Volume 11, Issue 1 (XIV)
January - March 2024

ISSN: 2394 – 7780

International Journal of Advance and Innovative Research

IJAIR
IMPACT FACTOR
8.12

International Journal of
Advance and Innovative Research

Indian Academicians and Researchers Association
www.iaraedu.com

International Journal of Advance and Innovative Research

Volume 11, Issue 1 (XIV): January - March 2024

International Journal of Advance and Innovative Research

IJAIR

IMPACT FACTOR

8.12

ISSN : 2394-7780

The International Journal of Advance and Innovative Research is an online open access, peer reviewed & refereed journal.

Scientific Journal Impact Factor

CERTIFICATE OF INDEXING (SJIF 2024)

This certificate is awarded to

International Journal of Advance & Innovative Research
(ISSN: 2394-7780)

The Journal has been positively evaluated in the SJIF Journals Master List evaluation process
SJIF 2024 = 8.126

SJIF (A division of InnoSpace)

SJIFactor Project Manager
International Advisory Services
INNOSPACE INTERNATIONAL

SJIFactor Project

 ISSN 2394 - 7780

CYBER SECURITY IN HEALTHCARE INDUSTRIES: CHALLENGES AND SOLUTIONS

Tanaya Pathak[1], Prof.Jitendra Musale[2], Ankita Terkhedkar[3], Sapna Shinde[4], Rohan Parvekar[5] and Soham Salvi[6]

[1, 2, 3, 4, 5,6]Computer Department of Anantrao pawar College of engineering and research, Parvati, Pune. Savitribai Phule Pune University Pune [1]tanayapathak24@gmail.com, [2]jitendra.musale@abmspcoerpune.org, [3]ankitaterkhedkar@abmsp.org, [4]Sapnalishinde97600@gmail.com, [5]rohanparvekar28@gmail.com and [6]salvisoham18@gmail.com

ABSTRACT

The case highlights inadequate preparedness in many industries, including healthcare, to address cybersecurity risks. The COVID-19 pandemic has highlighted the importance of creating cybersecurity in healthcare systems and connected devices. The article aims to provide a systematic approach to cybersecurity management in healthcare organizations by discussing cyber risks, potential consequences of attacks, and five critical cybersecurity challenges which will be shown. It also provides recommendations for establishing conservation measures in line with best practice. Smart homes and healthcare have become increasingly popular in recent years. Given the volume of data, it documents the need for a more secure approach to ensure security and privacy. Consequently, these mechanisms can ensure security and privacy in smart health. The intended outcome of this research paper is the data breaches that people may face related to security issues in their smart homes and to start a conversation about how healthcare devices come in logistics embedded in future homes are vulnerable to cyberattacks. After reviewing previous literature, this paper proposes blockchain as a way to improve security and privacy in smart homes and smart healthcare systems. Using this platform we debated the blockchain technology of the uprising that can help make these things happen and how its content can help keep healthcare running with absolute security in mind. This study discusses how blockchain based solutions can enable the future of home and healthcare based on the model frameworkThe case highlights inadequate preparedness in many industries, including healthcare, to address cybersecurity risks. The COVID-19 pandemic has highlighted the importance of creating cybersecurity in healthcare systems and connected devices. The article aims to provide a systematic approach to cybersecurity management in healthcare organizations by discussing cyber risks, potential consequences of attacks, and five critical cybersecurity challenges which will be shown. It also provides recommendations for establishing conservation measures in line with best practice. Smart homes and healthcare have become increasingly popular in recent years. Given the volume of data, it documents the need for a more secure approach to ensure security and privacy. Consequently, these mechanisms can ensure security and privacy in smart health. The intended outcome of this research paper is the data breaches that people may face related to security issues in their smart homes and to start a conversation about how healthcare devices come in logistics embedded in future homes are vulnerable to cyberattacks. After reviewing previous literature, this paper proposes blockchain as a way to improve security and privacy in smart homes and smart healthcare systems. Using this platform we debated the blockchain technology of the uprising that can help make these things happen and how its content can help keep healthcare running with absolute security in mind. This study discusses how blockchain based solutions can enable the future of home and healthcare based on the model framework

Keywords— Medical services, smart homes, Block chain, Cybersecurity, internet of things(IOT), malware, smart cities, healthcare, home automation, data privacy.

I. INTRODUCTION

Digital technologies have revolutionized the healthcare industry by introducing modern information systems and integrating smart devices. These advancements have enhanced communication with patients and improved their access to treatments. Several components of modern information systems have significantly impacted the quality and availability of healthcare services. While the application of modern technologies in healthcare has improved service quality and data collection, it also introduces potential vulnerabilities. Actions involving personal data can create system vulnerabilities due to software vulnerabilities, human errors, or security flaws. It is crucial to address these vulnerabilities to ensure the security and privacy of patient data. In the digital era, Cybersecurity plays a crucial role in ensuring the smooth operation of healthcare organizations and safeguarding sensitive information. Healthcare organizations rely on specialized hospital information systems, including electronic health record (EHR) systems, e- prescribing systems, practice management support systems, clinical decision support systems, radiology information systems, and computerized physician order entry systems. Furthermore, the Internet of Things (IoT) has introduced a multitude of devices that are interconnected and used in healthcare settings. These devices include smart elevators, H VAC systems, infusion pumps, remote patient monitoring devices, and many others. It is imperative to secure these IoT devices to prevent unauthorized access and potential exploitation. As society becomes increasingly reliant on technology, the threat of cybercrime has also grown. Cybersecurity breaches are projected to cost the world.

6 billion per year by 2021, doubling from 6 billion per year in 2021, and doubling from 3 billion by 2015 [1]. The healthcare industry is particularly vulnerable, with cyber attacks being the leading cause of security breaches [2]. Ironically, the healthcare sector has experienced more cybersecurity attacks since 2016 than even the financial sector [3]. While the impact of technological vulnerabilities on health has been extensively researched, how pandemics such as COVID-19 present opportunities for cybercriminals has received little attention. The purpose of this paper is to review the existing literature on cybersecurity issues related to healthcare and to propose possible solutions to mitigate data breaches. body:

The growing vulnerability of the health service: Increased reliance on technology in health care settings. Connecting medical devices and communication systems. The value of health information in the black market. Cybersecurity threats in the healthcare industry: Types of cyberattacks targeting healthcare organizations. Examples of critical cyberattacks in the healthcare industry. The impact of cyber attacks on patient safety and privacy. Vulnerabilities of healthcare organizations: Cybersecurity budgets and limited resources. Unskilled workers and lack of training. Legacy systems and old hardware. The role of pandemics in exacerbating cybersecurity risks:

They rely heavily on telehealth and remote disease management. Health systems have grown and narrowed their focus on cybersecurity. Increased anxiety and sensitivity to phishing and social engineering attacks. Potential solutions to enhance cybersecurity in healthcare: Strengthening cybersecurity policies and procedures. Invest in employee training and awareness programs. Used multifactor authentication and encryption. Sharing threat reports together with cybersecurity experts During the COVID-19 pandemic, cybercriminals took advantage of their increased reliance on technology to launch cyberattacks as emotional states heightened. They often masquerade as trusted organizations like the World Health Organization (WHO) to exploit individual weaknesses and fears. This has led to a sharp rise in cyberattacks, with the number of attacks increasing fivefold during the plague. To combat these cybersecurity risks in the healthcare industry, it is important to implement effective measures to protect patient data. The Office for Civil Rights has been slow to implement the Health Insurance Portability and Accountability Act (HIPAA) to make it easier to use alternatives like Zoom. However, this has also weakened the physical and technical defenses against cyberattacks. With 90% of healthcare providers already experiencing a data breach, it is important to take proactive steps to enhance cybersecurity.

Some recommended measures include implementing well- defined software upgrade programs, using secure networks such as Virtual Local Area Networks (VLANs), and regularly testing systems for continuity Features that provide personalization , healthcare organizations and employers are more vulnerable to cyber attacks By understanding, we can better prepare for future outbreaks and protect sensitive data. While there is an extensive literature on the risks of technological vulnerabilities in the healthcare industry, further research is needed to examine the specific cybersecurity challenges posed by pandemics such as COVID-19. This will help develop more targeted strategies to mitigate cyber risks and protect patient privacy. In a healthcare crisis such as the COVID-19 pandemic, healthcare organizations have become prime targets for cyberattacks. The use of telemedicine in patient care when turnover is low has become important. For example, at New York University, virtual emergency visits increased by 4,330% after the outbreak. The simplification of HIPAA enforcement by the Office for Civil Rights has facilitated the use of platforms such as Zoom, Skype and FaceTime for telemedicine, but has provided physical and technical anti- cyber safeguards so attacks have also been weakened

This is concerning, given that 90% of healthcare providers have already experienced a data breach in the past, despite these safeguards. Another challenge is the epidemic rise in workload of health care professionals, which has a significant positive correlation with the likelihood of falling victim to phishing emails This is a problem because workload can always reach a peak during health crises , making healthcare professionals more vulnerable to cyber attacks. It is important for healthcare organizations to prioritize cybersecurity measures to address these issues. This includes implementing strong security measures for telemedicine platforms, ensuring the use of secure communication channels, comprehensive training for staff on detecting and responding to hacking attempts abuse of Yoge Cybersecurity- Threats have become a major concern. The cost of cyberattacks is expected to reach US$6 billion annually by 2021. The COVID-19 pandemic is providing new opportunities for cybercriminals, with the number of attacks increasing fivefold Heightened sensitivity during a pandemic for individuals are vulnerable to fraud.

Cybercriminals often exploit this vulnerability by masquerading as trusted organizations such as the World Health Organization (WHO). Health care organizations are also prime targets in a health crisis. The use of telemedicine increased dramatically during the COVID-19 pandemic, but it also opened up new avenues for cyber attacks. The Office for Civil Rights has been slow in implementing the Health Insurance Portability and Accountability Act (HIPAA), weakening physical and technical protections against cyberattacks This is concerning, given that 90% of health care providers have already experienced a data breach in the past so. Hectic workloads and stress during an outbreak can further increase the likelihood of healthcare professionals falling for phishing emails.

II. IMPORTANCE OF TECHNOLOGY

I. Malware:
Malware is a broad term that includes malicious software and files. The user can click a link in the email or go to a web page that starts the download automatically. These elements typically infect the victim's computer without their knowledge or consent, and take the form of credential theft, hardware manipulation, or file corruption Phishing:

II. Phishing is usually done via email and the recipient is tricked into completing a transaction, such as initiating a transfer, sending a certificate to a fraudster, or clicking on a link that downloads malware

III. Disclosure of information:
In the last section, we discussed how data breaches often result from external attacks, but can also come from less malicious sources such as a lost laptop or inadvertent employee compromise

IV. Internal Threats:
No employer can afford to ignore the possibility that their employees are also dangerous. Residents have fair access to organizational systems, allowing them to bypass multiple assessments. That access can be problematic whether the employee is in bad faith or not. Employees who sell credentials pose a significant risk — and so does an employee who accidentally clicks on a suspicious link in their email.

V. Whaling:
Advanced phishing scams known as whaling can be used to target and defraud high-level employees. A hacker can ask for things like money orders, credentials, protected health information (PHI), or things like medications. These work better than regular phishing scams because they require extensive investigation of the victim and the person pretending to be them.

VI. Weaknesses of the system:
All employees should install software updates and patches as soon as they appear. Hackers can easily gain access to your website when you haven't yet fixed the necessary elements for a vulnerability.

III. LITERATURE REVIEW

Carefully review existing books, academic papers, industry reports and related publications to gain a comprehensive understanding of the topic. This step helps identify gaps in knowledge and provides a basis for research. Paper entitled "Cybersecurity Applications and Techniques to Protect the Healthcare Industry,".

[1] Aysha K Alharam and Wael Elmedany, presented at the 9th 2017 IEEE-GCC Conference and Exhibition, explore the growing targeting of cyberattacks in the healthcare industry. 19 Article entitled "Challenges and Cybersecurity Threats for Health Information Systems in the Age of Epidemics" [3] by Ying He , Aliyu Aliyu, Mark Evans, and Kunjin Luo published in the Journal of Medical Internet Research at in 2021 includes the impact of the COVID-19 pandemic on the resilience of health information systems. [4] The authors emphasize that the pandemic has posed significant challenges to achieving global health and well- being goals. They note that this problem has led to an increase in cyberattacks targeting organizations run by pharmaceutical companies, US. Department of Health and Human Services, WHO, and partners include Cybersecurity in Healthcare: Ransomware attacks and data breaches are hallmarks of the current risk landscape in healthcare (Smith). and others, 20). 19 ; Jones et al., 2020).

[6] Researchers, such as Brown et al. (2018), identified weaknesses in the healthcare system, emphasizing the need to protect medical devices and improve user awareness. [7] Best practices and policies related to healthcare cybersecurity, such as the NIST Cybersecurity Policy and HIPAA Security Rule compliance, have been discussed by Johnson et al (2017) and White et al. (2021) does the same.

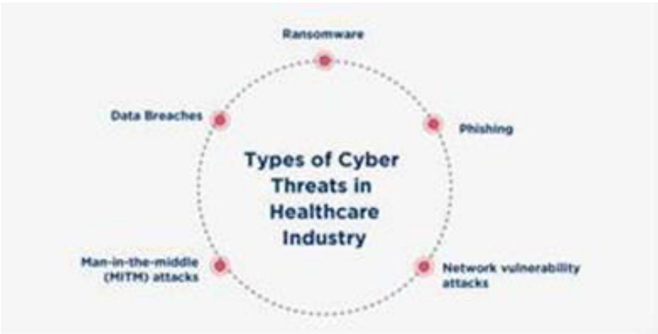
 ISSN 2394 - 7780

[8] The role of AI machine learning in advancing healthcare cybersecurity, especially in anomaly detection and threat prediction, has been explored in recent publications (Chen et al., 2022) Done (2018). Effective incident response and recovery strategies in the context of Of healthcare cybersecurity can be found in Mundy et al. (2019) and Patel et al. (2021) does the same. [10] This literature review provides a starting point, and further research could delve into these areas and evaluate recent sources providing comprehensive cybersecurity overviews in healthcare. (2019) and Jones et al. (2020) no. These assessments highlight growing threats such as ransomware attacks and data breaches.

[12] Brown and other researchers. (2018) identified weaknesses in the healthcare system, emphasizing the need to protect medical devices and improve user awareness. [13] Compliance with cybersecurity best practices and policies, such as the NIST Cybersecurity Framework and the HIPAA Security Rule, is discussed in the work of Johnson et al (2017) and White et al. (2021) does the same. [14] The role of AI and machine learning in improving healthcare cybersecurity, especially in anomaly detection and threat prediction, has been explored in recent publications by Chen et al (2022).

[15] The evolving regulatory landscape in healthcare cybersecurity, with an emphasis on GDPR and CCPA compliance, is discussed in a study by Lee et al (2018). [16] Mundy and colleagues have explored incident response and recovery strategies for effective healthcare cybersecurity. (2019) and Patel et al. (2021) does the same.

[17] These overviews provide a starting point for a literature review of cybersecurity in healthcare. Consider going further to provide a broader overview, exploring the latest sources and other areas of interest.



IV.RESEARCH METHEDOLOGY

Research Method……Cybersecurity in health care involves the protection of electronic data and assets from unauthorized access, use, and disclosure. Cybersecurity has three objectives: protecting confidentiality, integrity and availability of information, also known as the "CIA triad".

Here is the study assessment method:

A. **Define survey objectives:** Clearly define survey objectives, such as the current state of cybersecurity in healthcare, identifying common threats and vulnerabilities, or assessing existing security measures.

B. **Evaluation criteria:** Identify appropriate evaluation criteria based on the objectives. This can be quantitative methods (surveys, data analysis) or qualitative methods (interviews, case studies).

C. **Data Collection:** Collect data using selected research methods. This may include surveys, interviews, or analysis of existing data. Ensure data collection methods are consistent with ethical considerations and privacy laws.

D. **Data Analysis:** Analyze the collected data using appropriate statistical or qualitative analysis techniques. These steps help identify patterns, trends, and relationships in the data, allowing the researcher to draw meaningful conclusions.

E. **Recommendations:** Based on research findings, provides practical recommendations for improving cybersecurity in healthcare.

The CH approach included several steps for monitoring cybersecurity and data privacy risks. Here is a breakdown of the process.

A. **Cross-sectional, exploratory survey study:** The method began by collecting survey data from four professional groups in three European head offices (HOs). The purpose of this survey was to collect information on cybersecurity and data privacy risks.

B. **Risks:** Seven risks related to cybersecurity and data privacy were included in the survey. These categories likely included aspects of organizational security such as network security, data security, and access management.

C. **Writing:** After the data were collected, they were written and organized for further research. This stage involves converting the survey responses into a format suitable for analysis.

D. Risk-based strategy: The methodology proposes a risk- based strategy. This calculation divided the data collected by risk level if possible. Its goal was to translate the identified levels of risk into strategies for managing those risks.

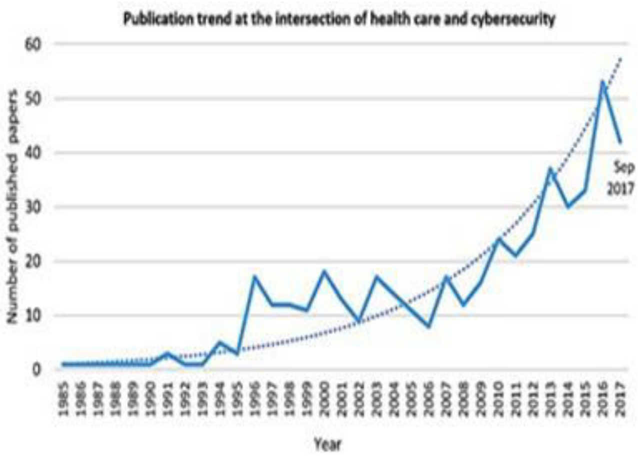
E. **Risk management strategies:** Based on the level of risk identified in the survey data provided recommendations or strategies to address the risks that may have been identified. These measures may include implementing specific safety measures, training employees, or adopting appropriate policies and procedures.

Overall, the CH approach collected survey data, analyzed it using risk-based methods, and derived strategies to address the identified cybersecurity and data privacy risksA. Writing: After the data were collected, they were written and organized for further research. This stage involves converting the survey responses into a format suitable for analysis.

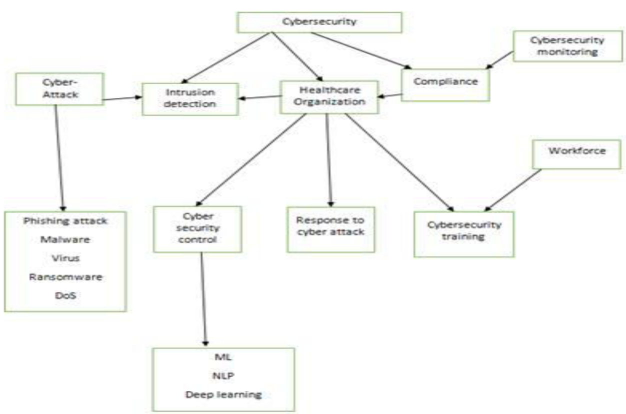
F. **Risk-based strategy:** The methodology proposes a risk- based strategy. This calculation divided the data collected by risk level if possible. Its goal was to translate the identified levels of risk into strategies for managing those risks.

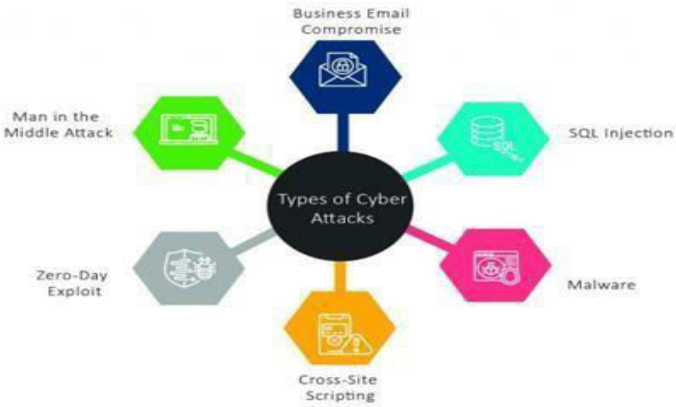
G. **Risk management strategies:** Based on the level of risk identified in the survey data provided recommendations or strategies to address the risks that may have been identified. These measures may include implementing specific safety measures, training employees, or adopting appropriate policies and procedures.

Overall, the CH approach collected survey data, analyzed it using risk-based methods, and derived strategies to address the identified cybersecurity and data privacy risks



V. FLOWDIAGRAM OF PROPOSED WORK





VI.ADVANTAGE OF PROPOSED MODEL OVER EXISTING MODEL

Like many industries, healthcare has gone through a digital transformation over the past few years. This increased digitalization has advanced medicine on many fronts, but it has also created new risks. As the industry relies more heavily on digital systems, cybersecurity in hospitals becomes more urgent. Healthcare is one of the most targeted sectors for cybercrime. In 2019, there are 525 data breaches in the region, more than a third of all incidents that year. The state of healthcare security is concerning, especially considering the potential consequences of a cyberattack on a hospital.

1. **Reduced risk of medical errors**

The electronic health record (EHR) is one of the most useful aspects of digitalisation in medicine. In 2017, 96% of hospitals had adopted certified EHRs, but this can be a risk without reliable cybersecurity. If a cyberattack compromises these records, it could affect how physicians access vital patient information.

2. **Improved patient privacy**

Physicians must abide by strict privacy rules when handling patient records. If a cybercriminal breaks into a hospital and obtains these, it can be dangerous. This can expose valuable information such as insurance details and addresses, and hospitals can face legal trouble.

3. **Adoption of safe technologies**

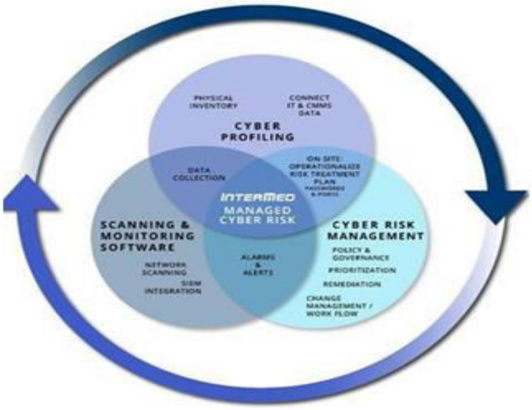
With cybercrime posing a serious threat to hospitals, some may shy away from adopting new technology. Organizations may be reluctant to use practical technologies for fear of increasing their vulnerabilities. If cybersecurity in hospitals is more reliable, the industry could see technology deployed faster and more securely.

4. **See patients early**

Better healthcare will lead to safer and more personalized medicines, but also faster. When EHRs work properly, they allow physicians to start treatment sooner, but interruptions can have the opposite effect. An annoying 72% of healthcare professionals experience delays or interruptions in their work due to communication issues.

5. **Safe use of medical devices**

The medical profession has seen growth in the use of communication technologies. This interconnectedness can enable faster and more efficient operations, but multiple endpoints translate into greater risk. To safely use these new medical devices, hospitals must ensure their safety.



VII. CONCLUSION

Cybersecurity threats are pervasive and cannot be ignored, especially in healthcare organizations. These organizations are favorite targets for attackers with potential benefits ranging from financial gain to public visibility. It is not the size of the organization that decides; They can target any information system related to medical, patient health record management, or medical device integration. Worryingly, even robust systems can fall victim to cyberattacks, as attackers continue to improve their techniques and sophistication. Thus, healthcare organizations should prioritize investments in cybersecurity to protect their patients and fulfill their role in healthcare delivery. Examining the available data on documented cyberattacks in healthcare organizations provides valuable insights and lessons for developing effective cybersecurity strategies. By learning from past events, organizations can enhance their security perimeter and better defend against future threats. Investing in cybersecurity not only protects sensitive patient information but also ensures the continuity of healthcare services and protects the reputation of healthcare organizations. It is imperative that healthcare organizations recognize the importance of cybersecurity and allocate resources appropriately to mitigate risks and maintain patient and stakeholder trust.

VIII. REFERENCES

[1] [HTML] Cybersecurity Challenges and Solutions under the Climate of Healthcare COVID-19: Scope Review

[2] [HTML] Cybersecurity of Hospitals: Discuss the challenges and work to mitigate the risk

[3] The impact of cybersecurity on the healthcare industry

[4] Cybersecurity Challenges in the Healthcare Industry

[5] [HTML] Towards an exploration of cybersecurity for the healthcare sectors: a comprehensive survey of recent practices and trends

[6] [PDF] Cybersecurity in Healthcare

[7] Challenges for healthcare in the cybersecurity era

[8] The impact of cybersecurity on the healthcare industry

[9] Cybersecurity in Health Care: A Narrative Analysis of Trends, Threats, and Ways Forward

[10] [HTML] Towards an exploration of cybersecurity for the healthcare sectors: a comprehensive survey of recent practices and trends

[11] Medicare & Medicaid Administration Centers [Internet]. Electronic Health Record (EHR) Incentive Program Baltimore, MD: CMS; 2016. URL: https://www.cms.gov/rules-and-guidelines/rules/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms. Accessed: 2016-08-0 (Archived from WebCite® at http://www.webcitation.org/6je8QNlo0).

[12] CW Services [Internet]. London, UK: (2016) . cybercrime timeline; URL:http://www.cwjobs.co.uk/career- advice/it-is-words/cyber-crime-timeline.Accessed: 2016-08-09. (Archived by WebCite® at http://www.webcitation.org/6je8V9 cyI).

[13] U.S. Department of Health and Human Services. Security standards: technical security [Internet]. Baltimore, MD: CMS, PhD; URL:http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/business/safeguards/techsafeguards.pdf. Accessed: 2016-08-0 (Archived by WebCite® at http://www.webcitation.org/6je8cfMpZ).

[14] U.S. Department of Health and Human Services. Fact sheet: ransomware and HIPAA [Internet]. Baltimore, MD: CMS,PhD; URL:http://www.hhs.gov/sites/default/file/RansomwareFact Sheet.pdf. Accessed: 2016-08-0 (Archived at Web Cite#174; at http://www.webcitation.org/6je8iBYI5).

[15] AHC Media LLC. Hackers are targeting hospitals with "ransomware". ED LAW LETT. (2016) February; 27: (4): 1-4

[16] Jayanthi A. The first reported ransomware attack in 1989 also targeted healthcare. http://www.beckershospitalreview.com/health-information- technology/the-first-known-ransomware-attack-in-1989- which-also-has-targeted-health-care -and-you.html.

[17] Luna R, , Rhine E, , Myhara M, , Sullivan R, , Cruz CS. Cyber risks to health information systems: a

ISSN 2394 - 7780

systematic review. Technol Health Care. (2016) February 27;24: (1): 1- 9. Available from: 10.3233/THC-151102.

[18] AHC Media LLC. Ransomware attacks are on the upward thrust and hackers are getting better.. ED LAW LETT. (2016) were written; 1: (4): 1-4

[19] Wu F, , Eagles S. Cybersecurity for medical device manufacturers: ensuring safety and performance. Biomed Instrum Technology. (2016) February 20; 50: (1): 23-3 Available from 10.2345/0899-8205-50.1.23.

A NEW ERA OF ART: THE REVOLUTIONARY IMPACT OF GENERATIVE ADVERSARIAL NETWORKS ON DIGITAL ART

Prem Kumar
Parul Institute of Design Parul University Vadodara, Gujarat

ABSTRACT

The use of Generative Adversarial Networks (GANs) have completely transformed the world of digital art. They blend the artificial intelligence (AI) and human creativity, and enable artists to create incredibly realistic digital artworks. This paper examines the impact of GANs on digital art, tracing its evolution from the 1960s alongside technological advancements. The study explores the significant impact of GANs on the creative process that allows artists to experiment with new concepts and even copy the styles of well-known artists. In addition to that, GANs have also given birth to new art forms like deepfake art and AI-generated artworks.

The paper further discusses the ethical considerations associated with GANs while creating art, and suggests for a balanced approach that fosters artistic innovation while addressing ethical concerns. Ownership issues, potential misuse leading to harmful content, and privacy implications are highlighted as ethical concerns. Other than that, for GANs to continue transforming digital art, technical issues like mode collapse and non-convergence must be resolved.

The future of GANs in art promise improved quality, interactive features, innovative applications, and morally sound solutions. This gives artists and researchers an opportunity to thoroughly investigate GANs' possibilities in the dynamic field of digital art.

Keywords: GANs, Generative Adversarial Networks, Generative AI, Art and Technology.

I. INTRODUCTION

The digital art industry is going through major transformations these days, and these changes may be linked mostly to the rise of Generative Adversarial Networks (GANs). These advanced computer systems are changing the way art and technology connect. This paper aims to investigate the creative revolution sparked by GANs in the field of digital art. This study covers several elements of GANs and digital art, with the goal to offer a holistic view of how GANs are profoundly changing the landscape of digital artistic expression.

A. Background and Context

It is necessary to understand the core concepts of Generative Adversarial Networks (GANs) in order to understand their impact on the art industry. In a related article published in 2023 [1,] Arham Islam defined Generative AI as a set of creative tools. These technologies are quite advanced, and are capable of engaging in human-like conversations, as seen in ChatGPT, or of translating words into pictures as exhibited by Midjourney. Such tools provide a promising insight into a future in which innovation and AI-powered creativity live together. GANs have made significant improvements in the field of generative AI since its introduction in 2014.

Generative Artificial Intelligence (Generative AI) offers an extensive range of options, with Generative Adversarial Networks (GANs) playing an essential role in this broad subject. The existing pool of knowledge on GANs is mostly unexplored, which indicates a wealth of undiscovered insights. The objective of this study is to consolidate this knowledge, and provide an introduction to GANs in the settings of digital art.

B. Understanding the Importance of Generative Adversarial Networks (GANs) in Digital Art

Generative Adversarial Networks, or GANs, have drastically transformed the way artists create art by giving them a platform to generate unique and compelling artworks. Artists can now experiment with different artistic aspects and styles and create original compositions using GANs. These tools work as strong instruments that enable artists to realize their full creative potential and generate inventive, artistic, and visually appealing works of art.

One significant benefit of GANs to the field of digital art is its ability to produce a wide variety of realistic images. They have in fact the ability to understand the patterns and structures present in a dataset to generate new images that bear a strong resemblance to the training data. With this ability, artists can create visually harmonious works of art with particular themes or styles [2], which further broadens their creative horizons and making it easier to produce inventive and aesthetically beautiful art.

