Engineering and 2018 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe),2018.
3. Md.Mahamud Hasan and Sadia Zaman Mishu, An Adaptive Method for Mining Frequent Itemsets Based on Apriori And FP Growth Algorithm, 2018 International Conference on Computer, Communication, Chemical, Material and Electronic Engineering (IC4ME2),2018.
4. Carlos Teixeira, José Braga de Vasconcelo and Gabriel Pestana , A knowledge management system for analysis of organisational log files, 13th Iberian Conference on Information Systems and Technologies (CISTI),2018.
5. Suhartina Hajrahnur,Muhammad Nasrun,Casi Setianingsih and Muhammad Ary Murti, Classification of posts Twitter traffic jam the city of Jakarta using algorithm C4.5,International Conference on Signals and Systems (ICSigSys), 2018.
6. Johannes De Smedt ,Galina Deeva and Jochen De Weerdt , Mining Behavioral Sequence Constraints for Classification,IEEE Transactions on Knowledge and Data Engineering,2019.
7. Sakti Pramanik ,AKM Tauhidul Islam and Shamik Sural , Predicted Edit Distance Based Clustering of Gene Sequences, IEEE International Conference on Data Mining (ICDM), 2018.
8. Ji Feng , Yan Wei, and Qingsheng Zhu,Natural neighborhood-based classification algorithm without parameter k, Big Data Mining and Analytics (Volume: 1 , Issue: 4 , December 2018)
9. Mingfeng Ye, The Datamining Algorithm on Knowledge Dependence,International Conference on Smart Grid and Electrical Automation (ICSGEA), 2018.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

ANOMALY DETECTION VIA ONLINE OVER-SAMPLING PRINCIPAL COMPONENT ANALYSIS

Sivabhalan[1] and Marrynal S Eastaff[2]
Student[1] and Assistant Professor[2], Department of Information Technology, Hindusthan College of Arts and Science

ABSTRACT
Anomaly detection has been an important research topic in data mining and machine learning. Many real-world applications such as intrusion or credit card fraud detection require an effective and efficient framework to identify deviated data instances. However, most anomaly detection methods are typically implemented in batch mode, and thus cannot be easily extended to large-scale problems without sacrificing computation and memory requirements. In this paper, we propose an online over-sampling principal component analysis (osPCA) algorithm to address this problem, and we aim at detecting the presence of outliers from a large amount of data via an online updating technique. Unlike prior PCA based approaches, we do not store the entire data matrix or covariance matrix, and thus our approach is especially of interest in online or large-scale problems. By over-sampling the target instance and extracting the principal direction of the data, the proposed osPCA allows us to determine the anomaly of the target instance according to the variation of the resulting dominant eigenvector. Since our osPCA need not perform eigen analysis explicitly, the proposed framework is favored for online applications which have computation or memory limitations. Compared with the well-known power method for PCA and other popular anomaly detection algorithms, our experimental results verify the feasibility of our proposed method in terms of both accuracy and efficiency[2][4].

I. INTRODUCTION
It would be difficult to speak on the successes of technology in past years without discussing the recent attacks on user data. The data explosion from technological growth has armed analysts with new strategies for predicting or detecting malicious activity. Taking data from previous attacks can help us prevent or stop future ones from emerging. This method of preventing attacks can be summarized as finding outliers in a data set – or an anomaly. An anomaly is a data point that veers away normal trends in a data set. From credit card fraud detection to cybersecurity attacks, detecting anomalies has become vital in ensuring privacy. Nevertheless, due to differences between data in these domains, a generalized solution for detecting out of the ordinary behavior becomes challenging. In this paper, we will focus on anomaly detection in cybersecurity of the 2011 VAST dataset challenge. Between the Internet of Things, the rapid advancement of technology and the lack of regulation in the past years, security has become a primary concern for millions of users. In addition, anomaly detection in networks has various layers of mathematical complexity. Deciding which data points seem out of place requires precise analysis of data. This, coupled with the enormous size of data sets, subtle correlation between data points, and potential long system waits for each run cycle makes the process known as feature engineering non-trivial [9]. Security issues have been steadily present in software companies as technology continues to grow in use and complexity. Considering how heavily embedded technology has become in everyday life, cybersecurity is an issue of the highest priority. Damage costs alone from cyber attacks are papered to reach $6 trillion by 2021 and breaches of personal information are occurring with higher frequency as time progresses . Over the past years, government records have been victimized of cyber attacks, for example, the Free Application for Federal Student Aid (FAFSA) experienced a security breach within its IRS retrieval application. This led to roughly 100,000 taxpayers information being compromised. As time and technology progresses, malicious infiltrations such as the FAFSA breach become increasingly more difficult to predict or detect. To protect user information, avoid denial of service attacks, along with other types of infiltration, it is vital to detect what has gone wrong in the past regarding security. Determining the root cause of these issues assist improving the security of critical information and user privacy. Anomaly detection has been researched extensively for cybersecurity due to the complexities that it entails. The University of Minnesota's, Anomaly Detection: A survey, looked at using network intrusions detection systems to find anomalies. However, detecting anomalous behavior through network data comes with several challenges. This type of dataset is inherently high dimensional and the domain continuously changes over time as intruders adapt and overcome intrusion detections advancements [20]. In this Major Qualifying Paper (MQP), we examined ways to diversify a dataset through feature engineering and analyze its relationship with Robust Principal Component Analysis (RPCA). Our contributions were the following:

• Created a user-friendly visualization system.

• Closed the loop between feature generation, mathematical analysis, and visualization.

ISSN 2394 - 7780

• Improved overall experience of system administrators by creating a streamlined process through careful construction of sound infrastructure in our code base. This report explains in depth what anomaly detection is, its process, the different statistical analysis methods that we will use or recommend to use, what feature engineering is, and the impact that the original data set we used had on our paper along with the assumptions made[10][13].

II. SYSTEM DESIGN

EXISTING SYSTEM

The existing approaches can be divided into three categories:

- Distribution (statistical),
- Distance and
- Density based methods.

Statistical approaches assume that the data follows some standard or predetermined distributions, and this type of approach aims to find the outliers which deviate form such distributions.

For distance-based methods, the distances between each data point of interest and its neighbors are calculated. If the result is above some predetermined threshold, the target instance will be considered as an outlier.

One of the representatives of this type of approach is to use a density based local outlier factor (LOF) to measure the outlierness of each data instance. Based on the local density of each data instance, the LOF determines the degree of outlierness, which provides suspicious ranking scores for all samples. The most important property of the LOF is the ability to estimate local data structure via density estimation. This allows users to identify outliers which are sheltered under a global data structure[5][9].

DISADVANTAGES OF EXISTING SYSTEM

Most distribution models are assumed univariate, and thus the lack of robustness for multidimensional data is a concern. Moreover, since these methods are typically implemented in the original data space directly, their solution models might suffer from the noise present in the data

PROPOSED SYSTEM

PCA is a well known unsupervised dimension reduction method, which determines the principal directions of the data distribution. This will prohibit the use of our proposed framework for real-world large-scale applications. Although the well known power method is able to produce approximated PCA solutions, it requires the storage of the covariance matrix and cannot be easily extended to applications with streaming data or online settings. Therefore, we present an online updating technique for our osPCA. This updating technique allows us to efficiently calculate the approximated dominant eigenvector without performing eigen analysis or storing the data covariance matrix[3][6].

ADVANTAGES OF PROPOSED SYSTEM

Compared to the power method or other popular anomaly detection algorithms, the required computational costs and memory requirements are significantly reduced, and thus our method is especially preferable in online, streaming data, or large scale problems.

DESCRIPTION OF MODELS

- Cleaning Data
- Detecting Outliers
- Clustering

MODULE – I: Cleaning Data

The osPCA is applied for the data set for finding the principal direction. In this method the target instance will be duplicated multiple times, and the idea is to amplify the effect of outlier rather than that of normal data. After that using Leave One Out (LOO) strategy, the angle difference will be identified. In which if we add or remove one data instance, the direction will be changed. For normal data instances this angle difference should be smaller and for outliers this might be larger[1][7].

A set of data instances in the original data set is taken as predefined input. This data may be contaminated by noise and incorrect data labelling etc., This data might be error free, because this is going to be used as training data. So the cleaning is done using Over-Sampling Principal Component Analysis (osPCA) method. And then the score of outlierness St is calculated for each data instances. The smallest St value is taken as the threshold value.

ISSN 2394 - 7780

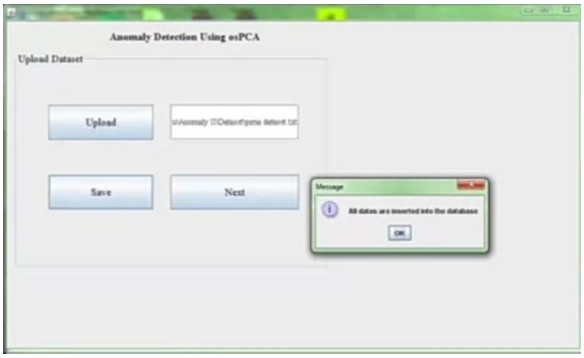


Figure-1: Start Screen

MODULE – II: Detection of outlieners

This is for detecting the outlierness of the user input. When the user giving the input to the system, the system calculate the St value for the new input. And then compare that new St value with the threshold value which is calculated in earlier.

If the St value of the new data instance is above the threshold value, then that input data is identified as an outlier and that value will be discarded by the system. Otherwise it is considered as a normal data instance, and the PCA value of that particular data instance is updated accordingly[8][11].

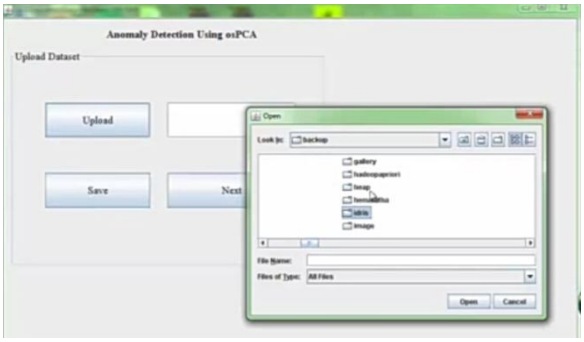


Figure-2: Choosing Files

MODULE – III: Clustering

The training data will be selected only by our assumption. So there is a possibility that some outlier data may be considered as normal data in the previous method due to our training data. So the clustering method is used to solve this problem. The clusters are formed for input data instances and then the outlier calculation is applied for each cluster to find the outlier exactly[12][15].

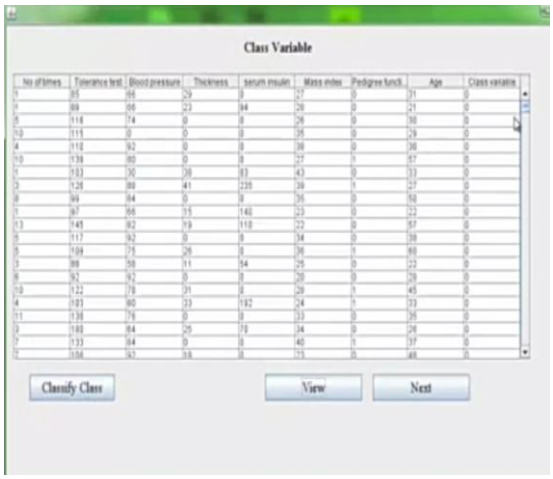


Figure-3: Clustering Class Variables

III SYSTEM IMPLEMENTATION

Implementation is the process of installing the software into the system so that it will be provided with original data to process. There are various cycle processes such as requirement analysis, design phase, testing and finally followed by the implementation phase which results in a successful paper management. These are analyzed step by step and the positive as well as negative outcomes are noted before the final implementation[16][14].

ISSN 2394 - 7780

IV CONCLUSION

we proposed an online anomaly detection method based on over-sample pca. we showed that the os pca will amplify the effect of outliers, and thus we can successfully use the variation of the dominant principal direction to identify the presence of rare but abnormal data. when oversampling a data instance, our proposed online updating technique enables the ospca to efficiently update the principal direction without solving eigen value decomposition problems. furthermore, our method does not need to keep the entire covariance or data matrices during the online detection process. therefore, compared with other anomaly detection methods, our approach is able to achieve satisfactory results while significantly reducing computational costs and memory requirements. thus, our online ospca is preferable for online large-scale or streaming data problems. future research will be directed to the following anomaly detection scenarios: normal data with multiclustering structure, and data in a extremely high dimensional space. for the former case, it is typically not easy to use linear models such as pca to estimate the data distribution if there exists multiple data clusters. moreover, many learning algorithms encounter the “curse of dimensionality” problem in a extremely high dimensional space. in our proposed method, although we are able to handle high dimensional data since we do not need to compute or to keep the covariance matrix.

V FUTURE ENHANCEMENTS

One could imagine some form of data smoothing being applied to the dataset to reduce noisy information and allowing outliers to become more apparent. data smoothing has not been applied in this paper, but from a mathematical perspective, it would be interesting to see how smoothing would affect the anomaly detection system for this dataset. in financial investment software smoothing has been used to explain the behavior of stocks and determine patterns in the market. to be able to use these features, think in terms of the manifold, and define what it means for two points to be close to each other could help increase the analysis of a dataset to help prevent attacks. . a network administrator could use rules with a firewall log file to detect certain instances of possibly malicious behavior. There can be a system where a set of rules exist for a data set. These rules could then be generated in a web platform by a user depending on what they are interested in.

REFERENCES

- Padmavathi, D. Shanmugapriya and M. Kalaivani, "A Study on Vehicle Detection and Tracking Using Wireless Sensor Networks," Wireless Sensor Network, Vol. 2 No. 2, 2010, pp. 173-185. doi: 10.4236/wsn.2010.22023
- Y.Zhang, A multilayer IP security protocol for TCP performance enhancement in wireless networks. IEEE Journal on Selected Areas in Communications, Vol. 22, n. 4, pp. 767-776, May 2004. NS-2 Network Simulator (Vers. 2.27),URL: http://www.isi.edu/nsnam/ns/nsbuild.html
- M. Luglio, A. Saitto, “Security of Satellite Networks”, chapter in H. Bidgoli (Ed), “The Handbook of Information Security”, John Wiley & Sons, Inc., 2006, Hoboken, N.J., Vol. 1, pp. 754-771.
- M. P. Howarth, S. Iyengar, Z. Sun and H. Cruickshank, “Dynamics of key management in secure satellite multicast”, IEEE Journal on Selected Areas in Communications, Vol. 22, n. 2, pp. 308-318.
- Partridge, and T. Shepard, TCP Performance over Satellite Links.IEEE Network, vol. 11, n. 5, 1997, pp. 44-49.
- W. Stevens, TCP/IP illustrated, Volume 1. Addison Wesley, 1994.
- ETSI TS 102 292, Broadband Satellite Multimedia (BSM); Functional Architecture
- Caini, C., et al.: PEPsal: A Performance Enhancing Proxy for TCP Satellite Connections. IEEE A&E Systems Magazine (August 2007)
- I-PEP specifications, Issue 1a. Satlabs group recommendations (October 2005), http://www.satlabs.org
- ETSI TS 102 463: Broadband Satellite Multimedia (BSM); Interworking with IntServQoS
- ETSI TS 102 464: Broadband Satellite Multimedia (BSM); Interworking with DiffServQoS
- Obanaik, V.: Secure performance enhancing proxy: To ensure end-to-end security and enhance TCP performance over IPv6 wireless networks. Elsevier Computer Networks 50, 2225–2238 (2006)
- Bellovin, S.: Probable plaintext cryptanalysis of the IPSecurity protocols. In: Proceedings of the Symposium on Network and Distributed System Security (February1997)

ISSN 2394 - 7780

- M. Annoniet al., "Interworking between multi-layer IPSEC and secure multicast services over GEO satellites," presented at the COST-272 Symp., Thessaloniki, Greece, June, 20–21 2002. Doc. TD-02-016-P.
- J. Arrkoet al., "MIKEY: Multimedia Internet Keying," IETF Internet Draft, work-in-progress, draft-ietf-msec-mikey-06.txt, Feb. 2003 , expires Aug. 2003.
- N. Assafet al., "Interworking between IP security and performance enhancing proxies for mobile networks," IEEE Commun. Mag., vol. 40, pp. 138–144, May 2000.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

FLEET MANAGEMENT SYSTEM

K. Rajathi[1] and Dr. V. Saravanan[2]
Student[1] and HOD & Professor[2], Department of Information Technology, Hindustan College of Arts and Science, Coimbatore

A**BSTRACT**
Fleet management is a web based vehicle fleet maintenance management the executives framework written in PHP with MySQL database back-end.. It is a web-based system which is accessible through browser. Fleet management was initially designed for trucking companies in mind but it can be useful for any person or company having a fleet of vehicles. It will enable the proprietors to have full control of the upkeep of vehicle fleet. The main objective is to design a web application for owner who wants to reduce manual effort while providing vehicle based services to small & medium based companies.

Fleet management is developed and customized for fleet owners and organizations. It really reduces Keep accurate records for any type of vehicles. This is the function that oversees, coordinates and facilities, various transport and transport related activities .For this purpose of the document it will cover vehicles involved of goods; the management of light vehicles fleets used in the transportation of people .It underpins and supports transport related activities through the management of the assets that are used. Successful fleet management the board goes for lessening and limiting generally costs through most extreme, savvy use of assets, for example, vehicles, fuel, save parts, tire and so on..,

I .INTRODUCTION

Fleet Maintenance Management software system designed with PHP and MySQL database backend. It is an web based framework which is available through an internet browser. And it was originally designed for trucking companies but it can be used for any other vehicle fleet.

Fleet Maintenance Management can be defined as the process whereby the operation of and costs relating to a fleet of vehicles are controlled. It is a specific management discipline. Fleet Maintenance Management must provide a full range of custom-made Fleet Maintenance Management services that will assist companies in managing and controlling costs. Various categories of fleet expenses must be managed and invoiced through a single Fleet Maintenance Management account. Fleet expense cost records should be state-of-the-art, precise and simple to get to. For reporting needs, Fleet Maintenance Management service providers must provide the convenience of a range of sophisticated, but easy-to-use tools to manage fleet expenses

Fleet Maintenance Management is the management of commercial motor vehicles such as cars, vans, trucks, specialist vehicles, and trailers Private vehicles used for work purposes Aviation machinery such as aircraft Ships Rail cars. Fleet (vehicle) management can include a range of functions, such as vehicle maintenance, fuel management etc.

II EXISTING SYSTEM

Current framework is a manual one in which representatives needs to present their applications for transport office just as for taxi office. Workers needs to catch up consistently with transport staff to know the status of their solicitations which is tedious and riotous.

2.1 Disadvantages

The following are the disadvantages of current system

1. It is difficult to track the occupancy.
2. Progressively manual hours need to produce required reports
3. It is dreary to follow the subtleties of taxis given by outsider.
4. There is no plausibility to follow the endorsements of solicitations.
5. No co-ordination between various departments.

III PROPOSED SYSTEM

Proposed system is a software application which avoids more manual hours that need to spend in record keeping and generating reports. This application keeps the data unified which is available to all of the customers at the same time. It is exceptionally simple to oversee recorded information in database. No particular preparing is required for the workers to utilize this application. They can without much of a stretch utilize the device that diminishes manual hours spending for typical things and thus builds the execution.

ISSN 2394 - 7780

3.1 Advantages

The following are the advantages of proposed system

1. Easy to process requests
2. Can generate required reports easily
3. Simple to oversee authentic information in a safe way
4. Centralized database helps in avoiding conflicts
5. Simple to utilize GUI that does not requires explicit preparing.
6. Implementation of approval process is very easy
7. Occupancy tracking helps in decision making

IV. MODULE DESCRIPTION

- Master Files
- Reports
- Fuel Records
- Repair
- Maintenance
- Renewal
- Accident Records
- Insurance Claims

4.1 Master Files

This module includes master data which is used in other modules.

4.2 Reports

This module includes customizable reports in fuel, stocks, repairs, maintenance and accidents.

4.3 Fuel Records

This module is used to record fuel related details. Fuel is the biggest fleet cost and basic to oversee and control Fuel cost increments majorly affect fleet cost – showed in fuel cost versus armada card fuel exchange esteems since 2010 .

4.4 Repairs

This module is used to record all vehicle repair details.

4.5 Maintenance

This module is for recording all the regular/periodic maintenance of vehicles. Vehicle maintenance costs are challenging to control. Fleet proprietors need to guarantee that vehicles are routinely adjusted, tires supplanted on time and manage specialized issues. Well maintained vehicles positively impacts resale values.

4.6 Renewals

This module is for recording all recurring expenses such as insurance.

4.7 Accident Records

This module records all vehicle accidents in detail and able to show whenever we needed. It’s a well maintained and organized by the users and the admin.

4.8 Insurance Claims

This module records all the claims received from the insurance companies. Vehicle protection (otherwise called vehicle protection, engine protection or collision protection) is protection for autos, trucks, engine bicycles and other street vehicles. Its primary use is to provide financial protection against physical damage or bodily injury resulting from traffic collisions and against liability that could also arise from incidents in a vehicle.

V SYSTEM IMPLEMENTATION

5.1 LOGIN

The appropriate user can login and access the system. Sometime the user or admin can forget the password forget password option is used to recover the password .The user like change the password using change password option.

ISSN 2394 - 7780

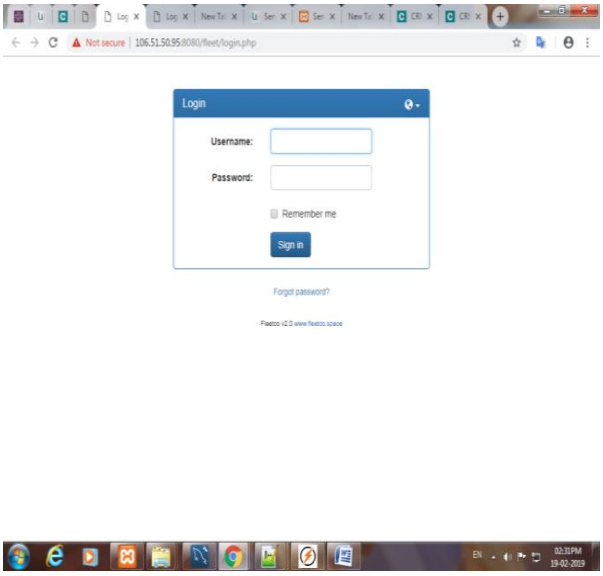


Figure-1: Login Form

5.2 MASTER FILES

The master forms will be used to add, edit and delete the details about vehicle, fuel, supplier, stock, service type, renewals and insurance claims .

Figure-2: Master Files list

The admin can only add, edit and delete the details for these master forms like these format and the stored details view from the database. .

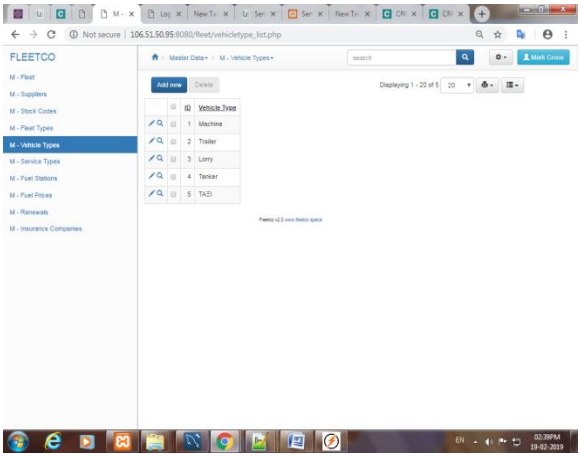


Figure-3: vehicle form

5.3 REPORTS AND CHARTS

Fleet management system can also generate charts and reports for fleet ,fuel, stock and maintenance list and accident reports. Reports and charts will be used to analyze the data's in very easily and gives appropriate estimation.

ISSN 2394 - 7780

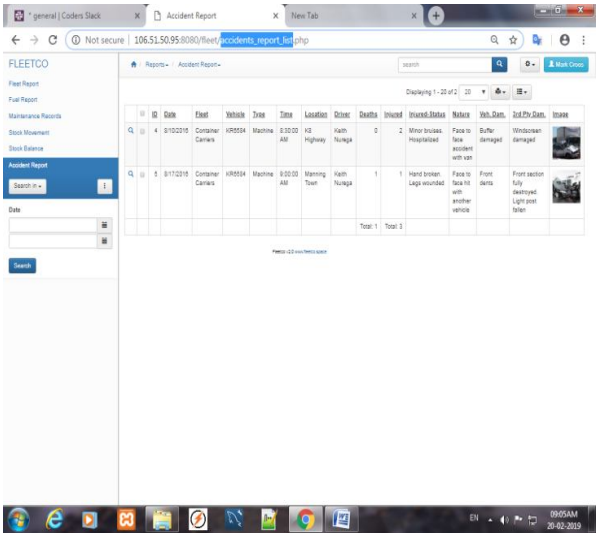


Figure-4: Report form

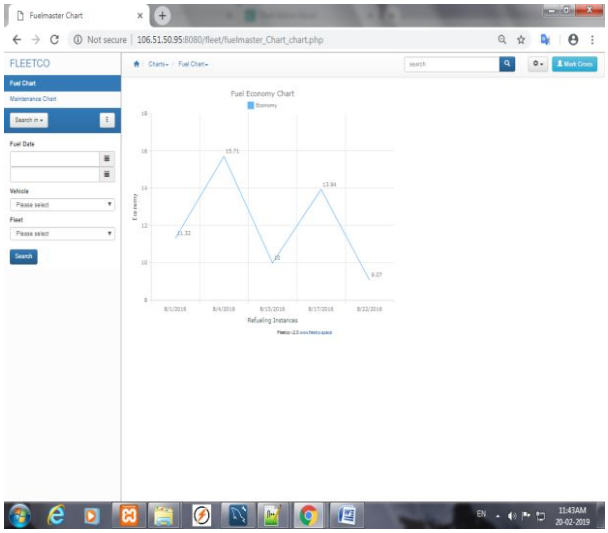


Figure-5: Chart

5.4 RENEWALS

This module is for recording all recurring expenses such as insurance.

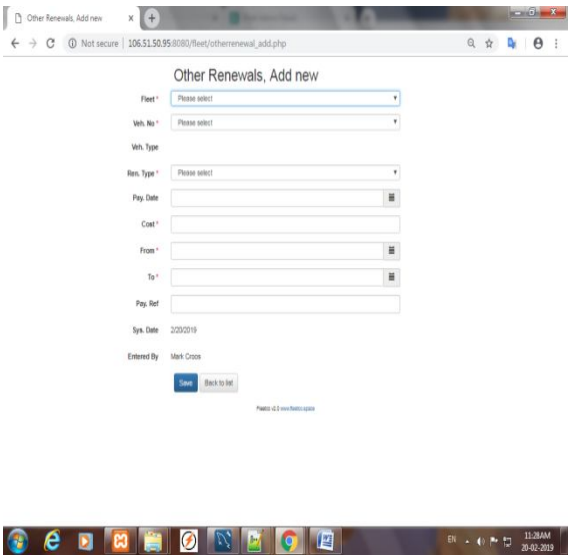


Figure-6: Renewal form

5.5 ACCIDENT RECORDS

This module records all vehicle accidents in detail and able to show whenever we needed. It's a well maintained and organized by the users and the admin.

ISSN 2394 - 7780

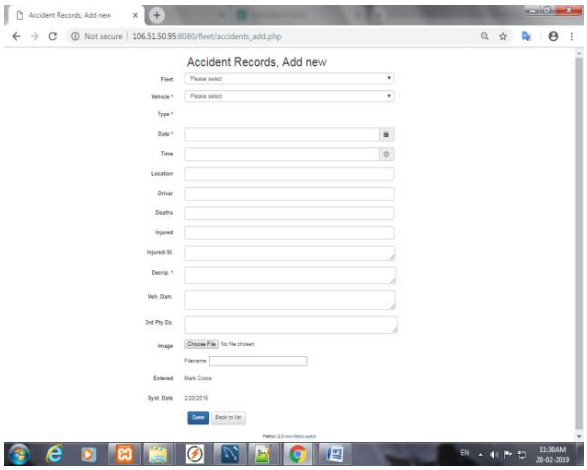


Figure-7: Accident form

5.6 INSURANCE CLAIMS

This module records all the claims received from the insurance companies. Vehicle protection (otherwise called vehicle protection, engine protection or accident coverage) is protection for autos, trucks, bikes and other street vehicles. Its basic use is to give cash related confirmation against physical mischief or generous harm coming about in light of auto collisions and against hazard that could in like manner rise up out of events in a vehicle.

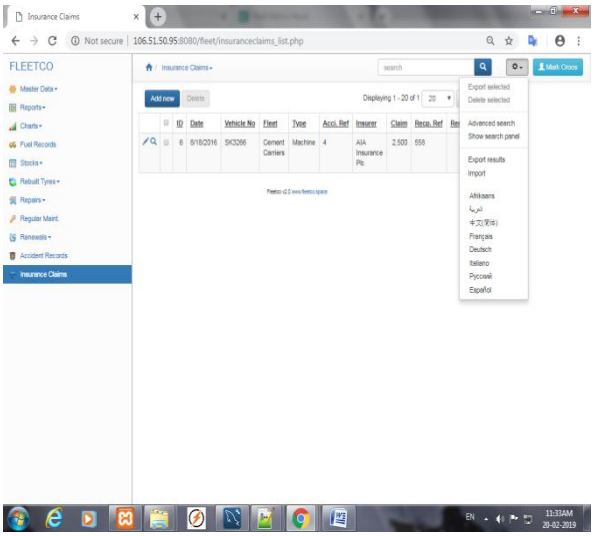


Figure-8: I nsurance form

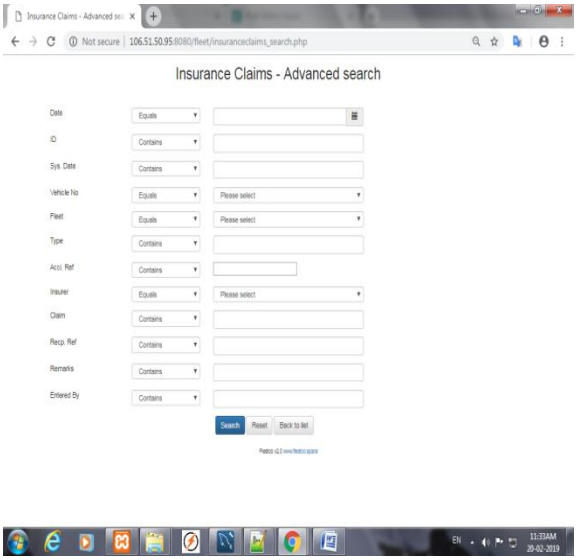


Figure-9: Insureance Claims form

5.7 ADMIN AREA

The admin can only add and edit the users group.

ISSN 2394 - 7780

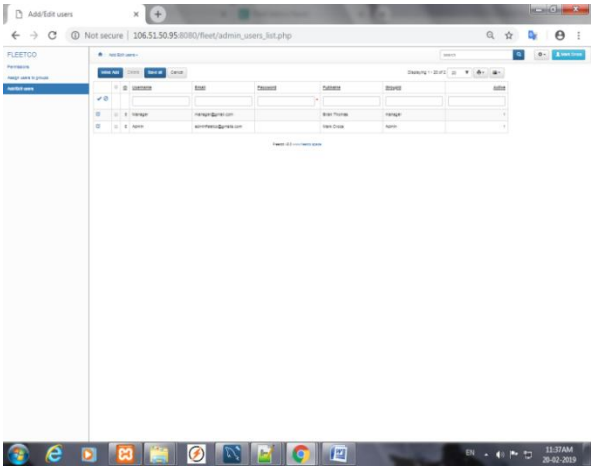


Figure-10: Add user group form

To Export the result using this export window.

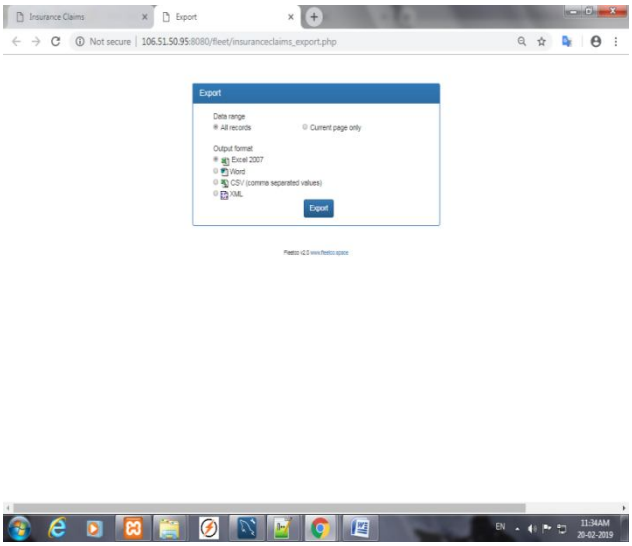


Figure-11: Eport window form

VI. CONCLUSION

It is concluded that the application works well and satisfy the end users. The application is tried great and mistakes are appropriately fixed. The application is all the while gotten to from more than one framework.

Synchronous login from more than one spot is attempted. This framework is easy to use so everybody can utilize effectively. Proper documentation is provided. The end client can without much of a stretch see how the entire framework is executed by experiencing the documentation. The system is tested, implemented and the performance is found to be satisfactory. All necessary output is generated. Thus, the paper is completed successfully. Further upgrades can be made to the application, with the goal that the application capacities appealing and valuable way than the present one. The speed of the exchanges turn out to be all the more enough at this point.

REFERENCE

[1] https://coderview.stackex-change.com/questions/179803/codeigniter-crud-using-ajax

[2] https://stackoverflow.com/quetions/34378825/how-to-search-the-keyword-using-ajax

[3] https://sites.google.com/site/ig-noubcafinalyearpapers/paper-report/fleet-management-system-paper-report

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

BOUNDLESS DYNAMIC VIDEO STREAMING FROM MOBILE DEVICES USING CLOUD AS A VIRTUAL SERVICE PROVIDER

P. Jayasree[1] and Dr. V. Saravanan[2]
Assistant Professor[1], Department of Computer Applications, Hindusthan college of Arts and Science
Head &Associate Professor[2], Department of Information Technology, Hindusthan College of Arts and Science

ABSTRACT
With the advent of extremely sophisticated technologies in today's mobile phones, almost all the phones support multimedia facilities which includes capturing photo, videos and making long distance video calls. Even though technologies exists for the efficient usage of mobile phones, a major bug which still exists in the modern phones is the shortage of memory space which flashes as an error message when the space required to store a video or audio exceeds the inbuilt memory. This flaw can be removed by transmitting the video or audio, for its storage by making use of the cloud. It is an efficient idea to integrate cloud computing with mobile devices. The aim of the proposed paper to store the video calls from the mobile device to the cloud as the cloud facilitates Storage as a Service (SaaS). The cloud can also be used as a secure and persistent storage for user data (which includes multimedia and all other rich media) for which all the nodes that are connected to the cloud provide their hardware resources. The memory space from these nodes are partioned into blocks of storage as per the client needs and are contolled and maintained by the central controller. These partitions could be used by the client as a hard drive and he would store the video calls from this mobile phone to the Cloud.

I INTRODUCTION
Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing provides speed application deployment, increase innovation, and lower costs, all while increasing business agility. It also can transform the way we design, build, and deliver applications.

The cloud service model varies from traditional outsourcers in a way that customers do not turn over their own IT resources to be managed and controlled. Instead they plug into the "cloud" for infrastructure services, platform (operating system) services, or software services, treating the "cloud" much as they would treat an internal data center or computer performing the same functions, essentially as a service.

1.1 TYPES OF SERVICE
It's useful to break down the definition of cloud computing into how resources are configured and what that enables you to do. Resources in a cloud have three basic characteristics:

- Pooled-All the resources in the cloud are organized and managed as a common shared pool. Pooling usually begins with servers and storage, which set the scene for data and applications. This , of course, demands common methods for structuring, connecting, and accessing the resources.
- Virtualized- All the resources in the pool are packaged in electronic "shipping containers." Each contains not only the resource itself, but also the business rules governing its access, use, and management.
- Networked- All these modular resources are accessible over a network using standard interfaces that enable them to be combined in "lego" fashion.

In more technical terms, they are available as "Web services."

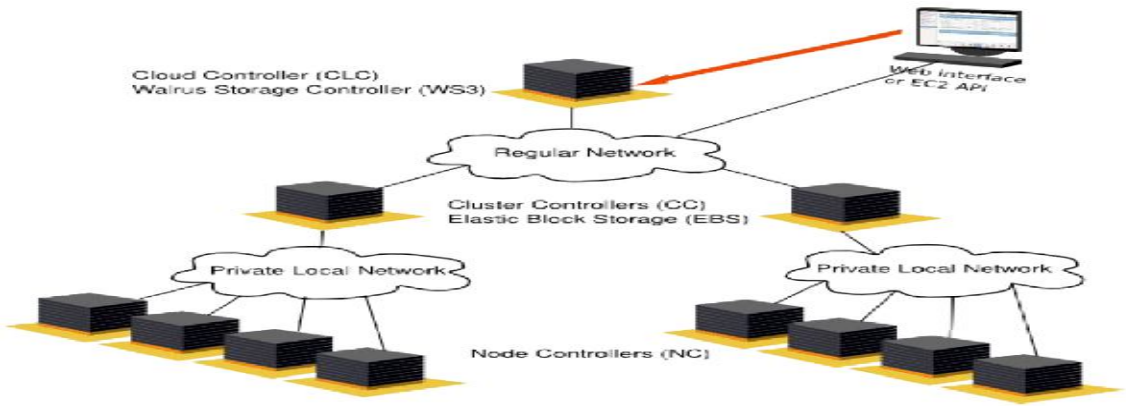


Fig-1: Cloud Architecture

ISSN 2394 - 7780

The main services provided by cloud computing service model can basically be divided into three main categories namely

1) Infrastructure-as-a-Service (IaaS)
Infrastructure-as-a-Service (IaaS) provides virtual servers with unique IP addresses. Also, it provides blocks of storage on demand. Customers benefit from an API from which they can control and manage their servers.

2) Platform-as-a-Service (PaaS)
Platform-as-a-Service (PaaS) is a set of software and development tools that are hosted on the provider's servers. Developers can create applications using the provider's API's. PaaS basically provides virtualized servers on which users can run existing applications or develop new ones without being worried about maintaining the operating systems, server hardware, load balancing or computing capacity.

3) Software-as-a-Service (SaaS)
Software-as-a-Service (SaaS) makes the broadest market. It is the most widely known and broadly used form of cloud computing. In this service, the providers allow the customers only to use their applications. The software through user interface interacts with the user. SaaS offers all the functions of a sophisticated traditional application.