Additionally, GANs are useful for "inpainting," which is the process of repairing or replacing damaged or destroyed portions of an image. This is especially useful for digital art restoration process since it makes it possible to use GAN-based inpainting techniques to digitally restore damaged or incomplete artworks [3]. This highlights the role that GANs contribution in conserving and restoring artistic heritage.

After the introduction of GANs, It has also become possible to create artwork in the recognizable styles of well-known painters [4]. Artists are now able to create original pieces of art and experiment with many artistic styles [4]. This flexibility shows how GANs have a significant impact on encouraging experimentation and creativity.

In addition, leading tech firms like Adobe and NVIDIA are working together to maximize the potential of generative AI with the goal of improving creative processes. They want to work together to develop state-of-the-art generative AI models with an emphasis on smooth integration into programs that are often used by world-class marketers and creative [5].

Several studies have shown the amazing powers of Generative Adversarial Networks, offering endless opportunities through the integration of art and technology in the current era of art-tech convergence.

C. Scope and Objective

The purpose of this study is to examine how Generative Adversarial Networks, or GANs, are affecting the field of digital art. It will try to explore the ways in which GANs are changing the process of creating art, as well as their potential for producing images, ethical issues that are associated with them, their impact on the art market, and their future prospects. The study will also look at how technology and art are evolving and what it means to the artists and the art world as a whole. To gather this information, a variety of sources have been examined, ensuring a comprehensive and thorough analysis.

II. Evolution of Digital Art

Digital art is distinct from traditional art forms because of the significant changes in artistic techniques and process brought about by its evolution. Digital Art basically includes anything that uses digital technology to enhance the creative process [6]. The use of digital technology has provided artists with the opportunity to experiment with new materials and techniques, leading to the creation of unique artworks. Digital painting, digital photography, computer-generated art, and interactive installations are all included in this vast field.

The world of digital art has undergone significant changes as a result of both advancements in the field of art and technological breakthroughs [7]. New digital norms for how to use visual and spatial data, as well as advances in computer vision, have totally transformed digital art [7]. These advancements have enabled artists to develop more sophisticated and inventive methods of creating and comprehending digital artworks.

Srivastava [8] explored the interesting journey of the evolution of digital art in a study. According to the study, it changed from being limited to conventional paintings and sculptures to a whole new universe where art is used to tell stories and messages. Artists started making use of computers and digital tools in the 1980s, which was a revolutionary step because it allowed them to combine traditional painting methods with new digital possibilities [9]. Looking back even further, the beginnings of digital art in the 1960s were shaped by significant events and assistance from various organizations such as Ars Electronica and ISEA [10].

The field of art history has also been greatly influenced by the growth of digital art. Although digital art history is still in its early stages but the progress that has been made in this area has huge promise. It offers us new, more sophisticated and in-depth ways to look at and understand works of art.

III. Traditional Methods of Digital Art Creation and Their Constraints

Digital art combines traditional artistic skills with digital tools and it offers artists innovative ways to express their creativity. Similar to painters and their brushes, artists use digital tools to bring their ideas to life through computers [11]. One notable thing about digital art is the ability to easily fix mistakes and make changes, which saves artists time and reduces the frustration of irreversible errors. Digital tools provide artists with extensive creative options, allowing them to experiment with various styles, textures, and colors without the need for physical materials. Additionally, digital art is highly accessible, as artists can easily share their work online. This gives them the opportunity to reach a diverse audience beyond traditional art exhibitions.

Digital art opens up a world of creative possibilities, but it does have its challenges. Learning new software and tools takes time and can impact the creative process. Maintaining consistency in digital art can also be difficult due to the fusion of art, science, and technology [12]. There are challenges in preserving it and ensuring people can access it [12]. Digital art is tricky because technology evolves quickly, and older tools might get outdated very soon. It is also hard to make sure digital work is real and hasn't been duplicated or changed [13].

 ISSN 2394 - 7780

In a nutshell, diving into digital art is exciting, but it comes with unique challenges. Staying up to date with technology, understanding the meaning behind the art, and keeping it secure can be tricky. Artists need to be patient, adaptable, and truly dedicated to creating exceptional digital artworks.

IV. Understanding Generative Adversarial Networks (GANs) and their Architectural Framework

Generative Adversarial Networks (GANs) were initially proposed by [14] as a collaborative framework with two primary components: the "generator" and the "discriminator." The generator's work is to create visuals that closely match reality, very similar to those of a skilled artist. Meanwhile, the discriminator acts like an art detective whose task is to judge if an image is real or produced by the generator. Initially, the generator's art might not be perfect, but the process gets exciting as the discriminator provides feedback (as shown in Fig. 1) to the generator, pointing out any mistakes. The generator uses the input to improve its artistic abilities. This conflict between the generator and discriminator continues. With each round of feedback, the quality of the produced artwork increases. Over time, it becomes really difficult for the discriminator to differentiate between actual and generated images [14]. This leads to the creation of output data that is more convincing and indistinguishable.

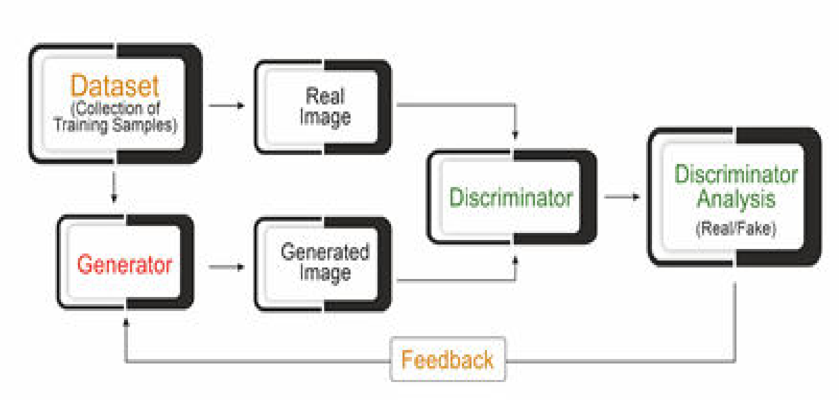


Fig. 1. Generative Adversarial Networks Architecture Diagram

The GAN architecture is impressive because of its competitive nature. This competition helps GANs learn and get better with practice, making digital art that's more and more realistic and high-quality.

V. The Process of Creating Digital Art using GANs

Initially, Generative Adversarial Networks (GANs) were developed for the purpose of image processing and generation, but due to its success in the art world, it swiftly emerged as a new creative approach. They have many exciting uses that push the boundaries of creative expression. Furthermore, GANs have facilitated human-AI collaboration in the creative industries. Artists can use GANs to make art that combines the unique perspectives and creativity, opening the door to fresh artistic ideas and going beyond the usual art forms.

Generative Adversarial Networks (GANs) have the ability to produce a range of digital artworks, including lifelike human faces, objects, and cartoons. They can also transform text into images. An important element of GANs is their ability to produce new data resembling the patterns of the data they learned from. This function has different creative uses, such as enhancing data for training, uncovering unique elements, and fostering creativity in various circumstances. When GANs are used in art, they also save time because they automate the process of making new and original content, which would take a lot of time and work without them.

The following steps are generally involved in the process of creating digital art with GANs:

- Training the GAN model on a dataset of real art samples.
- The generator's goal is to create images realistic enough to deceive the discriminator. While the discriminator is trained to accurately distinguish between real and fake images.
- The generator starts with a random noise vector and produces a new image.
- The discriminator receives both the generated image and a real image and provides a probability that indicates if the image is real or fake.
- Both the generator and the discriminator play a game together, aiming to defeat each other. They keep going up and down till the discriminator is fooled. This shows that the generator has generated believable results.

GANs can understand the complicated details, textures, and styles included in a dataset, allowing them to create new art works that closely replicate what they've learnt [15]. This makes GANs especially useful for activities such as image creation, image filling in gaps, and image resolution improvement [16].

GANs (Generative Adversarial Networks) are groundbreaking tools for artists, with the incredible power to streamline and speed the art creation process. GANs can manage multiple parts of creating artwork with only a prompt and a click, providing artists with a quick approach to generate ideas, develop prototypes, and experiment with diverse styles. This kind of automation speeds up the creation of content, reduces alterations, and allows for mass production, as well as improving the overall process.

VI. Applications of GANs in Digital Art

Generative Adversarial Networks (GANs) can be incredibly helpful in digital art creation, it lets artists try out loads of new things. Here are some ways artists can use GANs in digital art:

- **Artistic Style Mix:** Generative Adversarial Networks (GANs) allow you to combine the styles and content of two images to create amazing combinations [17]. GANs do well at producing outstanding stylistic adjustments to images.
- **AI-Created Art:** GANs assist artists in creating completely original works of art that combine human creativity with technological innovation. Even some fancy art galleries have featured some AI-generated artwork. By regulating the content and appearance of the generated image, GANs are used to create a variety of imaginative and unique artwork [18]. These AI-generated artworks have the potential to be extremely creative and original, going beyond what is possible with traditional art production.
- **Deepfake Art:** GANs are used to produce realistic video clips including well-known paintings or famous personalities. This new medium for expressing artistic ideas is the fusion of art and technology. While deepfakes often involve altering faces and identities, they can also be used to modify an image's appearance or style [19].
- **Art Restoration:** By repairing or restoring damaged or missing elements of an image, GANs can help to restore and improve damaged artworks [20]. Image inpainting technique is used to fill in the elements that are missing from an image by using their surroundings as a guide [20].
- **Unique works of Art:** GANs can be utilized by artists to produce one-of-a-kind digital artworks. Artists are able to produce work that is personalized for each viewer by utilizing the versatility and adaptability of GANs [18]. Artists can also experiment with diverse artistic expressions and create customized works of art by training GANs to generate art in different genres.
- **Generative Text and Poetry:** GANs are not limited to producing only visual art; they are also capable of creating text and poetry. GANs may produce new content that makes sense and matches the style of the training data by learning the patterns and structures of large amounts of text. This creates opportunities for automatically producing content, as GANs are able to produce text that is extremely similar to human writing in terms of both style and content [21].
- **Personalized Art Creation:** Artists can modify GANs to produce artwork that satisfies specific requirements, such as a particular color palette, motif, or atmosphere. A great example is the work of Obvious, a French art collective. They used GANs to make two series of paintings, and one of their works sold for over 400,000 dollars [22]. This shows how GANs have the potential to create unique and valuable art.
- **Art Market and Collectibles:** AI-generated art has entered the art market as well. GANs have opened up new possibilities for artists and collectors. Digital art can be easily copied and shared, making it accessible to more people.

In summary, GANs have a wide range of uses in digital art, from changing styles to creating content and even affecting the art market. These uses give artists strong tools to explore, be creative, and push the limits of artistic expression in the digital era.

VII. Ethical Considerations of using GANs in Digital Art Creation

GANs have transformed digital art, yet their application raises significant ethical concerns regarding the intersection of art and technology. The integration of artificial intelligence into the artistic process challenges conventional beliefs about creativity, authorship, and human expression. It raises questions about the role of the artist and the authenticity of the creative process. Here are some ethical considerations in using GANs in digital art creation:

- **Ownership and Attribution:** GANs are trained on large datasets of images, which may include copyrighted works and personal styles of artists. This raises questions about who owns and should get credit for the images GANs create [23].
- **Harmful Content:** GANs can be used to make harmful stuff, like fake news and deepfake videos that are really convincing [24]. This presents serious concerns regarding the accuracy of information being shared.
- Privacy: Privacy becomes a major ethical issue in the application of GANs in digital art. GANs often need huge datasets for training, and these datasets may contain personal or sensitive information. Using such data without proper consent raises concerns about privacy infringement and the danger of exploitation of personal information. GAN-generated images have shown vulnerabilities in security measures that depend on biometric systems, such as facial and fingerprint scanners [25]. Furthermore, copyright infringement has drawn criticism, particularly when GANs generate music that is exempt from royalties [26].
- **Deepfake Misuse:** Since GANs can produce believable deepfakes, there is a risk to people's privacy and reputation. They generate realistic-looking fake pictures which creates a confusion between actual and fake data [27]. The consequences of deepfake use include concerns like fake pornography, fraud, hate crimes, and the distribution of fake news and dangerous hoaxes [27].
- **Effect on Traditional Artists:** Another significant concern is how deepfake technology may affect traditional artists. Deepfakes can be used to make imitation of an artwork, which may devalue the actual work and harm the livelihood of artists [28]. his raises issues regarding intellectual property rights and the reliability of artistic creations. It is crucial to develop strategies to protect artists' rights and ensure that their art isn't harmed or misrepresented by deepfake technology.

To overcome these ethical challenges, we need a comprehensive approach. In order to start, we must develop strong regulations and laws to control how deepfakes are generated, exchanged, and exploited. These regulations should place a high priority on preserving people's privacy, making sure that utilizing someone else's image requires permission. Apart from that, penalties should be imposed for the use of deepfakes for malicious purposes [29].

Secondly, more investment should be made to develop better methods to spot deepfakes. This involves using smart algorithms and artificial intelligence to identify and validate digital content [30]. In addition, educating the public about the existence and possible dangers of deepfakes can help people become more selective digital media consumers [24].

Furthermore, it's very important to make sure that the development and use of GANs, the technology behind deepfakes, is transparent and responsible. One way to do this is to be clear about when deepfake technology is used in the media and how it should be used in an ethical way [31]. The policymakers, researchers, and tech companies must all work together to make these solutions work.

VIII. CHALLENGES

Generative Adversarial Networks (GANs) have become popular in digital art because it provides the artists with tools to express their creativity. However, using GANs in digital art production poses a number of technical difficulties for artists to overcome:

- A major hurdle when utilizing GANs for digital art creation is mode collapse. This problem occurs when the generator generates outputs that are identical to each other without displaying enough variation from the training dataset [32]. As a result, the produced digital art may be less imaginative and varied.
- Non-convergence and instability are also common challenges in training GANs. For GANs, it's crucial to strike a careful balance between the discriminator and generator networks, however achieving this can be really challenging [32]. Instability during training can lead to inconsistent and unpredictable results, hindering the generation of high-quality digital art.
- The quality of the images produced in GANs depends heavily on how the GAN architecture is designed. If the network is not designed well, it can lead to low-quality images or instability during the training process.

- Generating diverse images is a strength of GANs, but precisely controlling certain elements of the generated artwork, such as style, composition, or specific features, remains a challenging area that needs more study and development.
- The lack of diversity in generated samples is another challenge. GANs have been known to suffer from this problem, where the generated images may lack variation and appear similar [34]. This can limit the creativity and uniqueness of the digital art produced.
- It is difficult to reduce GANs' computational cost while maintaining photo-realistic images, particularly for use on devices with limited processing power [35]. Identifying efficient methods to compress GAN models without compromising the quality of the generated images is a constant problem.

In confronting these multifaceted challenges, artists and researchers embark on a journey to reshape the digital art landscape. The road ahead is full of exciting possibilities to unlock more creativity, gain better control, and shape the future of digital art using GANs. As we overcome these challenges, we're opening doors to a world where art and technology come together in new and amazing ways.

IX. Current Advancements and Future Directions

There are promising opportunities as we continue to look into the Generative Adversarial Networks (GANs). By combining GANs with new technologies like reinforcement learning and transfer learning, we can create advanced generative models. These models have the potential to be versatile and helpful in various tasks, such as generating images and assisting with data-related processes.

In 2023, a noteworthy innovation called DragGAN has emerged in the field of interactive and precise AI tools. This technology allows users to finely adjust generated images by easily manipulating elements like pose, shape, expression, and object arrangements. By clicking and dragging within the image, users can see the AI adapt every detail accordingly [36]. DragGAN is a ground-breaking technology that extends the possibilities of GANs and provides a simple way to edit and improve generated images. DragGAN, which is still in development, demonstrates the quick advancement of artificial intelligence and its significant influence on the visual arts.

In the exciting world of Generative Adversarial Networks (GANs), companies like NVIDIA, Adobe Research, and Google Brain are leading the way in digital art and design. NVIDIA is a pioneer in GAN technology with innovations like Progressive GANs for the generation of high-resolution images progressively and StyleGAN focused on controlling the style and appearance of generated images. These advancements have transformed how we create images and designs. Adobe Research is all about exploring where GANs and creativity meet, giving artists and designers amazing tools for editing images, transferring styles, and inventing new artistic flavors. Google Brain is making virtual worlds more real and crafting lifelike images that captivate our senses. These key players, along with others, are molding the landscape of GANs in the world of digital art and design through their dedicated research and development efforts [37].

Future directions for Generative Adversarial Networks (GANs) are also promising and diverse. Here are some of the potential future directions for GANs:

- **Higher Fidelity and Resolution:** GANs have already demonstrated remarkable capabilities in generating images and videos that are undetectable from reality. However, the future promises even higher fidelity and resolution, enabling the creation of immersive and visually stunning experiences.
- **Interactive and Controllable Nature:** As GANs architectures continue to evolve, users will gain unprecedented control over the generation process. Fine-grained adjustments of attributes, styles, and desired outputs will become possible. This will allow users to customize visuals, designs, and even entire virtual worlds, all with a few intuitive adjustments.
- **Novel Applications:** GANs have found applications in various domains, including art and design, medical imaging, fashion, gaming, and data augmentation. The future of GANs holds exciting possibilities, including enhanced creativity, better-unsupervised learning, and novel applications across various domains.
- **Improved Stability and Training:** When GANs create a narrow range of outputs, they frequently have to deal with issues like training instability and mode collapse. Recent improvements in regularization techniques and architectural changes are addressing these issues, pushing the field forward.
- **Expanding GANs' Scope:** Increasing the range of GAN applications in translational genomics has great promise for the future and could revolutionize drug discovery and development.

- **Improvements in GAN Architecture:** Ongoing research attempts to develop novel GAN designs that can produce a greater variety and quality of content. Artists would have more control over the final product as a result.
- **Ethical Considerations:** Future research efforts will focus on tackling ethical issues associated with the application of GANs, including ownership and attribution, possible misuse, algorithmic bias, authenticity, harmful content, privacy, and biases in training data.

GANs have enormous potential for creativity, innovation, and new applications in a variety of fields in the future. Researchers and practitioners can better use GANs to realize their full potential by being aware of these future directions.

X. CONCLUSION

Generative Adversarial Networks (GANs) have changed the world of digital art. It has offered some powerful tools for artists to create stunning and diverse pieces of art. While on one hand, this creative revolution has brought exciting possibilities, on the other hand, it has also raised some important ethical concerns and technical challenges. The responsible use of GANs is very crucial in navigating this transformative era in art.

Recent innovations such as DragGAN, along with contributions from industry leaders such as NVIDIA and Adobe Research, highlight the ongoing advancement and future potential of GANs. As GANs progress, they promise higher quality, interactive functions, and new applications of it. However, addressing ethical issues like ownership, privacy, and harmful content is essential for their responsible use. Establishing rules and regulations, investing in deepfake detection, and ensuring transparent GAN development are essential steps in using the full potential of this transformative technology in the world of digital art.

In conclusion, As we stand at the crossroads of creativity and responsibility in the world of digital art, a commitment to responsible use of the transformative power of Generative Adversarial Networks is needed. Artists, researchers, and technologists can work together to create a future where new ideas and social concerns can live together in peace. This will allow digital art to grow in a way that is both dynamic and long-lasting.

REFERENCES

[1] A. Islam, “A history of Generative AI: From GAN to GPT-4,” *MarkTechPost*, 21-Mar-2023. [Online]. Available: https://www.marktechpost.com/2023/03/21/a-history-of-generative-ai-from-gan-to-gpt-4/.

[2] S.-C. Huang and T.-H. Le, “Generative adversarial network,” in *Principles and Labs for Deep Learning*, Elsevier, 2021, pp. 255–281.

[3] J. Yu, Z. Lin, J. Yang, X. Shen, X. Lu, and T. S. Huang, “Generative image inpainting with contextual attention,” in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2018.

[4] T. Kusumi, N. Tosa, R. Nakatsu, and C. H. Mai, “Learning of art style using AI and its evaluation based on psychological experiments,” *Int. J. Arts Technol.,* vol. 14, no. 3, p. 1, 2022.

[5] Adobe. (2023, March 21). “Adobe and NVIDIA Partner to Unlock the Power of Generative AI” *Adobe.com.* [Online]. https://news.adobe.com/news/news-details/2023/Adobe-and-NVIDIA-Partner-to-Unlock-the-Power-of-Generative-AI/default.aspx

[6] V. Wang and D. Wang, “The impact of the increasing popularity of digital art on the current job market for artists,” *Art Des. Rev.,* vol. 09, no. 03, pp. 242–253, 2021.

[7] A. Brey, “Digital art history in 2021,” *Hist. Compass*, vol. 19, no. 8, 2021.

[8] A. Srivastava, “Digital art: A revolutionary form of art & visual communication,” *Int. J. Res. Granthaalayah*, vol. 7, no. 11, pp. 83–88, 2019.

[9] C. Paul, *Digital art*. London: Thames & Hudson, 2008.

[10] B. Wands, “25 years of curating digital art: 1993–2018,” in *Electronic Workshops in Computing*, 2018.

[11] K. S. Chari, "The Creation Process in Digital Art: Latest Developments," *International Journal of Emerging Technologies and Innovative Research*, vol. 1, no. 4, pp. 1956-1964, Sep. 2014. Available: http://www.jetir.org/papers/JETIR1701313.pdf

[12] P. Innocenti, “Theories, Methods and Testbeds for Curation and Preservation of Digital Art,” *Archiving Conference*, vol. 7, no. 1, pp. 13–17, Jan. 2010, doi: 10.2352/issn.2168-3204.2010.7.1.art00003.

 ISSN 2394 - 7780

[13] M. Stricot, “Digital art preservation: Practical answers to theoretical issues,” in *2013 Digital Heritage International Congress (DigitalHeritage)*, 2013.

[14] I. J. Goodfellow et al., "Generative Adversarial Networks," *arXiv:1406.2661 [stat.ML]*, Jun. 2014. Available: https://arxiv.org/abs/1406.2661 DOI: 10.48550/arXiv.1406.2661

[15] A. Radford, L. Metz, and S. Chintala, “Unsupervised representation learning with deep convolutional generative adversarial networks,” 2015. https://doi.org/10.48550/arxiv.1511.06434

[16] J. Li, Z. Chen, X. Zhao, and L. Shao, “MapGAN: An intelligent generation model for network tile maps,” *Sensors (Basel),* vol. 20, no. 11, p. 3119, 2020.

[17] J. Johnson, A. Alahi, and L. Fei-Fei, “Perceptual losses for real-time style transfer and super-resolution,” in *Computer Vision – ECCV 2016*, Cham: Springer International Publishing, 2016, pp. 694–711.

[18] H. Chen et al., “Creative and diverse artwork generation using adversarial networks,” *IET Comput. Vis.*, vol. 14, no. 8, pp. 650–657, 2020.

[19] H. Hou, J. Huo, J. Wu, Y.-K. Lai, and Y. Gao, “MW-GAN: Multi-warping GAN for caricature generation with multi-style geometric exaggeration,” *IEEE Trans. Image Process.,* vol. 30, pp. 8644–8657, 2021.

[20] H. Touvron, M. Douze, M. Cord, and H. Jégou, “Powers of layers for image-to-image translation,” 2020. https://doi.org/10.48550/arxiv.2008.05763

[21] I. Goodfellow et al., “Generative adversarial networks,” *Commun. ACM*, vol. 63, no. 11, pp. 139–144, 2020.

[22] G. Franceschelli and M. Musolesi, “Creativity and Machine Learning: A Survey,” *arXiv.org*, Jul. 05, 2022. https://arxiv.org/abs/2104.02726

[23] K. Mok, “The Power and Ethical Dilemma of AI Image Generation Models,” *The New Stack*, Jan. 06, 2023. https://thenewstack.io/the-power-and-ethical-dilemma-of-ai-image-generation-models/

[24] S. Ali, D. DiPaola, and C. Breazeal, “What are GANs?: Introducing Generative Adversarial Networks to Middle School Students,” Proceedings of the *AAAI Conference on Artificial Intelligence*, vol. 35, no. 17, pp. 15472–15479, May 2021, doi: https://doi.org/10.1609/aaai.v35i17.17821.

[25] F. Marra, D. Gragnaniello, L. Verdoliva, and G. Poggi, “Do GANs Leave Artificial Fingerprints?,” *2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR),* Mar. 2019, doi: https://doi.org/10.1109/mipr.2019.00103.

[26] Y. ÖZKAN and P. ERDOĞMUŞ, “Generative Networks and Royalty-Free Products,” *Sakarya University Journal of Computer and Information Sciences*, Dec. 2020, doi: https://doi.org/10.35377/saucis.03.03.724645.

[27] S. Tariq, S. Lee, H. Kim, Y. Shin, and S. S. Woo, “GAN is a friend or foe?,” *Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing*, Apr. 2019, doi: https://doi.org/10.1145/3297280.3297410.

[28] X. Zhang, S. Karaman, and S.-F. Chang, “Detecting and Simulating Artifacts in GAN Fake Images,” *2019 IEEE International Workshop on Information Forensics and Security (WIFS),* Dec. 2019, doi: https://doi.org/10.1109/wifs47025.2019.9035107.

[29] K. H. Onarheim, K. Wickramage, D. Ingleby, S. Subramani, and I. Miljeteig, “Adopting an ethical approach to migration health policy, practice and research,” *BMJ Glob. Health,* vol. 6, no. 7, p. e006425, 2021.

[30] Y. Jeong, D. Kim, Y. Ro, and J. Choi, “FrePGAN: Robust deepfake detection using frequency-level perturbations,” *Proc. Conf. AAAI Artif. Intell.,* vol. 36, no. 1, pp. 1060–1068, 2022.

[31] M. Minkkinen and M. Mäntymäki, “Discerning between the ‘easy’ and ‘hard’ problems of AI governance,” *IEEE Trans. Technol. Soc.,* vol. 4, no. 2, pp. 188–194, 2023.

[32] T. Salimans, I. Goodfellow, W. Zaremba, V. Cheung, A. Radford, and X. Chen, “Improved Techniques for Training GANs,” *arXiv [cs.LG],* 2016.

ISSN 2394 - 7780

[33] R. Abdal, Y. Qin, and P. Wonka, "Image2StyleGAN++: How to edit the embedded images?," in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR),* 2020.

[34] W. Li and Z. Zhong, "Research on cross-modal hashing method based on diffusion mode," in Eighth International Conference on Electronic Technology and Information Science (ICETIS 2023), 2023.

[35] Y. Tian, L. Shen, D. Tao, Z. Li, and W. Liu, "DGL-GAN: Discriminator Guided Learning for GAN Compression," *arXiv (Cornell University),* Dec. 2021, doi: https://doi.org/10.48550/arxiv.2112.06502.

[36] X. Pan, A. Tewari, T. Leimkühler, L. Liu, A. Meka, and C. Theobalt, "Drag your GAN: Interactive point-based manipulation on the generative image manifold," in *Special Interest Group on Computer Graphics and Interactive Techniques Conference Conference Proceedings,* 2023.

[37] K. Mansour, "Advancing Generative Modeling: The Power of GANs," May 31, 2023. https://www.linkedin.com/pulse/advancing-generative-modeling-power-gans-khaled-mansour/

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

A SYSTEMATIC REVIEW ON FUTURE OF WORK IN THE 21ST CENTURY

(Ms.) Charvi Hasmukh Shukla
Doctoral Student, HR XLRI- Xavier School of Management Jamshedpur, India

ABSTRACT
What will the future of work hold for the organizations? This topic is of continuous debate due to the impact of rising technological advances on work settings in today's digital era. Using the People-Process-Technology (PPT) framework, this article attempts to investigate the holistic viewpoint for comprehending the Future of Work (FoW) in the twenty-first century. The PRISMA approach is used to conduct a systematic review of the literature, which serves as a guide for the thematic analysis from the standpoint of the PPT framework. According to the study, the Future of Work will bring about a number of changes, such as the demand for IT skills, policy modifications to accommodate new technology, the development of a human-machine symbiosis, the facilitator role of leaders, and others. Towards the end, future directions are presented to explore new possibilities.

Keywords: future of work (FoW), industry 4.0, human- computer interaction, people-process-technology (PPT) framework, artificial intelligence (AI).

I. INTRODUCTION
Many believe that technological advancement will eliminate many jobs [26] and restructuring of jobs [25] is done to support value creation. Economies across the globe are undergoing fundamental shifts in the domain of future work [28]. To ensure flexibility, the gig economy has come into the picture. In this regard, employment in the future will need to understand the dynamics of autonomy [30] of a worker and its work arrangement in association with the technologies as well.

Since, in the coming times, a lot is expected to change, there is a fear of technology [21] among the people. This fear stems from the mismatch of skills an individual possesses in employment [2]. The routine and repetitive nature of work undergoes a transformation considering automation. The previously established work-life balance also goes for a toss when the superstructure of society changes due to innovations [13]. A by-product of such innovation is telecommuting [31] a trend marked at the start of this century. FoW literature showcases the debate concerning the various facets of work and technology. Fears of massive unemployment due to technological disruptions are common viewpoints among scholars [8]. Machines with artificial intelligence (AI) can quickly compute [10] and provide solutions compared to humans, giving rise to the potential of automation. Employees in such scenarios feel trapped in their jobs due to the detrimental effects of the nature of work in the presence of technological changes. Although the future is unknown, what is clear is the need to evolve with time. Humans, to survive in the job market, will need to match their competency levels with emerging technologies [17]. In this review, I aim to understand the future of work and employment considering the technological advancement in the new millennium era from a holistic perspective and share my views on the ongoing debate using People, Process, and Technology framework [32]. The research questions formulated to achieve the said objective are as follows,

RQ: How will tomorrow look? Looking at the Future of Work (FoW) from a multi-faceted perspective.