In addition to these standard services , cloud environment can also be used to provide Storage as a Service (SaaS).

1.2 STORAGE-AS-A-SERVICE (SAAS)
The Storage Controller sevice in the Cloud environment provides functionality which is similar to Amazon's EBS (Elastic Block Storage), allowing you to mount block devices (virtual hard disks) to your images that persist when the images are terminated.

EBS volumes provide persistent storage independent of the lifetime of the EC2 instance, and act much like hard drives on a real server. More accurately, they appear as block devices to the operating system. The OS is free to use the device however it wants. In the most common case, a file system is loaded and the volume acts as a hard drive. Another possible use is the creation of RAID arrays by combining two or more EBS volumes. RAID allows increases of speed and/or reliability of EBS. Users can set up and manage storage volumes of sizes from 1GB to 1TB. The volumes support snapshots, which can be taken from a GUI tool or the API. EBS volumes can be attached or detached from instances while they are running, and moved from one instance to another.

1.4 FEATURES OF STORAGE AS A SERVICE

- EBS allows you to create storage volumes from 1 GB to 1 TB that can be mounted as devices UEC instances. Multiple volumes can be mounted to the same instance.
- Storage volumes behave like raw, unformatted block devices, with user supplied device names and a block device interface. You can create a file system on top of EBS volumes, or use them in any other way you would use a block device (like a hard drive).
- EBS volumes are placed in a specific Availability Zone, and can then be attached to instances also in that same Availability Zone.
- Each storage volume is automatically replicated within the same Availability Zone. This prevents data loss due to failure of any single hardware component.
- EBS also provides the ability to create point-in-time snapshots of volumes . These snapshots can be used as the starting point for new EBS volumes, and protect data for long-term durability. The same snapshot can be used to instantiate as many volumes as you wish.

II RELATED WORKS
According to the data from reliable sources, the growth of number of mobile phones users has increased drastically in the past decade. Almost all the mobile phones provided by the companies have support for an internet connection. One main advantage of using cloud computing on mobile phones is the use of an application in a remote computer system in the user's mobile with the implementation of the interface and without the need for the implementation of the actual software.ie, if the product of two large numbers is to be known and if the phone does not have a calculator, it can be imported from another system which is connected to the cloud. There are efficient methods to form a cloud of mobile devices to facilitate the access of applications between the mobiles that form the cloud.

ISSN 2394 - 7780

The cloud can also be used as a common storage for data from which all the authorized users connected to the cloud can access and store the information. Integration of mobile phones and cloud computing has been stated in many works. The cloud can be used as the container for mobile applications. Applications are pre-processed based on the current context of the user minimizes the communication overhead with the cloud. But the applications stated above used either Infrastructure as a service (IAAS) or platform as a service (PAAS) or Software as a service. But we are concentrating on providing Storage as a service (SAAS) to the Cloud clients. In our proposal a common cloud is created through which transfer of multimedia files(audio, video etc.,) is going to be achieved. With the implementation of this proposal, a mobile user can take videos or audios even for days continuously without the need of memory sticks.

2.1 PROPOSED ARCHITECTURE

Since mobile phones do not have enough processing power or memory to support huge amounts of data, Cloud Computing seems to be the ideal solution for mobile phone users. Cloud computing will allow the mobile phone users to have the same amount of data access like "smart" phone users, except for the fact that mobile phone users will not physically have their data stored onto the phone (due to low memory capabilities), it will be on their cloud and accessible to them when required.

A private cloud employs cloud computing within a local or wide area network. (i.e) The same virtualization and highly flexible and scalable methods used in Internet-based datacenters are also used in the private cloud. In the proposed work, a private cloud (Ubuntu Enterprise Cloud - UEC) is set up using computers whose underlying OS is Ubuntu 11.04.

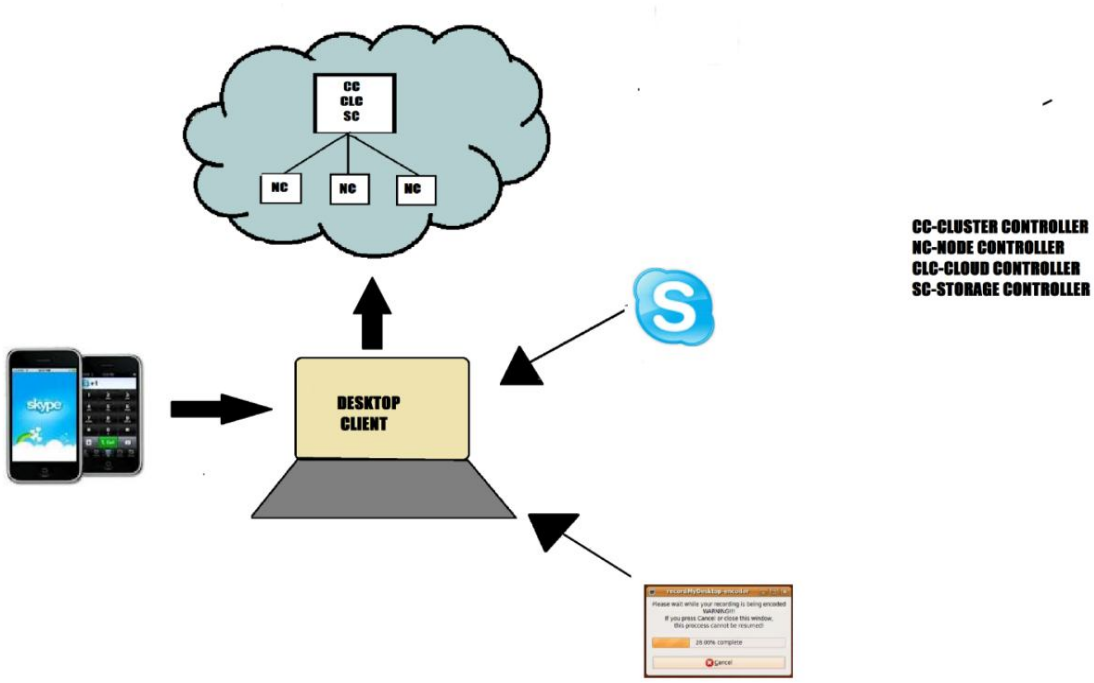


Fig-2: Proposed Architecture

As depicted in fig 2, one of the computer in the cloud architecture acts as the CLOUD CONTROLLER and administers the activities in the cloud. This Master node performs the authentication before providing the cloud services to the clients of UEC.

When the client contacts the cloud for storage (by making use of the web interface), the master node performs the authentication (i.e) the web clients register with their mail id and the authentication is based on passwords.

If the web client is found to be authorized, the master node checks for the node with largest available free space. The web client could partion the storage space available (from 1 GB to 1 TB) and could use it like a hard drive attached to his system.

The Web client makes a Skype call from the mobile device, live streaming of video from the mobile device to the client system is done using Dynamic HTTP Streaming technology. HTTP Live Streaming is an HTTP-based media streaming communications protocol which has the advantage of not requiring any firewall ports being opened outside of the normal ports used by web browsers. It allows video fragments to be cached by browsers, proxies, drastically reducing the load on the source server. Now the Web client could record the video session (streaming) at his system which could then be stored in the UEC.

ISSN 2394 - 7780

2.2 HTTP LIVE STREAMING

HTTP Live Streaming (also known as HLS) is an HTTP-based media streaming communications protocol implemented by Apple Inc as part of their QuickTime X and iPhone software systems. It works by breaking the overall stream into a sequence of small HTTP-based file downloads, each download loading one short chunk of an overall potentially unbounded transport stream. As the stream is played, the client may select from a number of different alternate streams containing the same material encoded at a variety of data rates, allowing the streaming session to adapt to the available data rate. At the start of the streaming session, it downloads an extended M3U (m3u8) playlist containing the metadata for the various sub-streams which are available. Since its requests use only standard HTTP transactions, HTTP Live Streaming is capable of traversing any firewall or proxy server that lets through standard HTTP traffic, unlike UDP-based protocols such as RTP. This also allows a Content delivery network to easily be implemented for any given stream.

An implementation of Live Video Streaming from mobile phone to the cloud with both the ends having compatible versions of skype is a cost effective and adaptive way for mobile devices has been used , which is integrated into the system.

HTTP Live Streaming consists of three parts:

[1] Server component,

[2] Distribution component

[3] Client software.

The **server component** is responsible for taking input streams of media and encoding them digitally, encapsulating them in a format suitable for delivery, and preparing the encapsulated media for distribution. In our paper we have used skype software on ubuntu platform as the server component for receiving video frames from the client which is the mobile phone.

The **distribution component** consists of standard web servers. They are responsible for accepting client requests and delivering prepared media and associated resources to the client. Skype supports a variety of web servers like apache, wamp server etc which are internally integrated with the skype software and are used based on the operating platform.

The **client software** is responsible for determining the appropriate media to request, downloading those resources, and then reassembling them so that the media can be presented to the user in a continuous stream. This is done by the skype version supported by the mobile phone.

In a typical configuration inside the skype , a hardware encoder takes audio-video input, encodes it as H.264 video and AAC audio, and outputs it i n an MPEG-2 Transport Stream, which is then broken into a series of short media files by a software stream segmenter. These files are placed on a web server. The segmenter also creates and maintains an index file containing a list of the media files. The URL of the index file is published on the web server. Client software reads the index, then requests the listed media files in order and displays them without any pauses or gaps between segments.

2.3 STREAMING WITH MOBILE DEVICES

Storing of Live videos on mobile devices is difficult because mobiles devices have limited memory resources . This flaw can be removed by transmitting the video or audio by making use of the cloud. It is an efficient idea to integrate cloud computing with mobile devices. According to the data from reliable sources, the growth of number of mobile phones is almost equal to the population of a country. This essentially means that almost every person in this world is an owner of a mobile phone. Almost all the mobile phones provided by the companies have support for an internet connection. One main advantage of using cloud computing on mobile phones is the use of an application in a remote node in the user's node(mobile). Live streaming established using http live streaming technique will provide adaptive bit rate streaming so that the video is streamed based on the connection and transfer speed of the mobile device.

ISSN 2394 - 7780

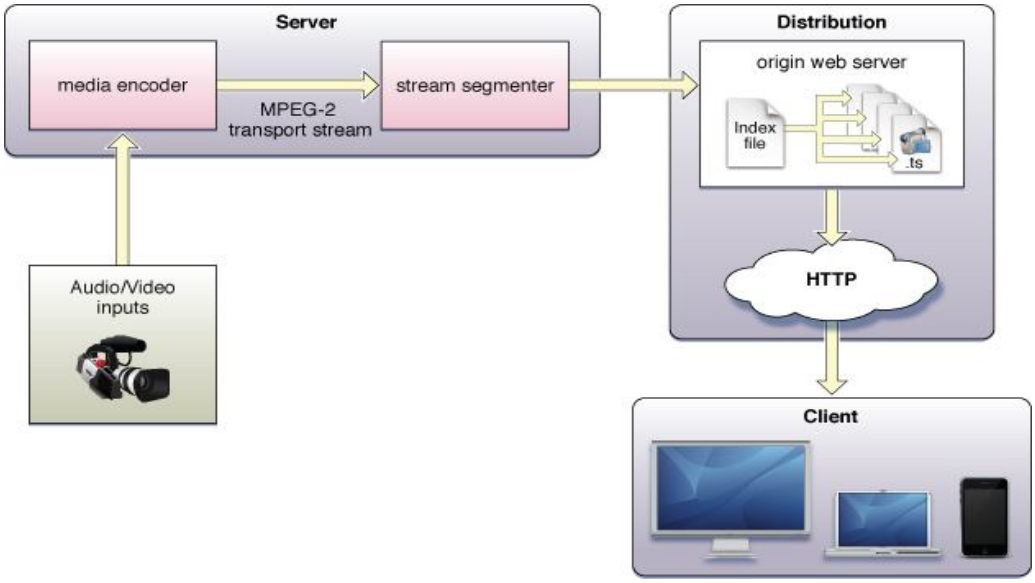


Fig-3: Http Live Streaming Architecture

Cloud computing will allow the mobile phone users to have the same amount of data access like "smart" phone users, except for the fact that mobile phone users will not physically have their data stored onto the phone due to low memory capabilities, it will be on their cloud and accessible to them when required.

III UEC INSTALLATION

Private Cloud is also called an internal cloud which is mainly designed to control the data of an organization, than by getting the resources from other hosted services. This section describes about the basic installation and configuration of Ubuntu Enterprise Cloud as well as the step for creating a virtual machine image and uploading the image to the private cloud.

❖ **Prerequisites**

To deploy a minimal cloud infrastructure, there is a need at least two dedicated systems:

a front end

one or more node(s)

❖ **Node(s)**

The system(s) which are nodes will run:

the node controller (nc)

❖ **Installing the Cloud/Cluster/Storage/Walrus Front End Server**

- Download the 10.04 Server ISO
- Select the "Install Ubuntu Enterprise Cloud".

The installer will detect if any other Eucalyptus components are present.Ifso, then the uec will automatically detect the presence of the controller by detecting its ip address.Hence only one cloud controller can be set up in a specified address range.

❖ **Choosing which components to install, based on the chosen topology**

Cloud Controller (CLC) - The CLC is responsible for exposing and managing the underlying virtualized resources (machines (servers), network, and storage) via user-facing APIs. Currently, the CLC exports a well-defined industry standard API (Amazon EC2) and via a Web-based user interface.

Walrus - Walrus implements scalable "put-get bucket storage." The current implementation of Walrus is interface providing a mechanism for persistent storage and access control of virtual machine images and user data.

Cluster Controller (CC) - The CC controls the execution of virtual machines (VMs) running on the nodes and manages the virtual networking between VMs and between VMs and external users.

Storage Controller (SC) - The SC provides block-level network storage that can be dynamically attached by VMs. The current implementation of the SC supports the Amazon Elastic Block Storage (EBS) semantics.

ISSN 2394 - 7780

Node Controller (NC) - The NC (through the functionality of a hypervisor) controls VM activities, including the execution, inspection, and termination of VM instances.

❖ **Installing the Node Controller(s)**

- Boot from the same ISO on the node(s)
- Select “Install Ubuntu Enterprise Cloud”
- It should detect the Cluster and preselect “Node” install
- Confirm the partitioning scheme
- The rest of the installation should proceed uninterrupted
- After completion of the installation, reboot of the node is done.

3.2 WEB INTERFACE

Once the cloud installation is complete, the cloud structure could be accessed by a web client using the web browser with the URL specific for the cloud installation. This url is in the form “https:<ip_address of the controller>:8443”.

The private cloud for our paper could be accessed with the URL “https:192.168.0.234:8443/”

The web interface lists the following:

- The available images in the store
- The credentials of the private cloud
- The images which have be installed
- The details about admin & various other users
- The other UEC tools available for installation.

The Web client accessing this URL, would be provided with a list of images from which he could run one instance. The instance represents an OS image that could be run using a hypervisor.

This instance is allotted with one IP address from the available list of IP addresses for the Cloud configuration. The image could be downloaded from the Store and could be run by following a set of commands. This instance can then be used to access the cloud resources from the Web clients’s computer system.

This instance can then contact the Cloud controller , partition the available storage space based on its requirements (from 1GB to 1 TB). This partition can then be mounted on the Web clients’s computer system and can be used like a hard drive attached to the system. This is done by running commands for portioning the memory space from the Node controllers (NC) and allocating the partition to the particular client by the Cloud controller (CC).

We make use of this partitions attached to the Client system, to store the video calls that gets stored in the Web client’s system from the Mobile device. The storage of video from the mobile phone is done by using live streaming technique which is described in the next section.

3.3 STREAMING FROM MOBILE DEVICES TO CLOUD

To stream the video captured using mobile devices an application called "SKYPE" is used. The application is installed in t mobile device and also in the desktop client. The Skype application acts as the transmitting end in t mobile device and the receiving end in t client desktop. The video captured through Skype is transmitted over the network using HTTP Streaming to the desktop. In the desktop client the "recordmydesktop" utility is used to store the streamed video in the local storage.

When the mobile device is used and a Skype session is started , theWeb client automatically runs the Recordmydesktop Utility to capture the live video session. This Utility could be used to store the video based on user customization.

IV CONCLUSION

Storage requirements are an important consideration when designing a video surveillance system and many other network video products. If working with video, especially HD video, there arises a need to find a solution in the market for more storage. Though simple external hard drives, portable recording devices, and memory

ISSN 2394 - 7780

sticks are available to serve this purpose they carry the disadvantage of being expensive, less reliable, insufficient to handle efficient throughput of data. The proposed system provides exceptional performance with the flexibility for true scalable storage for digital videos with unified storage features such as unlimited snapshots, high availability etc. The proposed paper eradicates the need of spending an ample amount of capital for storage needs. Also, the Elastic Block Storage of UEC provides secure and persistent video storage. This prevents malicious users from accessing the cloud resources and data stored in the cloud. The proposed paper provides an efficient and secure way to store the video taken by the mobile device using SaaS (Software as a Service) offered by the cloud.

4.2 FURTHER ENHANCEMENTS

The proposed paper requires the Client to start the storage of video from the mobile device to the Ubuntu client system. This could be automated so that the user video gets recorded once the Skype call starts. The software used to store Skype videos can be enhanced to be used for Yahoo and other video call softwares.

The softwares used in the mobile devices can be further developed to record video sessionss from the mobile without using Skype and other softwares (i.e) the mobile user can record his video calls made using Skype and also live video sessions directly captured from the mobile device camera(secondary & primary).

REFERENCES

1. Giurgiu, O. Riva, D. Juric, I. Krivulev, and G. Alonso , "Calling the cloud: enabling mobile phones as interfaces to cloud applications," *Middleware '09 Proceedings of the 10th ACM/IFIP/USENIX International Conferenceon Middleware*, New York, NY, USA, 2009.
2. J.H. Christensen, "Using RESTful web-services and cloud computing to create next generation mobile applications," *Proceeding of the 24th conference on Object oriented programming systems languages andapplications - OOPSLA '09*, New York, New York, USA: ACM Press, 2009.
3. X. Luo, "From Augmented Reality to Augmented Computing: A Look at Cloud-Mobile Convergence,"*International Symposium on Ubiquitous Virtual Reality*, 2009.
4. https://help.ubuntu.com/community/UEC/StorageController
5. http://kiranmurari.wordpress.com/2010/04/27/uec-storage-management/
6. http://ubuntu-tweak.com/source/dajhorn-skype-call-recorder/
7. http://www.howtoforge.com/creating-screencasts-with-recordmydesktop-on-ubuntu-10.04

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

MODERN TRENDS IN ARTIFICIAL INTELLIGENCE

Gowri A
Assistant Professor, Department of Information Technology, Hindusthan College of Arts and Science, Coimbatore

ABSTRACT
Artificial Intelligence (AI) is arguably the most revolutionary technology that is seen in several decades having the potential to completely turn the world upside down and then re-shape it with new contours. In the coming years, we will continue to witness the disruption what deep learning and AI-related technologies can bring to create an impact not only to the software and the internet industry but also to other verticals such as manufacturing, automobile, agriculture, and healthcare and so on. In this paper, we have presented a detailed survey of all the innovations and current trends in Artificial Intelligence.

Keywords: Artificial Intelligence; Contours; Deep Learning; Verticals; Innovations.

I. INTRODUCTION
Artificial intelligence is a approach to make a computer, a robot, or a product to think how smart human think. AI is a study of how human brain think, learn, decide and work, when it tries to solve problems. And finally study outputs intelligent software systems. The aim of AI is to improve computer functions which are related to human knowledge. The intelligence is intangible. It is composed of reasoning, learning, and problem solving, perception and linguistic intelligence. Artificial intelligence as it pushed even further into the mainstream, successfully automating more functionality than ever before. Companies are increasingly exploring applications for AI and the general public has grown accustomed to interacting with the technology on a daily basis. The stage is set for AI to continue transforming the world to technological innovations. In next section, we will give the overview of all the latest trends and innovations happened in AI field.

II. MODERN TECHNOLOGIES BASED ON AI

1. *Tesla's Autopilot*
With important advances in radar, cameras, and GPS, there has been a development of autonomous car technology. Driverless vehicles—which will include fleets of trucks, shuttles, and sharing economy services like Uber—are set to shake up the driving world for businesses and professionals. They are also expected to substantially lower accidents on the road. So what is a "driverless" vehicle? And what is "autonomous driving technology?" A deeper look at Tesla's Autopilot provides insight into the bigger picture of driverless car research. Autopilot does not turn a Tesla into a driverless car. It is Tesla's autonomous driving feature that aims to assist drivers on highways. Autopilot-enabled vehicles can automatically steer, change lanes, and apply brakes—but still require a human behind the wheel.

Fig-1: Tesla's Autopilot [3].

2. *Boxever*
It is an intelligent customer cloud that depends heavily on machine learning to improve the customer's experience in travel industry. So it can reimagining the customer's experience through machine learning and usage of Artificial Intelligence. Boxever activates the states around each customer clearly. It gives single contextual view of all thecustomers. Boxever is a brand based on AI using 1 to 1 personalization.

Fig-2: Boxever [4].

ISSN 2394 - 7780

3. Fin gesture

Fin is the latest innovation in the Wearable technology category which can be worn by the user at the thumb of his/her hand as a ring. The ring then converts the user's whole palm, fingers as numeric keypad and gesture space. Using it, the user can control upto three devices such as Smart TVs, smartphones and car radio just by using taps and swipes. The ring connects with these devices using Bluetooth. This wearable device can also act as a great help to the 285+ million visually impaired people in the world to interact with technology.

Fig-3: Fin gesture [5].

4. *AI robot*

Sophia uses voice recognition (speech-to-text) technology from **Alphabet Inc.** (parent company of Google) and is designed to get smarter over time. Sophia's intelligence software is designed by Hanson Robotics. The AI program analyses conversations and extracts data that allows her to improve responses in the future.

Fig-4: AI Robot [6]

5. *Vinci*

Vinci is the first smart headphones with AI that can understand you. You only have to tell Vinci and it reacts accordingly. You can change tracks accordingly and also gives information about your large queries.

Fig-5: Vinci [7]

6. *Affectiva*

Artificial emotional intelligence or Emotion AI is also known as emotion recognition or emotion detection technology. In market research, this is commonly referred to as facial coding. Affectiva has been offering industry leading technology for the analysis of facial expressions of emotions.Affectiva uses a webcam to track a user's smirks, smiles, frowns, and furrows, which measure the user's levels of surprise, amusement, or confusion.It also uses a webcam to measure a person's heart rate without wearing a sensor by tracking color changes in the person's face, which pulses each time the heart beats.

Fig-6: Affectiva [9].

ISSN 2394 - 7780

7. *Alpha go beat's*

Alpha go is a narrow Artificial intelligence, which is most widely used to play the board game Go. In 2015, it beats a human professional go player. It make use of Monti Carlo tree search to find its moves based on machine learning by Artificial Neural network by extensively training both human and the computer player.

Fig-7: Alpha go beats[10].

8. *Cogito*

Cogito uses real-time emotional intelligence software that incorporates AI and machine learning to analyze voice calls and assist call centers to better interact with their customers in addition to that evaluate and enhance their representatives' performance. It's very challenging to understand or read human emotions, which makes it hard to communicate with clients and to satisfy customers, especially on the phone. MIT Media lab spinoffs like Affectiva and Cogito are focusing on applying principles of Behavioral science to analyze complex human emotions and assist companies to improve their services and predict consumer behavior.

Fig-8: Cogito[11].

9. *Siri and Alexa*

Siri and Alexa Siri is basically a computer program that works as an intelligent personal assistant and knowledge navigator. It is the part of Apple Inc's ios. In other words, it is the voice assistant of Apple. By the help of machine learning, Siri undergone a large series of brain transplants through shifting its silicon- powered mind to Ai powered mind. After various attempts and trails, when apple started using machine learning, there occurred a dramatic improvement in Siri's voice recognition. Then using machine learning again and again, it gets smarter and began to understand our natural language. We can talk to Siri as we talk with our friends and it helps us to get various things done such as sending messages and play calls. It can show us the best route to any location as it works hand- free.

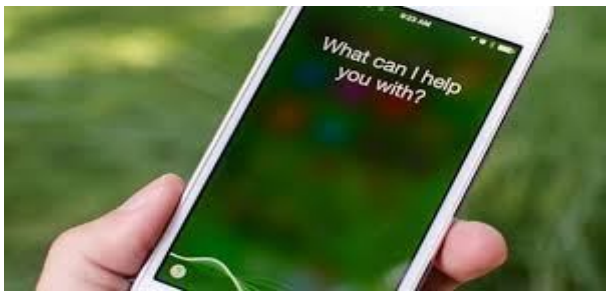


Fig-9: Siri[12].

It can also schedule dates, set our reminders, finddirections and give answers to all our queries. Same as Siri, another AI based technology is Alexa. It basically feels like an AI. She is the personal assistant that lives in cloud and always listening to us through a number of available physical devices that use their brain andcomparably she can hear better than Siri.

ISSN 2394 - 7780

Fig-10: Alexa[13].

10. ***Sense Smart Alarm***

Smart alarm clock with built-in artificial intelligence that can be customized weather, sleep coaching, voice control, environmental sensor and security.This smart clock, which makes active use of IFTTT, seems to be a step forward in smart tabletop clocking if the function is only functioning properly. It automates Voice control of home, Home security system connection, environmental sensors

Fig-1: Smart Alarm [15].

11. ***Netflix***

Netflix's new AI tweaks each scene individually to make video look good even on very slow internet. It uses Artificial intelligence techniques to analyze each shot in a video and then compresses it without affecting the image quality thus reducing the amount of data it uses [2]. Thus it does not only improve the quality of video to larger extent but also save data utility.

12. ***Real Fx***

Real Fx Real FX is an AI based revolution in R/C racings. It is the most realistic next generation racing system. Real FX uses Artificial Intelligence i.e. AI assist helps us to stay on the track but you have got to use your own skill to be the fastest driver in race. It can overtake your opponents, deal with track hazards and comply with pit- stop call- in. Thus, Real FX AI means it can read whatever race track you throw in front of them and both of you and car do not have need to learn.

13. ***AI- CD Beta Robot***

The robot will allow providing clients with work produced through logic-based creative direction grounded on past TV commercial data. In addition to giving creative direction for commercials, the AI-CD ß will also evaluate and gain learning's from results after the commercials have aired, to improve precision for future papers. The robot provides independence from the intangible experience and know-how of human creators, says the official communication from McCann Japan.

Fig-12: *AI- CD Beta Robot* [19].

ISSN 2394 - 7780

III CONCLUSION

From last few decades, a drastic advancement is seen in world of Artificial Intelligence not in only a specificfield but almost all the fields. It has completely revolutionized the world. Thus it is providing an automated path leading to a bright future. But it has disadvantages too if incorrectly used. It is also verycostly, difficult to manage, unemployment, etc. So, along with advantages of AI, it also can be dangerous if not properly handle with care.

REFERENCES

[1]http://www.biginnovationcentre.com/entrepreneurial -co-creation

[2] http://newsvader.com/id/17149773838

[3]https://www.technologyreview.com/s/600772/10-breakthrough-technologies-2016-tesla-autopilot/

[4]https://techcrunch.com/2014/03/05/boxever-apersonalization-platform-for-airlines-raises-6m-led-bypolaris/

[5] https://www.indiegogo.com/papers/fin-wearablering

[6]www.bgr.in/news/meet-jia-jia-chinas-firsthumanoid-robot

[7]https://www.kickstarter.com/papers/inspero/vincifirst-smart-3d-headphones-that-understand-yo

[8]https://en.wikipedia.org/wiki/Affectiva

[10]. https://deepmind.com/research/alphago/

[11]. www.expertsystem.com/cogito/

[12].https://www.recode.net/2016/10/17/13305914/applehire-cmu-artificial-intelligence

[13]. https://docs.api.ai/docs/alexa-integration

[14]. https://www.pandora.com/static/careers/all.html

[15]. https://www.kickstarter.com/papers/hello/senseknow-more-sleep-better

[16]. https://www.theguardian.com › Technology ›Hacking

[17]. https://www.brainasoft.com/braina/

[18].https://news.samsung.com/global/samsung-toacquire-viv-the-next-generation-artificial-intelligenceplatform

[19]. https://en.wikipedia.org/wiki/Reel_FX_Creative_Studio

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

NOVEL ARCHETYPE FOR SENTIMENT MINING USING BIG DATA

A. Raja[1] and Dr. S. Prema[2]
Assistant Professor[1], Kavitha's Gemgates Arts & Science College, Kothampadi, Attur, Salem, Tamil Nadu
Assistant Professor[2], K. S. R. College of Arts & Science, Tiruchengodu, Namakkal, Tamil Nadu

ABSTRACT
Sports Data classification is a significant field of research for prediction of human emotions towards sports-based machine learning algorithms. Sporting events have long served as a natural laboratory to study cognitive processes and emotion in particular. Because they follow uniform rules, are repeated many times, and elicit a variety of measurable (and faithfully recorded) events, sport provides a rich source of data against which to test psychological and economic theories. sporting events command our interest and evokes strong emotions, yet do so in a structured and repeatable way that makes them of particular interest to social science research. Athletics has long served as a natural laboratory for investigating psychological and economic theory. This research, in turn, shapes the way sports are played as, for example, sports economists use findings to make games more exciting and addictive to their fans. Sport involves high stakes for the participants and stimulates strong emotions and considerable economic investment on the part of spectators. Here, we illustrate ways that sentiment analysis techniques can expand our ability here, there are various techniques, their classification and implementation using various types of software tools and machine learning techniques.

I INTRODUCTION
The Web is a huge virtual space for expressing and sharing one's opinions, that influences many aspects of life, with implications for marketing and communication alike. Social Media are influencing consumer's preferences by shaping their attitudes and behaviors. Monitoring the Social Media activities is a good way to measure customer's loyalty, keeping a track on their sentiment towards brands or products. Social Media are the next logical marketing arena. Currently, Facebook is leading the digital marketing space, followed closely by Twitter. Social media sells, and selling drives the internet. The clear, reliable information about consumer preferences is needed which will lead to increasing interest in high level analysis of online social media content. Sentiment analysis is a new, interesting and innovative field.

II. RELATED LITERATURE
Li *et al (*2010) mainly focuses on the document level sentiment classification. In his work, he added sentiment classification is to classify a text according to the sentimental polarities it contains in it. Favorable or unfavorable is the best example for it. Sentiment classification achieved state-of-art performance.

Kawade and Oza*et al (2017)* retrieved tweets about the Uri attack and they found out the emotions in those tweets with the help of machine learning approach. In this work, they recorded the emotions of the people through their tweets. They successfully recorded 5000 tweets and dataset were created for frequently appearing words.

Sentiment analysis with Hadoop was done by Ingle *et al (2015)*. They proposed that analysis of the sentiments of Twitter users through their tweets in order to extract what they think using Hadoop which will process large amount of data and clustering is done faster in Hadoop. Contextual polarity of text can be determined by sentiment analysis.

Dorle*et al (2017)* presents the survey on various sentiment Analysis methodologies and approaches. They stated that some of the methods were not efficient in extracting the sentiment features from the given content of text. Naive Bayes, Support Vector Machine are the machine learning algorithms which has only a limited sentiment classification ranging from between positive and negative.

Yuan (2016) proposed that people are expressing their emotions in twitter and it is one of the easiest ways to express the emotions with all over the world. In this work, Author examined the different methodologies used in the sentiment analysis. In this research data were crawled and manually cleaned. Approximately 20000 tweets were recorded for this research work.

III NLP AND BIG DATA
Natural language processing is complex and is the intersection of artificial intelligence, computational linguistics, and computer science. The user has to import a file containing text should perform the following steps for natural language processing.

1. Sentence Segmentation

ISSN 2394 - 7780

2. Tokenization
3. Stemming/Lemmatization
4. Part-of-Speech tagging
5. Parsing
6. Named Entity Recognition
7. Co-reference resolution

Sentence segmentation – It identifies starting of sentence and ending of sentence in the given text

Tokenization – It identifies different words, numbers, and symbols.

Stemming – It removes the ending of words like 'eating' is reduced to 'eat.'

Part of speech (POS) tagging – It deputizes each word in a sentence its respective part-of-speech tag such as labeling word as noun or adverb.

Parsing – It involves breaking down given text into different categories.

Named Entity Recognition – It identifies entities such as individuals, place and time within the documents.

Co-Reference resolution – It is about explaining the relationship of given word in a sentence with a previous and the next sentence.

IV DRAWBACKS OF EXISTING METHOD

The following difficulties in sentimental analysis were listed.

1. Shortness of messages, really poor representation
2. Usage of informal language
3. Frequent misspellings
4. Use of emoticons
5. Mentions to Particular user
6. Sentiment depends on the opinion holder
7. Sentiments depends also on the social context

V PROPOSED METHOD

In existing methods, SVM is utilized for the problem. The drawback of the SVM is slow in test phase and complex in size. A new learning algorithm for Single Hidden Layer Feed Forward Networks (SLFNs), called Extreme Learning Machine (ELM), which helps in solving regression and classification problems. Mainly ELM is employed to predict the sentiments. This algorithm also used to reach good solutions analytically and its learning speed is faster than other traditional methods. In this process randomly selecting the input weights and systematically identifies the output weights of SLFNs. This algorithm will have the best generalization performance at extremely faster speed. The structure of ELM network is shown in figure 2. ELM contains the three layer they are input layer, hidden layer and an output layer. ELM has several important features which are differ from traditional learning algorithms applied for feed forward neural networks.

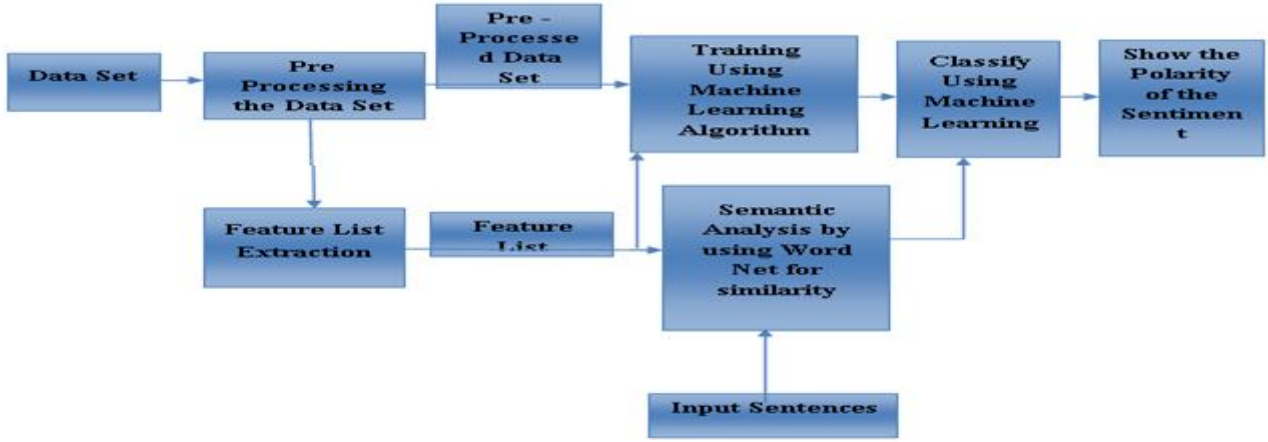


Figure-1: Sentimental Analysis using Machine Learning Algorithm

ISSN 2394 - 7780

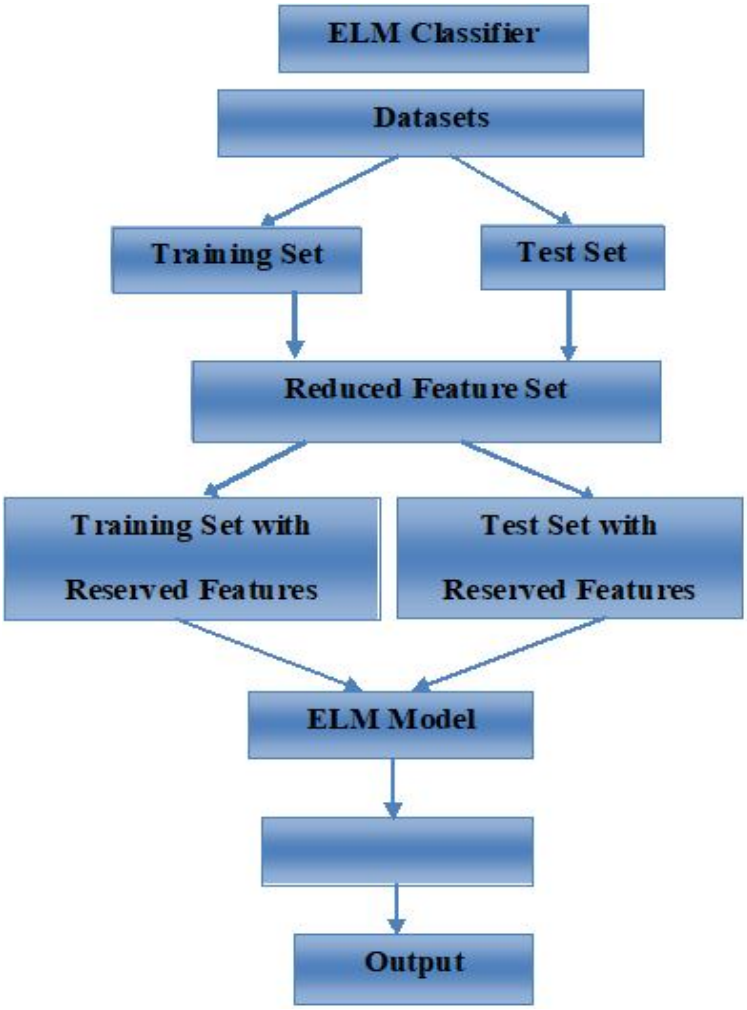


Figure-2: Proposed Archetype

VI CONCLUSION

Sports Data classification is a significant field of research for prediction of human emotions towards sports-based machine learning algorithms. Sporting events have long served as a natural laboratory to study cognitive processes and emotion in particular. Because they follow uniform rules, are repeated many times, and elicit a variety of measurable (and faithfully recorded) events, sport provides a rich source of data against which to test psychological and economic theories. sporting events command our interest and evokes strong emotions, yet do so in a structured and repeatable way that makes them of particular interest to social science research. Athletics has long served as a natural laboratory for investigating psychological and economic theory. This research, in turn, shapes the way sports are played as, for example, sports economists use findings to make games more exciting and addictive to their fans. Sport involves high stakes for the participants and stimulates strong emotions and considerable economic investment on the part of spectators. Here, we illustrate ways that sentiment analysis techniques can expand our ability here, there are various techniques, their classification and implementation using various types of software tools and machine learning techniques.