Here, a common element across the literature concerning the FoW talks about people or process or technology at large. So, one of the best ways to map the FoW is using the People-Process-Technology (PPT) framework. The idea of people- process-technology roots back to the 1960s. It talked about four factors, namely- people, tasks, structure, and technology. Over the years, the model was reimagined into a golden triangle by the practitioner and research community

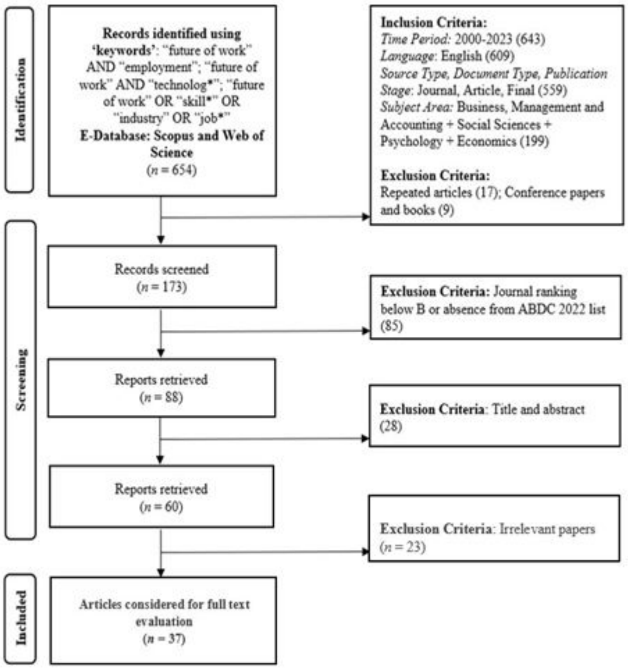
[6] [35]. It was largely brought into the information technology domain by Bruce Schneier in the 1990s. This ultimately is known as the people-process-technology (PPT framework) today to serve modern organizations and build a balance between the people, process, and technology aspects of an organization to improve efficiency and effectiveness.

Moving ahead, the study will explore themes relevant to the FoW domain from the lens of the PPT framework and will aim to establish a relationship between it.

II. METHODOLOGY

In this study, I have used a systematic review to summarize the existing evidence in the literature to provide an extension to the PPT framework for understanding the FoW phenomenon [22].

Fig.1. PRISMA method of article selection

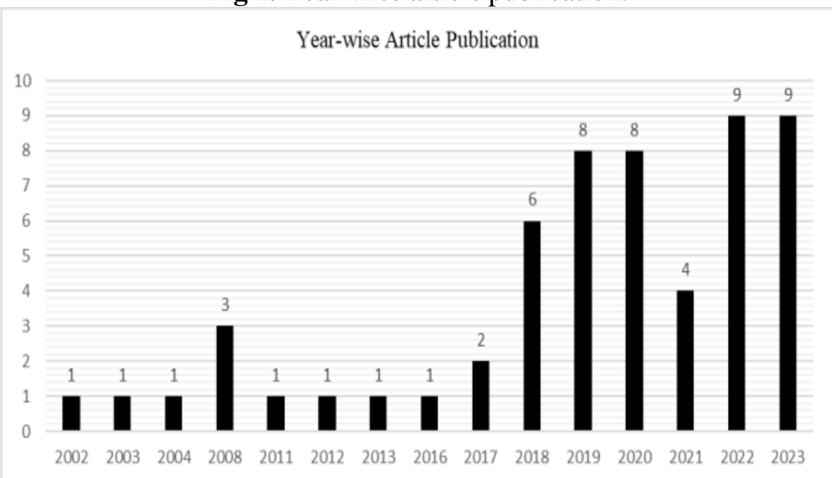


A. Article Selection Process

The article selection follows the PRISMA method using Scopus and Web of Science. Figure 1 shows the detailed steps followed. The following inclusion criteria are adopted after eliminating any repetition of articles. Period 2000 to 2023, English language, content type will be full text in journal or research article, which yielded 173 articles. Further, to ensure only high-quality articles were reviewed, an exclusion criterion is applied to all the articles that are published in journals with ABDC journal ranking 2022 "C" or not present. This brings the article number to 88. After manual abstract and title screening with the final count of articles as 37.

The year-wise article publication details are depicted in Figure 2. The results show that in recent years, 2022 and 2023, the highest number of publications in the FoW domainwas observed.

Fig 2. Year-wise article publication.



B. Methods of Analysis

To answer the RQ, a thematic analysis was conducted on the existing stream of literature. [7] Six steps of thematic analysis are employed.

Table I. Sample of thematic analysis

Articles	Descriptive Codes	Sub-Themes	Main Theme
[4]	Information technology skills	Skills and values	People
[14]	Skill specific occupational decline		
[19]	Employment inclusion of young adults with disabilities	Diversity and demographic changes	
[34]	Leading by feelings in future of work	Leadership	
[11]	De-routinization of job structures	Job structure	Process
[12]	Role of labour flexibility on future of work	Policy implications	
[39]	Parental leave, social inequalities, and the future of work		
[38]	The digital transformation of teams from conventional to virtual	Online mode of working	
[3]	AI and human collaboration	Artificial intelligence and other digital technologies influence on humans	Technology
[36]	Software Automation and the Future of Work		

To start with the first step, a thorough reading of all the 37 articles selected for the review was done to be familiar with their written content. An Excel workbook was maintained to present clarity of thought while manually coding each document based on the central idea of the article. At this stage, the descriptive codes were given to each article. Once all 37 articles had descriptive codes, a rigor manual screening was performed to identify and sort the articles based on their potential themes as per their described codes. Emergent themes were found using thecodes, and then the themes were given specific labels.

Finally, the themes were again checked after a week, andthe whole six-step process was repeated to ensure that I could synthesize the data similarly. After completing these two rounds, the themes were finalized for all the articles under this review. Table 1 shows the sample of the in-depth process employed for the thematic analysis as per the study objective.

III.PEOPLE

The scope of "People in the PPT framework" surrounds the human element who are the ultimate users of technologyand need it to perform at work. The sub themes of the peopleaspect are- Skills and Values, Diversity as DemographicChanges, and Leadership.

A. Skills and Values, Diversity as Demographic Changes,and Leadership

These sub-themes regarding people's perspectives in the PPT framework elaborate on the human aspects future of work. In terms of skill-based employment, [14] found that job roles that are less flexible to change have already started reducing. This also holds true when automation is added to the picture. Here, computers and other digital technologies tend to replace humans easily in routine and repetitive job roles due to the cognitive ability of the machine [9]. Hence, itis evident that we humans cannot beat these super-humans in routine job roles. Job roles in both private and public sectors where humans can work better surround the non-routine and non-repetitive jobs where, through persistence and human cognitive ability, better performance can be showcased.

A rationale that exists in the world is that the future is non-deterministic and widely depends on the choices humans make [41]. The desired results of such choices account for awareness about one's work and ability to foresee possible job outcomes [33] through acquiring the necessary education levels. Another element of the people's perspective is the demographic composition of the population at large. For anyorganization, the gender ratio is essential when newtechnology is being considered. [16] have highlighted the preexisting inequality in the labour market for gender relations. Occupations related to care and health, which have more females than males, have lower chances of automobility than manual jobs, which are dominated by males [29]. FoW must create employment opportunities, keeping people's diversity in mind. Being accountable for different genders and age groups to people with disabilities [19].

The technologies might be neutral, but the users or programmers might not. Here, what must be noted is that such inequalities might remain invisible if not examined in the digital era [27]. The role of leadership becomes of key importance when any new technology is being introduced due to such facets.

B. **How will tomorrow look?**

Emotional Intelligence will become noteworthy for leaders [34] to operate in the 21st-century workplace, which is prone to change management. The role of automation will direct the flow of gender composition in the industries and not vice versa. Although the inequalities in the labour marketare undeniable, it is said that gender will not influence decisions to automate jobs. Rather, these technological changes will impact specific sectors or industries [29]. Hence, the focus relies on the skills people possess in the job market. This transformation of labour from routine roles to non-routine roles and from non-cognitive domains tocognitive domains.

Although technological advancement like the introduction of Artificial intelligence (AI) in the workplace poses a threat to highly skilled jobs, it still won't eliminate people aspects from it. The anticipated future skill will answer to the need for flexibility and an attitude of "learning to learn," which will be an outcome of the education and training received by an individual [33] [41]. Information Technology (IT) skills will be an essential component of the human capital for any organization [4]. Basic IT skills and digital knowledge will become fundamentals of any job role.

IV.PROCESS

The scope of "Process in the PPT framework" surrounds the regulation-policy elements and is available to support theuse of technology at the workplace. The sub themes of the process aspects are- Job Structure, Policy Implication, OnlineMode of Working.

A. **Job Structure, Policy Implication, Online Mode ofWorking.**

These sub-themes regarding process perspective in the PPT framework elaborate on the operational aspects of the future of work. The technological changes result in changes in the employment structure and the work itself [11]. The increased use of computers in the workplace tends to replace occupations with routine task structures of work with that machine. [12] showed that the higher the rigidity of labour regulations is, the slower the substitution of robots and other machines for workers. In terms of cost, the stricter regulations lead to greater anticipation of robot adoption dueto the existing trade-off. Considering accounting for digitalization, the policy frameworks need to be constantly revised [39].

In the digital era, knowledge transfer has become crucial to teams across the globe. Changes in the mode of communication forces [38] process changes in the traditional workplace setup and display a need for building learning platforms. Agile organizations are the preferred workplaces soon. HR policies must include different sets of work arrangements, from flexitime to job sharing. Due to such changes, the firms now operate in a highly risky environment. To avoid any friction with the budding technology, the policies need to be designed in a flexible manner. Policymakers need to strike the perfect balancebetween the human and robot substitution scenario [12].

B. **How will tomorrow look**

Policymakers, when introducing automation at the workplace, should focus on redesigning the jobs and rebuilding the industrial relations with the authorities. Such policy formation will allow the workers and their leaders to rebalance the equilibrium disturbed while adopting new technology [5]. Here, for efficient processes, organizations should aim at achieving a fitment between governance and job design in the age of automation. When accounting for thecost factor in the long run, it can be said that technological advancements are likely to accelerate. Based on this, it can be said that in the coming decades, a prominent shift will be witnessed by organizations from conventional setups to online or virtual modes.

The firms need to achieve a competitive advantage [1] over their competitors, which needs constant innovation. Here, for these global firms, having a change manager [38] isvital to look after the strategic transformations of the business considering technological advancement. Such job roles will enable the smooth flow of processes throughout the organization. To further facilitate the processes, a digital communication structure must be adopted, with necessary training programs being conducted for the employees.

V. TECHNOLOGY

The scope of "Technology in the PPT framework" surrounds the technical elements which are central to the development of people and can be either a tool, target, or facilitator. Sub themes of the technology aspects are- Artificial Intelligence, Robotics, Other Digital Technologies.

A. **Artificial Intelligence, Robotics, Other DigitalTechnologies.**

These sub-themes regarding the technology perspective in the PPT framework elaborate on the technological advancements of the future of work. Among all the new technologies, Artificial Intelligence (AI) is the current hot topic of discussion [37]. Societies are divided in their views on AI and work as anticipation for the FoW. AI is an application based on algorithmics that performs cognitive tasks undertaken by humans through incorporating machine learning [3]. The risk of mass unemployment is common among people in today's world. Here, technological advancement is not only limited to the role of AI but also to software automation at large. Big data, digital technologies, machine learning, and robotics are a few other technologies that will transform the relationship between work and employment [36]. Few physical and software robots are also creating a collection of tools known as robotic process automation, with cognitive automation as a dominant feature[40].

This software automation needs huge investments. Leaders are required to make a call to invest either in technologies or in people. Such disruptions require the reconfiguration of organizations from the grassroots level. The dynamism of firms is enduring quality investors look forward to in this digital age [36].

B. How will tomorrow look?

One of the key elements to look forward to from the technology perspective is building a sustainability discourse [37]. Just like humans influence future resources, technologies might also have a similar outcome, giving rise to a technological sustainability advancement viewpoint. How things unfold will be interesting to witness in the coming times, with AI and employment factors intersecting each other. The sophisticated machines must be module as per the sociotechnical system, and the foundation for technological determinism [20] will be presented to support platform economies. In the competitive times of technological advancements, a new culture of trust is vital tobuild among employees [24].

Super teams are a new narrative that can be heard in the digital era. These super teams are referred to elaborate on the budding human-machine relationship [18]. Such symbiosis between the key actors will ensure smooth working of them together. It is said that humans will perform better in intuitive decision-making, and AI will perform better in analytical decision-making, leaving room for humans and machines to coexist in partnership. Such interactions and constant learning will make both smarter with time and shape the FoW in a more progressive way for employment.

VI. DISCUSSION

How tomorrow will look is a question of possibilities. Prima facie relies on balancing the various aspects of the FoW. This paper focused on understanding how the FoW will be shaped based on the PPT framework [6] [35] and hasadopted this framework to suggest tomorrow's employment case.

In any scenario drawn for future work, what remains constant is the viewpoint of striking a balance between people, process, and technology. Although these three occur independently, there is a co-dependency between them in real life. When technological advancements unfold in a digital world, people and processes must acquire necessary upgrades to stay relevant. This article focuses on ensuring self-check mechanisms within the PPT framework and extending the idea of merrier balancing the three aspects. Instead, it initiates a debate that due to the rise of one aspect because of demand or advancements, the other two aspects of the PPT framework work towards achieving a similar level of efficiency and effectiveness.

A. Conclusion on, “How will tomorrow look?”

From a technology perspective, AI, along with otherdigital technologies, will enter the workplace of tomorrow. Here, technologies will take a sociotechnical view and aim tobuild a coexistence relationship between humans and machines. Technologies, along with constant innovation, can only succeed in the FoW when symbiosis between bothparties is achieved.

To undergo a successful digital transformation, apart from striking a balance between people, process, and technology, organizations need to keep a check on government regulations as well. With constant friction between machines and humans, many policymakers [15] act as driving forces of change [2] to address the social issues ofopportunity inequalities across the globe. To survive in the digital age, organizations must be ready for change management. From a leader's lens, they need toaccommodate the new forms of organizations that will be self-managed and people-centred due to the decentralization [23] brought in by technological advancements.

B. Limitation and Future Directions

No study is free of limitations. Even this study has certain constraints. This study takes a bird's eye view and doesn’t provide industry-specific future directions for the organizations. Further, it adopts the PPT framework and doesnot account for the economic and social factors that might influence the FoW. Going ahead, scholars can conduct research in a specific industry to highlight the skills requiredfor FoW. They can also identify the most used theories in thedomain and study its chronological evolution in the 21st century.

REFERENCES

[1] A. Aloisi and V. Stefano, “Regulation and the future of work: The employment relationship as an innovation facilitator,” *International Labour Review*, vol. 159, no. 1, pp. 47–69, Mar. 2020, doi: https://doi.org/10.1111/ilr.12160.

[2] M. Annunziata and H. Bourgeois, “The future of work: how G20 countries can leverage digital-industrial innovations into stronger high-quality jobs growth,” *Economics: The Open-Access, Open- Assessment E-Journal*, vol. 12, no. 1, 2018, doi: https://doi.org/10.5018/economics-ejournal.ja.2018-42.

[3] C. Anthony, B. A. Bechky, and A.-L. Fayard, “‘Collaborating’ with AI: Taking a System View to Explore the Future of Work,” *Organization Science*, vol. 34, no. 5, Jan. 2023, doi: https://doi.org/10.1287/orsc.2022.1651.

[4] H. Atasoy, R. D. Banker, and P. A. Pavlou, “Information Technology Skills and Labor Market Outcomes for Workers,” *Information Systems Research*, vol. 32, no. 2, pp. 437–461, Jun. 2021, doi: https://doi.org/10.1287/isre.2020.0975.

[5] F. Belloc, G. Burdin, L. Cattani, W. Ellis, and F. Landini, “Coevolution of job automation risk and workplace governance,” *Research Policy*, vol. 51, no. 3, p. 104441, Apr. 2022, doi: https://doi.org/10.1016/j.respol.2021.104441.

[6] S. Berkun, Making things happen : mastering project management. Sebastopol: O’reilly Media, 2015.

[7] V. Braun and V. Clarke, “Using Thematic Analysis in Psychology,” *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006, doi: http://dx.doi.org/10.1191/1478088706qp063oa.

[8] D. Brougham and J. Haar, “Technological disruption and employment: The influence on job insecurity and turnover intentions: A multi-country study,” *Technological Forecasting and Social Change*, vol. 161, p. 120276, Dec. 2020, doi: https://doi.org/10.1016/j.techfore.2020.120276.

[9] E. Brynjolfsson, M. Liu, and G. Westerman, “Do Computers Reduce the Value of Worker Persistence?,” *Journal of Management Information Systems*, vol. 39, no. 1, pp. 41–67, Jan. 2022, doi: https://doi.org/10.1080/07421222.2021.2023406.

[10] M. Dean and J. Spoehr, “The fourth industrial revolution and the future of manufacturing work in Australia: challenges and opportunities,” *Labour & Industry: a journal of the social and economic relations of work*, vol. 28, no. 3, pp. 166–181, Jul. 2018, doi: https://doi.org/10.1080/10301763.2018.1502644.

[11] E. Fernández-Macías, M. Bisello, E. Peruffo, and R. Rinaldi, “Routinization of work processes, de-routinization of job structures,” *Socio-Economic Review*, vol. 21, no. 3, Jul. 2022, doi: https://doi.org/10.1093/ser/mwac044.

[12] M. Fornino and A. Manera, “Automation and the Future of Work: Assessing the Role of Labor Flexibility,” *Review of Economic Dynamics*, vol. 45, Jul. 2021, doi: https://doi.org/10.1016/j.red.2021.07.002.

[13] E. Granter, “A dream of ease: Situating the future of work and leisure,” *Futures*, vol. 40, no. 9, pp. 803–811, Nov. 2008, doi: https://doi.org/10.1016/j.futures.2008.07.012.

[14] L. Hensvik and O. Nordström Skans, “The Skill-Specific Impact of Past and Projected Occupational Decline,” *SSRN Electronic Journal*, vol. 81, 2020, doi: https://doi.org/10.2139/ssrn.3534479.

[15] G. M. Hodgson, “The Future of Work in the Twenty-First Century,” *Journal of Economic Issues*, vol. 50, no. 1, pp. 197–216, Jan. 2016, doi: https://doi.org/10.1080/00213624.2016.1148469.

[16] D. Howcroft and J. Rubery, “‘Bias in, Bias out’: gender equality and the future of work debate,” *Labour & Industry: a journal of the social and economic relations of work*, vol. 29, no. 2, pp. 213–227, Apr. 2019, doi: https://doi.org/10.1080/10301763.2019.1619986.

[17] A. Jain and S. Ranjan, “Implications of emerging technologies on the future of work,” *IIMB Management Review*, vol. 32, no. 4, Dec. 2020,doi: https://doi.org/10.1016/j.iimb.2020.11.004.

[18] M. H. Jarrahi, “Artificial Intelligence and the Future of work: Human- AI Symbiosis in Organizational Decision Making,” *Business Horizons*, vol. 61, no. 4, pp. 577–586, Jul. 2018, doi: https://doi.org/10.1016/j.bushor.2018.03.007.

ISSN 2394 - 7780

[19] A. Jetha et al., "The future of work in shaping the employment inclusion of young adults with disabilities: a qualitative study," *Equality, Diversity and Inclusion: An International Journal*, vol. 42, no. 9, pp. 75–91, 2023.

[20] S. Joyce, C. Umney, X. Whittaker and M. Stuart, "New social relations of digital technology and the future of work: Beyond technological determinism," *New Technology Work and Employment*, vol. 38, no. 2, pp. 145–161, 2023.

[21] E. K. Kelan, "Automation Anxiety and Augmentation Aspiration: Subtexts of the Future of Work," *British Journal of Management*, vol. 34, no. 4, Nov. 2022, doi: https://doi.org/10.1111/1467-8551.12679.

[22] B. A. Kitchenham, *Procedures for Performing Systematic Reviews*. Keele : Keele University, 2004.

[23] S. Khallash and M. Kruse, "The future of work and work-life balance 2025," *Futures*, vol. 44, no. 7, pp. 678–686, Sep. 2012, doi: https://doi.org/10.1016/j.futures.2012.04.007.

[24] C. A. Makridis and J. H. Han, "Future of work and employee empowerment and satisfaction: Evidence from a decade of technological change," *Technological Forecasting and Social Change*, vol. 173, p. 121162, Dec. 2021, doi: https://doi.org/10.1016/j.techfore.2021.121162.

[25] J. Morgan, "Will we work in twenty-first century capitalism? A critique of the fourth industrial revolution literature," *Economy and Society*, vol. 48, no. 3, pp. 371–398, Jul. 2019, doi: https://doi.org/10.1080/03085147.2019.1620027.

[26] J. Morris, "The future of work: organizational and international perspectives," *The International Journal of Human Resource Management*, vol. 15, no. 2, pp. 263–275, Mar. 2004, doi: https://doi.org/10.1080/0958519032000158509.

[27] B. Ozkazanc-Pan, "Diversity and future of work: inequality abound or opportunities for all?," *Management Decision*, vol. ahead-of-print, no. ahead-of-print, Dec. 2019, doi: https://doi.org/10.1108/md-02-2019- 0244.

[28] L. Pangrazio, C. Bishop, and F. Lee, "Old Media, New Gigs: The Discursive Construction of the Gig Economy in Australian News Media," *Work, Employment and Society*, vol. 37, no. 3, pp. 606-624, 2021.

[29] D. Peetz and G. Murray, "Women's employment, segregation and skills in the future of work," *Labour and Industry: A Journal of the Social and Economic Relations of Work*, vol. 29, no. 1, pp. 132–148, 2019.

[30] F. Pichault and T. McKeown, "Autonomy at work in the gig economy: analysing work status, work content and working conditions of independent professionals," *New Technology, Work and Employment*, vol. 34, no. 1, pp. 59–72, Mar. 2019, doi: https://doi.org/10.1111/ntwe.12132.

[31] E. E. Potter, "Telecommuting: The future of work, corporate culture, and American society," *Journal of Labor Research*, vol. 24, no. 1, pp. 73–84, Mar. 2003, doi: https://doi.org/10.1007/s12122-003-1030-1.

[32] B. Rajput, "Understanding Modus Operandi of the Cyber Economic Crime from People-Process-Technology Frameworks Perspective," *Journal of Emerging Technologies and Innovative Research*, vol. 5, no. 3, 2018.

[33] M. Rhisiart, E. Störmer, and C. Daheim, "From foresight to impact? The 2030 Future of Work scenarios," *Technological Forecasting and Social Change*, vol. 124, pp. 203–213, Nov. 2017, doi: https://doi.org/10.1016/j.techfore.2016.11.020.

[34] S. Saha, R. Das, W. M. Lim, S. Kumar, A. Malik, and B. Chillakuri, "Emotional intelligence and leadership: insights for leading by feeling in the future of work," *International Journal of Manpower*, vol. 44, no. 4, pp. 671–701, Jan. 2023, doi: https://doi.org/10.1108/ijm-12- 2021-0690.

[35] B. Schneier, *Secrets and lies : digital security in a networked world*. Indianapolis, Indiana: John Wiley & Sons, Inc, 2015.

[36] B. Shestakofsky, "Working Algorithms: Software Automation and the Future of Work," *Work and Occupations*, vol. 44, no. 4, pp. 376–423, Aug. 2017, doi: https://doi.org/10.1177/0730888417726119.

[37] L. Vicsek, "Artificial intelligence and the future of work – lessons from the sociology of expectations," *International Journal of Sociology and Social Policy*, vol. ahead-of-print, no. ahead-of-print, Oct. 2020, doi: https://doi.org/10.1108/ijssp-05-2020-0174.

[38] D. Vuchkovski, M. Zalaznik, M. Mitręga and G. Pfajfar, “A look at the future of work: The digital transformation of teams from conventional to virtual,” *Journal of Business Research*, vol. 163, 2023.

[39] G. Whitehouse and M. Brady, “Parental leave, social inequalities and the future of work: possibilities and constraints within the Australian policy framework,” *Labour & Industry: a journal of the social and economic relations of work*, vol. 29, no. 3, pp. 257–272, Jul. 2019, doi: https://doi.org/10.1080/10301763.2019.1677203.

[40] L. Willcocks, “Robo-Apocalypse cancelled? Reframing the automation and future of work debate,” *Journal of Information Technology*, vol. 35, no. 4, pp. 286–302, Jun. 2020, doi: https://doi.org/10.1177/0268396220925830.

[41] R. Wilson, “Skills anticipation—The future of work and education,” *International Journal of Educational Research*, vol. 61, pp. 101–110, Jan. 2013, doi: https://doi.org/10.1016/j.ijer.2013.03.013.

 ISSN 2394 - 7780

A CONCISE REVIEW OF POTHOLE DETECTION TECHNIQUES

Mitali Suhas Javadekar[1], Ruchi Manojkumar Jha[2], Vedant Nawange[3] and Prof. Shubhada Labde[4]
[1, 2, 3,4]Computer Department, K.J Somaiya Institute of Technology Mumbai, India

ABSTRACT

Potholes present a challenge for road infrastructure and public safety. It is crucial to detect and address these road defects to maintain efficient transportation systems. Our study offers a summary of approaches used for pothole detection highlighting advancements as well as the remaining challenges. The review encompasses sensing technologies, methods for processing data, and machine learning paradigms that are used to solve the issue of pothole detection. Additionally, it explores limitations and unresolved questions in this field such as the need for real-time detection reliability in weather conditions and the development of cost-scalable solutions. By providing a synopsis of the state-of-the-art research and recognizing areas for further investigation this review aims to be resourceful, for both research personnel and practitioners interested in pothole detection systems.

Keywords—Pothole detection, Object detection, Image Processing, CNN, R-CNN, YOLOv1, YOLOv2, YOLOv3, YOLOv4, YOLOv5, YOLOv7.

I. INTRODUCTION

For as long as humans have migrated, roadways have proved to be one of the main forms of transportation. Over the decades, the transportation medium has evolved and so has the state of the roads. The development of a nation can be measured by the condition of its roads. In recent years, India has risen to be the second-largest roadway network. Nearly 90% of India's population and 65% of our country's freight transportation uses roadways. Poorly constructed roads riddled with potholes, faulty concrete speed breakers, and outdated drainage networks together are contributors to an increase in accidents and injuries throughout the country. Encountering potholes during one's journey is not only uncomfortable but also poses a safety hazard to both humans as well as the vehicle. According to a newspaper article of BMC's data, despite the concretization of roads, around 60,000 potholes have been recorded in Mumbai to date in 2023 which has significantly increased from 2022 having roughly 38,000 and in 2021 having 44,000 potholes.

The detection of instances of a particular class's semantic objects in digital photos and videos is the focus of the computer technology called object detection, which is associated with image processing and computer vision. Object detection models are trained using a training dataset to return the coordinates of the objects in an image that it has been trained to recognize. The system does so with varying levels of accuracy which we term as the confidence of the system. Over the years a significant evolution has been there has been a significant evolution in the models used for object detection. Traditional computer vision techniques that relied on handcrafted features were used earlier. During the 2010 decade, the use of R-CNN was the earliest known attempt to apply the concept of deep learning to object detection. Faster R-CNN was an improvement upon R-CNN.

The year 2015 brought with it the advantages of fast inference time by dividing the image into a grid and predicting bounding boxes and class probabilities directly, using YOLO. Joseph Redmon and Santosh Divvala introduced the popular object detection algorithm, You-only-look-once, which presents the key idea of viewing object detection as a single regression problem instead of breaking down the tasks of object detection into multiple steps.In other words, YOLO uses a single, comprehensive view of the image to concurrently predict bounding boxes and class probabilities.YOLO is used in various real-time cases.

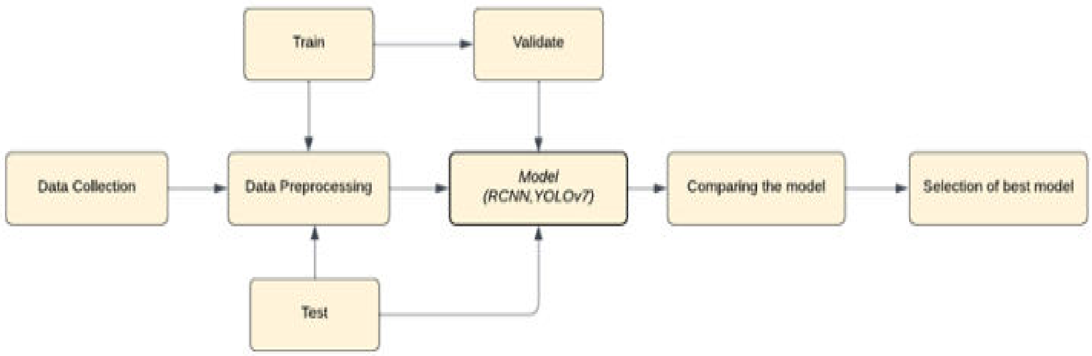


Fig 1 Generic Flowchart of Object detection

Fig 1.1, as given below shows the generic flow of object detection and hence identifying potholes on the road.