REFERENCES

[1]. Li, S., Lee, S. Y. M., Chen, Y., Huang, C. R., & Zhou, G. (2010, August). Sentiment classification and polarity shifting. In Proceedings of the 23rd International Conference on Computational Linguistics (pp. 635-643). Association for Computational Linguistics.

[2]. Kawade, D. R., &Oza, K. S. (2017). Sentiment Analysis: Machine Learning Approach. International Journal of Engineering and Technology (IJET), 9(3).

[3]. Ingle, A., Kante, A., Samak, S., & Kumari, A. (2015). Sentiment analysis of twitter data using hadoop. International Journal of Engineering Research and General Science, 3(6).

[4]. Dorleet, S., &Pise, N. N. (2017). Sentiment Analysis Methods and Approach: Survey.

[5]. Yuan, B. (2016). Sentiment Analysis Of Twitter Data. Rensselaer Polytechnic Institute, New York.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

SECURED TECNIQUES OF DATA ANONYMIZATION FOR SECLUSION PRESERVATION

S. Saranya[1] and K. Nandini[2]
[1]Assistant Professor, Hindusthan College of arts and Science, Coimbatore
[2] Student, Sri Ramakrishna College of Arts and Science for Women, Coimbatore

ABSTRACT
The information there on the widespread use of internet should be made available in a way that a person's privacy is not affected. Recently, numerous organizations are accumulating massive amounts of information which are stored in enormous databases. Information publisher collect information from data holders, and publicize this information to data receiver for mining, statistical analysis etc. The publish information is useful for data mining & research. The released information can disclose secret in sequence of a person. For providing safety to the information, many anonymization techniques have been designed for isolation preserving and micro data publishing. Such as generalization and bucketization, have been designed for privacy preserving microdata publishing. Recent work has shown that generalization loses considerable amount of information, especially for high dimensional data. Bucketization, on the other hand, does not prevent membership disclosure and does not apply for data that do not have a clear separation between quasi-identifying attributes and sensitive attributes. In the proposed method, the new novel technique called slicing. In this system it will partition the data set both vertically and horizontally. Vertical partitioning is done by grouping attributes into columns based on the correlations among the attributes. Each column contains a subset of attributes that are highly correlated. Horizontal partitioning is done by grouping tuple's into buckets. Finally, within each bucket, values in each column are randomly permutated (or sorted) to break the linking between different columns. When the data is published the sensitive value attributes are not easily readable by any user. This method can enhance the security of the data as an adversary cannot easily identify the value of the sensitive attributes.

I INTRODUCTION
Data mining is looking for concealed, suitable, and potentially useful patterns in enormous data sets. Data Mining is all about discovering unsuspected/ earlier unknown associations amongst the information. It is a multi-disciplinary ability that uses machine learning, statistics, and AI and database knowledge. The insights imitative via Data Mining can be used for marketing, fraud detection, and scientific discovery, etc. Data mining is also called as information discovery, Knowledge extraction, data/pattern analysis, information harvesting, etc.

In trendy and commercial world can be sharing any type of confidential information's day-by-day. Commonly, the conceptual mechanism anonymization is protects the confidential information's or secret data. Data Anonymization is a method that makes data valueless to anyone except the holder of the information. It is one of the methods for transforming the information that it prevents identification of key in order from an illegal person

The Anonymization is to reduce the difficulties of the real world by strategically reducing the ancillary and unnecessary details. But the anonymization is not a process that only removes and selects the data. Anonymization is one of the confidentiality preserving techniques that control the in sequence, making the data detection difficult to anybody except the owners. It is different from that of data encryption Anonymization involves replacing (or recoding) a value with a less specific but semantically consistent value. Anonymization is a viable technique to secure data. It limits the mistreatment of sensitive information, but is not a entire solution to preserve confidentiality. Lots of techniques for anonymization have been implemented, but still there is a panic of security breach.

There are number of techniques for anonymizing the data before it is published. The popular methods are suppression, generalization, bucketization and slicing

Suppression has assured values of the attributes are replaced by an asterisk '*'. All or some standards of a column may be replaced by '*'. In the anonymized table below, we have replaced all the standards in the 'Name' attribute and all the standards in the 'Religion' attribute with a '*'.

Generalization: This procedure replaces quasi identifier attributes with fewer precise standards. For example, Birth date may be widespread to year of birth only.

Bucketization is to separation the tuples in T into buckets, and then to split the responsive attribute from the non-sensitive ones by indiscriminately permuting the susceptible attribute values within each bucket. The

ISSN 2394 - 7780

sanitized information then consists of the buckets with permuted susceptible values. We use bucketization as the technique of construct the published information from the creative table T, although all our results grasp for full-domain overview as well. Partitition the tuples into and within every bucket, we apply an self-governing random permutation to the line containing S-values. The resulting set of buckets, denoted by B, is then available.

III METHODOLOGY

Suppression will replaces tuple or attribute values with special symbol "**" that is instead of the original value we replace it with some anonymous value throughout the database in dataset sensitive data will generated by suppression. Such as the value of name and the type of disease is replaced with an "**"

Generalization will replaces attribute values with semantically unvarying but less particular value. Due to this substitution, many files have same QI values. Generalization replaces exact values with a more general description to hide the details of attributes, making the QIDs less identifying. If the value is numeric, it may be transformed to a range of values. The attributes like, age attribute value 45 can be changed to range 40- 60. If the value is a categorical value, it may be changed to another categorical value denoting a broader concept of the original categorical value.

Bucketization is similar to generalization, but it does not modify any QI attribute or sensitive attribute. Instead, after it divides the records into a number of partitions, it assigns a distinctive ID known as GID to each partition, and all tuple's in this partition are said to have the same GID value. Then, two tables has been proceeded, namely quasi attribute (QI) table and the sensitive table. The anonymize information consist of a set of buckets with permuted susceptible attribute values. Note that the grouping formed by bucketization is equivalent to the grouping formed by generalization, except that bucketization data contains all the original tuple values while generalization data contains some generalized tuple's values. In particular, bucketization has been used for anonym zing high-dimensional data. Bucketization has the benefit of allowing users to obtain the original exact values for data study. Bucketization data contains all the original tuple values unlike generalization data. It also allows users to obtain the original specific values for data analysis but it does not prohibit membership disclosure. It also needs a clear difference between QIs and SAs.

In the proposed method, the new novel technique called slicing. It improves the current state of the art. Slicing partitions the data set both vertically and horizontally. Vertical partitioning is complete by combination attributes into columns based on the correlations among the attributes. Each column contains a subset of attributes that are highly correlated. Horizontal partitioning is done by combination tuples into buckets. Finally, within every bucket, values in each column are indiscriminately permutated (or sorted) to break the linking between different columns. This reduces the dimensionality of the information and conserves improved utility than generalization and bucketization. But this method can be made safer by adding a characteristic of encryption into it. In this scheme it will division the data set both vertically and horizontally and then encrypts the sensitive information attributes so that when the information is published the sensitive value attributes are not easily readable by any user. The method of decryption can be tell to only some precise users and then they can use the information, for all the other users the information will be in encrypted form only. This technique can enhance the protection of the information as an adversary cannot easily recognize the value of the sensitive attributes.

IV EXPERIMENTAL RESULTS:

Slicing methodology is one of the best methods for privacy preserving information publishing as it provides feature disclosure as well as conserve information utility and it can also better effort on high dimensional data. The slicing method which divides the data’s as both horizontally and vertically. It is one of the best techniques of anonymization. Compared with generalization, slicing efficiently utilizes the information and dissimilar bucketization it prevents membership disclosure. Slicing will efficiently work on high dimensional data. However, the proposed method, the information is available the sensitive value attributes are not simply readable by any user The various sensitive attributes will not be able to be viewed by any adversary which will decrease the chances of violation of any individual's confidentiality drastically. Therefore, it is an efficient technique for privacy preserving information publishing.

ISSN 2394 - 7780

The following table 1 is the published original table

patsecid	patname	Fullname	age	gender	addr	email	phone	pincode	doentry
1	1	nandhu	21	female	vadavalli	nandhu96@gmail.com	1234567890	641041	15-02-2019
6	11	saranya	45	female	vadavalli	saran96@gmail.com	8188373583	641022	05-03-2019
5	12	ram	22	male	coimbatore	ram23@yahoo.com	8222373583	640041	02-03-2019
7	15	gangagowri	23	female	kerala	ganga23@yahoo.com	8111373583	641022	06-03-2019
2	2	shankar	23	male	anna nagar	shankar@gmail.com	8133373582	641042	19-02-2019
8	22	guna	55	female	vadavalli	hguna@yahoo.com	8222373587	641045	06-03-2019
9	3	lassie	32	female	Tata bath bangalore	lassieshe@yahoo.com	7867088865	640054	14-03-2019
3	4	gowri	42	female	gandhipuram	gowri23@yahoo.com	8144575685	641022	02-03-2019
4	5	raj	41	male	gandhipuram	raj23@yahoo.com	8144373583	641042	02-03-2019

Table 2 is the published data by suppression

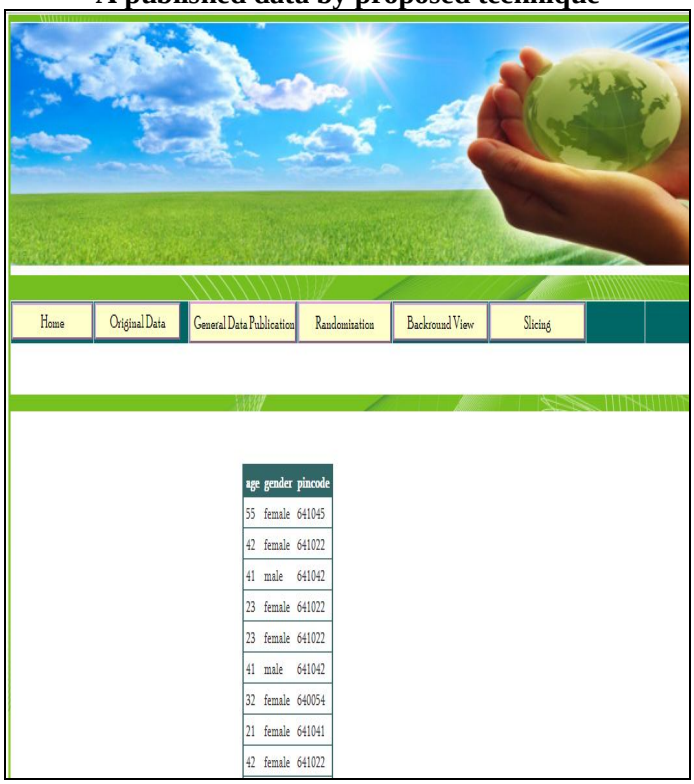
patsecid	patname	fullname	age	symp	disease	hospname	docname	checkup	doreport
####	***	$$$$$$$$$$	32	Fever	Pneumonia	kg	raj	Weekly	@@@@@@
####	***	$$$$$$$$$$	21	stomach pain	Stomach Cancer	krish	krishna	instfin	@@@@@@
####	***	$$$$$$$$$$	21	stomach pain	Cancer	kg	hema	ok	@@@@@@

A published table by generalization and bucketization

Age	sex	Zipcode	group_id
[20-40]	*	6400**	2
[20-40]	*	6410**	2
[20-40]	*	6410**	2
[20-40]	*	6410**	1
[20-40]	*	6400**	3
[40-60]	*	6410**	3
[40-60]	*	6410**	2
[40-60]	*	6410**	2
[40-60]	*	6410**	2

ISSN 2394 - 7780

A published data by proposed technique



CONCLUSION

Data anonymization is one of the significant technique to protected the publish information. There are different techniques of data anonymization like generalization and bucketization. These method have been used for preserving seclusion of publish information. Anonymization is a realistic method to protect the information. It restricts the mishandling of sensitive information, but is not a absolute solution to preserve confidentiality. In the proposed work, the new method for preserving the privacy data is done by the slicing. Slicing is promising technique for handling high-dimensional data. By using slicing for the huge datasets, can help to secrete the original data from real world, identity the records will be changed or removed and then shown to the real world. This makes database more protect and also keep data privacy in the real world.

REFERENCES

[1] P.Samarati and L. Sweeney, "Protecting privacy when disclosing information:-anonymity and its enforcement through generalization and suppression," SRI International, SRI-CSL-98-04, 1998

[2] M. Barbaro and T. Zeller, "A face is exposed for AOL searcher no. 4417749," New York Times, 2006.

[3]. S.Saranya and Dr. Punithavalli:" An Efficient Centroid Selection Algorithm for K-means Clustering", International Journal of Multidisciplinary ResearchAcademy,vol1,issue3,pg:124-140

[4] Ms S Saranya, Ms P Deepika, Ms S Sasikala, S Jansi, Ms A Kiruthika: "Accelerating Unique Strategy for Centroid Priming in KMeans Clustering" IJIRST (International Journal for Innovative Research in Science & Technology),volume3,pg:40-47

[5] Aggarwal. C., "On K-Anonymity and the Curse of Dimensionality," In Conf. Very Large Databases (VLDB), pages 901-909, 2005.

[6] D. J. Martin, D. Kifer, A. Machanavajjhala, J. Gehrke, and J. Y. Halpern. Worst-case background knowledge for privacy-preserving data publishing. In ICDE, pages 126–135, 2007

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

AN IOT BASED SMART HEALTH MONITORING SYSTEM

Dr. S. Sasikala[1], M. Selvapriya[2] and Pandiyarajan[3]
Associate Professor[1], Department of Computer Applications, Hindusthan College of Arts and Science, Coimbatore
Assistant Professor[2], PG and Research Department of Computer Science, Hindusthan College of Arts and Science, Coimbatore
Student[3], Department of BCA, Hindusthan College of Arts and Science, Coimbatore

ABSTRACT
Our paper is a working model which incorporates sensors to measure parameters like body temperature, heart beat rate. An Arduino microcontroller board is used for analyzing the inputs from the patient Temperature, heartbeat. This paper provides a device which will continuously monitor the vital parameters to be monitored for a patient. If any critical situation arises in a patient, this unit also raises an alarm. This is very useful for future analysis and review of patient's health condition. For more versatile medical applications, this paper can be improvised, by incorporating dental sensors and annunciation systems, thereby making it useful in hospitals as a very efficient and dedicated patient care system. In recent years, the world is facing a common problem that the number of elderly people is increasing. Hence, the problem of home-care for elderly people is very important. In this, IoT is becoming a major platform for many services & applications, also using Node MCU not just as a sensor node but also a controller here. Paper proposes a generic health monitoring system as a step forward to the progress made in this department till now.

I INTRODUCTION
Improving the efficiency of healthcare infrastructures and biomedical systems is one of the most challenging goals of modern-day society. In fact, the need of delivering quality care to patients while reducing the healthcare costs and, at the same time, tackling the nursing staff shortage problem is a primary issue. As highlighted, in fact, current procedures for patient monitoring, care, management, and supervision are often manually executed by nursing staff. This represents, de facto, an efficiency bottleneck, which could be a cause of even tragic errors in practices. Recent advances in the design of Internet-of-Things (IoT) technologies are spurring the development of smart systems to support and improve healthcare- and biomedical-related processes. Automatic identification and tracking of people and biomedical devices in hospitals, correct drug–patient associations, real-time monitoring of patients' physiological parameters for early detection of clinical deterioration are only a few of the possible examples.

REVIEW OF HEALTH CARE TECHNIQUES IN ARDUINO
The implementation of universal health insurance has changed medical behavior in Taiwan. Because of advances in medical technology and an increase in national income, the life expectancy at birth in Taiwan is gradually rising. Therefore, aging has become a widespread social phenomenon. According to the Ministry of the Interior, the number of people aged 65 years and older reached 2,868,163 (12.22% of the population) in June 2015.

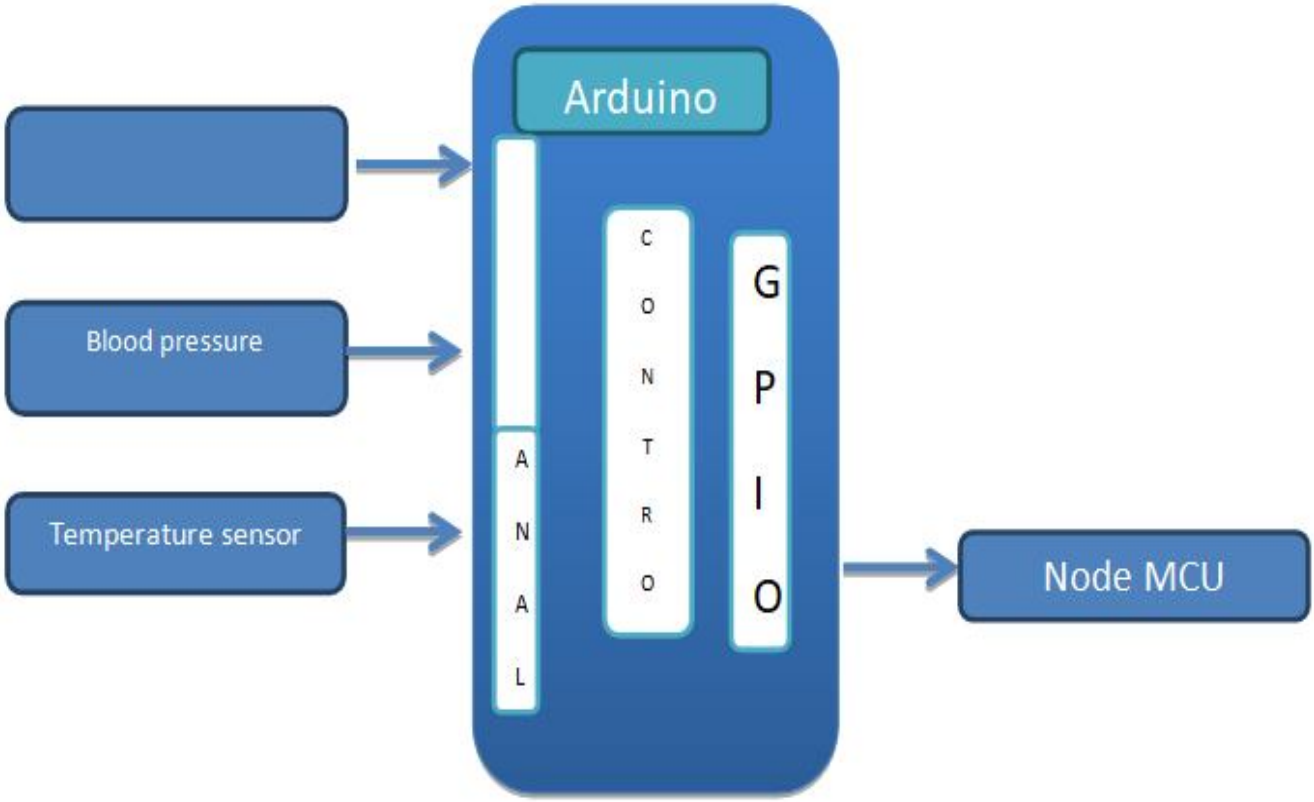
Along with a swift decline in the fertility rate, population aging is a serious challenge for Taiwan. In the future, the healthcare system will become even more crucial, because most elderly people require a high level of care and the population of elderly people with disabilities is expected to grow rapidly. Home-based long-term care is a key government policy, a major part of which is the development of "Tele-Home Care" (THC). THC provides family caregivers with the physiology and living information of elderly patients through their mobile phones and Internet devices, and can thereby reduce the cost of national health insurance and help people stay and live at home as independently as possible.

II SYSTEM STUDY
EXISTING SYSTEM
- Manual monitoring
- Distance between patient and monitoring unit are minimum.
- In existing 8051 controller is used.
- Single parameter monitoring system.

PROPOSED SYSTEM
- Remote monitoring

ISSN 2394 - 7780

- Monitoring the patient as easy one.
- In proposed Arduino microcontroller is used.
- Multi parameter monitoring system.



The figure shows the functional block diagram of the system hardware. The system has been designed to take several inputs to measure physiological parameters of human such as temperature, heart rate. The inputs from the sensors are integrated and processed. The results are displayed on the Monitor. The program is a user interface, allowing a report on the current status of the individual.Once the user has connected to the receiver unit, data is automatically updated on the screen. Heartbeat and body temperature were displayed on the display. The design is modular which makes it rather easy and straight forward to add extra sensors for measuring and monitoring other parameters.

This paper introduces a wireless health monitoring system that can monitor a human 24x7. This system consists of a number of the part. Controlling and data processing is done through the Arduino Uno board, all the sensors are connected to Arduino UNO. Through this system, we can measure ECG, heartbeat, BP, and spo2. Through sensors, it is possible to measure all these values. Here all the sensors are powered using a solar power system. All these analog sensors can be connected to Arduino through any of the six analog pins. These values are then used for detecting any critical situation. In case of a critical situation, an alert can be given as a message. Also, it is possible to monitor the person's health from any location in the world through the Thingspeak cloud. Data from sensors is uploaded to the Thingspeak periodically without any interruption if the internet is available. Here ESP8266 wifi module is used for connecting Arduino to the internet.

Health is the most important part of any human's life without health it is useless to any treasure of life. Most humans live a busy life in which going to a doctor for weekly or even monthly checkup is an impossible task. Without monitoring your health it is not possible to whether you are a healthy or sick person. This problem leads to the design of a product which monitors your health every day without going to a doctor. In this paper, a system is designed as a prototype for monitoring alerting based on the health of a person.

This system is fully automated little or no human help is needed. Any doctor can monitor this person from anywhere through the internet.

DRAWBACKS OF EXISTING SYSTEM

- Diagnosing with help of a doctor
- Conventional devices that can only measure a particular parameter

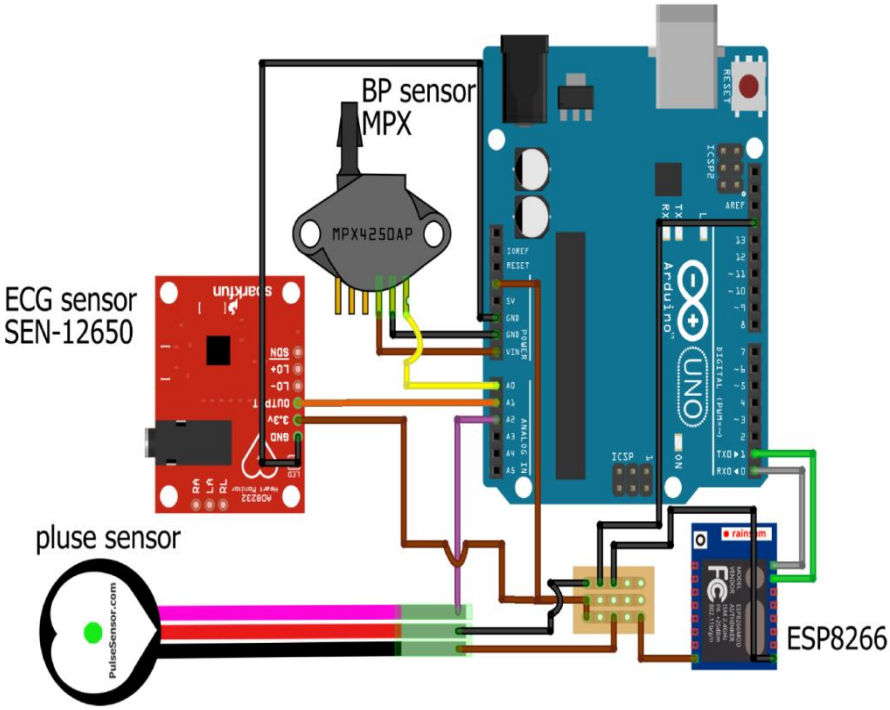
ISSN 2394 - 7780

- Devices that have to be connected invasively to get measurements
- No automated system exists
- Smart watches are expensive and not specifically for healthcare

ADVANTAGES OF PROPOSED SYSTEM

- In this paper, a system for 24x7 human health monitoring is designed and implemented
- In this system, the Arduino Uno board is used for collecting and processing all data
- Different sensors are used for measuring different parameters
- All this data is uploaded to thingspeak for remote analysis
- An ESP8266 module is used for connecting to the internet
- A solar power system is provided for powering all the sensors

CIRCUIT DIAGRAM



III. SYSTEM REQUIREMENTS

SENSOR

- The heartbeat sensor is based on the principle of photo plethysmography. It measures the change in volume of blood through any organ of the body which causes a change in the light intensity through that organ.
- Temperature sensor is a qualitative measure for classifying how matter appears to be hot or cold

HARDWARE REQUIREMENTS

- Arduino UNO
- Heart beat sensor
- Temperature sensor
- LCD
- Node MCU
- Buzzer

SOFTWARE REQUIREMENTS

Arduino IDE

ISSN 2394 - 7780

IV. SYSTEM IMPLEMENTATION

HEARTBEAT SENSOR

A person's heartbeat is the sound of the valves in his/her's heart contracting or expanding as they force blood from one region to another. The number of times the heart beats per minute (BPM), is the heart beat rate and the beat of the heart that can be felt in any artery that lies close to the skin is the pulse.

PRINCIPLE OF OPERATION

The heartbeat sensor is based on the principle of photo plethysmography. It measures the change in volume of blood through any organ of the body which causes a change in the light intensity through that organ (a vascular region). In case of applications where heart pulse rate is to be monitored, the timing of the pulses is more important. The flow of blood volume is decided by the rate of heart pulses and since light is absorbed by blood, the signal pulses are equivalent to the heart beat pulses.

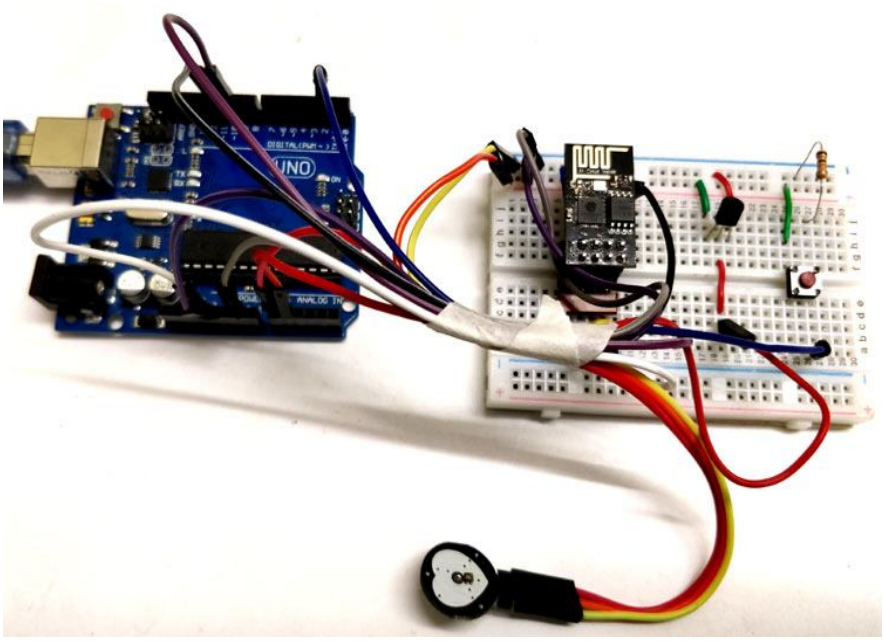
The basic heartbeat sensor consists of a light emitting diode and a detector like a light detecting resistor or a photodiode. The heart beat pulses causes a variation in the flow of blood to different regions of the body. When a tissue is illuminated with the light source, i.e. light emitted by the led, it either reflects (a finger tissue) or transmits the light (earlobe). Some of the light is absorbed by the blood and the transmitted or the reflected light is received by the light detector. The amount of light absorbed depends on the blood volume in that tissue. The detector output is in form of electrical signal and is proportional to the heart beat rate.

This signal is actually a DC signal relating to the tissues and the blood volume and the AC component synchronous with the heart beat and caused by pulsatile changes in arterial blood volume is superimposed on the DC signal. Thus the major requirement is to isolate that AC component as it is of prime importance.

SENSOR USING IN HEALTH MONITORING SYSTEM

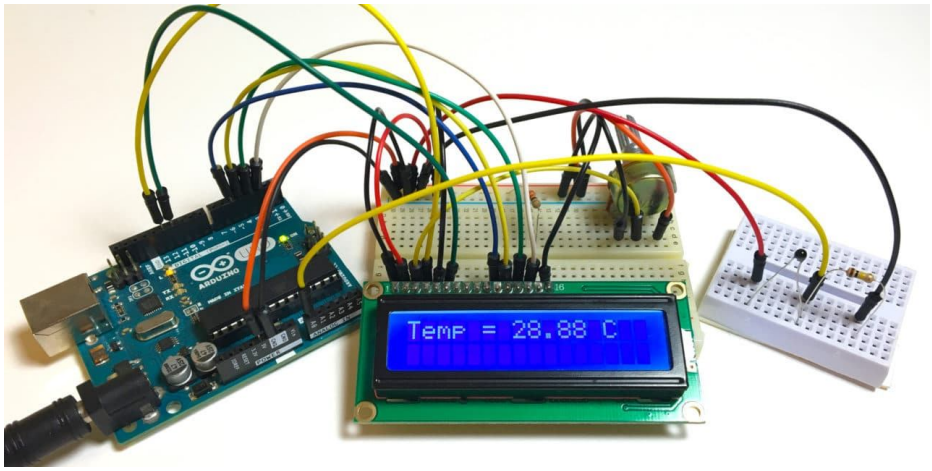
Heartbeat Sensor is an electronic device that is used to measure the heart rate i.e. speed of the heartbeat. Monitoring body temperature, heart rate and blood pressure are the basic things that we do in order to keep us healthy.

ISSN 2394 - 7780

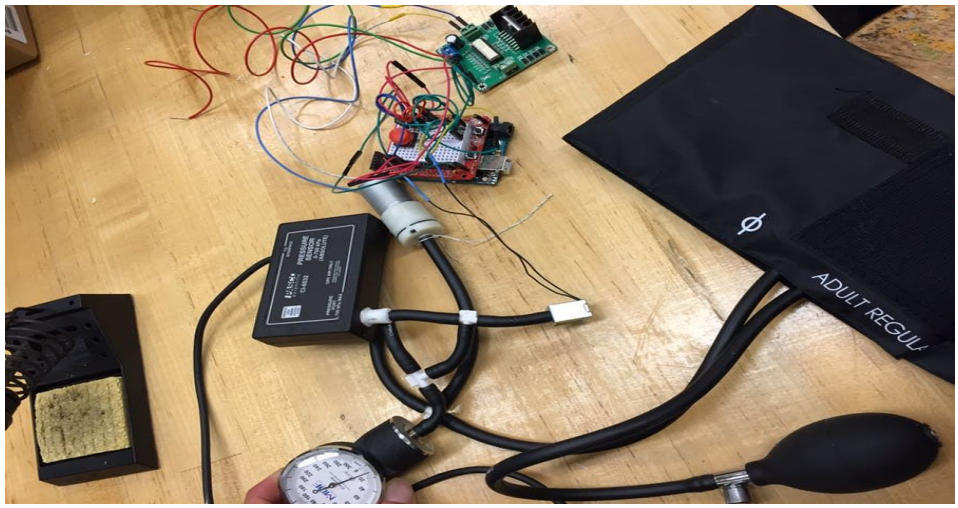


HEARTBEAT SENSOR

The Temperature Sensor LM35 series are precision integrated-circuit temperature devices with an output voltage linearly proportional to the Centigrade temperature.



TEMPERATURE SENSOR



BLOOD PRESSURE SENSOR

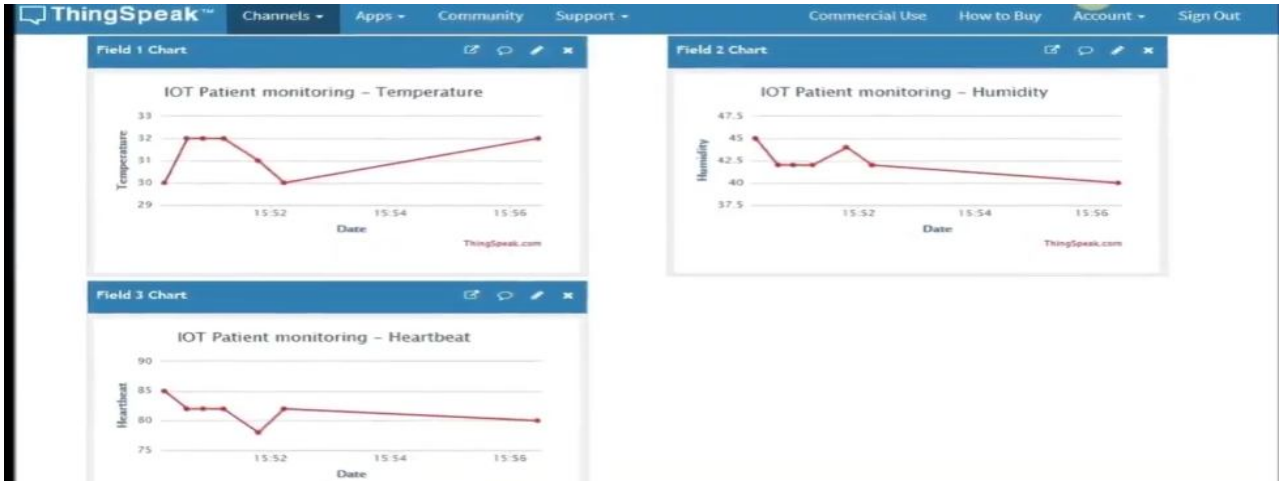
Blood pressure monitors are primarily used in clinical settings to analyze patient's blood pressure and in order to prescribe the best treatment. This low cost monitor inflates and deflates the blood pressure cuff in order to

ISSN 2394 - 7780

determine the mean arterial pressure. It then roughly approximates the diastolic and systolic pressures based on the mathematically relationship between mean arterial pressure, diastolic, and systolic pressures. The results are then displayed on the LCD screen.

EXPERIMENTAL RESULTS

OUTPUT IMAGE OF HEALTH MONITORING SYSTEM



The above figure shows the graphical representations of levels of temperature , humidity and heartbeat are uploaded to the thingspeak cloud. This page can be accessed by any person who has the username and the password of the account.

VI CONCLUSION

Being an application of Internet of Things (IoT), this paper proves to be an autonomous health monitoring system. The said paper is able to continuously sense pulse rate and body temperature of the person wearing the band. The paper can be further extended to create a whole new system of connected smart health bands so that everyone will be monitored and given proper treatment at right time. With more advanced and reliable sensors, the health band can be more efficient. This paper can be a life saying band for people who do not have sufficient time to take care of their health or people who live alone and do not have someone to look after.

REFERENCE

1. http://www.instructables.com/id/HealthBand/
2. Temitope O. Takpor and Aderemi A. Atayero, “Integrating Internet of Things and eHealth Solutions for Students’ Healthcare”, WCE 2015, July.
3. https://pulsesensor.com Fig.4. Displaying temperature value on the cloud.Fig.5.Displaying pulse value on the cloud.Fig.6. Live values displayed in an android application.Fig. 7.SMS with pulse and location link. IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI-2017) 1686
4. https://www.sparkfun.com/products/11574
5. https://www.elprocus.com/heartbeat-sensor-workingapplication/
6. https://www.sparkfun.com/products/8777
7. https://www.espressif.com/sites/default/files/0aesp8266ex_datasheet_en_1.pdf
8. SiddharthKokalki, RiteshSontakke, PawanMundada, Akshay Mali “A novel Temperature Sensing and Monitoring Using IoT”
9. http://www.instructables.com/id/Temperature-Sensingand-Monitoring-Using-Arduino-a/
10. David Lake, Rodolfo Milito, Monique Morrow and Rajesh Vargheese Internet of Things: Architectural Framework for eHealth Security.
11. Srijani Mukherjee, KoustabhDolui, SoumyaKantiDatta “Patient health management system using e-health

ISSN 2394 - 7780

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

A COMPARITIVE ANALYSIS OF DSR AND AODV ROUTING PROTOCOL IN MOBILE ADHOC NETWORK

S. Sasikala
PhD Research Scholar, Department of Computer Science, Sri Saraswathi Thyagaraja College, Pollachi

ABSTRACT
Mobile Ad hoc network is an infrastructure less network where nodes communicate without central administration or network transportation. MANET can use multiple hops to exchange data. Routing protocols are needed to finding path to deliver of messages between nodes to destination. The various reactive and Proactive Protocols is used to compare Ad hoc routing protocols. In this paper, we compare a two popular routing protocols, DSR and AODV based on various performance metrics such as Routing overhead, End to end delay ,Packet delivery Ratio, Throughput and Network life time. The comparative study analyzes the performance of both DSR and AODV protocol with respect to the metrics comparison, which could be useful for future research.

Keywords: Manet, Aodv, Dsr

I. INTRODUCTION

Wireless networks is a network which provide connection without wired between sender and receiver. The network is connected by radio waves for communication where it can be extended to any place or building without the need for a wired connection. The Wireless networks are classified into two categories: Infrastructure networks and AdHoc networks as shown in Figure1.

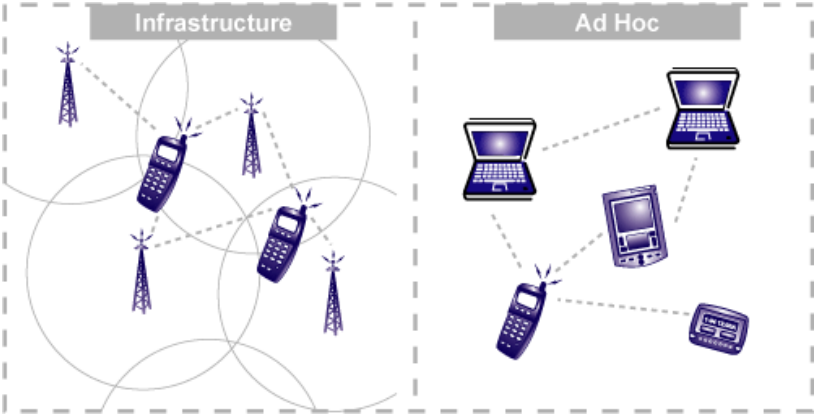


Fig-1: Wireless network structure

II. INFRASTRUCTURE NETWORK

Infrastructure network is a networking framework 802.11 in which devices communicate through Access point(AP).In a infrastructure network it communicates through AP with a wired network. A set of wireless station is referred as Basic Service Set(BSS).It provides communication between set of two or more BSSs to form a single subnetwork[1].