II. Related Work

Maheshwari Kotha, et.al (2020) suggested a real-time pothole detection mobile application. The paper suggested two techniques, accelerometer-based detection which had about a 55% accuracy rate in identifying potholes, and vision-based detection achieved nearly 60% accuracy. The application identifies potholes using both methods and is plotted on Google Maps, serving as a safety measure for various vehicle users. The model uses 400 image datasets where 150 images are real-time and 250 images are obtained from the Internet. [15]

Aaquib Javed et.al.,(2021) presented a system for identifying potholes using a Region-Based Convolutional Neural Network. The study introduces a solution based on object detection, employing the R-CNN and SSD Mobile Net algorithms, and it is trained using a dataset from Bangladesh containing diverse pothole images. The outcomes reveal effective pothole identification with a peak confidence level of 93%.[8]

Kavitha R et.al., (2021) introduced a system that can be used by autonomous vehicles to detect potholes using YOLOv3 to train the CNN model. A newly created dataset consisting of classes of objects uses CNN and a max-pooling layer for prediction to improve accuracy in the detection of small targets.The experiment result shows the detection of all classes of objects with a high score and accurate detection of bounding boxes. The autonomous vehicle's ability to detect potholes on Indian roads enables it to go smoothly and avoid being struck by them. [12]

Oche Alexander Egaji et.al., (2021) proposed an Android application-based approach for pothole detection in terms of binary classification.A dataset of 30,808 was collected from Android phones.The research used a combination of the stratified K-fold cross-validation technique and holdout. With a comparable accuracy of 0.8889, the Random Forest and KNN demonstrated enhanced results using the test dataset After random search hyperparameter adjustment the Random Forest model’s accuracy is 0.9444. Further annotations will help the model categorize the potholes in more detail.[17]

Khaled R. Ahmed, (2021) has developed an efficient deep-learning CNN model for real-time, accurate pothole detection. Using a dataset accumulated from multiple sources as well as images from a smartphone video camera set up on the windshield of the vehicle. The experimental outcome indicates that Ys model should be used in real time situations, such as embedding in automobiles, as it has demonstrated a fast detection rate. Faster R-CNN with ResNet50 can be used for more complex hardware configurations when accuracy is top priority. MVGG16, which is smaller than both, can be utilized if the size of the Faster R-CNN model is an issue. [20]

Yongjin Zeng, et.al (2022) utilizes deep learning for identifying cracks in roads on collected road images, using the YOLOV5 model for training and detection. Five groups are identified from the gathered collection of road crack data: mesh cracks, potholes, repairs, and regular transverse and longitudinal cracks. A rectangular frame with a 4:3 aspect ratio is employed to capture the full image in order to extract the local features of road fractures.[16]

E Sai Tarun Kumar Reddy et.al.,(2022) used CNN and YOLO v7 Algorithm for detecting potholes. The dataset used in the algorithm consists of 289 images, which is separated into groups for training, testing, and validation. The proposed model used YOLO v7 and CNN for image classification. The model shows good accuracy and speed due to the use of the YOLO v7 algorithm. The latitude and longitude coordinates can be used to mark the potholes in the future.[3]

Madarapu Sathvik et.al.,(2022), suggested YOLOv7 pothole detection, a robust object detection model which provides an increase in accuracy without a corresponding rise in inference costs. The dataset of 289 images gives a confidence level of 0.5 mAP, recall of 0.95 and precision of 1.In comparison to other models used for pothole, YOLOv7 achieves an accuracy level of 2% higher compared to R-CNN, while concurrently exhibiting 509% faster inference time as well as an F1 score of 0.51. Locating individual potholes on the map using latitude and longitude coordinates as well as forming reports to find the most effective strategy to navigate them is a future advancement.[7]

Priyanka Gupta et.al., (2022) presented a novel method for detecting potholes in roads using deep learning techniques. The proposed model convolutional neural networks (CNNs), specifically the ResNet50 model, which employs transfer learning to fine-tune the model for the purpose of identifying potholes. The outcomes of the experiment show the model's effectiveness, achieving a high validation accuracy of 98%, outperforming previous pothole detection methods. [10]

Muhammad Haroon Asad, et.al (2022) suggested a real-time pothole identification system utilizing multiple deep learning methods. Two models, YOLO family and SSD-mobilenetv2, have been trained on the same dataset. Even though YOLOv5 achieved mAP@0.5 95% but failed to detect distant potholes and exhibited misclassification. Whereas, mAP@0.5 for YOLOv4 and Tiny-YOLOv4 were 85.48% and 80.04%, respectively with Tiny-YOLOv4 demonstrating faster inference times.[14]

M. Vasudev Rao et al. (2022) propose an innovative method to tackle the problem of dimension estimation and pothole detection with cutting-edge deep learning techniques. Around 600 image dataset is used and covers images from various seasons, providing a diverse range of road conditions. The tiny YOLO model has 53 convolutional layers,is used to identify the potholes with their approximate dimensions present on the roadside. Because of its lightweight design, the suggested model can store videos for shorter periods of time and with less space.[9]

Au Yang Her et.al.,(2022) provided an enhanced YOLOv5 pothole detection system in real time for cars in Malaysia. The paper introduces a solution using computer vision technology installed in vehicles, employing YOLOv5, a Convolutional Neural Network-based deep learning model. The results demonstrate improved accuracy, with YOLOv5 models achieving mAP@0.5 scores of 80.8%, 82.2%, and 82.5% on various versions.[5]

Boris Bucko et.al.,(2022) demonstrated a pothole detection system based on computer vision in difficult circumstances. The dataset includes clear weather images labeled with a structured format and additional subsets for unfavorable circumstances, accumulating 1052 photos. The outcomes demonstrate how poorly Yolo v3-SPP functioned in wet, dusk, and nighttime conditions. In almost every difficult scenario, Yolo v3 was outperformed by Sparse R-CNN.[21]

Aketi Ajay, et.al(2022) proposes a method to detect potholes using a camera mounted on a vehicle, with the aid of image processing methodologies. The system aims to reduce manual effort and improve efficiency by promptly identifying and notifying authorities about potholes. Various image processing techniques such as edge detection and Hough transforms are employed for pothole detection. The proposed work extracted frames from a video and achieved an accuracy of 77% for more than 50 images of the dataset. [13]

Shrinjoy Sen et.al., (2023), Talk about the potential application of the YOLO algorithm. Initially the model used Yolov3 a 600-image short dataset clicked at 30 to 45 degrees of angles yielded a 70 percent accuracy rate in detecting potholes at a distance of approximately 10 meters from the vehicle traveling at 30 km/h. To improve accuracy, additional datasets are employed at 20 to 90 degree angles with respect to the ground which gives an accuracy of 85 to 90 percent. Potholes at 50 meters distance from a 60km/h driven vehicle are detected allowing the driver roughly four to five seconds to apply the brakes or reduce the speed of the vehicle.[1]

Rohan Chorada et.al.,(2023), propose a CNN-based Real-time pothole detection model using InceptionV3 CNN architecture which reached a high detection rate of 95.2% while reducing false positives. The accuracy achieved by the model is 80\%. One of the key features of the research paper is that the proposed method provides a more effective way to observe potholes by providing live video capturing which enables real-time monitoring and detection of potholes, thus helping in road safety.[2]

R. Sathya et.al.,(2023), proposes the use of YOLOv3 for detecting potholes which provides an improvement in mAP of 83.26 while a significant reduction in computing cost is observed. On comparing the performance measure of YOLOv3 to previous versions, the proposed model increases the precision of detecting small objects with an incredible processing speed of 45 fps. In order to help with road maintenance, the method can also be started using a GPS module that, after the dashboard module has located the pothole, generates the coordinates.[4]

Savita Chougule et.al (2023) used deep learning algorithms, specifically YOLOv3 and YOLOv5, to detect potholes from video images captured by a camera module. Images from Google Image Search and photos taken with an Android phone camera from roads with damage are included in the dataset. The central processor of the suggested system is a Raspberry Pi 4B, which processes the recorded video stream and executes the pothole detection algorithm. The YOLOv5 was found to be working more effectively than YOLOv3, in terms of precision, sensitivity, and average precision (AP) values of 0.763, 0.548, and 0.635, respectively.[11]

Tejas B S et.al.,(2023) presented a “Real Time Detection of Humps and Potholes”. A custom dataset of 150-200 images of urban roads are used in the proposed model. Raspberry Pi, Open CV are used for capturing images, saving them, TensorFlow is used for detection of potholes and humps from images stored. The model

ISSN 2394 - 7780

gives an accuracy of 90%.In future findings, with increased CPU and GPU capabilities, live feed from camera better processing can be achieved.[18]

Yang Zou et.al.,(2023) presented an improved YOLOv5-based lightweight pothole detection technique. The paper introduces a streamlined pothole detection model based on an improved YOLOv5s framework enhanced with attention mechanisms and innovative techniques. Through experiments conducted on a dataset that combines publicly available data and self-captured images, the enhanced YOLOv5s model achieves notable improvements, boasting a 90.7% accuracy and an 89.1% average accuracy.[6]

III. LITERATURE REVIEW

Table 1. Comparative Analysis

Paper Cited	Method	Merits	Challenges
15	Using vehicle Accelometer along it's z-axis	60% classification accuracy	Classification accuracy needs to be improved
8	R-CNN, SSD mobile net algorithm	93% confidence level	Failed in low quality images/videos
12	YOLOv3, Darknet 53, Rasberrypi 4, Tensorflow	Detects boundary boxes and potholes with highscore	Model needs to be trained to detect more objects.
17	Machine learning algorithms	RF Tree and KNN showed the accuracy of 89%. Accuracy after hyperparameter tuning is 94%	More samples are required.Further annotation is needed to categorize potholes.
20	YOLOv5, faster-RCNN, Deep Learning	Better mean precision and shorter inference time.	Developing a sustainable model to address extreme conditions in pothole detection.
10	ResNet50, ResNet	Accuracy of ResNet 50 is 98.05% and ResNet model is 97.08%.	The severity of the pothole needs to be detected with the region
14	YOLO family and SSD Mobilenettv	YOLOv4 with accuracy of 90% and 31.76 FPS	Detect road depressions, classify roads as per quality, and depth estimation of potholes
9	YOLO, Darknet-53	68% classification precision	Classification accuracy needs to be improved
13	Filtering technique, Edge detection, Morphological imaging	77% classification accuracy	Model needs to be trained and classification accuracy needs to be improved
16	YOLOv5 algorithm	Better detection results through YOLOv5 network under different networks	The computational efficiency can be optimized to reduce the processing time.
3	CNN and YOLO v7	High accuracy and speed due to YOLO v7	More training dataset needed
5	YOLO v5m, YOLO v5s, YOLO v5n	YOLO v5n performs better than other with 82.5% classification accuracy	Classification accuracy needs to be improved

ISSN 2394 - 7780

19	Laser based methods	5.2% and 14.4% depth error in static and dynamic conditions respectively	The depth error in dynamic conditions needs to be decreased and classification accuracy needs to be improved
21	YOLO v3, Sparse R-CNN	Sparse R-CNN achieved better results than YOLO v3	The performance of selected models on different hardware configurations
7	YOLOv7, YOLOv4, YOLOv5	YOLOv7 has better accuracy and faster inference process than R-CNN.	Training model for different types of potholes
11	YOLOv3 and YOLOv5	YOLOv5 model outperforms the YOLOv3 model with accuracy of 97.22%	the model can be trained by hyper tunning the training parameter like Faster RCN
6	SimAM-C3 module, YOLO v5s, CARAFE	SimAM-C3 attached YOLO v5s model gives better accuracy than YOLO v5s.	The model doesn't classify different weather and pavement conditions
18	Rasberry Pi 3, Open CV,	90% classification accuracy	Single axis Gyroscopes needs to be used for increasing accuracy
1	YOLOv3,YOLOv4, CNN	Can alert the driver 5 seconds in advance when pothole is about 50 m from car	Mapping the potholes and alerting driver about next pothole in advance
2	InceptionV3 CNN,SGD,ConvNe t	High detection rate of 95.2% and F1 score of 0.91	Dataset should be augmented to enhance accuracy and resilence of CNN
4	YOLO v3, YOLO v2, YOLO v1	The performance of YOLO v3 is better than the others	Integrating pothole detection system with smart transportation systems to enhance overall road safety.
22	Machine learning models	SVM, Random Forest Tree, and KNN provides best accuracies of 82%, 80% and 78%.	Additional annotation is required to develop a model that categorize potholes in details
23	CNN, Mask RCNN, YOLOv3	YOLO family is faster and consumes less time than CNN or R-CNN	Model needs to be trained with diverse dataset.
24	vision based, vibration method and 3D construction based methods	Model predicts shape of potholes and measure their volume using sterio vision technology	Improvements in pothole detection accuracy and real-time pothole detection is to be done
25	R-CNN, DAISS, HMS	Model accurately reflected the level of risk due to road surface damage	Limitations of using data from smartphone. Model doesn't take speed into consideration

26	Smartphone GPS sensors, K-means	65% accuracy classification	The positioning accuracy of smartphone GPS sensors was limited
27	CNN	Optimized pre-pooling CNN achieved recognition precision of 98.95%	Additional comparison with other existing models is missing
28	CNN	97.08% accuracy using pre-trained CNN model	Drawback of using thermal imaging as weather condition may change the accuracy and results

IV. SUMMARIZED FINDINGS

From our analysis of the above-mentioned studies, we have outlined the following findings:

1. According to several authors, determining the accurate dimensions of the potholes and assessing their level of severity posed to be a significant challenge which was later overcome using Darknet CNN and Tiny YOLO on a diverse dataset.
2. Tracking and storing the coordinates of the potholes using a camera feed which can be plotted on a map is a promising advancement in this research field.
3. The limitations in accuracy can be resolved in the case of YOLOv5 by improving the classification of potholes to detect distant potholes.
4. Pothole detection using Random forest can be remarkably improved by hyperparameter tuning.
5. In future, the implementation of detailed datasets of various other conditions of roads other than potholes can help to detect humps and cracks as well.
6. The lack of a proper dataset proves to reduce the accuracy of the model which can be solved by using data augmentation.
7. Issues arising due to the usage of datasets with images of potholes under challenging conditions like low-intensity lights and different weather conditions can be conquered using computer-vision techniques.

V. RESULT

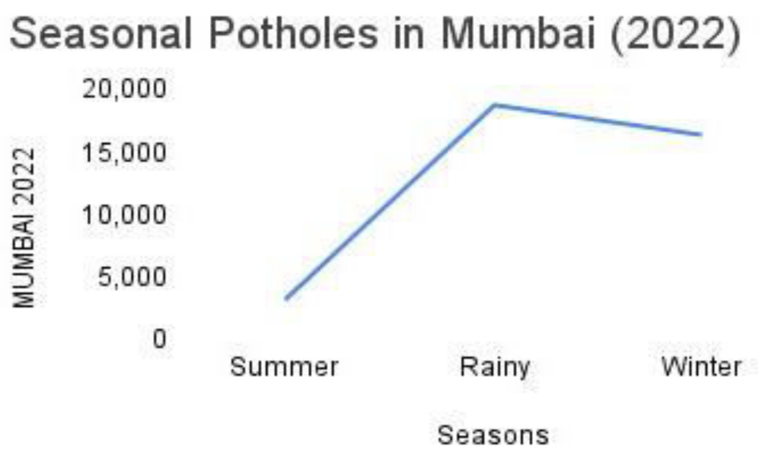


Fig 2 Seasonal Potholes in Mumbai (2022)

Fig 2, represents the variations in the number of potholes in 2022 in Mumbai city over the 3 seasons.The months are classified into 3 seasons February-May are the Summer months, June-September are the rainy season months and October-February are the Winter Season months.

We see a gradual increase in the number of potholes from the summer to the rainy season and a decrease from the rainy to the winter season.

ISSN 2394 - 7780

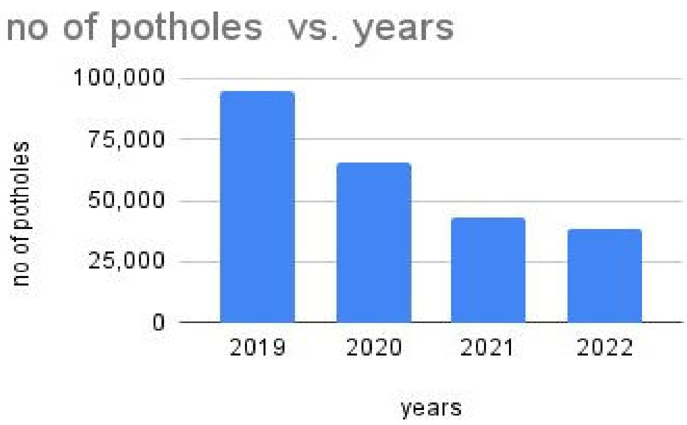


Fig 3 Year-by-year analysis of the number of potholes

Fig 3 shows a comparison of the number of occurrences of potholes in Mumbai over the years. The years considered are 2019-2022. The number of potholes over the years has significantly reduced due to the detection of potholes and timely road maintenance done by the Brihanmumbai Municipal Corporation(BMC).

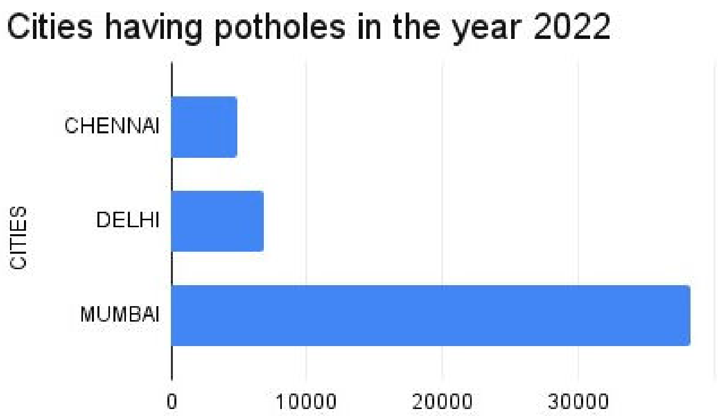


Fig 4 Occurrence of Potholes in the Metropolitan Cities in 2022

Fig 4, compares the number of potholes in the three metropolitan cities of India- Chennai, Delhi, and Mumbai.The cities have varying weather conditions which is why the number of potholes in the three cities vary.

VI. CONCLUSION

The automation of Pothole detection has proven to be a key automation in the development of our country and is expected to continue growing. The scientific community has made great strides in creating novel approaches to find potholes and enhance road infrastructure. The studies highlighted in this paper unveil the ongoing efforts to address the grave issue of pothole detection and their concerns with road safety using advanced technologies.

The above-mentioned papers have implemented a wide range of methodologies for object detection and image processing such as machine learning and deep learning algorithms, CNN and R-CNN architecture, InceptionV3, Darknet, and various versions of YOLO.The study depicts different models having different accuracies which depend on the parameters used in the training and testing dataset. Some of the key findings include real-time detection for timely alert systems, analyzing their depth, and increased classification accuracy by using YOLOv5. Researchers are exploring ways to integrate the aforementioned systems into vehicles to prevent and optimize road safety and infrastructure.

Together, these studies show how pothole detection could be greatly enhanced by sophisticated technology, with a particular emphasis on real-time capabilities and detection accuracy. As these technologies continue in their development and adaptation, the objective of mitigating accidents and improving the upkeep of road infrastructure remains attainable.

ISSN 2394 - 7780

REFERENCES

[1] Shrinjoy Sen, Deep Chakraborty, Biswanil Ghosh, Bhabnashre Dutta Roy, Krittika Das, Jyoti Anand, Prof. Aniket Maiti, "*Pothole Detection System Using Object Detection through Dash Cam Video Feed*", International Conference for Advancement in Technology (ICONAT) Goa, India. Jan 24-26, 2023.

[2] Rohan Chorada, Hitesh Kriplani, Biswaranjan Acharya, "*CNN-based Real-time Pothole Detection for Avoidance Road Accident*", 7th International Conference on Intelligent Computing and Control Systems, 2023.

[3] E Sai Tarun Kumar Reddy, Rajaram V, "*Pothole Detection using CNN and YOLO v7 Algorithm*", Proceedings of the Sixth International Conference on Electronics, Communication and Aerospace Technology (ICECA 2022), 2022

[4] R.Sathya, B.Saleena, B. Prakash, "*Pothole Detection Using YOLOv3 Model*", 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science, 2023.

[5] Au Yang Her, Weng Kean Yew, Pang Jia Yew, Melissa Chong Jia Ying, "*Real-time pothole detection system on vehicle using improved YOLOv5 in Malaysia*", IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society, 2022

[6] Yang Zou, Jiangcheng Wan, Binjie Wang, "*Lightweight pothole detection method based on improved YOLOv5*", 2023 IEEE 3rd International Conference on Information Technology, Big Data and Artificial Intelligence, 2023.

[7] Madarapu Sathvik, G.Saranya, S.Karpagaselvi, "*An Intelligent Convolutional Neural Network based Potholes Detection using Yolo-V7*", International Conference on Automation, Computing and Renewable Systems, 2022.

[8] Aaquib Javed, Md. Sayem Mahmud, Md. Takbir Alam, Md. Foysal Bin Ohab, Khandakar Ratul Ali, Abdullah Al Jobaer, M. Monir Uddin, "*Pothole Detection System Using Region-Based Convolutional Neural Network*" 2021 IEEE 4th International Conference on Computer and Communication Engineering Technology, 2021

[9] M. Vasudev Rao, Satish Kumar Dubey, Abhishek Badholi, "*Pothole Identification and Dimension Approximation with YOLO Darknet CNN*" Proceedings of the International Conference on Inventive Research in Computing Applications (ICIRCA 2022), 2022

[10] Priyanka Gupta, Manish dixit, "*Image-based Road Pothole Detection using Deep Learning Model*" 14th IEEE International Conference on Computational Intelligence and Communication Networks, 2022

[11] Savita Chougule, Alka Barhatte, "*Smart Pothole Detection System using Deep Learning Algorithms*" International Journal of Intelligent Transportation Systems Research, 2023, https://doi.org/10.1007/s13177-023-00363-3

[12] Kavitha R, Nivetha S, "*Pothole and Object Detection for an Autonomous Vehicle Using YOLO*" 5th International Conference on Intelligent Computing and Control Systems, 2021.

[13] Aketi Aajy, S.Revathy, Bheemireddy Naga Vijay Siva Surya Prakash Reddy, Mary Posonia, B. Ankayarkanni, "*Application of Image Processing Techniques for Pothole Detection* "Proceedings of the Sixth International Conference on Intelligent Computing and Control Systems (ICICCS 2022),2022

[14] Muhammad Haroon Asad, Saran Khaliq, Muhammad Haroon Yousaf , Muhammad Obaid Ullah , Afaq Ahmad, "*Pothole Detection Using Deep Learning: A Real-Time and AI-on-the-Edge Perspective* "Advances in Civil Engineering, Volume 2022, Article ID 9221211, 13 pages, 2022

[15] Maheshwari Kotha, Mounika Chadalavada, Sri Harshitha Karuturi, Hrishikesh Venkataraman, "*PotSense - Pothole Detection on Indian Roads using Smartphone Sensors*" In Proceedings of the 1st ACM Workshop on Autonomous and Intelligent mobile systems (AIMS'20), January 11, 2020. https://doi.org/10.1145/3377283.3377286

[16] Yongjin Zeng, Jie Chen, and Jian Mao, "*Deep Learning-based Road Crack Detection Technology*", 6th International Conference on Electronic Information Technology and Computer Engineering (EITCE), 2022 https://doi.org/10.1145/3573428.3573530

[17] Oche Alexander Egaji, Gareth Evans, Mark Graham Griffiths, Gregory Islas, "*Real-time machine learning-based approach for pothole detection*", Expert Systems With Applications 184 (2021) 115562, 2021.

[18] Tejas B S, V Pavan, Rohith H, Pranam J, "*Realtime Detection of Humps and Potholes*", 2023 International Conference on Smart Systems for applications in Electrical Sciences(ICSSES), 2023

[19] Adeel Ahmed, Moeez Ashfaque , Muhammad Uzair Ulhaq , Senthan Mathavan, Khurram Kamal, and Mujib Rahman, "*Pothole 3D Reconstruction With a Novel Imaging System and Structure From Motion Techniques*", IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 23, NO. 5, 2022.

[20] Khaled R. Ahmed, "*Smart Pothole Detection Using Deep Learning Based on Dilated Convolution*", MDPI Open Journal,2021, DOI: https://doi.org/10.3390/s21248406

[21] Boris Bucko, Eva Lieskovska, Katarina Zabovska, Michal Zabovsky, "*Computer Vision Based Pothole Detection under Challenging Conditions*", Sensors, EISSN 1424-8220, Published by MDPI, 2022

[22] Oche Alexander Egaji, Gareth Evans, Mark Graham Griffiths, Gregory Islas, "*Real-time machine learning-based approach for pothole detection*", Expert Systems With Applications 184, 2021.

[23] Rohitaa R, Sangoju Shreya, Amutha R, *"Intelligent Deep Learning based Pothole Detection and Reporting System*", 2021 Fourth International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2021

[24] Young-Mok Kim, Young-Gil Kim, Seung-Yong Son, Soo-Yeon Lim, Bong-Yeol Choi, Doo-Hyun Choi, *"Review of Recent Automated Pothole-Detection Methods"*, MDPI Open Journal, 2022

[25] Choong Heon Yang, Jin Guk Kim, Sung Pil Shin, *"Road Hazard Assessment Using Pothole and Traffic Data in South Korea"*, Journal of Advanced Transportation, vol. 2021, Article ID 5901203, 10 pages, 2021.

[26] Shahram Sattar, Songnian Li, Michael Chapman, *"Developing a near real-time road surface anomaly detection approach for road surface monitoring*", Measurement Volume 185, 2021.

[27] Wanli Ye, Wei Jiang, Zheng Tong, Dongdong Yuan & Jingjing Xiao (2021) Convolutional neural network for pothole detection in asphalt pavement, Road Materials and Pavement Design, 22:1, 42-58, DOI: 10.1080/14680629.2019.1615533

[28] Aparna a, Yukti Bhatia a, Rachna Rai a, Varun Gupta a, Naveen Aggarwal b, Aparna Akula, "*Convolutional neural networks based potholes detection using thermal imaging*", Journal of King Saud University - Computer and Information Sciences.

[29] Yen-Sok Poon, Chih-Chun Lin, Yu-Hsuan Liu, and Chih-Peng Fan,"*YOLO-Based Deep Learning Design for In-Cabin Monitoring System with Fisheye-Lens Camera*",IEEE International Conference on Consumer Electronics (ICCE),2022.

[30] Xiaodong Yu, Ta Wen Kuan, Yuhan Zhang, Taijun Yan*,"YOLO v5 for SDSB Distant Tiny Object Detection*",10th International Conference on Orange Technology (ICOT),2022.

[31] Xiaohan Wang, Xiaoyue Jiang, Zhaoqiang Xia, Xiaoyi Feng,"*Underwater Object Detection Based on Enhanced YOLO*",International Conference on Image Processing and Media Computing (ICIPMC),2022.

[32] Mansi Mahendru , Sanjay Kumar Dubey,"Real Time Object Detection with Audio Feedback using Yolo vs. Yolo_v3", 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence),2021.

[33] Yankai Ma,Jun Yang,Zhendong Li,ZiqiangMa,"YOLO-Cigarette: An effective YOLO Network for outdoor smoking Real-time Object Detection"Ninth International Conference on Advanced Cloud and Big Data (CBD),2021.

[34] Liu Ting ,Zhou Baijun,Zhao Yongsheng,Yan Shun,"Ship Detection Algorithm based on Improved YOLO V5",6th International Conference on Automation, Control and Robotics Engineering (CACRE),2021.

[35] Shani Verma,Dr. Shrivishal Tripathi,Dr. Anurag Singh,Dr. Muneendra Ojha,Dr. Ravi R Saxena,"Insect Detection and Identification using YOLO Algorithms on Soybean Crop",2021 IEEE Region 10 Conference (TENCON),2021.

[36] Lanfa Liu, Baitao Zhou,Guiwei Liu, Duan Lian,"YOLO-Based Multi-Model ensemble for Plastic Waste Detection along Railway Lines",IEEE International Geoscience and Remote Sensing,2022.

[37] Kwaghe, O. P.,Abdusalam Ya'u Gital,A.G Madaki,Mustapha Lawal Abdulrahman,Ismail Zahraddeen Yakubu,Iosun Stephen Shima,"A Deep Learning Approach for Detecting Face Mask Using an Improved Yolo-V2 With Squeezenet",IEEE 6th Conference on Information and Communication Technology,2022.

[38] Wang Yang , Ding BO ,Li Su Tong,"TS-YOLO:An efficient YOLO Network for Multi-scale Object Detection",IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC),2022.

[39] Xilin Zhang,"Traffic Sign Detection Based on YOLO v3",IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA),2023.

[40] Daniel Padilla Carrasco, Hatem A.Rashwan, Miguel Angel Gracia, Domenec Puig,"T-YOLO: Tiny Vehicle Detection Based on YOLO and Multi-Scale Convolutional Neural Networks",IEEE Access,2021.

[41] Yen-Sok Poon, Ching-Yun Kao, Yen-Kai Wang, Chih-Chin Hsiao,Ming-Yu Hung,Yu-Ching Wang,Chih-Peng Fan"Driver Distracted Behavior Detection Technology with YOLO-Based Deep Learning Networks", IEEE International Symposium on Product Compliance Engineering - Asia (ISPCE-ASIA) ,2021.

[42] Tian-Hao Wu, Tong-Wen Wang,, Ya-Qi Liu,"Real-Time Vehicle and Distance Detection Based on Improved Yolo v5 Network",3rd World Symposium on Artificial Intelligence,2021.

[43] Sushil Kumar,CRS kumar,"Deep Learning based Target detection and Recognition using YOLO V5 algorithms from UAVs surveillance feeds",2023 International Conference for Advancement in Technology (ICONAT),2023.

[44] Anand Upadhyay,Bhavesh Sutrave,Abhishek Singh,"Real time seatbelt detection using YOLO deep learning model",IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS),2023.

[45] Rakesh Chandra Joshi,Saumya Yadav,Malay Kishore Dutta,"YOLO-v3 Based Currency Detection and Recognition System for Visually Impaired Persons",International Conference on Contemporary Computing and Applications (IC3A),2020.

[46] Wesley Lin,"YOLO-Green: A Real-Time Classification and Object Detection Model Optimized for Waste Management",IEEE International Conference on Big Data (Big Data),2021.

[47] Yongtian Ma ,Jiaxiang Zhao,Jianjun Fang,Qiushi Zhang,"Research on the Application of YOLO v3 in Railway Intruding Objects Recognition", IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA), 2022.

[48] Rong Han,Xiaohong Liu,Ting Chen1,"YOLO-SG: Salience-Guided Detection of small objects in Medical images",IEEE International Conference on Image Processing (ICIP),2022.

[49] Jiaqi Zhang,Xunlei Chen,Yingling Li,Tianxiang Chen,Liqiang Mou ,"Pedestrian detection algorithm based on improved Yolo v3 ",IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS),2021.

[50] Median Hardiv Nugraha,Dina Chahyati,"Tourism Object Detection Around Monumen Nasional (Monas) Using YOLO and RetinaNet",IEEE Xplore,2020.

[51] Liu Sheng ,Liu Liwei ,Shang Fang ,Wang Qiang ,Ao Jin ,Li Dandan ,Yu Xiang ,Pei Jiuxiang,"Research and Implementation of Birds and Floating Objects Target Detection Technology in Transmission Lines", 10th Joint International Information Technology and Artificial Intelligence Conference(ITAIC),2022.

[52] Abdou Ambarka,Tahirou Djara,Abdou-Aziz Sobabe,Horace Fayomi,"Prediction of malaria plasmodium stage and type through object detection",5th International Conference on Bio-engineering fro Smart Technologies(BioSMART),2023.

[53] Zillur Rahman, Amit Mazumder Ami, Muhammad Ahsan Ullah,"A Real-Time Wrong-Way Vehicle Detection Based on YOLO and Centroid Tracking",IEEE Region 10 Symposium (TENSYMP),2020.

[54] Li Yajing, Dai Zhongjian,"Abnormal Behavior Detection in Crowd Scene Using YOLO and Conv-AE",3rd Chinese Control and Decision Conference(CCDC),2021.

[55] Ansh Sharma,Rashmi Gupta,"Efficient Detection of Small and Complex Objects for Autonomous Driving Using Deep Learning",IEEE International Conference on Communication System, Computing and IT Applications (CSCITA 2023),2023.

[56] Kanyifeechukwu Jane Oguine,Ozioma Collins Oguine,Hashim Ibrahim Bisallah,"YOLO v3: Visual and Real-Time Object Detection Model for Smart Surveillance Systems(3s)",5th Information Technology for Education and Development (ITED),2022.

[57] Sarah Hraybi, Mostafa Rizk,"Examining YOLO for real-time face-mask detection",IEEE Xplore,2021.

[58] Ning Wang,Meng Joo Er,Jie Chen,Jian Guo Wu,"Marine Object Detection Based on Improved YOLOv5",The 5th International Conference on Intelligent Autonomous Systems,2022.

[59] Ms.Swati B. Patil,Mr. Jay Chandrakant Shimpi,Mrs.Archana Girish Tanawade,Mrs.Pranali Gajanan Chavan,Mrs.Vrushali Shrimant Tandulkar,"Autonomous Object Detection and Counting using Edge Detection and Image Processing Algorithms",7th International Conference on Trends in Electronics and Informatics (ICOEI 2023),2023

[60] Zainal Rasyid Mahayuddin,A F M Saifuddin Saif,"Edge Feature based Moving Object Detection Using Aerial Images: A Comparative Study",6th ICCED International Conference on Computing, Engineering and Design,2020

[61] Zipeng Deng, Zongyong Cui, Zongjie Cao,"Super Resolution Detection Method of MOving Object Based on Optical Image Fusion with MMW Radar, 2022 IEEE International Geoscience and Remote Sensing Symposium IGARSS,2022

[62] Manisha Vashisht,Brijesh Kumar,"A Survey Paper on Object Detection Methods in Image Processing",*,2020

[63] Omer Ozdil,Yunus Emre Esin,Safak Ozturk,"An Improved Approach for Small Object Detection in Hyperspectral Images",9th International Conference on Electrical and Electronics Engineering,2022

[64] Bhavatarini N, Akash B N, A Renard Avinash, Akshay H M,"Object Detection and Classification of Hyperspectral Images Using K-NN",Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT),2023

[65] Ahmad Mansour,Wessam M Hussein,Ehab Said ,"Small Objects Detection in Satellite Images Using Deep Learning",IEEE Ninth International Conference on Intelligent Computing and Information Systems (ICICIS),2019

[66] Syed Aley Fatima,Ashwani Kumar,Ajay Pratap,Syed Saba Raoof,"Object Recognition and Detection in Remote Sensing Images: A Comparative Study",International Conference on Artificial Intelligence and Signal Processing (AISP),2020

[67] Merve Yildirim, Ozgur Karaduman,Hasan Kurum,"Real-Time Image and Video Processing Applications Using Raspberry Pi",IEEE 1st Industrial Electronics Society Annual On-Line Conference (ONCON),2022

[68] Ayman Beghdadi, Malik Mallem Lotfi Beji, "Benchmark Performance Of Object Detection Under Image Distortions In An Uncontrolled Environment ", 2022 IEEE International Conference on Image Processing (ICIP), 2022

[69] Mangalraj,Akankshya Mohanty,Sakshi Singh,"Salient Object Detection Using Water Flow Approach and Image Boundary Contrast Map,"International Conference on Computing, Communication, and Intelligent Systems (ICCCIS),2021

[70] Mehmet Bilge Han Tas, Muhammed Coşkun Irmak,Sedat Turan,Abdulsamet Haşıloğlu,"Real-Time Puddle Detection Using Convolutional Neural Networks with Unmanned Aerial Vehicles",6th International Conference on Computer Science and Engineering (UBMK)2021

ISSN 2394 - 7780

[71] Keisuke Maesako,Liang Zhang,"AVIS: An Innovative Image Preprocessing Method for Object Detection of Aerial Images",IEEE Wireless Communications and Networking Conference (WCNC),2022

[72] Jianjun Ni, Zubair Khan, Shihao Wang, Kang Wang and Syed Kamran Haider, "Automatic Detection and Counting of Circular Shaped Overlapped Objects Using Circular Hough Transform and Contour Detection", 2016 12th World Congress on Intelligent Control and Automation (WCICA) June 12-15, 2016, Guilin, China.

[73] Byeongho Heo,Kimin Yun,Jin Young Choi,"Appearance and motion based deep learning architecture for moving object detection in moving camera",IEEE International Conference on Image Processing (ICIP),2017

[74] Xianru Liu,Zixing Cai,"Advanced obstacles detection and tracking by fusing millimeter wave radar and image sensor data",International Conference on Control, Automation and Systems (ICCAS),2010

[75] Xiaoshuai Song,Yu Du,"Obstacle tracking based on millimeter wave radar",3rd International Conference on Systems and Informatics (ICSAI),2016

[76] Bing Tian,Liang Li,Yansheng Qu,"Video Object Detection for Tractability with Deep Learning Method",Fifth International Conference on Advanced Cloud and Big Data (CBD),2017

[77] Nandhini T J, K Thinakaran, "SIFT algorithm-based Object detection and tracking in the video image", 2023 Fifth International Conference on Electrical, Computer and Communication Technologies (ICECCT).

[78] Guang-Yi Chen, Wen-Fang Xie, "Invariant Pattern Recognition using Ring-protection and Dual-Tree Complex Wavelets", Proceedings of the 2011 International Conference on Wavelet Analysis and Pattern Recognition, Guilin, 10-13 July, 2011.

[79] Konstantinos Makantasis, Konstantinos Karantzalos, Anastasios Doulamis, Nikolaos Doulamis, "Deep Supervised Learning for Hyperspectral Data Classification through Convolutional Neural Networks", 978-1-4799-7929-5/15/$31.00 ©2015 IEEE

[80] Dumitru Erhan, Christian Szegedy, Alexander Toshev, Dragomir Anguelov, "Scalable Object Detection using Deep Neural Networks", 2014 IEEE Conference on Computer Vision and Pattern Recognition.

[81] Xinghao Ding, Xinxin Wang, Quan Xiao, "Color Image Enhancement with a Human Visual

[82] System Based Adaptive Filter", 978-1-4244-5555-3/10/$26.00 ©2010 IEEE. A. Kourgli and Y. Oukil, "Edge-Enhancing of Color Segmented Images," 2012 Eighth International Conference on Signal Image Technology and Internet Based Systems, 2012.

[83] David Anglada-Rotger, Ferran Marques, Montse Pardas, "Color Deconvolution Applied To Domain Adaptation In Her2 Histopathological Images ", 2023 IEEE International Conference on Acoustics, Speech, and Signal Processing Workshops, 2023

ISSN 2394 - 7780

ANALYSING THE PROGRESS MADE IN SENTIMENT ANALYSIS (SA), SPECIFICALLY IN THE CONTEXT OF SANSKRIT LITERATURE, INCLUDING THE PROBLEMS FACED AND RECOMMENDED SOLUTIONS

Akanksha Singh[1] and Dr. Ajay Parikh[2]
[1, 2]Department of Computer Science Gujarat Vidyapith Ahmedabad, India

ABSTRACT
Sanskrit was used to write the Valmiki Ramayana and Mahabharata. This paper reviews Indian language Sentiment Analysis (SA) literature, including Sanskrit literary works. Sanskrit literature in SA, its historical evolution, and Indian SA resources were examined in a thorough literature study. The research also highlights the challenges of sentiment analysis in Indian languages with limited resources. It suggests resolving these limits to improve sentiment analysis algorithms. The Ramayana's concepts should be examined to show the emotional differences and parallels between these two works of literature. This research may illuminate the emotional impact of great literature on current readers. Findings suggested that more work needs to be done in the field of Sanskrit literature with the improvised methods of sentiment analysis.

Keywords: Machine Learning, Valmiki Ramayana, Sanskrit Literature, Sentiment Analysis (SA)

I. INTRODUCTION (*HEADING 1*)

The Valmiki Ramayana is a mystically significant piece of Sanskrit literature from ancient India. This sacred literature contains Dharma's ethical and moral principles. Lord Rama and other individuals in this tale demonstrate these lessons. Millions of Hindus and people of other religions use the texts given in this literature as a spiritual guide to morality and to lead a successful path in life. Epic poetry, deep subject exploration, and rich character development make the Ramayana a masterpiece of literature and culture. It has influenced many Indian and Southeast Asian literary, artistic, choreographic, and musical works. Research is essential to understanding and preserving this literary and cultural heritage [1].

The Ramayana's understanding of ancient India's civilization, history, and society makes it historical. It discusses the social, administrative, and cultural elements of its era. By studying the epic, academics may rebuild ancient Indian society. The Valmiki Ramayana contains morality. Scholars might study the characters' ethical difficulties and find timeless lessons for modern society [2].

The Ramayana has been interpreted and adapted many times to suit different cultures. Research enables the study of adaptations, interpretations, and their effects on Indian and worldwide cultures. A noteworthy linguistic object is the Ramayana. Due to its complex verses and grammar, Sanskrit language, poetry, and literature provide study advantages. Comparative religion studies examine the Ramayana and other religious texts to see how Indian religion developed and interacted. Some experts have undertaken archaeological and geographical research to identify Ramayana places. This study investigates the narrative's historical accuracy. The Ramayana shaped Indian culture and patriotism. The epic has symbolised cultural pride and promoted national identity. The epic and Indian nationalism are studied in this context. The Ramayana influences Southeast Asian cultures outside India. This discipline studies how the epic affects local culture, art, and beliefs [3].

Need of Sentiment Analysis (SA) in Sanskrit Literature

Conducting research on SA applied to ancient writings such as the Valmiki Ramayana might provide useful insights and fulfil many significant objectives, as given below:

Cultural and Historical Understanding: Analysing the sentiments expressed in ancient writings may provide academics and researchers with a more profound comprehension of the cultural and emotional milieu during the period in which the work was composed.

Feelings may reveal the story's emotional aspects and historical and cultural connections. Researchers found emotional patterns and character development in the Valmiki Ramayana. The Valmiki Ramayana is an epic ethical and philosophical guide.

SA may be used in educational environments to facilitate students' interaction with and enhance their comprehension of the affective aspects of the written material.

Analysing the thoughts expressed in writings such as the Valmiki Ramayana may significantly aid in the preservation and archiving of cultural heritage.

Sentiment research may reveal the way certain segments of the epic provoke emotional reactions from readers or listeners.

Interdisciplinary research involves collaboration among professionals in fields such as SA, linguistics, literature, and cultural studies. This collaboration may result in valuable research that connects technology with the humanities.

The use of SA methods and methodologies in vast collections of ancient writings enables comprehensive quantitative evaluations, facilitating the identification of patterns and trends in emotional content.

In general, the use of SA in literature such as the Valmiki Ramayana may provide novel insights into the tale, facilitating a more thorough comprehension of the emotions, characters, and cultural backdrop depicted in the book.

This study has the potential to enhance the area of digital humanities and make valuable contributions to the preservation and understanding of historic cultural and literary artefacts.

Lacking resources Language-specific terminology is necessary for indigenous language data. This study offers annotated datasets, linguistic and lexical resources for pre-processing, and approaches for sentiment analysis in Indian languages. The paper critically examined studies on South Asian languages, with particular emphasis on research conducted on texts written in the Sanskrit language.

A comprehensive literature review has been conducted to investigate the several existing SA approaches or methods for Indian languages, with a greater focus on Sanskrit, utilising the resources that are already accessible or have been produced.

II. Related Works: A Literature Review in Indian Languages

The present work presents a comprehensive investigation of SA in the context of Indian languages. This paper examines the present state of SA in Indian languages, the historical development of SA in Indian languages, and the existing resources for SA in Indian languages. Additionally, it underscores the difficulties encountered in doing SA for Indian languages that lack adequate linguistic resources and proposes the need to tackle these constraints to enhance the effectiveness of SA algorithms. Nevertheless, it is imperative to integrate contemporary breakthroughs in the fields of SA and machine learning [4].

The paper reviews Indian regional language SA approaches, problems, and trends. A text's emotions are categorised as good, negative, or neutral via SA. Many businesses, including banking, advertising, marketing, and hospitality, use it. Most research focuses on global languages like English, although SA in local languages is growing [5].

Some experts also looked back at recent events in South Asia. In this study, they looked at about 31 SA papers that were written in Indian languages like Tamil, Malayalam, Telugu, Hindi, and Bengali. A list of corpora and NLP tools for different Indian languages was also given. Sentiment labelling methods like lexicon-based, mixed, and machine-learning techniques are also used. In machine learning, types of dictionaries like SentiWordNet, WordNet, domain-specific texts, and Stop words are used, along with SVM, NB, and Decision Tree. Because so many Indian languages haven't been fully studied yet, these languages should be considered in future work on SA. They also concluded that Marathi is one of the languages with the fewest resources for making things and running SA. They didn't say much about the problems and limitations of SA in the Indian diaspora, concerning our ancient languages like Sanskrit [6].

A review on multilingual opinion mining is also done for Indian Indigenous Languages. They discussed that there hasn't been much study done on SA in native languages for larger datasets. Also, they analysed that Deep Learning Algorithms are Used Less, Lack of corpus, absence of SWNs and WordNet, absence of Code-Mix Languages, and Less Progress on the SA at the Aspect Level [7].

The survey papers related to SA in Indian Languages are available in the public domain. However, there is a need to comprehend the work done in the field of Sanskrit Literature.

III. LITERATURE REVIEW IN

Researchers have conducted studies on Sentiment Analysis (SA) in Indian Literature. They have specifically focused on analysing the semantic and emotional features of selected translations of the Bhagavad Gita. This analysis was done using a linguistic framework called BERT [8]. Although advancements in deep learning language models and sentiment analysis (SA) may provide some improvements in translating the Bhagavad

Gita, it is crucial to approach the analysis of sacred texts with an unbiased perspective that incorporates human expertise and understanding.

- Sentiment Analysis (SA) in Sanskrit Literature

The following are a few techniques and strategies for Sanskrit SA:

Supervised learning algorithm
Work in Sanskrit Text analytics is done to predict the sentiment of Valmiki Ramayana. In this paper, the BiLSTM model gives better results compared with other models like BERT. Also, they achieved 87.50% and 92.83% accuracy in machine translation and sentiment classification, respectively [9]. However, aspect-based SA has the potential to give better results if used in the present framework. In addition, this comparison of results with the labelled data set can also help to achieve more accuracy.

Rule-Based Methods:
Lexicon-Based Methods: Creating Sanskrit sentiment lexicons that include word sentiment polarity ratings and using them to assess the sentiment of texts. Building a thorough lexicon for Sanskrit, however, may be difficult [10], [11].

Machine Learning Methods:
1) Feature engineering is the process of taking important characteristics, including part-of-speech tags, syntactic features, and word embeddings, out of Sanskrit text and feeding them into machine learning models [12].
2) Supervised learning refers to the process of training machine learning models, like decision trees, recurrent neural networks (RNNs), and transformers, utilising tagged Sanskrit text data to make predictions about sentiment. This approach is often referred to as supervised learning. This research examines Bidirectional Encoder Representations from Transformers (BERT), A Lite BERT (ALBERT), and Robustly Optimised BERT (RoBERTa) as language models specifically designed for the Sanskrit language. The models underwent training using an extensive corpus of Devanagari Sanskrit. The characteristics derived from these models were used to acquire a concise summary of a Sanskrit text. The writers published Sanskrit Devanagari literature [13].

Semantic Analysis:
Semantic role labelling involves analysing word and phrase functions in sentences to infer their meanings and connections [14].

1) Topic modelling involves identifying topics and relating them to emotions in Sanskrit literature. This helps capture nuances of feeling in some subjects [15].

Contextual Analysis:
1) Dependency Parsing: Analysing Sanskrit phrases' grammar to understand word relationships and meaning [16].
2) Co-reference resolution: Identifying concept or entity references in text and establishing their attitude [17].

Cultural & Historical contexts, along with Human Expertise:
To comprehend a text's emotions, it is important to consider its cultural and historical context, as well as human expertise. The author, place, and cultural references may be included. Scholars are studying Valmiki Ramayana's music, culture, and history [18].

Cross-lingual Models:
Cross-lingual Models from Hindi and other Indo-Aryan languages may be used for Sanskrit due to linguistic similarities [19].

Data Augmentation:
To improve model performance, consider using data augmentation approaches like translation, crowdsourcing, or synthetic data to complement limited Sanskrit sentiment data [20].

IV. Challenges in Sanskrit Text

Sanskrit literature in SA struggles with a lack of annotated data. Given the necessity for Sanskrit language and SA experts, building a large dataset with sentiment labels for Sanskrit literature is difficult. OCR was used for research [21]. Consider the difficulty of finding annotated data to determine whether a Ramayana statement is positive, negative, or neutral.

 ISSN 2394 - 7780

Sanskrit is known for its complex syntax and large vocabulary. The English language has many synonyms and complex words, making sentiment-bearing words and phrases difficult to identify and classify [22]. For instance, the compound word “बुद्धिमान्नीतिमान्वाग्मी” is difficult to analyse owing to its many words and intonation It might be difficult to classify and determine the emotional tone of the components.

Sanskrit texts use context and other factors to convey meaning. Words and phrases may have different meanings based on circumstances. Understanding contextual elements and cultural variations in the text is necessary to accurately determine sentiment [23]. For instance, In the shloka

“सर्व एव तु तस्येष्टा श्चत्वारः पुरुषर्षभाः।

स्वशरीराद्विनिर्वृत्ताश्चत्वार इव बाहवः।।2.1.5।।”

author wants to convey: Dasaratha saw his four sons as four separate parts of himself, according to Valmiki. He loved everyone equally.

According to word meaning, Dasaratha, a bull among men, adored his four sons like his arms.

सर्व एव तु तस्येष्टा श्चत्वारः पुरुषर्षभाः।

स्वशरीराद्विनिर्वृत्ताश्चत्वार इव बाहवः।।2.1.5।।

चत्वार: four, पुरुषर्षभा: bull among men, सर्वे एव तु all of them, तस्य his, स्वशरीरात् from his body, निर्वृत्ता: originated, चत्वार: four, बाहव: इव just as arms, इष्टा: dear

Dasaratha, a bull among men, loved all his four sons equally just as the arms of his own body.

Fig. 5. Valmiki Ramayana Sholka with an explanation on a given website (Source: https://www.valmiki.iitk.ac.in)

Sanskrit literature includes religious texts, epics, poetry, philosophy, and more. A SA model that can handle varied genres' expressions and feelings is difficult to create [24]. Researchers often struggle with negation. In Sanskrit, negation constructions may flip emotions, as shown in the shloka “नचानृतकथो विद्वान् वृद्धानां प्रतिपूजकः। अनुरक्तः प्रजाभिश्च प्रजाश्चाप्यनुरञ्जते।।2.1.14।।”. Sentiment classification requires precise component analysis.

Sanskrit literature is deeply rooted in Indian culture and history. The texts may be associated with cultural references and historical events, making them foreign to non-culturalists [25]. Understanding the cultural and intellectual context of the Bhagavad Gita or Upanishads may help comprehend its feelings.

Sanskrit texts can combine many emotions in one sentence. SA algorithms must be able to gather and differentiate several sentiments [26]. For example,

दृष्ट्वा तु विदितम् शीतम् पुष्पिताम् माल्य मालिनीम् |

तस्या अनुगता मृदया हनुमान् अपवादयत् || ४-२४-१५ ||

ताम् दृष्ट्वा तु अपि अत्यर्थम् माल्य आवृताम् बली बलौ |

सर्व अर्थ वृत्ति दशनौ बाष्प आकुलम् इव उपजयत् || ४-२४-१६ ||

न सिता अपि अथ ताम् दृष्ट्वा हनूमान् अभ्य अपद्यते |

रावणेन अपि अत्यर्थम् वाचः कुपितो अयम् अवधीयते || ४-२४-१७ ||

In this shloka, Hanuman is depicted as experiencing a mix of emotions, including caution, sadness, and indignation, as he encounters Sita's attire and flower garlands in Lanka while searching for her. These shlokas depict a complicated emotional environment in Ramayana's Sundar Kand [27].

Diverse eras of Sanskrit literature have had diverse syntax, vocabulary, and feelings. These historical changes must be included in models [28]. For instance, "पुरुष" may indicate "consciousness", "self", "spirit" or "person" Situations substantially impact emotion detection.

ISSN 2394 - 7780

Encoding data requires digitizing Sanskrit text and parsing, tokenizing, and encoding [29]. Modern computers don't identify several Sanskrit symbols and diacritics, making this procedure harder [30]. English and Sanskrit literature employ commas and full stops differently. As given in shloka,

तपःस्वाध्यायनिरतं तपस्वी वाग्विदां वरम् |

नारदं परिपप्रच्छ वाल्मीकिर्मुनिपुङ्गवम् || १||

The availability of language processing tools, libraries, and resources for Sanskrit is somewhat restricted when compared to contemporary languages. The issue hinders Sanskrit SA-specific NLP models and approaches [31].

Due to linguistic and contextual differences, SA models trained in modern languages may perform poorly in Sanskrit literature [32].

Proposed Method

The aspect-based SA of Indian literature like "Valmiki Ramayana" involves identifying and examining various elements or concerns in the book, and then studying the feelings associated with each component. A suggested sequential strategy for completing this activity is below

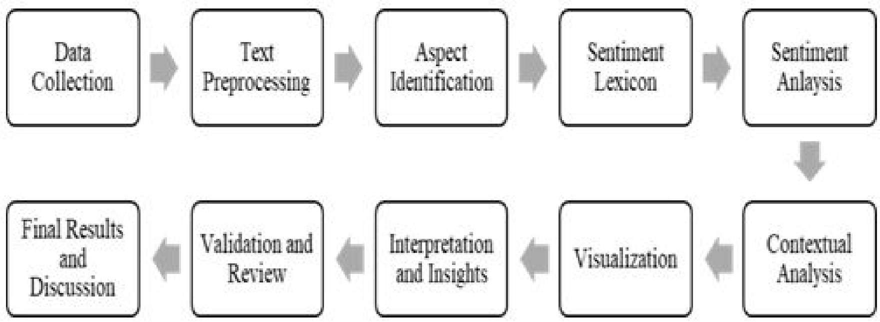


Fig. 6. Proposed method for Aspect Based Sentiment Analysis (ABSA) for Sanskrit Literature

- **Text Preprocessing:** Obtain digital "Valmiki Ramayana" text. Investigating the text may need digitization or electronic copies. Text preprocessing involves sentence and word breakdown into segments. Removing irrelevant data is done in this step.
- **Aspect Identification:** Recognize certain features or topics in the text for SA analysis. The "Ramayana" includes characters, themes, places, and events. For instance, "Rama", "Sita", "Hanuman", "Lanka", "Dharma" etc.
- **Sentiment Lexicon:** Create or acquire a Sentiment Lexicon with ratings for words or phrases. This lexicon classifies opinions and words as positive, negative, or neutral to link them. For the "Valmiki Ramayana," one may use pre-existing or bespoke lexicons.
- **Sentiment Analysis:** Estimate sentiment for each element in step 2 by associating sentiment scores to corresponding words or phrases. Machine learning models, sentiment scoring, or sentiment lexicon-based analysis may determine each constituent's sentiment polarity (positive, negative, neutral).
- **Contextual Analysis:** Assess emotional expression in diverse contexts. Character emotions, narrative tone, and cultural and moral standards are integral parts of "Valmiki Ramayana" with a variety of feelings and emotions.
- **Data Visualization:** Create visual representations of SA results. Sentiment heatmaps, bar charts, and word clouds may effectively represent text sentiment.
- **Analysis and Understanding:** Analyse SA results to comprehend the emotion conveyed in the "Valmiki Ramayana" via numerous components. Analyse the epic's emotional milieu, characters' emotional development, and morality.
- **Validation and Results:** Verify results and analysis for accuracy and relevance. To improve accuracy, consult Indian literature or SA experts.

V. CONCLUSION

SA improves our understanding of the Valmiki Ramayana in various ways. It allows researchers to discern and value the intricate emotions, intricate character development, and profound storytelling found in the Ramayana. SA uncovers the cultural and ethical aspects of the epic, providing an understanding of the moral conflicts

ISSN 2394 - 7780

experienced by its protagonists and the fundamental principles of dharma. Its fosters cross-cultural comprehension by emphasising how emotions depicted in the Ramayana have surpassed cultural limitations and had an impact on art, literature, and values across South and Southeast Asia. Research in this field promotes cooperation among specialists in literature, linguistics, computer science, and cultural studies.

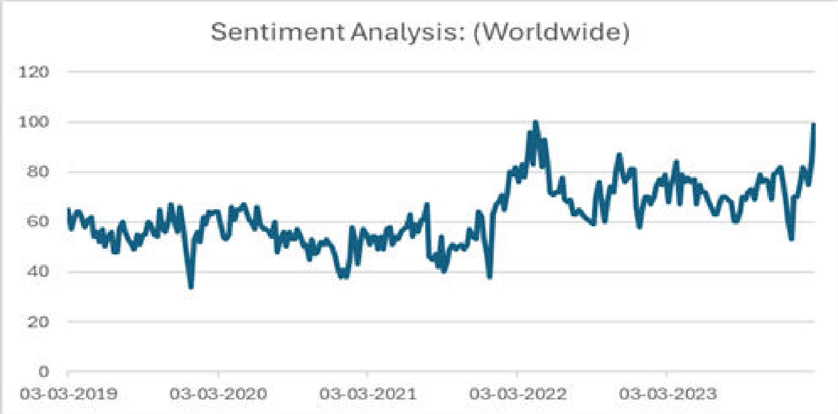


Fig. 7. SA Google Trends Data

Also, according to Google Trends SA, this is a trending topic. This study leads to the conclusion that the Indo-Aryan language family has been the subject of the majority of research, followed by the Dravidian language family, and so on. Also, NLP Deep Learning Methods are gaining popularity in the SA domain (approximately 90% in this survey). As Sanskrit Texts are ancient among Indo-Aryan Families, various efforts are made to use their data by applying various NLP methods to get desired outcomes. However, the NLP methods were using transliterated text for the same.

There is a pressing need for an innovative strategy, one that may try to employ the Sanskrit language directly to achieve the desired result. In addition, using SentiWordnet for Sanskrit Text is strongly suggested as a need. The field of research that is concerned with Sanskrit SA comprises several different fields, including resource building, multilingual SA, aspect-based SA, negation handling, multimodal SA, ethical implications, real-world applications, and cooperation with linguists.

VI. FUTURE SCOPE

Additional research and discussion should be conducted to explore the wider ramifications of the study and how SA of the "Valmiki Ramayana" might enhance comprehension of this epic and its influence on readers.

Several academics have conducted comparative sentiment analysis on different versions or translations of these texts to understand variations in emotional expression and interpretation. The ancient Sanskrit Literature has been put adjacent to illustrate their contrasting emotional states and similarities. Sentiment analysis (SA) has been used to inspect the emotional reactions of bibliophiles and scholars towards texts in book reviews, comments, and debates. The texts of Sanskrit Literature have undergone analysis utilising advanced sentiment analysis methods like emotion detection to identify and categorise their emotions. Contextual analysis has been used to comprehend the affective and circumstantial elements of Sanskrit texts.

REFERENCES

[1] H. Pallathadka, L. K. Pallathadka, Pushparaj, and T. K. Devi, “Role of Ramayana in Transformation of the Personal and Professional Life of Indians: An Empirical Investigation Based on Age and Regions,” Integr. J. Res. Arts Humanities, vol. 2, no. 6, pp. 116–122, Nov. 2022, doi: 10.55544/ijrah.2.6.15.

[2] R. B. Nanjegowda and R. N. Munoli, “Rama—The Epitome of Indian Ethics: Relevance to Modern Mental Health,” Indian Journal of Private Psychiatry, vol. 15, no. 2, pp. 108–111, Dec. 2021, doi: 10.5005/jp-journals-10067-0093.

[3] R. D. Bajpai, “Ramayana: The Indian Epic and Its Relevance to Global IR,” International Relations.

[4] S. Rani and P. Kumar, “A journey of Indian languages over sentiment analysis: a systematic review,” Artif Intell Rev, vol. 52, no. 2, pp. 1415–1462, Aug. 2019, doi: 10.1007/s10462-018-9670-y.

[5] S. D. Kale, R. Prasad, G. P. Potdar, P. N. Mahalle, D. T. Mane, and G. D. Upadhye, “A Comprehensive Review of Sentiment Analysis on Indian Regional Languages: Techniques, Challenges, and Trends,” IJRITCC, vol. 11, no. 9s, pp. 93–110, Aug. 2023, doi: 10.17762/ijritcc.v11i9s.7401.

[6] M. B. Shelke and S. N. Deshmukh, “Recent Advances in Sentiment Analysis of Indian Languages,” International Journal of Future Generation Communication and Networking, vol. 13, no. 4, Art. no. 4, Oct. 2020, Accessed: Nov. 15, 2023. [Online]. Available: http://sersc.org/journals/index.php/IJFGCN/article/view/32962

[7] S. R. Shah and A. Kaushik, “Sentiment Analysis on Indian Indigenous Languages: A Review on Multilingual Opinion Mining,” MATHEMATICS & COMPUTER SCIENCE, preprint, Nov. 2019. doi: 10.20944/preprints201911.0338.v1.

[8] R. Chandra and V. Kulkarni, “Semantic and Sentiment Analysis of Selected Bhagavad Gita Translations Using BERT-Based Language Framework,” IEEE Access, vol. 10, pp. 21291–21315, 2022, doi: 10.1109/ACCESS.2022.3152266.

[9] P. Kumar, K. Pathania, and B. Raman, “Zero-shot learning based cross-lingual sentiment analysis for sanskrit text with insufficient labeled data,” Appl Intell, vol. 53, no. 9, pp. 10096–10113, May 2023, doi: 10.1007/s10489-022-04046-6.