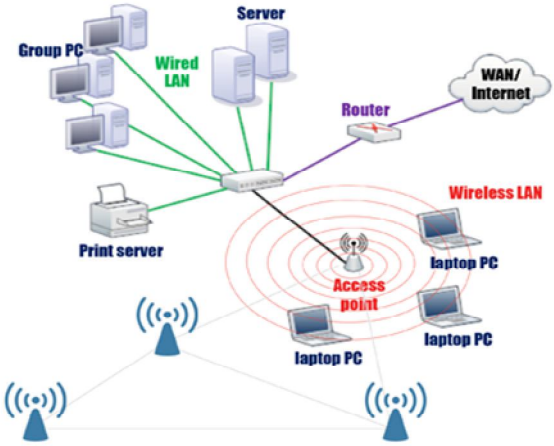


Fig-2: Infrastructure Network

ISSN 2394 - 7780

WIRELESS ADHOC NETWORK

Wireless ad-hoc network is a decentralized network becoming one of the most animated networks. It is as movable dynamic field of communication networks has increased significantly in recent years. A mobile ad-hoc network (MANET) communicates through wireless links with one another. Mobile Adhoc Network is formed by collecting portable devices like laptops, smart phones, sensors, etc. that communicate through wireless links with one another. This network creates various applications by functioning with multiple points of connection with cellular networks. It is an infrastructure less network where wireless communication that can join together at any time and at any place dynamically. In this type of network mobile hosts, act as a router, that is connected to one another by wireless links. This network can easily move randomly and dynamically change[2]. Due to the autonomous system the mobile nodes have no base station. In MANET each node has limited transmission range so packets are transmitted to any node in the network with the help of multiple hops.

III COMPARISON OF DSR AND AODV ROUTING PROTOCOL

A routing protocol plays a vital role in measuring the performance of a reactive and proactive protocol. In a proactive protocol when nodes move from one position to another, it's less efficient to use where route will be already established before a packet is sent. Therefore, in (on –demand) reactive protocols such as Dynamic Source Routing (DSR) protocol are more suitable to be used in MANET networks. In our research we compare t two well-known popular routing protocols; AODV and DSR .based on various performance metrics such as Network life time, End to end delay, Packet delivery Ratio, Throughput and Normalized routing overhead[3].

DSR PROTOCOL

DSR uses 'source routing' i.e. the senders node is aware of the entire hop-by-hop route to the destination and these routes area unit keep in its route-cache. In route cache variety of routes could also be offered to the destination[4]. Once the destination isn't distinguished caches the packet and finds the routing data to the destination by causing route queries to any or all end nodes. Then it sends the Route Replies back the provider so information measure overhead reduces, battery power conserves and enormous routing updates are going to be avoided. The DSR routing protocol uses 2 major mechanisms to find routes and maintain the route data from one node to a different. These are: Route discovery – to find the route between the supply and destination and Route maintenance – facing with route failure, another route is invoked from the destination [5].

DSR incorporates a distinctive advantage that provides routing Since the route could be a partial of the packet, routing loops, each short – lived or long – lived, cannot be created as detection or eliminating quickly. This property creates variety of useful optimizations for DSR. This routing protocol responds the thought of supply routing, which means that the supply defines the total path from the sender to the destination node that the messages ought to be transmitted, and so ensures that routing is inconsequently loop free within the network[6]. In DSR every packet carries all data associated with route in its header. Therefore, the intermediate nodes unit permissible to accumulate the route knowledge in their routing tables for future usage [7]. If a node ought to send a packet to a distinct one, and it's no route, it initiates a route discovery methodology. The route discovery in DSR is performed by flooding the network with RREQ packets. However, the most distinction is that the RREQ packet contains a route record throughout this protocol. Whereas the RREQ traverses the intermediate nodes, each node performs a cache check to look at, if it's a route to the destination; if it doesn't, it appends its own address within the route record and forwards the packet to consequent node. Once the RREQ packet reaches the destination or Associate in Nursing intermediate node that has the destination route, it generates a RREP message, that contains the route record of the RREQ as well as the addresses of the intermediatenodes.Therefore,the supply node can presumably receive

Several RREP packets from completely different nodes containing multiple routes to the destination. The DSR protocol selects one in all these routes that constitutes the shortest one and caches the others just in case of a link failure. DSR permits those nodes that have already controlled a RREQ message to reject to any extent further RREQ relating to a similar supply node[8]. One huge advantage is that intermediate nodes will learn routes from the supply routes within the packets they receive. Since finding a route is a costly operation in terms of your time, information measure and energy, this can be a robust argument for mistreatment supply routing. Another advantage of supply routing is that it avoids the necessity for up-to-date routing data with in the intermediate. Finally, it avoids routing loops simply as a result of the whole route is decided by one node rather than creating the choice hop-by-hop [9]. If any link of this route is broken, the supply node is au fait by a route error (RERR) packet and this route is discarded from cache. Intermediate nodes store the supply route in their cache for future use [10].

ISSN 2394 - 7780

AODV PROTOCOL

AODV is on-demand routing protocol, during which the route search method is initiated between the deliver and destination node as once required. During this protocol every node maintains routing info within the range of a routing table having one entry per destination [11] .AODV uses the destination sequence range to ensure the route freshness and loop freedom of the route . The disadvantage of such protocols is that broadcasting springs from request for packets. Hence, some stale routes may be gift within the routing tables that aren't updated. It suggests that act us routing isn't detectable speedily Whenever missive of invitation is received for causation a message by Associate in Nursing AODV router, its routing table is going to be checked for existence of a route. Once a route exists, the message is forwarded to succeeding hop by the router. Otherwise, the message are going to be sent in an exceedingly message queue, then a route request are going to be initiated to search out a route[12].

Four varieties of management messages are utilized in AODV protocol. Route Request (RREQ) and Route Reply (RREP) messages are used for route finding. Route Error (RERR) message sand hi messages are utilized for route repairs[13].Route discovery method begins one among the nodes needs to send packets. That node sends Route Request (RREQ) packets to its neighbors. Neighbors come back RREP, packets if they need corresponding route to destination. However, if they don't have corresponding route, they forward RREQ packets to their neighbors, except the origin node. Also, they use these packets to create reverse ways to the supply node. This method happens till a route has been found [14]. Each mobile node maintains a next hop routing table, that contains the destinations to that it presently includes a route.

In AODV, once a supply node need to send packets to the destination however no route is accessible, it initiates a route discovery method[15].The reactive property of the routing protocol implies that it solely requests a route once it wants one and doesn't need that the mobile nodes maintain routes to destinations. If Associate in deliver intermediate node is unable to forward the packet to succeeding hop or destination because of link failures, it generates the route error (RERR) message by tagging it with a better destination sequence range[16].once the sender node receives the RERR message, it initiates a replacement route discovery for the destination node [17,18].

V SIMULATION RESULTS OF AODV AND DSR PROTOCOL

1. Average end-to-end delay: **-** It signifies how long it will take a packet to travel from source to destination node. This metric is useful when delay caused while discovering path from source to destination.

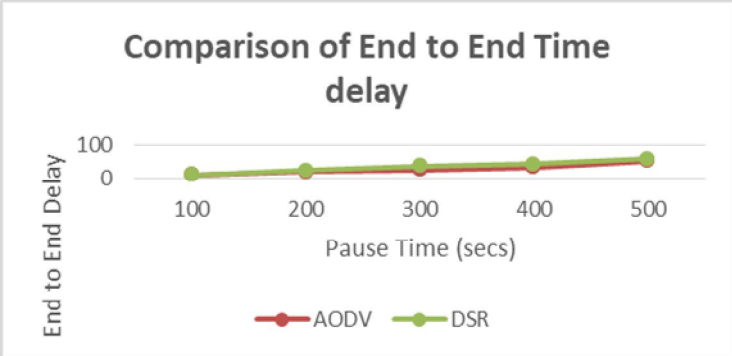


Fig-3: Average End to End delay for AODV and DSR

Metrics	AODV	DSR
100	9.706	9.7147
200	19.756	24.2686
300	25.246	36.8946
400	34.457	42.9894
500	54.258	59.0124

Fig-4: End to End Delay Metrics value for AODV and DSR

2. ***Packet Delivery Ratio***- It is defined as the number of packets totally delivered to the Destination, number of data packets supposed to be received .

ISSN 2394 - 7780

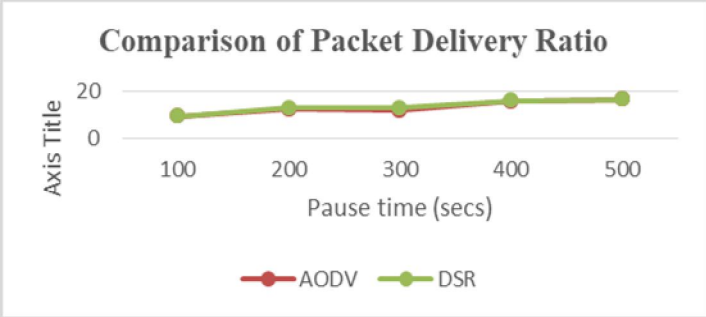


Fig-5: Packet Delivery Ratio for AODV and DSR

Metrics	AODV	DSR
100	9.5547	9.5689
200	9.756	10.2686
300	11.246	11.8946
400	12.457	12.9894
500	14.258	15.0124

Fig-6: PDR Metrics value for AODV and DSR

3. ***Throughput-*** Throughput is the ratio of number of packets sent and total number of packets delivered .

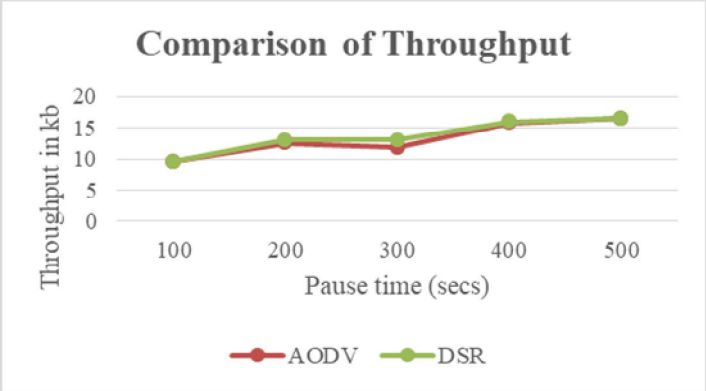


Fig-7: Throughput of DSR and AODV

Metrics	AODV	DSR
100	9.5487	9.5609
200	12.564	12.987
300	11.789	12.987
400	15.789	15.994
500	16.487	16.487

Fig-8: Throughput Metrics value for AODV and DSR

4. ***Normalized Routing Overhead:*** It represent the ratio of number of routing packets and number of received packets at the destination.

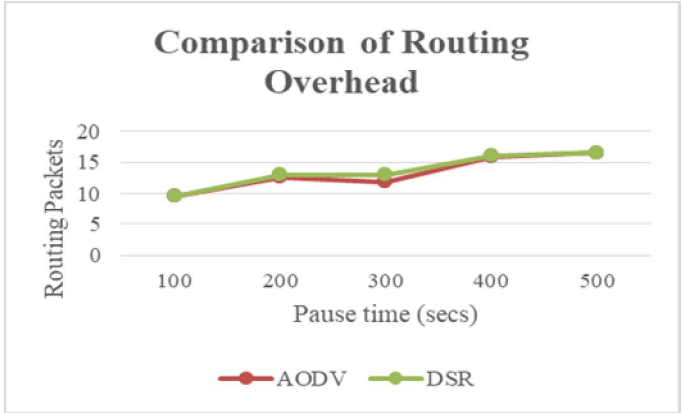


Fig-9: Routing Overhead for AODV and DSR

ISSN 2394 - 7780

Metrics	AODV	DSR
100	9.7168	9.7043
200	10.984	10.991
300	14.487	15.789
400	15.201	15.217
500	16.478	16.784

Fig-10: Routing Overhead Metrics value for AODV and DSR

5. ***Network life time***

It is the period of time from the moment of network performs until it runout of battery.

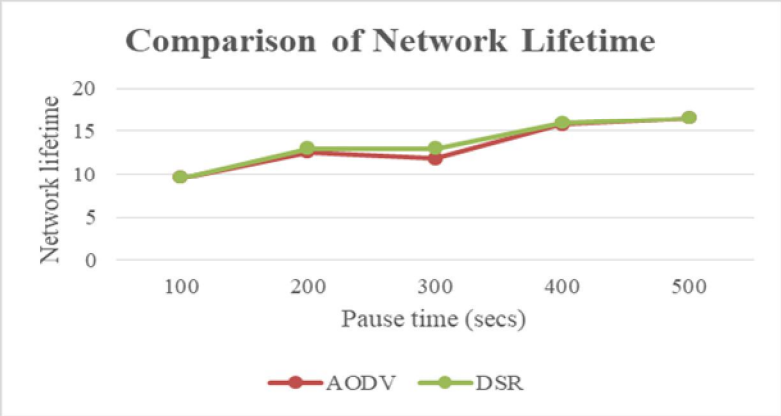


Fig-11: Network Life Time for AODV and DSR

Metrics	AODV	DSR
100	9.5467	9.5589
200	10.956	11.012
300	11.278	11.898
400	12.457	12.944
500	13.878	13.4871

Fig-12: Network Life Time metrics value for AODV and DSR

V CONCLUSION

In this paper, we discussed the performance of two MANET reactive routing protocols; AODV and DSR. The different performance metrics were simulated using Ns-2. However, both protocols have illustrated comparable results of performance metrics.DSR provide better result when compared to AODV. In our experiments, DSR has shown better performance in terms of efficiency for a packet size, routing overhead, Throughput, End to End delay, and network life time.

REFERENCES

1. Banoj Kumar panda, Janmejaya Swain, Durga Prasad Mishra,Benudhar Sahu, “Analysis of effect of Mobility and Transmission power on AODV and DSR in Mobile Adhoc Network,” IEEE,2014.
2. Mehdi Barati, Kayvan Atefi, Farshad Khosravi and Yashar Azab , “Performance Evaluation Of Energy Consumption for AODV and DSR Routing Protocol in MANET, ” International Conference on Computer and information Science, IEEE,2012.
3. N. Adam, M.Y. Ismail, J. Abdullah, “Effect of Node Density on Performances of Three MANET Routing Protocols, “International conference on electronics devices, system and application,2010.
4. Tanya Koohpayeh Araghi, Mazdak Zamani, Azizah Abdul Mnaf, “Performance Analysis in Reactive Routing Protocols in Wireless Mobile Ad Hoc Networks Using DSR, AODV and AOMDV ,”International Conference on Informatics and Creative Multimedia, IEEE,2013.
5. Sabina Barakovi, Jasmina Barakovi, “Comparative Performance Evaluation of Mobile Ad Hoc Routing Protocols,’’ MIPRO, May, 2010, Opatija, Croatia.
6. Bhabani Sankar Gouda, Ashish Kumar Dass, K.Lakshmi Narayana, “A Comprehensive Performance Analysis of Energy Efficient Routing Protocols in different traffic based Mobile Ad-hoc Networks, IEEE, 2013.

ISSN 2394 - 7780

7. Michalis Papadopoulos, Constandinos X., Georgios Skourletopoulos, “Performance Analysis of Reactive Routing Protocols in Mobile Ad hoc Networks.
8. “Wireless Ad Hoc Networks” Zygmunt J. Haas, Jing Deng,Ben Liang, Panagiotis Papadimitratos, and S. Sajama Cornell University School of Electrical and Computer Engineering.
9. Hemanth Narra, Yufei Cheng,Egemen K. Çetinkaya, JustinP. Rohrer and James P.G. Sterbenz“Destination-SequencedDistance Vector (DSDV) Routing Protocol Implementationin ns-3”.
10. AkshaiAggarwal,SavitaGandhi,NirbhayChaubey,”Performanc e Analysis of AODV,DSDV and DSR in MANETs”.
11. P. Manickam T. Guru Baskar , M.Girija, Dr.D.Manimegala“Performance Comparisons of Routing Protocols in MobileAd- Hoc Networks”.
12. Sabina Barakovic, Suad Kasapovic, and JasminaBarakovic,” Comparison of MANET Routing Protocols inDifferent Traffic and Mobility Models”, Telfor Journal, Vol.2, No. 1, 2010.
13. D.Verma, D.Chandrawanshi, “Comparative Performance Evaluation of AODV over CBR andTCP Traffic, International Journal of Computer Science and Technology,” Vol. 2, Issue 2, June 2011.
14. T. Dyer, R. Boppana, “A Comparison of TCP Performance over Three Routing Protocols forMobile Ad Hoc Networks, ACM Symposium on Mobile Ad Hoc Networking & Computing(Mobihoc),” October 2001.
15. S. Gupta, Ashish Chourey, “PERFORMANCE EVALUATION OF AODV PROTOCOL UNDERPACKET DROP ATTACKS IN MANET,” International Journal of Research in ComputerScience ISSN 2249-8265 Vol. 2, Issue 1, 2011.
16. B. Paul , Md. Ibrahim , Md. Bikas , “Experimental Analysis of AODV & DSR over TCP & CBRConnections with Varying Speed and Node Density in VANET,” International Journal ofComputer Applications (0975 – 8887) Vol. 24, No.4, June 2011.
17. T. Asma, G. Rajneesh, T. Sunil, “Comparative Performance Analysis of DSDV, AODV and DSRRouting Protocols in MANET using NS2,” in International Conference on Advances inComputer Engineering, Bangalore, Karnataka, India, 2010, 330.
18. J. Broch, D. A. Maltz, D. B. Johnson, Y. Hu, J. Jetcheva, “A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols,” in Fourth Annual ACM/IEEE InternationalConference on Mobile Computing and Networking, Ballas, Texas, 1998.
19. S. Sagar, J. Saqib, A. Bibi, N. Javaid, "Evaluating and Comparing the Performance of DYMOand OLSR in MANETs and in VANETs," in Multitopic Conference (INMIC), 2011 IEEE International, Karachi, Pakistan,2011.
20. M. Quan-xing, X. Lei, "DYMO Routing Protocol Research and Simulation Based on NS2," inInternational Conference on Computer Application and System Modeling, Taiyuan, Shanxi,China, 2010, V14-41.

International Journal of Advance and Innovative Research
Volume 6, Issue 2 (XI): April - June, 2019
ISSN 2394 - 7780

CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD

M. Surendhar[1] and G. Sivabrindha[2]
Student[1] and Assistant Professor[2], Department of Information Technology, Hindusthan College of Arts and Science

ABSTRACT
Distributed computing has shaped the applied and infrastructural reason for tomorrow's processing. The worldwide figuring foundation is quickly moving towards cloud based design. While it is essential to take focal points of could based processing by methods for sending it in enhanced parts, the security angles in a cloud based processing condition stays at the center of intrigue. Cloud based administrations and specialist co-ops are being advanced which has brought about another business pattern dependent on cloud innovation. With the presentation of various cloud based administrations and geologically scattered cloud administration suppliers, delicate data of various elements are typically put away in remote servers and areas with the potential outcomes of being presented to undesirable gatherings in circumstances where the cloud servers putting away those data are undermined. In the event that security isn't vigorous and reliable, the adaptability and focal points that distributed computing brings to the table will have little believability. This paper shows an audit on the cloud processing ideas just as security issues inborn inside the setting of distributed computing and cloud framework.