[10] N. Bhadwal, P. Agrawal, and V. Madaan, “A Machine Translation System from Hindi to Sanskrit Language using Rule based Approach,” SCPE, vol. 21, no. 3, pp. 543–554, Aug. 2020, doi: 10.12694/scpe.v21i3.1783.

[11] N. Sethi, A. Dev, P. Bansal, D. K. Sharma, and D. Gupta, “A Pragmatic Analysis of Machine Translation Techniques for Preserving the Authenticity of the Sanskrit Language,” ACM Trans. Asian Low-Resour. Lang. Inf. Process., p. 3610582, Jul. 2023, doi: 10.1145/3610582.

[12] Sitender and S. Bawa, “Sanskrit to universal networking language EnConverter system based on deep learning and context-free grammar,” Multimedia Systems, vol. 28, no. 6, pp. 2105–2121, Dec. 2022, doi: 10.1007/s00530-020-00692-3.

[13] K. Bhatnagar, S. Lonka, J. Kunal, and M. R. M. G, “San-BERT: Extractive Summarization for Sanskrit Documents using BERT and its variants,” 2023, doi: 10.48550/ARXIV.2304.01894.

[14] A. Shukla, C. Bansal, S. Badhe, M. Ranjan, and R. Chandra, “An evaluation of Google Translate for Sanskrit to English translation via sentiment and semantic analysis.” arXiv, Feb. 27, 2023. Accessed: Nov. 15, 2023. [Online]. Available: http://arxiv.org/abs/2303.07201

[15] R. Chandra and M. Ranjan, “Artificial intelligence for topic modelling in Hindu philosophy: Mapping themes between the Upanishads and the Bhagavad Gita,” PLoS ONE, vol. 17, no. 9, p. e0273476, Sep. 2022, doi: 10.1371/journal.pone.0273476.

[16] J. Sandhan, A. Krishna, A. Gupta, L. Behera, and P. Goyal, “A Little Pretraining Goes a Long Way: A Case Study on Dependency Parsing Task for Low-resource Morphologically Rich Languages,” 2021, doi: 10.48550/ARXIV.2102.06551.

[17] S. Khosla and C. Rose, “Using Type Information to Improve Entity Coreference Resolution,” 2020, doi: 10.48550/ARXIV.2010.05738.

[18] Laxman Majhi and Śri Binod Bihari Rout, “The Musical Aspect in Vālmīki Rāmāyaṇa,” Apr. 2023, doi: 10.5281/ZENODO.7857277.

[19] G. Lample and A. Conneau, “Cross-lingual Language Model Pretraining.” arXiv, Jan. 22, 2019. Accessed: Nov. 15, 2023. [Online]. Available: http://arxiv.org/abs/1901.07291

[20] G. Arora, “iNLTK: Natural Language Toolkit for Indic Languages,” in Proceedings of Second Workshop for NLP Open Source Software (NLP-OSS), Online: Association for Computational Linguistics, 2020, pp. 66–71. doi: 10.18653/v1/2020.nlposs-1.10.

[21] A. Dwivedi, R. Saluja, and R. K. Sarvadevabhatla, “An OCR for Classical Indic Documents Containing Arbitrarily Long Words,” in 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Seattle, WA, USA: IEEE, Jun. 2020, pp. 2386–2393. doi: 10.1109/CVPRW50498.2020.00288.

[22] Zamorski and Jakub, “Sanskrit Grammar in Early Modern East Asia-a Study of Kiben’s Guidelines for Studying the Eight Cases of the Chinese Language,” 2019. Accessed: Nov. 15, 2023. [Online]. Available:

https://www.semanticscholar.org/paper/Sanskrit-Grammar-in-Early-Modern-East-Asia-a-Study-Zamorski-Jakub/e107f330e86460e1d4775c720b4200e3863ad217

[23] Y. Madhani et al., "Aksharantar: Open Indic-language Transliteration datasets and models for the Next Billion Users," 2022, doi: 10.48550/ARXIV.2205.03018.

[24] P. Barman, "Kushan Gaan: Retelling of the Ramayana," in Cultural Forms and Practices in Northeast India, K. C. Baral, Ed., in People, Cultures and Societies: Exploring and Documenting Diversities. , Singapore: Springer Nature Singapore, 2023, pp. 85–97. doi: 10.1007/978-981-19-9292-6_7.

[25] J. Sandhan et al., "Aesthetics of Sanskrit Poetry from the Perspective of Computational Linguistics: A Case Study Analysis on Siksastaka," 2023, doi: 10.48550/ARXIV.2308.07081.

[26] P. Banerjee, "The Modern, the Untimely, and the Planetary: 100 Years of Ranajit Guha," Critical Times, p. 10800321, Jun. 2023, doi: 10.1215/26410478-10800321.

[27] G. C. Jhala, The Vālmīki Rāmāyaṇa: Critical Edition, vol. V (Sundarakāṇḍa). 1966. Accessed: Nov. 15, 2023. [Online]. Available: http://archive.org/details/RmyaaCriticalEdition5EDGCJhala1966

[28] S. Booth and C. Mounsey, Eds., Reconsidering extinction in terms of the history of global bioethics. in Routledge advances in the history of bioethics. New York: Routledge, 2021.

[29] A. Krishna, A. Gupta, D. Garasangi, P. Satuluri, and P. Goyal, "Keep it Surprisingly Simple: A Simple First Order Graph Based Parsing Model for Joint Morphosyntactic Parsing in Sanskrit," in Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP), Online: Association for Computational Linguistics, 2020, pp. 4791–4797. doi: 10.18653/v1/2020.emnlp-main.388.

[30] P. Cherkashin, "Indra Proposal. Constitutional Version," Open Science Framework, preprint, Aug. 2023. doi: 10.31219/osf.io/y4ckt.

[31] J. Sandhan, A. Agarwal, L. Behera, T. Sandhan, and P. Goyal, "SanskritShala: A Neural Sanskrit NLP Toolkit with Web-Based Interface for Pedagogical and Annotation Purposes," 2023, doi: 10.48550/ARXIV.2302.09527.

[32] A. Petrocchi, "Medieval Literature in Comparative Perspective," Journal of Medieval Worlds, vol. 1, no. 2, pp. 57–76, Jun. 2019, doi: 10.1525/jmw.2019.120004.

A DEEP LEARNING APPROACH FOR COMPREHENSIVE MULTICLASS CLASSIFICATION OF BANANA LEAF DISEASES

Sivakannan Subramani[1], Ashwin S[2] and Vignesh M[3]
[1, 2,3]Department of Advanced Computing St. Joseph's University Bengaluru, India

ABSTRACT

Bananas are an important fruit in the global food market. Bananas are a healthy source which contains fibre and vitamins, and various other antioxidants. However, its in the context of production and export are having bad affects by the infection due to fungi, bacteria, and various other viruses. Hence, it is very important to detect the diseases as early as possible for proper precautions. Implementing an automated system can help detect the disease at the earliest. This paper projects a Deep Learning algorithm for the banana leaf classification of different diseases like cordana, pestalotiopsis, and Sigatoka. The algorithms used in this paper are MobileNetV2, VIT Transformer, AlexNet and InceptionV3, the highest accuracy was achieved in ViT Transformer with accuracy of 98%. This research donates to the field of agriculture and food security helping us to immediately identify the diseases and provide real-time information on effective measures to be taken at the earliest.

Keywords: Banana leaf classification, deep learning, Agriculture, food security, Disease classification.

I. INTRODUCTION

The cultivation of bananas has an extensive history spanning many centuries, with the promotion of their health benefits passed down from our ancestors to the contemporary era. In the present day, bananas are grown in over 150 countries, predominantly in tropical regions, encompassing Africa, India, North and South America, and China. The medical properties of bananas are used in special diets where they ease digestion, improve health of heart, diabetes management, weight control and quicker or efficient workout recovery. Bananas provide various vitamins and minerals Magnesium. Just like fruits, even banana leaves play a vital role in health and other use cases in the medical field. Banana leaf contains bioactive phytonutrients that help in healing wounds, healing ulcers, anti-cancer activity, enhancing digestion, anti-diarrhoeal activity, acting as an antioxidant, antibacterial and antifungal activity. There are also general uses for banana leaves like serving hot food due to its inexhaustibility and hard texture, food wrappers for dishes and fresh leaves that may be crushed with water to make juice.[1]

Worldwide production of bananas is about 164 million tons contributing over 18 percent of fruit production. Bananas in terms of export market by different countries are pegged at 13.8 Billion dollars with 20.07 million tonnes of trade out of which Grand Naine accounts for more than 90 percent of international banana trade. India currently is dominating the industry of production of bananas in the world and accounts for 36b per cent of the world's banana production.[2] The estimated banana production across the globe is 19 million tonnes and India produces 31.5 million tonnes of it. Despite being one of the largest producers it plays only a minuscule role in the international food market with a contribution of 2.33 lakh tonnes of bananas worth Rs. 740.32 crores during 2020-2021.

The adoption of deep learning technologies along with the area expansion in non-traditional banana growing regions has increased the overall production and the productivity of the banana crop manifold thus leading to a sharp increase in the exports to various other countries by keeping the food security into consideration and doubling the farmer's income. Therefore it is highly possible to identify new markets and explore market channels to make cultivation and trade sustainable amidst the competition from other commodities [4].

Also, India is a country with diverse agro-climatic conditions for producing a wide variety of agri products. Several agricultural products which are based out of India have Geographical Indications (GI tags). The Geographical Indication (GI) tag guarantees a certain level of quality and unique characteristics associated with the product's origin within a specified geographical area, region, or country. The GI-certified bananas in the country are Nanjangud Banana and Kamalapura Red Banana in Karnataka, Virupakshi and "Sirumalai Hill Banana" in Tamil Nadu, "Chengalikodan Nendran Banana" in Kerala, Jalgaon in Maharashtra, Mandoli at Goa which have been identified for creating brand image to the Indian origin varieties popular across the globe.

The strength of soil can also be identified with the help of disease in the banana plant. Further we can take necessary actions to improve the soil condition[9]. Banana cultivation once considered to be profitable and enhanced farmers' income manifold became a victim of irregular monsoon, loss of soil fertility, poor and age-old agricultural techniques, and the emergence of new diseases like cordana, pestalotiopsis, and Sigatoka and

 ISSN 2394 - 7780

the emergence of new insect pests like scaring beetle with new tropical race 4 will affect all the clones of banana including Cavendish Group.

Further, the low volume export of bananas is due to improper pre and post-harvesting techniques that have been carried out, non-adoption of GAP which includes the right choice of plants, planting method, bunch covering, growth regulator spray, non-ideal post-harvesting techniques, lack of proper storage facilities, outdated banana handling procedure etc. Due to mishandling of the produce nearly 25-30 percent is being wasted. This leads to an imbalance in the wholesale and retail price of spatial and temporal which affects the income of farmers also losing the market share in the global market.

Several researchers across the world have performed various experiments on automotive leaf disease classification using ML techniques [4,5] and DL methods.

Implementing an automated system can help detect the disease at the earliest. This paper portrays a DL algorithm for banana leaf classification of different diseases like cordana, pestalotiopsis, and Sigatoka. The algorithms used in this paper are mobileNetV2, VIT Transformer, AlexNet and InceptionV3, the highest accuracy was achieved in ViT Transformer with accuracy of 98%. This research contributes to the field of agriculture and food security helping us to immediately identify the diseases and provide real-time information on effective measures to be taken at the earliest.

II. RELATED WORKS

Jonalee et.al deals with classifying the banana leaves into two categories such as healthy leaf and disease leaf. It employed both Self-constructed CNN and Support Vector Machine classifier Machine Learning algorithms with an accuracy of 99.1% (training accuracy) and 92.8%(test accuracy)[3]. Deepthy Mathew et.al classifies three different types of leaf spot disease. The dataset contains three types of disease: Sigatoka, Deightoniella and Cordana leaf. This paper has used CNN and achieved an accuracy of 91.7% WITH backbone called DenseNet 121, which proved better than other models like Xception, mobileNet and Inception V3[4]. N. Bharathi et.al compares the different analyses and various classification models. The paper focuses on detecting illnesses in leaves including black spot, banana streak virus, Sigatoka disease and moko disease. The model used in this paper is CNN which has an accuracy of 91.78% [5]. Vidhya's et.al classifies and detects the healthy leaf and disease leaf using various ML techniques. In this paperwork, two common diseases of banana leaves, leaf spot and Sigatoka are identified using ML and DL algorithms. The ML algorithms used in this paper are KNN, SVM and Alexnet with an accuracy of 76.49%, 84.86% and 96.73% respectively [6]. M. Shyamala et.al worked on predicting the leaf diseases using CNN**.** This dataset contains diseases like Sigatoka, Cordana, Pestalotiopsis and health. This paper employed 8 Layered DCNN with proposed accuracy of 98.75%, Precision of 96.42%, Recall 98.75% and F1-Score 97.57% [7]. Vandana et.al using neural networks they have detected disease in both leaf and fruit of a banana plant. Also it focuses on the classification of diseases in bananas and fruit like Black Sigtoka, Freckle Leaf, Anthracnose and Freckle fruit. The Deep learning model that was used is ANN [8]. Dabalos et.al with the help of disease in the banana leaf, this paper identifies the macronutrient deficiency in the soil using ML technique with an accuracy of 91.64% [9].

III. Preliminary

The Deep Learning (DL) model is built with three algorithms such as MobileNet V2, VIT Transformer, Alexnet and Inception V3. The algorithms used in the Banana Leaf disease classification are mentioned in this section.

3.1Mobile Net V2

The MobileNet V2 architecture has 53 convolutional layers and 1 avgPool operation, resulting in approximately 350 billion floating-point operations (GFLOP) per second. The core components of MobileNet V2 are the Inverted Residual Block and Bottleneck Residual Block, each with distinct features. MobileNetV2 consists of two kinds of CNN netword. Each architectural construction component has a standardised design with three distinct layers: Depthwise Convolution, Convolution with Relu6, and Convolution without inclusion of linearity. Notably, MobileNet V2 is split into two Blocks, each with its own configuration and purpose. The bottleneck level in MobileNet V2 can be represented by either a stride 1 or stride 2 block, an inverted residual block, a bottleneck residual block, or both. Each Convolution layer in the design is defined by a set of parameters that go in the following order: Height and width of output, Output Channel, Height and Width of stride, Height and Width of padding. In summary, the 53 convolutional layers that make up MobileNet V2's architecture are unique, and an extra AvgPool operation produces roughly 350 GFLOP. The 1x1 convolution and 3x3 depthwise convolution make up most of the convolution layers.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

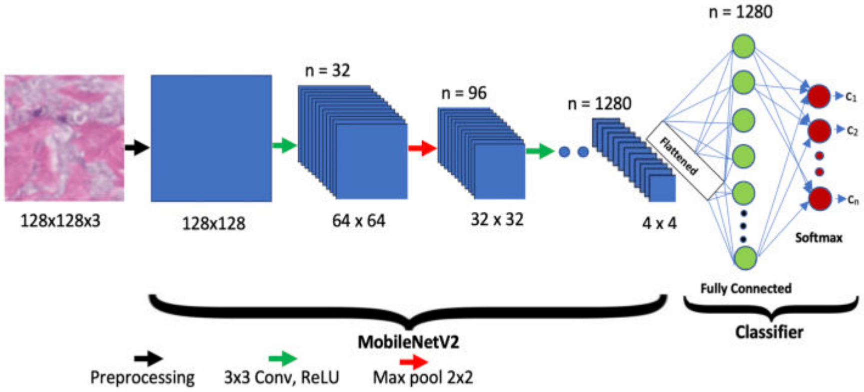


Fig.1. An illustration of MobileNet V2 architecture

3.2 VIT Transformer

An architecture for image analysis and processing called the Vision Transformer (VIT) uses a transformer-based methodology. The VIT model processes visual data using a transformer architecture as opposed to traditional convolutional neural networks. The core components of the VIT architecture are feedforward neural networks, a collection of linear transformations, and self-attentional mechanisms. Together, these parts extract and process characteristics from input image patches. In the VIT model, the image is first divided into fixed-size patches. The output patches are then extrapolated linearly to represent in lower dimension. In the next step the transformed patches are fed to the transformers. This information fed is inter communicated across different layers of transformers that carry forward this information. The VIT architecture enables the establishment of the relationship and features for every patch. The feature extraction and representation is improved by carrying out this process in several iterations using multiple layers of transformers. Hence the conventional methodologies of image processing are eliminated by the use of Vision Transformers (VIT). .It presents patch-based image processing and effectively uses feedforward neural networks, self-attention processes, and linear transformations to extract and improve information from image patches. The attention mechanisms and transformer layers of the model facilitate efficient interaction and integration of information across the patch embeddings, hence improving feature representation for ensuing image analysis tasks.

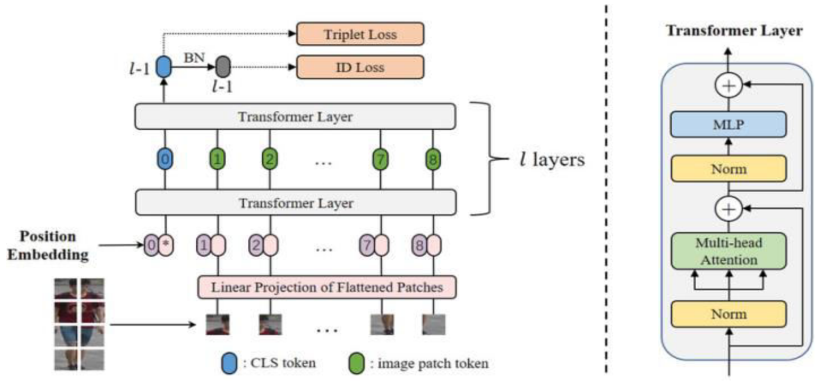


Fig.2 An Architecture of VIT architecture

3.3 AlexNet

The architecture of AlexNet has a unique structure made up of eight weighted layers, three fully connected layers and five convolutional layers. “ReLU” activation function is used after every layer, with the exception of the last layer, which uses softmax to produce outputs that span 1000 class labels. Dropout is used in the first two fully connected layers. Specifically, to maximise computational efficiency, the kernels of particular convolutional layers are selectively connected to the kernel maps in the layer before.

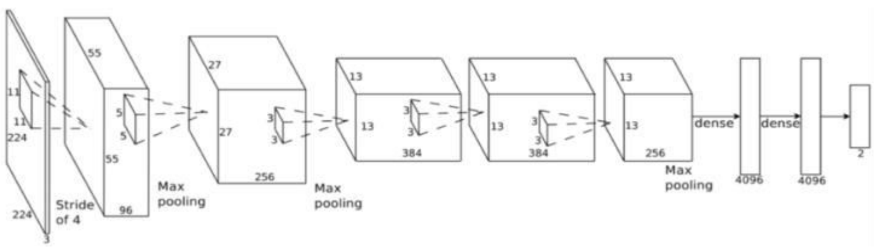


Fig.3. An Architecture of AlexNet architecture

 ISSN 2394 - 7780

3.4 Inception V3

As part of the Vision Inception architecture, the Inception V3 model suits are used in the field of image processing. It uses the Inception module, which deviates from conventional convolutional neural network architectures by judiciously combining different filter sizes within a single layer. The model can now capture the features at various scales thanks to this. Multiple Inception modules that combine 1x1, 3x3, and 5x5 convolutional filters with max-pooling operations make up the architecture of Inception V3. Effective use of features at different receptive fields is ensured by this fusion. In order to promote more stable training and improve gradient flow, intermediate stages of the model also include auxiliary classifiers .In order to improve the stability and efficacy of training the batch normalisation - a technique of Inception V3 model, is employed. Further this reduces the spatial dimensions and it produces a representation for classification.

High performance in feature extraction is ensured by the deployment of Inception model across multiple scales. The batch normalisation technique and the bottle neck layers strengthens the image processing task.

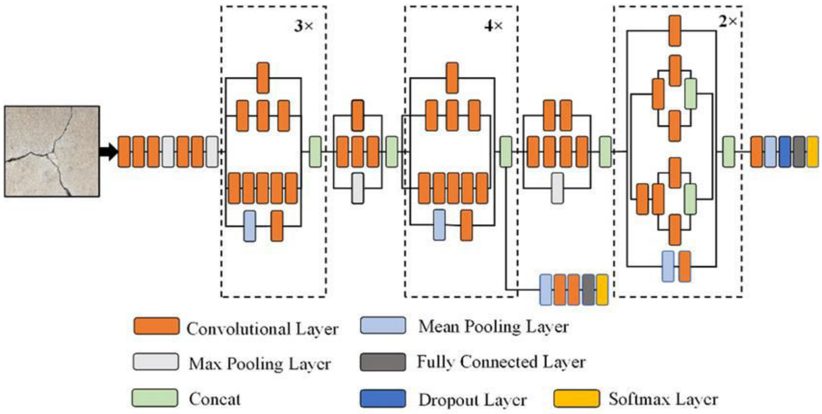


Fig.4. An Inception V3 architecture.

IV. Methodology

In this section we discuss the working and techniques. The working of methodology involves three steps: (1) Acquiring data, (2) Preprocessing data, and (3) Employing deep learning algorithms.

The data for this study was collected from various parts of Karnataka, Kerala and Tamil Nadu using a Canon 600D DSLR, an entry level DSLR with 18-megapixel sensor. The dataset contains four types of images like healthy, Pestalotiopsis, Cordana and Sigatoka. After augmentation the total number of images were 2279.

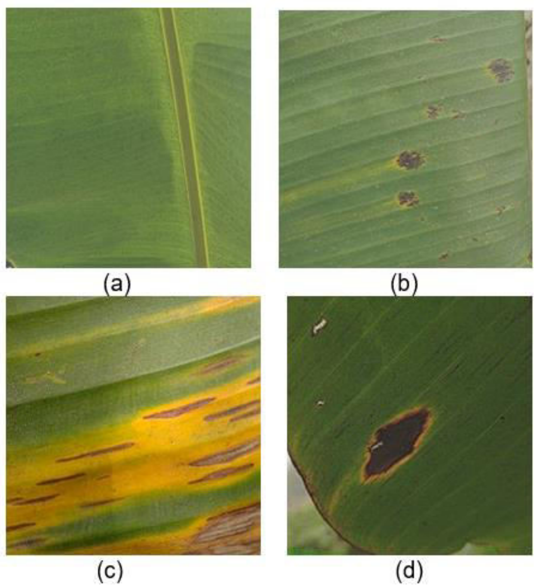


Fig. 5. (a) Healthy (b) Pestalotiopsis (c) Sigatoka (d) Cordana

The block diagram shows a sequence of steps, which include preprocessing the dataset and dividing it into subsets namely training set and testing sets. The DL models are meant to learn or trained on the training set, and their performance is assessed and validated on the test set.

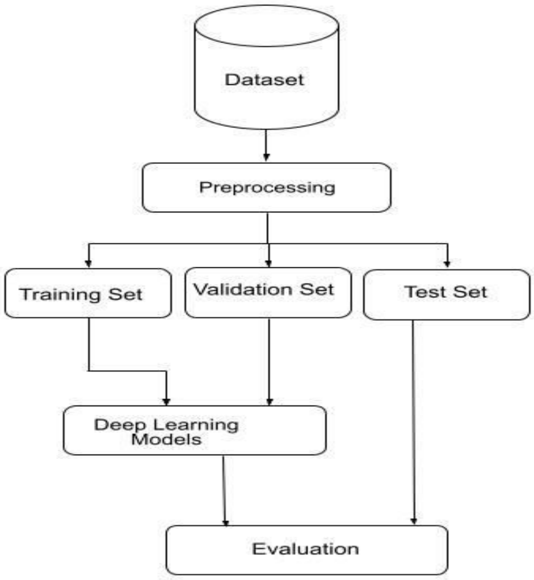


Fig.6. Block diagram for proposed model

Data preprocessing pipeline for this study is stratified partitioning the dataset into discrete units for training, validation, and testing." This crucial method makes sure that machine learning models that have been trained generalise well to new data. To maintain the distribution of these classes across each subset, the dataset—which consists of four classes representing three different leaf diseases—is meticulously stratified. Approximately 70% of the images are assigned to the training folder (four classes) with an emphasis on balanced representation, giving the models significant exposure to the underlying patterns in the data. For avoiding overfitting and enabling the adjustment of model hyperparameters, a 20% subset is set aside for validation. The remaining 10% of the dataset has been set aside for the test subset, which serves as an unobservable baseline to evaluate the models' overall performance. Augmentation of Images, a unique method to address data imbalances and add more diversity to our training dataset. However, we didn't use it on the test or validation sets—we only used it on the training set. Gaussian blur, horizontal flip, cropping, linear contrast adjustments, shear transformations, translations, and rotational changes are the augmentation techniques that are applied. These all reinforce the generalisation abilities of our deep learning model. When combined, they improve spatial invariance and noise resistance of the model's feature extraction. Adjusting the contrast makes an image more readable. A model can be made to adapt to different angles by rotating and shearing. Our model can more effectively adjust to real-world environments thanks to the modifications we made to the training procedure. After that, it can improve its performance and accuracy in classifying leaf illnesses.

Table 1. Dataset Details

Original Image Set		**Augmented Image Set**	
Classes	**No. of Images**	**Classes**	**No. of Images**
Cordana	162	Cordana	593
Healthy	129	Healthy	588
Pestalotiopsis	173	Pestalotiopsis	591
Sigatoka	473	Sigatoka	507

Table 2. Accuracy comparisons of the employed model

Model	**Precision Metric**	**Recall Metric**	**F1-Score**	**Accuracy**
MobileNetV2	0.85	0.87	0.86	0.87
AlexNet	0.83	0.81	0.81	0.81
Inception V3	0.98	0.98	0.98	0.98
VIT Transformer	0.98	0.98	0.98	0.98

This table compares the performance metrics of four models. Accuracy, Precision metric, Recall metric and F1-score are the measurements used. Both the “ViT Transformer” and “Inception V3” models performed significantly better overall when compared to the others. The values of metrics were all very close to 1. On the other hand, “MobileNetV2” did not perform that well in any category, especially with regard to its recall. In terms of performance “AlexNet” was just average when it came to this group of models.

The MobileNetV2 model was trained using a dataset containing 1467 images distributed across 4 classes, with 579 images designated for validation. The training process spanned 15 epochs, with each epoch consisting of 45 steps.In the initial epochs, the model exhibited an accuracy of around 63%, which gradually increased as the training progressed. The loss decreased from a starting value of 0.8960 to 0.0355 by the final epoch. The model's validation accuracy began at 31.77% but significantly improved over it. The trained model was evaluated on a test dataset containing 313 images from the same 4 classes, achieving a test accuracy of 77.32%. Generally the training process shows that the model can learn and update from the provided data leading to accuracy and decreasing of loss as the training progresses. The test accuracy of 77.32% indicates that the model can make predictions, on unrecognised data with a peak of 76.39%, during the final epoch.

The VIT Transformer model went through a training process that lasted for 5 epochs. The training dataset consisted of 1467 images divided into 4 classes. There was also a validation set with 579 images. During the epoch the VIT Transformer model showed an accuracy of 73.45%. The validation accuracy during this phase was more remarkable at 99.83% indicating its ability to learn quickly and adapt. As the subsequent epochs progressed the model's accuracy improved further. Reached 98.95% by the end of the fifth epoch. The training loss started at 0.6749. Significantly decreased to 0.0389 by the fifth epoch. The validation loss initially stood at 0.0242. Experienced an increase but remained consistently low which suggests that the model is resistant to overfitting.

When evaluated using a test dataset the VIT Transformer model showcased performance with an impressive test accuracy of 99.36%. This training process highlights how effectively the VIT Transformer can learn patterns in data. Its outstanding validation and test accuracies demonstrate its precision and practical applicability, across domains.

The AlexNet model was trained over a period of 10 epochs. During the training a dataset consisting of 1467 images spread across 4 classes was used while a separate test dataset of 313 images was employed for evaluation purposes. In the epoch the model showed an accuracy of 37.84% which suggested that it was still in the stages of learning. However as subsequent epochs progressed there was an improvement in accuracy. The accuracy gradually. Reached 76.59% by the end of the epoch. Additionally, there was also a reduction in loss percentage throughout the epochs starting from 1.2673 and decreasing to 0.5837 in the epoch. This decrease in loss demonstrates that the model became more effective at reducing prediction errors over time. Following completion of the training process an independent test dataset was used to evaluate the model’s performance which yielded a test accuracy rate of 84.98%.

The Inception V3 model has undergone two training stages each consisting of five epochs. The learning rate was re-adjusted to 0.0001 from the previous value of 0.001 after the first stage during the training process.

Phase 1 Training (Epochs 1-5, Learning Rate: 0.001). Completed five epochs. Throughout this phase the model's accuracy linearly improved, showing its ability to adapt and learn from the provided train data. In order to improve the performance of the model the learning rate was re adjusted to 0.0001 to have better convergence of the solution.

Phase 2 Training (Epochs 6-10, Learning Rate: 0.0001). In this phase epochs 6-10 were used. The accuracy was improved as a result of setting the learning rate value to 0.0001. The model was checked with a dedicated test dataset and resulted in an overall accuracy of 99.36%. The model was able to predict positively for the unseen data.

V. RESULTS & DISCUSSION

Compare to the existing paper which employed machine learning algorithms where Random Forest model resulted in highest accuracy of 91.64, our proposed paper achieved the accuracy of 98% by employing transformer model Inception V3 and ViT models [9].

Confusion matrix provides us the performance of four different DL models on a banana leaf disease classification task. The models are: MobileNet, Vit Transformer, AlexNet, Inception V3. The confusion matrix shows the number of cases for each distinct class that were predicted correctly and incorrectly by each model. For example, the MobileNet model correctly predicted 63 cases of the cordana class, but it also incorrectly

ISSN 2394 - 7780

predicted 14 cases of the pestalotiopsis class as cordana. Overall, the Inception V3 model has the accurate performance on this task, with an accuracy of 97%. It also has the most efficient performance for all four classes, with precision, recall, and F1-scores all above 94%.

MOBILENET V2

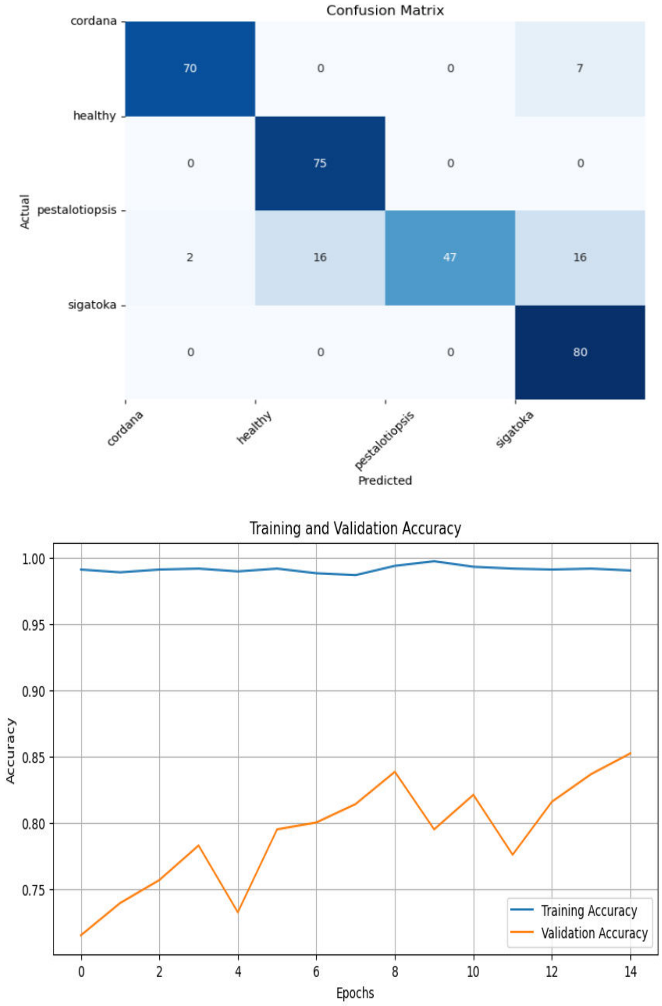
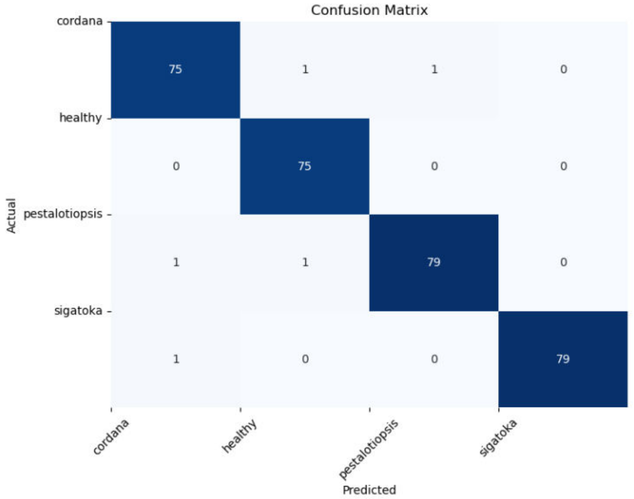


Fig.7. Confusion Matrix and Accuracy plot (MobileNetV2)

MobileNet V2 confusion matrix portrays how the model is having troubles when identifying classes like cordana where 70 images classified correctly, 7 classified as sigatoka, healthy class was classified properly all 75 images were true Positives, Pestalotiopsis images was underpredicted as 2 were classified as cordana, 16 as healthy and 16 as sigatoka, and lastly Sigatoka class was correctly classified.

About the Train/Validation plot its evident that the training accuracy across epochs stayed constant. Validation accuracy on the other hand had a linear increase during training.

ViT Transformer



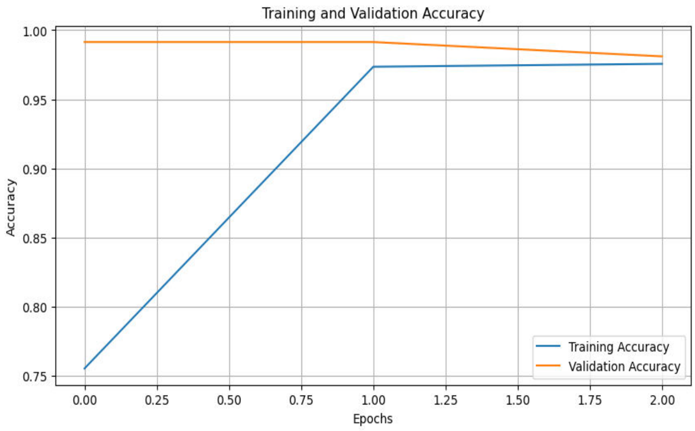


Fig. 8. Confusion Matrix and Accuracy plot (ViT)

ViT Transformer confusion matrix portrays how the model is having exceptional results when identifying classes like Cordana where all 75 images was classified correctly, Healthy class was classified properly out of all 75 images, same was the results for classes Pestalotiopsis and Sigatoka class was correctly classified.

Train and Validation plot of the transformer shows linear increase in training accuracy which later on stabilises on after few epochs, Validation accuracy was constant throughout.

ALEX NET

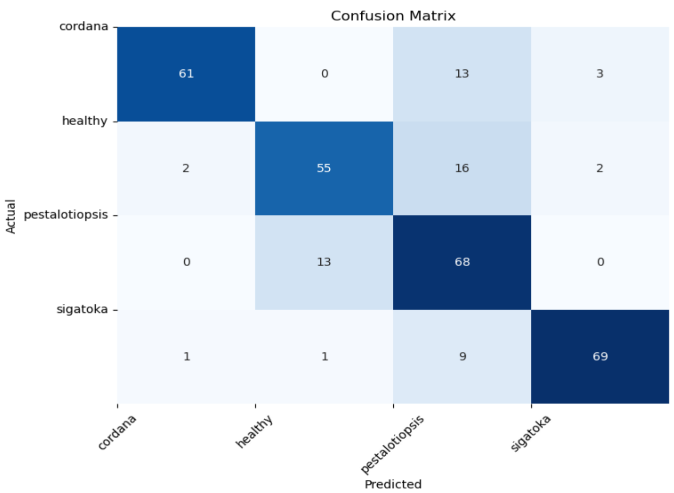
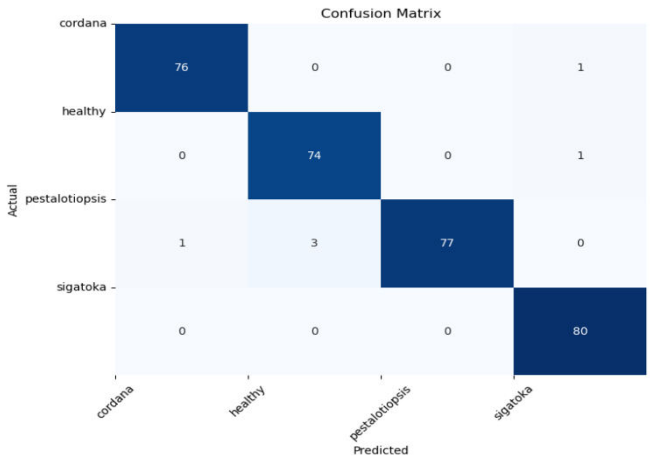


Fig. 9. Confusion Matrix and Accuracy plot (AlexNet)

AlexNet confusion matrix portrays how the model is having troubles when identifying classes like cordana where 61 images were classified correctly, 13 classified as Pestalotiopsis, healthy class were 55 images was correct and 16 images was falsely classified as Pestalotiopsis , Pestalotiopsis images also having trouble as 13 out of total images was classified as healthy and 9 out of the images in sigatoka class was incorrectly classified as Pestalotiopsis.

Train and Validation plot of the transformer shows linear increase with few dips in the middle epochs in training accuracy, whereas Validation accuracy also follows the same trend.

Inception V3



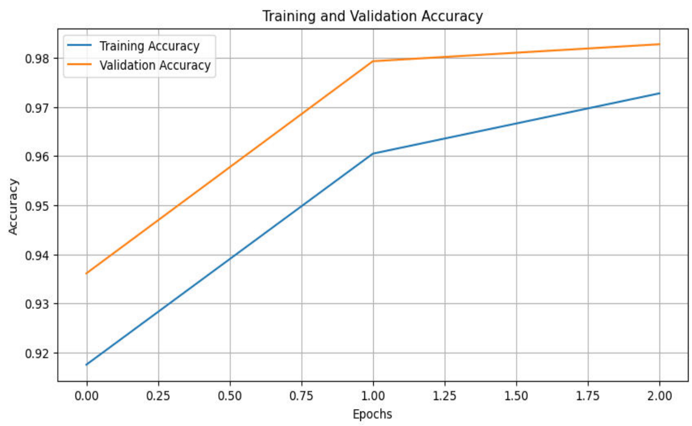


Fig. 10. Confusion Matrix and Accuracy plot (InceptionV3)

AlexNet confusion matrix portrays how the model is having exceptional results as well when identifying classes like Cordana where all 75 images were classified correctly, Healthy class was classified properly out of all 75 images, same was the results for Sigatoka class was also correctly classified but Pestalotiopsis class had a small hiccup were 3 images out of 80 images was incorrectly classified as healthy.

 ISSN 2394 - 7780

Train and Validation plot of the transformer shows linear increase in training accuracy which later stabilises on after a few epochs, Validation accuracy also following the same trend where it stabilised on the last few epochs.

Output Comparison

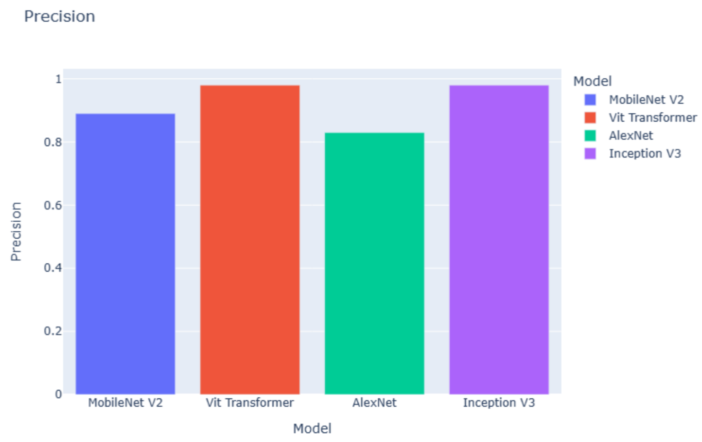


Fig. 11. Precision of models

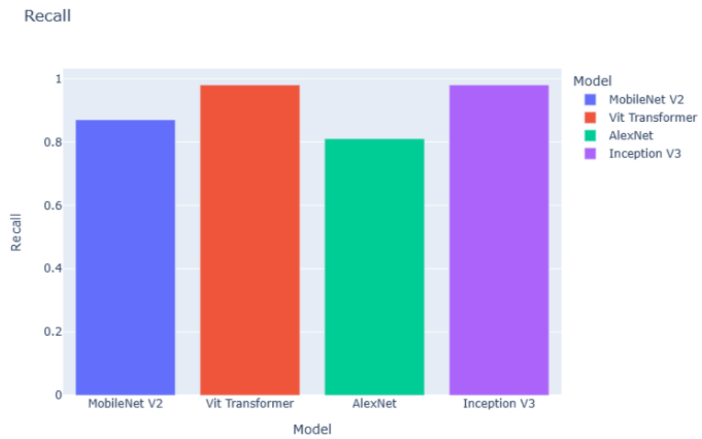


Fig. 12. Recall of models

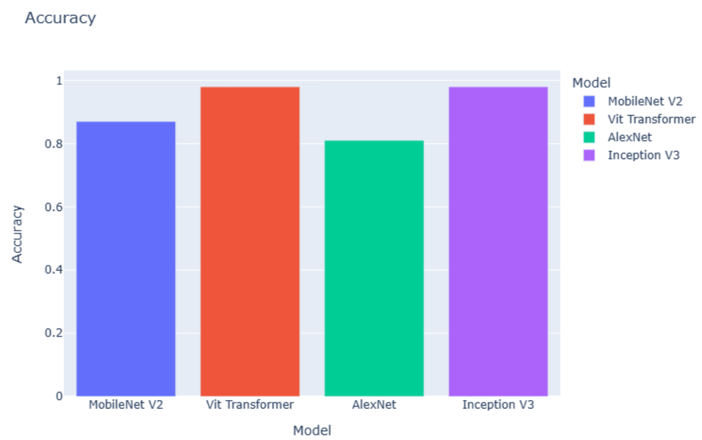


Fig. 13. Accuracy of models

In output comparison the Models ViT Transformer and Inception V3 has outperformed MobileNet V2 and Alexnet in terms of classification metrics Precision, F1 Score, Recall, Accuracy. ViT and Inception V3 are hand in hand in terms of the performance during classification.

VI. CONCLUSION

In this paper, the classification of Banana leaf is elucidated using algorithms such as MobileNet V2, VIT Transformer, Alexnet, and Inception V3. In terms of accuracy, ViT Transformer emerged as the most accurate of 98%, followed by Inception V3 97%, MobileNet V2 82% and Alexnet 81%. The undeniable observation is that ViT Transformer outperformed all other algorithms employed in this research in terms of accuracy.

The classification model presented in this paper proficiently categorises various diseases associated with banana leaves. Considering the significant role that bananas and their leaves play in addressing world hunger and supporting farmers' income, this approach proves beneficial for farmers in conducting quality assessments. As farmers globally transition from traditional approaches to technology-driven methods, our project aims to assist agriculturalists in ensuring the production of high-quality bananas and leaves, ultimately contributing to the reduction or management of world hunger and bolstering farmers' income. Enlarging the dataset's scope is planned, enabling the development of more sophisticated applications for classifying banana leaf diseases.

Compare to the existing paper which employed machine learning algorithms, our proposed paper achieved highest accuracy by employing Deep Learning models such as CNN networks and Transformer models.

VII. REFERENCES

[1] Britannica, The Editors of Encyclopaedia. "banana".Encyclopedia Britannica, 14 Nov. 2023, https://www.britannica.com/plant/banana-plant. Accessed 21 November 2023.

[2] https://www.fao.org/economic/est/est-commodities/oilcrops/bananas/bananafacts/en/

[3] Kakati, Jonalee Barman, and Tapashi Kashyap Das. “Classification of Healthy and Unhealthy Banana Leaves Using Deep Learning Approach: A Comparative Assessment.” 2023 4th International Conference on Computing and Communication Systems (I3CS), 16 Mar. 2023, https://doi.org/10.1109/i3cs58314.2023.10127309. Accessed 23 Nov. 2023.

[4] Mathew, Deepthy, et al. “Classification of Leaf Spot Diseases in Banana Using Pre-Trained Convolutional Neural Networks.” 2023 International Conference on Control, Communication and Computing (ICCC), 19 May 2023, https://doi.org/10.1109/iccc57789.2023.10165629. Accessed 23 Nov. 2023.

[5] Raja, N. Bharathi, and P. Selvi Rajendran. “Comparative Analysis of Banana Leaf Disease Detection and Classification Methods.” 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), 29 Mar. 2022, https://doi.org/10.1109/iccmc53470.2022.9753840. Accessed 23 Nov. 2023.

[6] P, Vidhya N, and Priya R. “Detection and Classification of Banana Leaf Diseases Using Machine Learning and Deep Learning Algorithms.” 2022 IEEE 19th India Council International Conference (INDICON), 24 Nov. 2022, https://doi.org/10.1109/indicon56171.2022.10039912. Accessed 23 Nov. 2023.

[7] Devi, M. Shyamala, et al. “Eight Convolutional Layered Deep Convolutional Neural Network Based Banana Leaf Disease Prediction.” 2022 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 4 Nov. 2022, https://doi.org/10.1109/icccis56430.2022.10037628. Accessed 23 Nov. 2023.

[8] Chaudhari, Vandana. Banana Leaf Disease Detection Using K-Means Clustering and Feature Extraction Techniques 1.

[9] Gara, Glenn, et al. LeafCheckIT: A Banana Leaf Analyzer for Identifying Macronutrient Deficiency LeafCheckIT: A Banana Leaf Analyzer for Identifying Macronutrient Deficiency. 2017, https://doi.org/10.1145/3162957.3163035. Accessed 23 Nov. 2023.

ISSN 2394 - 7780

TRANSFORMING FLEET TELEMATICS RISK ASSESSMENT: A FEDERATED LEARNING APPROACH

Shlok Mangle[1], Rujuta Joshi[2] and Prachi Satam[3]
[1, 2,3]Department of Information Technology SVKM's Dwarkadas J. Sanghvi College of Engineering Mumbai, India

ABSTRACT

There is a significant change happening in the insurance and risk management sectors regarding how risk assessment is being carried out in the field of fleet telematics. Tele-matics firms help clients balance risk and growth while- aiming for top-notch service.

This research presents a unique method for risk evaluation. It reshapes risk e-valuation using the FedAdagrad method and Federated Learning (FedML). Information is gathered and studied in partnership with fleet telematics firms to minimize possible risks. Fleet clients and telematics gadget makers are involved in the study from the get-go, including discussion and approval stages. After this, AI-based models estimate and scrutinize fleet operation risks. This enables insurance pros to give the-ir customers the finest quotes. These models make risk ratings for different situations. These cover individual driver risk, automobile risk, route risk, and comparative risk study for fleet te-lematics companies.

This study shows how FedML has the potential to transform risk assessment methodologies in the fleet telematics industry. FedML is a viable alternative to traditional centralised approaches because it effectively manages data privacy concerns, improves cost-efficiency, and enables real-time model refinement via data updates. As telematics data volumes grow, this approach could improve risk evaluation, leading to safer roads and personalised insurance, benefiting telematics companies and their clients.

Keywords - Federated Adagrad, Federated Machine Learning, Deep Neural Network, Fleet Risk Management, Privacy Preservation

I. INTRODUCTION

Fleet telematics is a game-changer in the insurance and risk management sectors, altering the traditional methods of risk assessment and management. The convergence of technology and data analytics within the realm of fleet operations offers unprecedented opportunities for improving road safety, optimizing insurance pricing, and enhancing overall service quality. Recent data emphasizes how critical this transition is: According to a recent report by GPS Insight, fleets reported an average of 4.5 accidents per driver per year, with over a third attributing fault to the driver. In addition, the global fleet management market has witnessed staggering growth, with a value of $19.47 billion in 2020, projected to reach $52.50 billion by 2030, reflecting a remarkable CAGR of 10.6% from 2021 to 2030. According to an additional report by GlobeNewswire, the installed base of fleet management systems in India is projected to experience a compound annual growth rate of 14.0 percent, set to nearly double from 3.5 million units in 2020 to almost 6.8 million units by 2025. An urgent need to reevaluate risk assessment methods and the rapidly increasing demand for fleet management systems is indicated by these statistics.

Telematics companies help clients monitor and manage risk, and predict future growth and service opportunities, in our rapidly changing world. This work is based on a thorough research study that developed a machine learning model using Federated Learning (FedML) to generate risk scores to tackle these challenges faced by telematics companies. Additionally, a Streamlit dashboard visualizes and compares risk scores for drivers, vehicles, routes, and different fleet companies. This FedAdagrad-based plan intends to revolutionize-fleet telematics risk assessment. It engages everyone in a dynamic system of communication, data gathering, and approval to create succeeding machine learning models. These models apply predictive analysis to assess and calculate possible risks related to flee-t operations. Thus, allowing insurance experts to provide more precise insurance quotes by computing risk scores for drivers, vehicles, routes, and fleet telematics companies.

This research paper conducts a comprehensive examination of the dynamic environment in fleet telematics, with the objective of not only conforming to industry demands but also facilitating the development of safer roads and customised insurance options. FedML's capacity to address data privacy concerns, enhance cost-effectiveness, and enable real-time model refinement via data updates will improve risk assessment and result in a more secure, data-oriented, and customer-focused future for the insurance and risk management sectors as telematics data grows.

II. LITERATURE REVIEW

As the insurance and risk management landscape continues to evolve, the domain of fleet telematics stands at the heart of this transformative journey. This literature review delves into the dynamic shifts in risk assessment methodologies, with a focus on the utilization of Federated Learning (FedML). Risk assessment has traditionally relied on centralised data processing, which inherently has privacy and transfer costs issues. Recent data insights highlights the need of reforming existing methods and embracing innovative approaches.

The paper “Federated Learning for Collaborative Prognosis” by Dhada, Maharshi, Parlikad, Ajith Kumar, and Palau, Adria Salvador suggests Federated Learning for data-driven prognosis. The authors train feed-forward and recurrent neural networks to predict simulated turbofan fleet failures using Federated Averaging algorithm using condition monitoring data to predict remaining useful industrial asset lifespan. The authors conclude that Federated Learning is a promising technique for training machine learning models on decentralized data and enables collaborative prognosis without sharing sensitive operational data as each device updates locally. [1]

The paper “FLeet: Online Federated Learning via Staleness Awareness and Performance Prediction” presents a novel approach to federated learning (FL) that combines the privacy of standard FL with the precision of online learning. The authors propose FLeet, the first online FL system, introducing two core components of FLeet, I-Prof and AdaSGD, which enable frequent (online) model updates. FLeet provides a 2.3x quality boost over standard FL while using 0.036% of the battery per day and AdaSGD converges 18.4% faster than FL approaches on heterogeneous data. [2]

The paper “Federated Learning and Privacy: Building privacy-preserving systems for machine learning and data science on decentralized data” by Kallista Bonawitz, Peter Kairouz, Brendan McMahan, and Daniel Ramage discusses the use of Federated Learning (FL) and Secure Multiparty Computation (MPC) as privacy-preserving solutions for training machine learning models on decentralized data FL enables users to train models on decentralised data without the need to transfer it, while MPC allows multiple parties to privately compute a function over their respective inputs. [3]

The paper “Federated Learning with Uncertainty-Based Client Clustering for Fleet-Wide Fault Diagnosis” by Hao Lu, Adam Thelen, Olga Fink, Chao Hu, and Simon Laflamme proposes a novel clustering-based federated learning (FL) algorithm to address the challenges of optimizing the federation strategy without leaking sensitive data and addressing the issue of client dataset heterogeneity in fault diagnosis applications. Each client sets aside a local test dataset and then clustered evaluating the other clients' model prediction accuracy and uncertainty on it to quantify dataset similarity without sharing data. [4]

The paper "Personalized Federated Learning of Driver Prediction Models for Autonomous Driving" by Manabu Nakanoya, Junha Im, Hang Qiu, Sachin Katti, Marco Pavone, and Sandeep Chinchali presents a novel variant of personalized federated learning (FL) to specialize robust robot learning models for diverse user distributions. The paper aims to improve trajectory forecasting models for autonomous vehicles (AVs) by proposing an algorithm that outperforms standard FL benchmarks by up to 2x in real user studies where human-operated vehicles must merge lanes with simulated AVs in the standard CARLA and CARLO AV simulators. [5]

The paper “Data-driven fleet management using MOORA: a perspective of risk management” by Santosh B. Rane, Prathamesh Ramkrishana Potdar, and Suraj Rane investigates the best fleet for a new purchase based on multi-objective optimization on the basis of ratio (MOORA), reference point, and multi-MOORA methods. The study uses Monte Carlo simulation to identify fleet performance monitoring critical parameters and determine their optimal range. The study showed that a pilot run of 300 fleets saved Rs. 2,611,013/- (US$36,264.065) annually in maintenance and FC costs as well as concludes CO2 emission reduction (4.83%) improving human health.[6]

The paper “Data-Driven Intelligent Transportation Systems: A Survey” by Junping Zhang et al. provides a comprehensive survey on the development of data-driven intelligent transportation systems (D2ITS). Authors use survey-based approach to provide an overview of D2ITS development and highlight that D2ITS is a multifunctional data-driven intelligent transportation system; changing an ITS from a conventional technology-driven system into a powerful multifunctional data-driven intelligent transportation system. [7]

The paper “Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges” by Dalton A. Hahn, Arslan Munir, and Vahid Behzadan provides a comprehensive classification of security and privacy vulnerabilities in Intelligent Transportation Systems (ITS). The authors discuss and identify ITS security and privacy vulnerabilities suggesting ways to improve them. [8]

The paper "Towards Federated Fleet Learning Leveraging Unannotated Data" by Viala Bellander, Alexander Ghafir, Yazan proposes a new federated learning framework called Federated Fleet Learning (FFL) is able to leverage unannotated data to improve the accuracy of the model and achieve better performance than Federated Averaging when the amount of annotated data is limited or when the distribution of the data is non-IID. [9]

The paper titled "Federated Alternate Training (FAT): Leveraging Unannotated Data Silos in Federated Segmentation for Medical Imaging" by Erum Mushtaq, Yavuz Faruk Bakman, Jie Ding, Salman Avestimehr proposes an alternate training-based framework, Federated Alternate Training (FAT), that alters training between annotated data silos and unannotated data silos to strengthen data privacy with limited data migration costs. [10]

The convergence of technology and data analytics within fleet telematics has given rise to a promising era where the quantification and management of risks intersect with the pursuit of growth and elevated service quality. This comprehensive literature review highlights the shift in risk assessment strategies, the crucial role of telematics companies, and FedML's potential to redefine risk assessment methodologies and serves as the foundation for the subsequent sections of this research.

A. Gaps/Challenges:

The existing methodologies for risk assessment in the fleet telematics sector have shown significant strengths, yet they also present gaps and challenges that require careful investigation. Some of the key challenges and gaps are listed as follows :

- **Data Privacy and Security Challenges:** One of the foremost challenges lies in ensuring the security and privacy of the telematics data, which often includes sensitive information. The centralization of data for analysis raises privacy and risk of breach concerns. Finding a balance between data accessibility and privacy is a complex issue that needs to be addressed.
- **Scalability Constraints:** The existing methodologies may struggle to efficiently scale with the increasing volume of telematics data. Scalability issues arise when handling larger datasets, more fleet participants, and real-time model updates.
- **Generalization of Risk Assessment Models:** The ability of current risk assessment models to generalize across diverse scenarios, such as various fleet operations and telematics companies, requires improvement. Models must accurately assess risk in various environments, which can be challenging.

Addressing these gaps and challenges is crucial to improving fleet telematics risk assessment methods. These challenges offer opportunities for research and development, method refinement, safer roads and more personalised insurance offerings.

III. METHODOLOGY

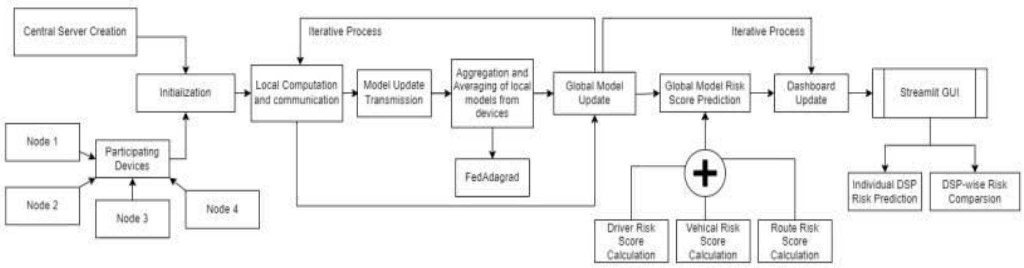


Fig. 1. Process Flow Diagram of the proposed Federated Learning methodology

The methodology utilized in this research encompasses two primary components: Federated Learning (FedML) with Machine Learning and the development of an application-side dashboard. These components work together to enable risk assessment within the field of fleet telematics(Fig. 1.).

- **Federated Machine Learning:** The core of this methodology centers on the development of a FL-based machine learning model, primarily focused on calculating the risk score of a given telematics company. This approach employs the Federated Adagrad strategy in particular to ensure privacy-preserving model training, allowing for the safe processing of data and risk assessment for a variety of telematics businesses.
- **Application Side:** Along with the FL-based model is the creation of a centralised interactive Streamlit dashboard designed to visualize the risk scores associated with drivers, vehicles, and routes of trips. In

addition, it offers the necessary features to compare risk scores across various fleet companies, giving a complete view of risk assessment in the telematics field.

A. System Architecture

In this methodology, the system architecture has been designed to utilize federated learning for the computation of risk scores in the context of telematics firms. This approach involves the development of a system architecture that utilises federated learning to calculate risk scores in the context of telematics industry. The architecture is built on principles of data privacy, scalability, and user friendliness to ensure a seamless and secure experience for all stakeholders involved.

- **Real-Time Data Upload Mechanism:** A fundamental element that not only enables the secure collection of data but also plays a crucial role in improving scalability and the ability to ingest data in real-time. This mechanism ensures that data from participating telematics companies can be efficiently collected and processed, facilitating the rapid growth of data volumes while maintaining data security.
- **Local Deep Neural Network (DNN) Models:** Deployed on distinct nodes, these local models enable data processing and risk assessment at the source.
- **Centralized Federated Adagrad (FedAdagrad) Model:** A central model responsible for aggregating updates from local models resulting in a refined global model for risk assessment.
- **Streamlit Graphical User Interface (GUI) Platform:** This platform, integrated into the architecture, functions as the user-friendly dashboard for visualizing individual Delivery Service Provider (DSP) risk scores. Additionally, it facilitates easy comparisons among different DSPs.

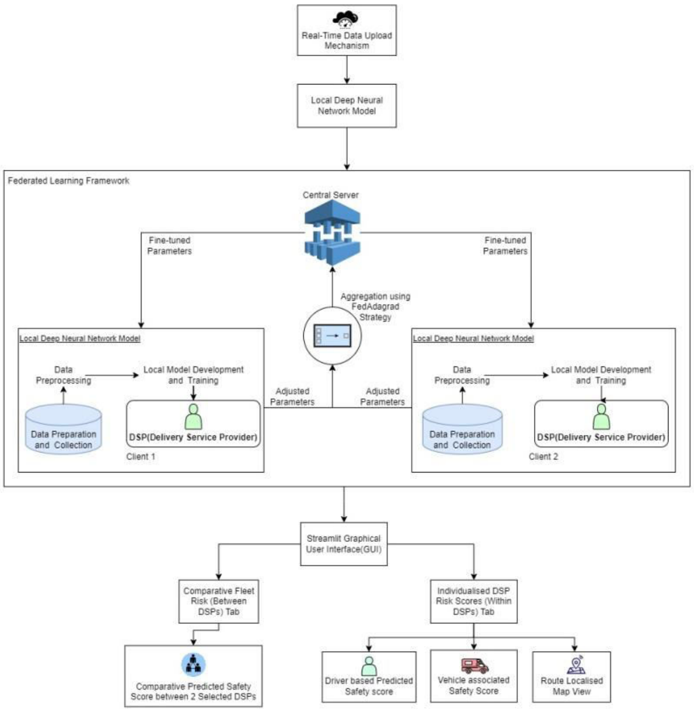


Fig. 2. System Architecture of the proposed solution

This system architecture has been carefully designed to prioritize data confidentiality, ensuring the safe and precise evaluation of risk, complemented by intuitive graphical representations (Fig. 2.). The subsequent sections provide a detailed breakdown of the methodology, including data collection, preprocessing, model training, and dashboard development, shedding light on the technical intricacies that define this approach.