I. INTRODUCTION
Ongoing advancements in the field of could processing have gigantically changed the method for figuring just as the idea of processing assets. In a cloud based processing framework, the assets are regularly in another person's reason or arrange and got too remotely by the cloud client (Petre, 2012; Ogigau-Neamtiu, 2012; Singh and jangwal, 2012). Handling is done remotely suggesting the way that the information and different components from an individual need to be transmitted to the cloud framework or server for handling; and the yield is returned endless supply of required handling. At times, it may be required or possibly conceivable for an individual to store information on remote cloud servers. This gives the accompanying three touchy states or on the other hand situations that are of specific worry inside the operational setting of distributed computing:

• The transmission of individual touchy information to the cloud server,

• The transmission of information from the cloud server to customers' PCs and

• The capacity of customers' close to home information in cloud servers which are remote server not possessed by the customers.

All the over three conditions of distributed computing are extremely inclined to security break that makes the research and examination inside the security parts of distributed computing practice a goal one. There have been various diverse mixes that are being utilized in distributed computing domain, be that as it may, the center idea stay same – the framework, or generally, the assets remain elsewhere with another person's possession and the clients 'lease' it for the time they utilize the framework (Bisong and Rahman, 2011; Rashmi, Sahoo and Mehfuz, 2013; Qaisar and Khawaja, 2012). Now and again, put away touchy information at remote cloud servers are additionally to be checked. Security has been at the center of safe figuring rehearses. When it is workable for any undesirable gathering to 'sneak' on any private PCs by methods for various methods for 'hacking'; the arrangement of broadening the degree to get to somebody's close to home information by methods for distributed computing in the end raises further security concerns .Cloud is for the most part sorted as private cloud, network cloud, open cloud and half and half cloud (Ogigau-Neamtiu, 2012; Singh and jangwal, 2012; Rashmi et al., 2013; Qaisar and Khawaja, 2012; Kuyoro, Ibikunle and Awodele, 2011; Suresh and Prasad, 2012; Youssef,2012) - the dialog in this paper expect just a single class of cloud exists which is open cloud; as this suspicion will well fulfill every one of the attributes of any other kind of cloud. Because of its enhanced probability, the way to deal with distributed computing is being thought to be as the fifth utility to join the class of existing utilities water, power, gas and communication (Buyya, Yeo, Venugopal, Broberg and Brandic, 2009) instead of being simply one more administration

II. CLOUD COMPUTING INFRASTRUCTURE
The term distributed computing is fairly an idea which is a summed up importance developed from dispersed and lattice figuring. Distributed computing is depicted as the posterity of disseminated and framework figuring by a few creators (Che, Duan, Zhang and Fan, 2011).The clear importance of distributed computing alludes to the highlights and situations where all out registering should be possible by utilizing another person's system

ISSN 2394 - 7780

where responsibility for and delicate assets are of outside parties. As a rule practice, the dispersive idea of the assets that are viewed as the 'cloud' to the clients are basically as conveyed registering; however this isn't clear or by its meaning of distributed computing, don't basically need to be evident to the clients. As of late, the cloud has developed in two wide viewpoints – to lease the framework in cloud, or to lease a particular administration in the cloud. Where the previous one manages the equipment what's more, programming utilization on the cloud, the later one is restricted just with the 'delicate' items or administrations from the cloud administration and framework suppliers. The registering scene has been presented with various wordings like SaaS (Software as a Service), PaaS (Platform as a Service) what's more, IaaS (Infrastructure as a Service) with the development of distributed computing. As talked about before, the term 'distributed computing' is fairly an idea, so are the phrasings to characterize distinctive mixes of distributed computing.

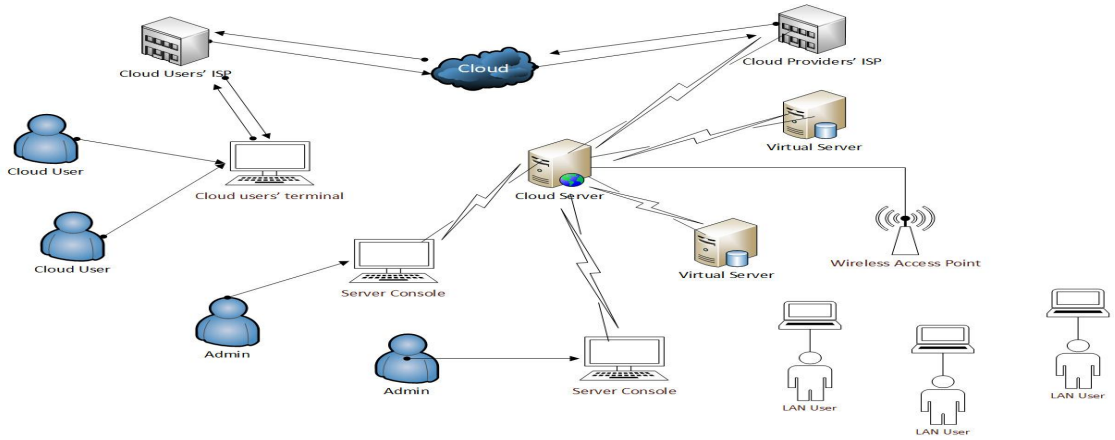


Figure-1: A Typical Cloud Architecture

The outline of cloud engineering in figure 1 is a least difficult one where couple of complex attributes of distributed computing (for example repetition, server replication, and geographic scattering of the cloud suppliers' system) are not appeared the reason for the representation is to set up the course of action that makes the idea of distributed computing an unmistakable one. The system design is clear as crystal with the recognizable proof of cloud clients when considered in-accordance with the discourse of the distributed computing idea introduced before. One eminent part from the design is that, while the cloud clients are obviously recognized and named as needs be expected to their remote area and methods for remote access to the cloud servers, the administrator clients who are managing the cloud servers are not cloud clients in any structure as for the cloud administration supplier's system in the situation.[4]

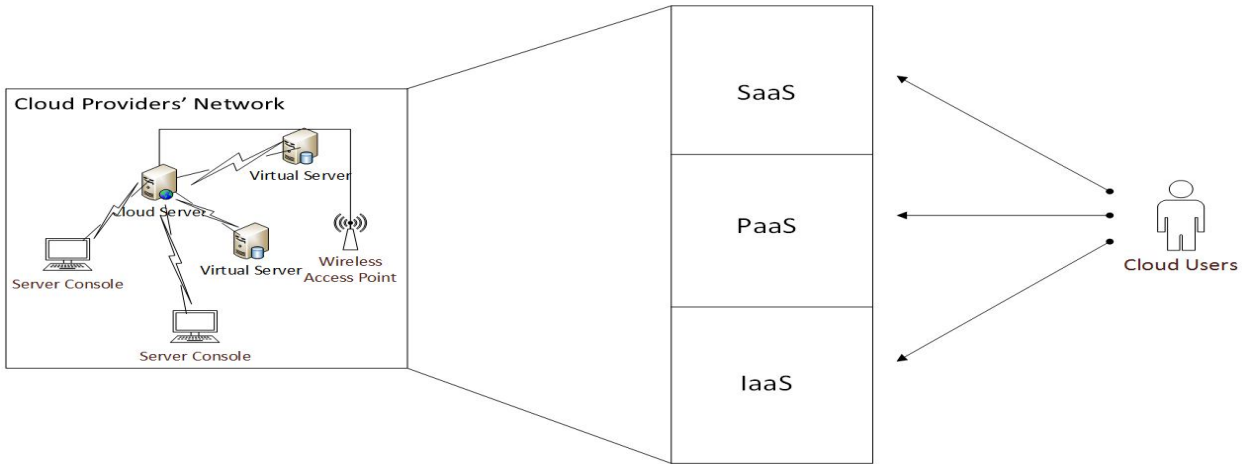


Figure-2: Cloud Service Hierarchy

As delineated in figure 2, the specialized subtleties, game plans and the board of the cloud administration suppliers' system is straightforward to the cloud client. From the finish of the cloud client, the administration from the supplier comes as SaaS, PaaS or IaaS where the cloud client has no expectation or on the other hand stress over what goes on in the interior course of action of the cloud specialist organizations' system. Any disturbance of any structure for whatever is the reason, consider to the cloud clients either as administration inaccessibility or quality weakening – its effect and approaches to counter this interruption is a basic part for the cloud foundation. Security issues may assume an animating job as a driving element for any previously mentioned disturbance.

ISSN 2394 - 7780

III. AUTHENTICATION IN CLOUD

Security is the most organized perspective for any type of registering, making it a self-evident desire that security issues are critical for cloud condition too. As the distributed computing approach could be related with having clients' delicate information put away both at customers' end also as in cloud servers, character the executives and verification are vital in distributed computing (Kim and Hong, 2012; Emam, 2013; Han, Susilo and Mu, 2013; Yassin, Jin, Ibrahim, Qiang and Zou, 2012). Check of qualified clients' accreditations and ensuring such qualifications are a piece of fundamental security issues in the cloud - infringement in these territories could prompt undetected security rupture (Kumar, 2012) at any rate to some degree for some period. A conceivable confirmation situation for a cloud framework is outlined in figure 3

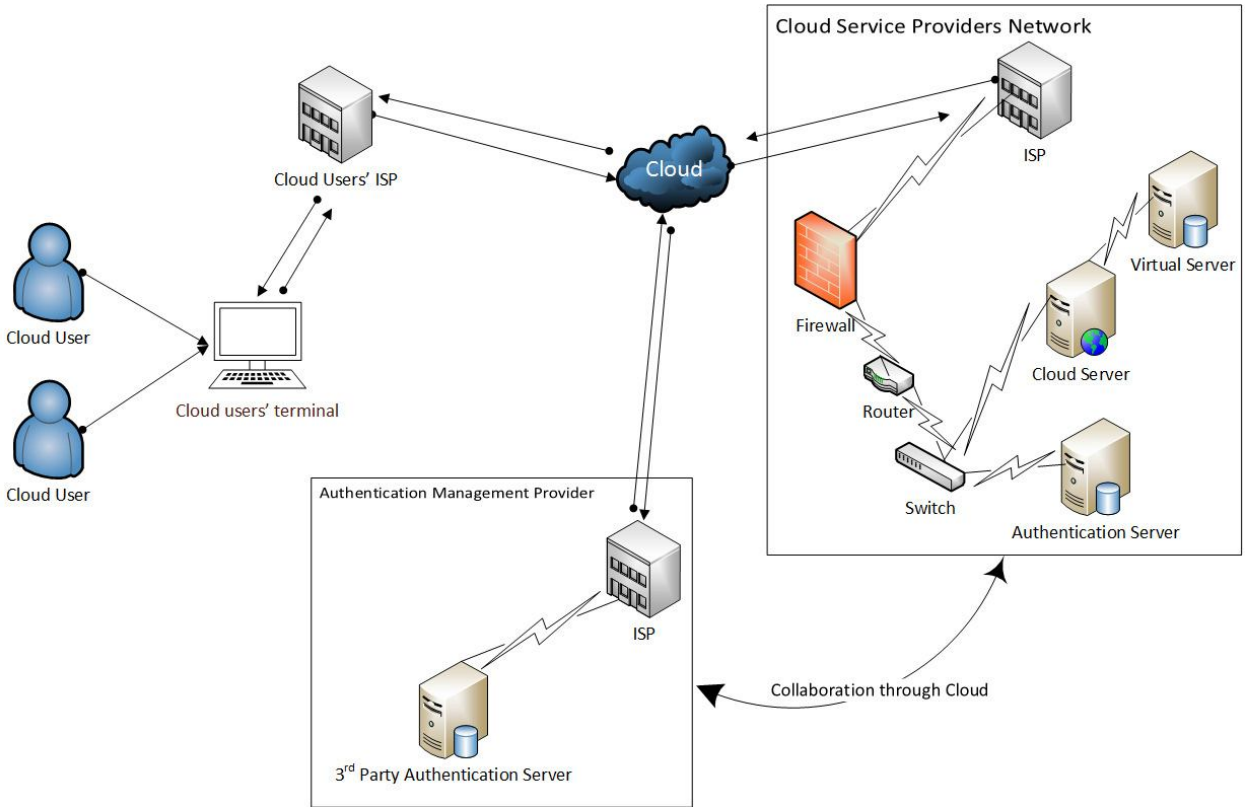


Figure-3: Authentication in the Cloud

The representation exhibited in figure 3 passes on that the verification for the cloud clients can be done either by the cloud specialist co-op or the specialist organization can redistribute the personality the executives and validation administration to outsider experts (Gonzalez, Miers, Redigolo, Simplicio, Carvalho, Naslund and Pourzandi, 2012; Sharma and Mittal, 2013). In the later case, the cloud specialist co-op is required to have joint effort with the outsider verification master – the joint effort between the cloud specialist co-op and the outsider verification master amid the validation procedure of cloud clients is done basically through cloud. This include includes execution overheads and security issues to the cloud setting as the message going between outsider validation the executives specialist and the cloud specialist organization as a feature of cooperation may basically be done through cloud foundation.[3][5]

IV.SECURITY ISSUES IN CLOUD

Distributed computing accompanies various conceivable outcomes and difficulties all the while. Of the challenges, security is viewed as a basic obstruction for distributed computing in its way to progress (Khorshed, Ali and Wasimi, 2012). The security challenges for distributed computing approach are to some degree dynamic and immense. Information area is an essential factor in distributed computing security (Teneyuca, 2011). Area straightforwardness is one of the conspicuous adaptabilities for cloud registering, which is a security risk in the meantime – without knowing the particular area of information stockpiling, the arrangement of information insurance represent some locale may be seriously influenced and abused. Cloud clients' close to home information security is along these lines a pivotal worry in a distributed computing condition (Joint, Baker and Eccles, 2009; Ismail, 2011; King and Raja, 2012). As far as clients' close to home or business information security, the key strategies of the cloud suppliers are of most astounding essentialness (Joint and Baker, 2011) as the specialized security exclusively isn't satisfactory to address the issue. Trust is another issue which raises security worries to utilize cloud administration (Ryan and Falvy, 2012) for the reason that it is straightforwardly

ISSN 2394 - 7780

identified with the believability and credibility of the cloud specialist co-ops. Trust foundation may turn into the way to build up a fruitful distributed computing condition. The arrangement of trust show is fundamental in distributed computing as this is a typical intrigue region for all partners for some random distributed computing situation. Trust in cloud may be subject to various elements among which some are mechanization the executives, human components, procedures and approaches (Abbadi and Martin, 2011). Trust in cloud is not a specialized security issue, however it is the most compelling delicate factor that is driven by security issues characteristic in distributed computing all things considered. A wide range of assaults that are appropriate to a PC arrange and the information in travel similarly applies to cloud based administrations – a few dangers in this classification are man-in-the-center assault, phishing, listening in, sniffing and other comparative assaults. DDoS (Distributed Denial of Service) assault is one basic yet significant assault for cloud figuring framework (Dou, Chen and Chen, 2013). The outstanding DDoS assault can be a potential issue for distributed computing, however not with any special case of having no choice to moderate this. The security of virtual machine will characterize the respectability and dimension of security of a cloud condition to more noteworthy degree (Rakhmi, Sahoo and Mehfuz, 2013; Agarwal and Agarwal, 2011). Bookkeeping and confirmation just as utilizing encryption falls inside the act of safe figuring - they can be very much considered as a component of security worries for distributed computing (Lee, 2012; Ogigau-Neamtiu, 2012; Singh and Jangwal, 2012). Nonetheless, it is vital to recognize among hazard and security worries in such manner.

As distributed computing typically implies utilizing open systems and in this manner putting the transmitting information presented to the world, digital assaults in any structure are foreseen for cloud processing. The current contemporary cloud based administrations have been found to experience the ill effects of defenselessness issues with the presence of conceivable security escape clauses that could be abused by an assailant. Security and protection both are worries in distributed computing because of the idea of such processing approach (Bisong and Rahman, 2011). The methodology by which distributed computing is finished has made it inclined to both data security and system security issues (Rakhmi, Sahoo and Mehfuz, 2013; Qaisar and Khawaja, 2012). Outsider relationship may develop as a hazard for cloud condition alongside other security dangers inalienable in infrastructural and virtual machine viewpoints (Hashizume et al., 2013). Elements like programming bugs, social building, human blunders make the security for cloud a progressively difficult one (Kim, 2009). Interruption discovery is the most vital job in consistent system checking to diminish security dangers. On the off chance that the contemporary IDSs (Intrusion discovery Systems) are wasteful, the resultant outcome may be undetected security rupture for cloud condition (Westphall et al., 2011).

The expansion of versatile cloud in the situation would support execution, however it would likewise include another layer of security issue not exclusively to the versatile cloud clients, yet additionally to the absolute foundation of the cloud administration supplier. The various leveled course of action of distributed computing encourages diverse dimension of extensibility for the cloud clients with fluctuating level of related security issues (Che et al., 2011). Security issues for distributed computing are depicted by a few creators as a conspicuous one due to its inclination. In a plan of action, the dangers for the shoppers are identified with and reliant on the pertinent methodologies and strategies of the cloud specialist co-ops the purchasers are managing. Utilizing cloud items or administrations may prompt security worries for the shoppers in the event that they are most certainly not very much aware with the sort and points of interest of the items or administrations they are to acquire or to use in a cloud situation; this is likewise identified with the cloud suppliers' character and dependability. One of the inborn issues in this setting is that, the buyers may typically not have the capacity to recognize or anticipate every one of the dangers engaged with the particular cloud exchange they are managing or associated with (Svantesson and Clarke, 2010).[6][2]

V.CONCLUSION

Distributed computing has colossal prospects, yet the security dangers installed in distributed computing approach are straightforwardly relative to its offered favorable circumstances. Distributed computing is an incredible opportunity and worthwhile alternative both to the organizations and the aggressors – either gatherings can have their own points of interest from distributed computing. The huge conceivable outcomes of distributed computing can't be overlooked exclusively for the security issues reason – the continuous examination and research for hearty, steady and incorporated security models for distributed computing could be the main way of inspiration. The security issues could seriously influence could frameworks. Security itself is conceptualized in distributed computing framework as an unmistakable layer (Dukaric and Juric, 2013).As an outcome, when managing distributed computing also, its security issues, specialized just as epistemological variables are similarly vital to take into thought. In view of the way that the effect of distributed computing can incorporate both the specialized and social settings, the exploration on distributed computing and its related concerns are most certainly not related just with processing perspectives. Administration situated engineering

ISSN 2394 - 7780

and different attributes of distributed computing proposes that the idea of distributed computing would require to investigate the common sense in accordance with social, business, specialized and legitimate points of view – every one of these aspects will consolidate security issues either in specialized or vital structure. Despite the idea of security issues, it tends to be without a doubt presumed that the serious unfavorable impacts as a result of security breaks in distributed computing, the sending of any type of distributed computing ought to manage the security concerns relating to those of the wellbeing basic frameworks.[1]

REFERENCES

1. Abbadi, I.M. and Martin, A. (2011). Trust in the Cloud. Information Security Technical Report, 16, 108-114. doi:10.1016/j.istr.2011.08.006
2. Agarwal, A. and Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. International Journal of Computer Applications in Engineering Sciences, 1 (Special Issue on CNS), 257-259.
3. Arshad, J, Townsend, P. and Xu, J. (2013).A novel intrusion severity analysis approach for Clouds. Future Generation Computer Systems, 29, 416–428. doi:10.1016/j.future.2011.08.009
4. Atayero, A.A. and Feyisetan, O. (2011). Security Issues in Cloud Computing: The Potentials of Homomorphic Encryption. Journal of Emerging Trends in Computing and Information Sciences, 2(10), 546-552.
5. Bisong, A. and Rahman, S.S.M. (2011). An Overview of the Security Concerns in Enterprise Cloud Computing. International Journal of Network Security & Its Applications, 3(1), 30-45. doi:10.5121/ijnsa.2011.3103
6. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J. and Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems, 25, 599–616.

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.