B. Data Collection and Preparation

- **Data Collection:** The methodology begins with the collection of data from various telematics companies. These companies gather information from their respective fleet operations, including details about routes, drivers, and vehicles. This process is designed to capture diverse range of features that play important role in risk assessment.
- **Data Upload Mechanism:** A secure data upload mechanism is created to handle data from multiple sources and formats, streamlining the data integration process.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

C. Route, Driver, and Vehicle Data Parameters

- **Route Data Parameters:** Route data is gathered and prepared for analysis. This dataset contains various parameters such as environmental factors (e.g., weather conditions like rain, temperature, pressure, and wind speed), as well as a safety score assigned to each route. These parameters provide information about external conditions that may affect overall risk levels during trips.
- **Driver Data Parameters:** Driver-specific parameters include various metrics related to driving behavior and experience. This includes total miles driven, miles driven in urban and rural areas, the total number of tickets received, and instances of distracted driving. This data is extremely important for evaluating the risk associated with individual drivers.
- **Vehicle Data Parameters:** The dataset related to vehicles provides information on the condition and heath of the fleet. Parameters include variables like oil level, fuel level, total miles driven, battery health, battery voltage, and safety scores.

These parameters offer a comprehensive evaluation of each vehicle's impact on risk levels.

D. Risk Score Calculation (Route, Driver, and Vehicle)

1) **Safety Score Calculation:** *The risk assessment involves the calculation of safety scores for routes, drivers, and vehicles. Safety scores are numerical evaluation that measure risk associated with each respective aspect. These scores are calculated by aggregating and averaging the parameters within each category (Route, Driver, and Vehicle). Calculating the average of these scores for the entire dataset ensures a thorough evaluation of risk levels.*

a) **Route Safety Score:** *The Route Safety Score is calculated by averaging the safety scores related with each route within the dataset.*

$$\text{Route Safety Score} = (\Sigma \text{Safety Score\_route}_i) / N_r \quad (1)$$

Where:

SSafety Score_route$_i$ *is the sum of the safety scores for all routes within the dataset.*

N_r *is the total number of routes in the dataset.*

Driver Safety Score: *The Driver Safety Score is determined by averaging the safety scores of individual drivers.*

$$\text{Driver Safety Score} = (\Sigma \text{Safety Score\_driver}_j) / N_d \ (2)$$

Where:

ΣSafety Score_driver$_j$ *is the sum of the safety scores for all drivers within the dataset.*

N_d *is the total number of drivers in the dataset.*

Vehicle Safety Score: *The Vehicle Safety Score is calculated by averaging the safety scores linked to each vehicle in the dataset.*

$$\text{Vehicle Safety Score} = (\Sigma \text{Safety Score\_vehicle}_k) / N_v \quad (3)$$

Where:

ΣSafety Score_vehicle$_k$ *is the sum of the safety scores for all vehicles within the dataset.*

N_v *is the total number of vehicles in the dataset.*

2) **Fleet Risk Score Calculation:** *The Fleet Risk Score of a telematics company (Delivery Service Provider or DSP) is calculated by taking the average of the safety scores obtained from all the drivers, vehicles, and routes associated with that specific DSP in the dataset. This score provides a complete measure of the risk exposure faced by the DSP, taking into account all contributing factors.*

$$1/3 \text{ (Route Safety Score + Driver Safety Score + Vehicle Safety Score)} \quad (4)$$

E. Federated Learning Framework

Federated Learning is a distributed machine learning approach that allows multiple parties to collaboratively train a shared model while keeping their data decentralized and private. It is particularly important while dealing with sensitive data, such as telematics information for multiple fleet companies. The Federated Adaptive Gradient, or FedAdagrad, efocuses on personalized learning, empowering clients to individually train models with adaptable learning rates that are later aggregated by a central server. This section discusses the fundamental concepts and steps for implementing the FedAdagrad algorithm for risk score prediction.

1) Federated Learning Setup

The structure of Federated Learning treats each telematics company's DSP as a participant. Data is divided among these participants, so every company can handle its own data. The process of Federated Learning happens in stages. These stages, or communication rounds, allow the exchange- of model updates between the main server and the devices taking part.

a) Model Initialization:

At the beginning of each communication round, a common risk scoring model is initialized on the central server. This model serves as the basis for risk score prediction and is shared with the participating devices. The goal is to iteratively improve this model based on the unique data held by each company.

b) Communication Rounds:

i. Model Distribution:

In each communication round, the central server shares the current global model with the participating devices. The model is sent to each company, and local training is performed on their respective data. The model is applied to the local datasets, and model parameters are updated based on the gradients computed. Mathematically, this can be expressed as:

θ_local(t) = θ_global(t) - η∇L(θ_global(t),D_local) (5)

Where:

- **θ_local(t) represents the local model parameters at time t.**
- **θ_global(t) represents the global model parameters at time t.**
- **η is the learning rate.**
- **∇L(θ_global(t),D_local) is the gradient of the loss function with respect to the global model parameters θ_global(t) on the local dataset D_local.**

ii. Model Aggregation:

After local training, the participating devices send their updated model parameters back to the central server. These parameters include the changes in the model's weights after training on local data.

iii. Model Averaging:

The central server aggregates the received model parameters using the Federated Averaging approach. This involves averaging the weights of the local models to obtain a refined global model. The aggregation can be mathematically represented as:

θ_global(t+1) = (1/N)Σ(θ_local(t+1)) (6)

Where:

- **θ_global(t+1) represents the global model parameters at the next time step.**
- **N is the number of participating devices.**

c) Iterations:

Next, we repeat stages 2 through 4 a certain number of times. These cycles help make the whole model better without giving up private data kept by all the telematics groups.

d) Evaluation and Risk Scoring:

After the rounds are done, we use the final model to find risk scores for drivers, vehicles, and roads. The model trained to calculate risks is then brought into play on specific data to create risk scores, hinging on the model's guessed outcomes.

The FedAdagrad algorithm, is excellent at training models on split up data, but still keeps the data private. It's really important to our process of working together to estimate risk scores. It makes sure we get exact, useful risk reviews while still protecting highly private telematics data.

ISSN 2394 - 7780

F. Dashboard Development

Individual DSP Risk Score Prediction and Visualization: *The first section of the dashboard predicts and shows risk scores for different tracking service providers (DSPs). Users can easily interact and see the risk tied to specific drivers, vehicles, and paths under a DSP.*

Comparative Analysis of DSPs and Global Risk Scores: *The second section of the dashboard helps compare and visualize overall risk scores of DSPs. Users can playfully juxtapose risk evaluations among tracking services and notice trends or disparities in risk degrees. To achieve this, we colle-ct and analyze data deeply, compute risk scores, clean the data be-forehand, and design an accessible dashboard to allow efficient risk measurement and comparison of service providers.*

IV. Results And Analysis

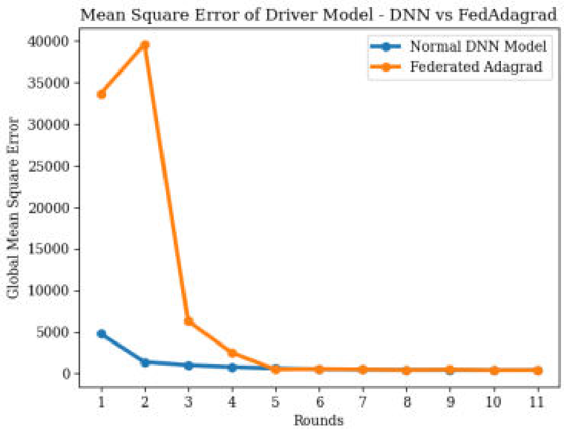


Fig. 3. Driver Model Fed vs DNN MSE

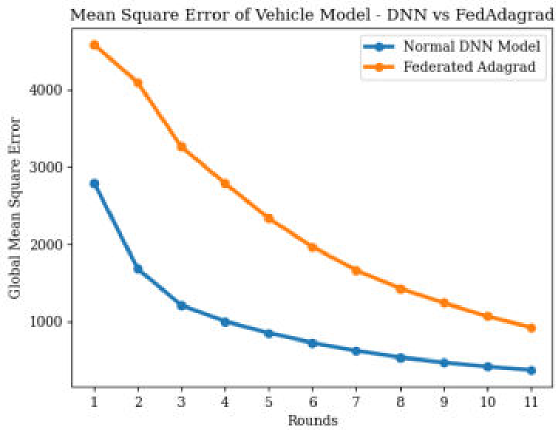


Fig. 4. Vehicle Model Fed vs DNN MSE

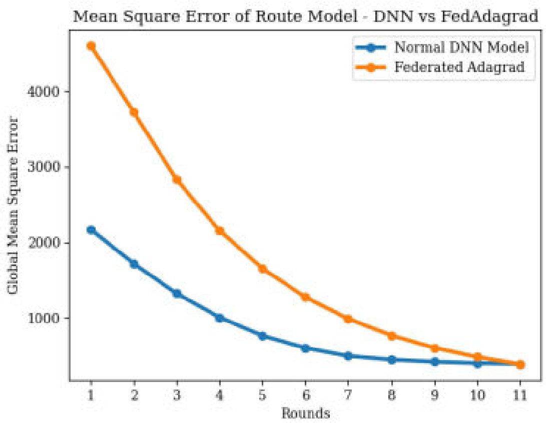


Fig. 5. Route Model Fed vs DNN MSE

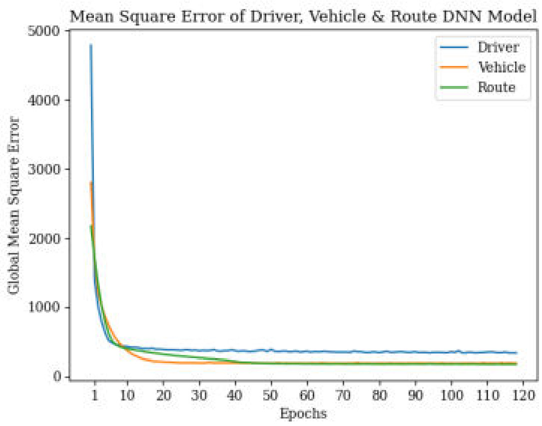


Fig. 6. Combined DNN Model MSE

TABLE I. COMPARATIVE TABLE OF MSE FED VS DNN

Entity	Mean Squared Error	
	Fed Adagrad Strategy	***Deep Neural Network***
Driver	390.8258	426.9556
Vehicle	923.6912	367.8880
Route	426.5146	394.6208

Fig. 3., Fig. 4., and Fig. 5. present a comparative analysis of the mean square error during the training of the driver, vehicle, and route models using both a standard Deep Neural Network (DNN) and a DNN enhanced with the FedAdagrad strategy over 11 rounds. Furthermore, Fig. 6. shows the mean squared error for the same models that were trained on a deep neural network (DNN) extended to 119 epochs.

The results highlight an interesting trend in early stages of FedAdagrad, where the mean squared error for the driver, vehicle, and route models is significantly greater compared to their counterparts trained solely on DNN.

Specifically, in the driver model (Fig. 3.), there is a significant dip observed during the third round for both FedAdagrad and the standard DNN but from the 5th round onwards, the mean square error remains relatively constant for both models until the 11th round.

Both the DNN with FedAdagrad and the normal DNN exhibit a gradual decrease in the mean square error across the 11 rounds for the vehicle model (Fig. 4.). Nevertheless, the overall mean square error remains lower for the standard DNN throughout the 11 rounds.

Similar observations are noted for the route model (Fig. 5.), as both the DNN with FedAdagrad and the standard DNN exhibit a gradual decrease in mean square error. While the overall mean square error is lower for the standard DNN over 10 rounds, the mean square error of DNN with FedAdagrad becomes less than the standard DNN in the 11th round.

Fig. 6. offers a broader perspective by illustrating the mean square error for all three models trained on a standard DNN for 119 epochs. The initial high mean square error for all three models experiences a substantial dip until the 9th epoch, after which the decrease becomes nearly horizontal. This indicates the mean square error stabilizes and undergoes minimal change after the 9th epoch.

To summarise (Table. 1.), the findings confirm that both the standard DNN and the DNN with FedAdagrad display distinct patterns in mean square error over different rounds and epochs. While FedAdagrad initially experiences higher errors, its performance stabilizes, and comparative analysis reveals varied trajectories for different models. This research highlights the effectiveness of these methodologies in dealing with risk assessment challenges in fleet telematics industry.

V. FUTURE SCOPE

The current research's potential future application, Federated Learning for Risk Assessment in Telematics Companies, can be expanded to include a variety of cutting-edge features and real-time monitoring capabilities. The present study identifies potential areas for future scope:

- **Real-time Vehicle and Driver Monitoring:** By integrating advanced computer vision methodologies and recognition algorithms, real-time monitoring of diverse driver parameters, including drowsiness, seat belt usage, detection of distractions, continuous monitoring of crucial vehicle metrics, such as tracking violations of traffic signs and monitoring lane changes ensuring compliance with safety regulations and reducing the risk of injuries while driving.
- **Environmental Monitoring:** Extend risk assessment model to include real-time monitoring of environmental factors such as weather conditions, road surface conditions, and visibility enhancing risk assessment accuracy and provide drivers with timely warnings about hazardous driving conditions.
- **Multi-Sensor Data Fusion:** Utilize data fusion techniques to combine data from various onboard sensors, such as GPS, accelerometers, cameras, to create a comprehensive view of driver behavior and vehicle conditions resulting in more robust risk assessment models and a comprehensive understanding of driving risks.

VI. CONCLUSION

In summary, this research highlights the need to transform risk assessment methodologies within the fleet telematics sector. Telematics companies play a crucial role in risk quantification and management.

Our approach, incorporating Federated Machine Learning (FedML) with the FedAdagrad strategy, offers means to redefine risk assessment methodologies. Collaboration with fleet customers, telematics device providers and firms ensures a comprehensive evaluation of risk- spanning drivers, vehicles, routes, and comparative analysis. Our methodology combines privacy-preserving FedML with user-friendly Streamlit dashboard, giving real-time risk assessment, visualisation, scalability and encouraging data-driven, customer-centric approach. It integrates route, driver, and vehicle data parameters with data preprocessing to generate precise risk scores, and utilizes FedAdagrad algorithm to maintain data privacy while delivering accurate predictions.

This research could transform risk assessment, promising safer roads, personalized insurance offerings, and mutual benefits for telematics companies and their clientele. As telematics data volumes grow, insurance and risk management insights reveal more secure, efficient, and service-oriented future. Transforming risk assessment is an ongoing process, and this study paves way for fleet telematics' rapidly evolving risk assessment process.

 ISSN 2394 - 7780

REFERENCES

[1] Maharshi Dhada, Ajith Kumar Parlikad, and Adrià Salvador Palau, "Federated Learning for Collaborative Prognosis," Mar. 2020, doi: https://doi.org/10.17863/cam.50577.

[2] G. Damaskinos, R. Guerraoui, A.-M. Kermarrec, V. Nitu, R. Patra, and F. Taiani, "FLeet: Online Federated Learning via Staleness Awareness and Performance Prediction," ACM Transactions on Intelligent Systems and Technology, vol. 13, no. 5, pp. 1–30, Sep. 2022, doi: https://doi.org/10.1145/3527621.

[3] K. Bonawitz, P. Kairouz, B. McMahan, and D. Ramage, "Federated learning and privacy," Queue, vol. 19, no. 5, pp. 87–114, 2021. doi:10.1145/3494834.3500240

[4] H. Lu, A. Thelen, O. Fink, C. Hu, and S. Laflamme, "Federated Learning with Uncertainty-Based Client Clustering for Fleet-Wide Fault Diagnosis," arXiv (Cornell University), Apr. 2023, doi: 10.48550/arxiv.2304.13275.

[5] M. Nakanoya et al., "Personalized federated learning of driver prediction models for autonomous driving," arXiv.org, https://arxiv.org/abs/2112.00956 (accessed Nov. 28, 2023).

[6] S. B. Rane, P. R. Potdar, and S. Rane, "Data-driven fleet management using Moora: A perspective of risk management," Journal of Modelling in Management, vol. 16, no. 1, pp. 310–338, 2020. doi:10.1108/jm2-03-2019-0069

[7] J. Zhang et al., "Data-Driven Intelligent Transportation Systems: A survey," IEEE Transactions on Intelligent Transportation Systems, vol. 12, no. 4, pp. 1624–1639, 2011. doi:10.1109/tits.2011.2158001

[8] D. Hahn, A. Munir, and V. Behzadan, "Security and privacy issues in intelligent transportation systems: Classification and challenges," IEEE Intelligent Transportation Systems Magazine, vol. 13, no. 1, pp. 181–196, 2021. doi:10.1109/mits.2019.2898973

[9] Viala Bellander, Alexander and Y. Ghafir, "Towards Federated Fleet Learning Leveraging Unannotated Data," Handle.net, 2023. http://hdl.handle.net/20.500.12380/306240 (accessed Nov. 29, 2023).

[10] E. Mushtaq, Y. F. Bakman, J. Ding, and S. Avestimehr, "Federated alternate training (fat): Leveraging Unannotated Data Silos in federated segmentation for Medical Imaging," 2023 IEEE 20th International Symposium on Biomedical Imaging (ISBI), 2023. doi:10.1109/isbi53787.2023.10230533

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

PEER-TO-PEER NON-FUNGIBLE TOKEN (NFT) MARKETPLACE: A BLOCKCHAIN-ENABLED SOLUTION FOR P2P NFT TRADING

Paranjay Haldar[1], Rajdeep Roy[2], Sourav Banerjee[3] and Utpal Biswas[4]
[1, 2, 3,4]Department of Computer Science and Engineering University of Kalyani Kalyani, India
[2]https://orcid.org/0000-0003-1616-3501 and [3]https://orcid.org/0000-0002-0104-967X

ABSTRACT
Nowadays, the adoption of Blockchain technology has surged, with artists utilizing its capabilities to create and showcase digital content on the Blockchain. All the digital content on the Blockchain is called a Non-Fungible Token (NFT), which follows a standard known as the Ethereum Request for Comment (ERC-721). NFT resides on the InterPlanetary File System (IPFS), and the Content IDentifier (CID) is stored in the smart contract. This paper proposed a marketplace framework that can transfer ownership of the NFT upon fulfillment of certain conditions. Artist can create their NFT in the Smart Contract. As marketplace is built on smart contracts, each NFT trade can be seen on the Blockchain Explorer, which provides transparency in the framework. In future, integration of ERC-20 token into the framework can be used to buy NFT.

Keywords: Blockchain, Ethereum, ERC-721, IPFS, Marketplace, NFT, Smart Contract, Transparency

I. INTRODUCTION
Trading of digital assets like e-gold, digital art, or any other digital form of asset is carried out by centralized exchanges like banks. These exchanges have some limitations like high transaction fees, low settlement time, and a centralized database, which can lead to low transparency in the system. A marketplace for trading digital assets should be transparent in nature with low transaction fees, as there will be huge number of transactions with less settlement time. The order book should be decentralized in nature. In the present era, due to the increasing dominance of Blockchain technology, there has been a profound transformation in the creation and trading of digital assets. On the Blockchain domain, digital assets are known as NFTs. To identify a specific NFT on a particular Blockchain, it is important to know the smart contract address and the NFT identity (mainly known as the token ID) of that NFT. NFT follows a particular standard known as ERC-721 which provides the following functionalities such as ownerOf which returns the NFT owner of that particular NFT, balanceOf which returns the number of NFT an address holds, transfer method help the owner of NFT to transfer the NFT to new owner, using approve method owner of NFT give permission to an address to transfer a particular NFT on owner’s behalf, setApprovalForAll method is similar to approve except owner of NFT will give permission to an address to transfer all the NFT on owner’s behalf, transferFrom method transfer the NFT to a new owner but there is a difference with transfer method. In transfer method only the owner of the NFT can transfer the NFT to a new owner but in transferFrom method owner as well as the approver can transfer the NFT to a new address. There are few additional functions such as: name method which returns the name of the NFT collection, Symbol method which returns the symbol of the NFT collection, as the NFT resides in the IPFS, the CID is stored in the Blockchain. TokenURI method returns the CID of a particular NFT. Presently, Blockchain technology is applied in various application in diverse domains, including Internet of Things for vehicles [1], Electronic Health Records [2], toll tax collection [3], and public distribution systems [4].

This paper proposed the design of a NFT marketplace using Blockchain technology [5], and by utilizing the smart contract, it provides transparency and trust in the system. Users can create and trade NFT in the marketplace. Since the smart contract is deployed on the public Blockchain, ledger that contains all the transactions will be decentralized and immutable in nature. To sell the NFT, owner doesn’t need to pay any gas fees as order will be placed off-chain. Owner of the NFT need to sign the order details and while buying the NFT, the signature will be verified on-chain and once, it is verified, then only transfer of ownership of NFT will be processed. Signing will be done by NFT owner’s private key and verification of the signature is done in the smart contract which returns the public key of the NFT owner.

The present study is collocated as follows. Part II expounds reappraisal of current work. Part III arrays the contemplated work while Part IV depicts the try out upshots of the proposed framework and conclusively Part V sewed up the paper with some futuristic edicts.

II. RELATED WORKS
Entriken et al., 2018 [6] proposed the ERC-721 regarding Non Fungible Token Standard. This standard is now widely used for creating NFTs. The motivation behind proposing this standard is to provide a standard interface

that will allow wallet/broker/auction application to work with any NFT on Blockchain. Since a standard is followed for creating NFT, standard Application Programming Interface (API) can be created.

Johnson et al.,2001 [7] proposed Elliptic Curve Digital Signature Algorithm (ECDSA) which is used for generating a public-private key pair. This algorithm is used to create wallet with a public key and private key. Using the private key a message is signed by the owner's wallet and during verification process, it returns the public key. If the returned public key is the desired public key, then the verification is successful otherwise, it fails. In the proposed marketplace, this idea have been implemented to carry out off-chain listing of NFT.

Binance Smart Chain (BSC) [8] testnet Blockchain have been used to deploy the Smart Contract. BSC support Solidity code which is used to write the Smart Contract. It is more faster than Ethereum Blockchain and more environment friendly as it uses the combination of Delegate Proof of Stake and Proof of Authority known as Proof of Staked Authority.

Benet, 2014 [9] proposed a new peer-to-peer distributed file system known as InterPlanetary File System (IPFS). In this instance more focus has been given to content based addressing than that of location based. File with same content return the same Content IDentifier (CID). Since, this storage is implemented on peer-to-peer distributed system, it is most suitable storage for storing the metadata of the NFT.

Web3.js [10] is a library used to deal with the smart contract. It is used to connect with the Blockchain node using http or IPC or web socket. It have methods to interact with the Smart Contract.

Ethereum Request for Comments 20 or ERC-20 [11], is a standard used to create fungible tokens on the Ethereum Blockchain. ERC-20 standard outlines a set of rules and functions that developers must implement to create tokens compatible with the Ethereum ecosystem. Similarly Binance Smart Chain Evolution Proposal 20 or BEP 20 is used to create tokens on BSC network. These tokens have some common functionalities, such as transferability and balance checking. BEP-20 token can be used to purchase the NFT.

III. Proposed Blockchain-Based NFT Marketplace

This section focus on the proposed work. The proposed marketplace acts as a bridge between buyer and seller of NFT. Artist can earn by selling the NFT, buyer can get the original digital content whereas marketplace creator can earn from the platform fee which is applicable on every sell of NFT.

System Overview

The framework involves three different entities. The entities are artists who creates the NFT, buyer who buy the NFT and the admin who creates and deploy the NFT smart contract and marketplace smart contract where seller and buyer can trade the NFT. The proposed framework would involve the following steps as follows:

Step 1: Admin will create and deploy the smart contract for NFT creation and NFT marketplace.

Step 2: Artist can create digital content in the form of NFT. The proposed framework support creation of NFT using ERC-721 standard. The NFT is stored in the IPFS and CID is stored in the smart contract. By utilizing IPFS, it ensures decentralization of NFT metadata.

Step 3: Once, the NFT is created by the artist, artist will approve the marketplace to transfer the NFT on artist's behalf.

Step 4: After successful approval to marketplace, artist will list NFT for sell. Listing of NFT is done off-chain to save the gas fees of the artist, but artist need to sign a data (data will be created by encrypting the NFT smart contract address, NFT token Id, selling price of NFT and the time of listing the NFT in the marketplace in Epoch format) using the private key.

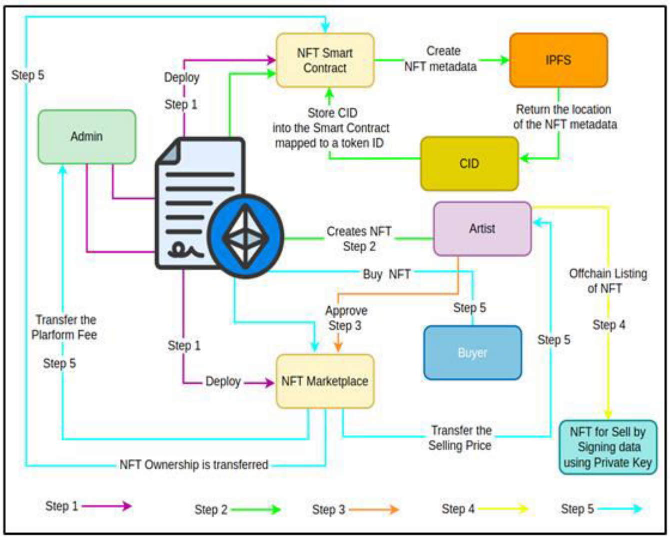


Fig.1. Functionality of Proposed Framework.

Step 5: The buyer needs to provide the data for signature verification. If the signature verification is successful, on paying the selling price plus marketplace platform fee, buyer can transfer the ownership of the NFT. If any of the condition failed, the ownership of the NFT will not transferred. Figure 1 potraits overall employability of the pripounded work.

Creation of NFT

Artist can create NFT by providing the name, image and description of the NFT. This details of NFT is stored in the IPFS. The details are uploaded in the IPFS and can be accessed using

https://ipfs.io/ipfs/bafyreib7j53y4ecex2kyuu7k6cmsk3hwt45httkdb2gulrvtnyff6yutvi/metadata.json . Once the NFT details are uploaded in the IPFS, it returns a CID. This CID is stored in the NFT smart contract mapped to a token Id. User wallet address will mapped to this token Id. Transaction details for creating the NFT can be found from

https://testnet.bscscan.com/tx/0xcc9d47f651f9a5698dae46eb523abc25cb4b37d0d81f001d66fed021aa71ee47.

Figure 2 briefly describe the process of creation of NFT by the artist.

Algorithm 1: Creation of NFT

1. Start.
2. Input: NFT Name, NFT Image, NFT Description.
3. Upload the details in the IPFS.
4. Output: IPFS will return the CID.
5. Input: CID
6. Call the NFT Smart Contract Function To Create NFT.
7. Transfer the NFT to the Caller's account.
8. Mapped the CID to the tokenId and map the tokenId to the caller's wallet.
9. Increment the tokenId by 1 and caller's balance by 1.
10. Stop.

Fig.2. Algorithm for creating NFT

Approval of NFT

Once, the NFT is successfully created on the Blockchain, artist can approve the marketplace to transfer the NFT on artist behalf. Without successful approval of marketplace, buyer cannot buy NFT from marketplace.

Sell order of NFT

In order to do a transaction in Blockchain, user needs to pay gas fee. To prevent users from paying gas fee for selling NFT, this framework support off-chain listing of NFT. Owner of NFT needs to sign a message which will be verified on-chain. The message is created using NFT contract address, token Id, selling price and the time of listing. Once, the owner of the NFT signs the message, NFT will be listed in the marketplace for sell. Figure 3 shows the encryption of message and the signature done by the owner.

```
{
  message: '0xd8c53ad8dd33b3cd9c48e521a7b2622ba5c394bcc50c2cddbff25a13310c37eb',
  messageHash: '0xa73cafb7e4d3477fe735e152dc69f241f0fb62780fa4b585459c47c88c248061',
  v: '0x1c',
  r: '0x9e77de6ccd039beff30b659433f8b966a5228a6f38884ee83406980b5fe869a7',
  s: '0x77e8c2bb1b4fce31285f7b88851728c36f4563d0910b6f8f29f370a6ef508614',
  signature: '0x9e77de6ccd039beff30b659433f8b966a5228a6f38884ee83406980b5fe869a777e8c2bb1b4fce31285f7b88851728c36f4563d0910b6f8f29f370a6ef5086141c'
}
```

Fig.3. Encryption of Message and Signature.

IV. Experimental Results

This section focus on the experimental result of the proposed framework. This framework is completely decentralized, transparent and immutable in nature as it is utilizing the smart contract for achieving the marketplace features.

Environment Setup

Smart Contract [12] have been implemented in the Visual Studio Code. Smart Contract is written in Solidity[13]. The smart contract is now live on the Binance Smart Chain using Truffle framework [14]. Web3.js have been used to interact with the Smart Contract. Below table 1 have been given where tools with their version are mentioned.

TABLE I. TOOLS USED FOR THE EXPERIMENT

Tools	Description	Version
Operating System	Ubuntu Operating System is used	20.04.5 LTS
Visual Studio Code	Code Editor for writing the code.	1.74.0
NodeJs	Runtime Environment for executing JavaScript code.	18.12.1
Truffle	Used to Create and Deploy the Smart Contract.	5.8.1
Solidity	Used to write Smart Contract.	0.8.19
Web3Js	Used to interact with the Smart Contract.	1.8.1

Smart Contract Deployment

The Smart Contract have been deployed on the Binance Smart Chain testnet Blockchain. Two Smart Contract have been developed to achieve the desired outcomes of the framework. One Smart Contract is ERC-721 NFT Smart Contract and another is marketplace. The deployed Smart Contract address are https://testnet.bscscan.com/address/0x8423dee52705e50b77947638347a9a335d9a529e#code and https://testnet.bscscan.com/address/0x3d15dc7b8f94cf7217381d906423208db30e66d9#code for NFT Smart Contract and marketplace respectively.

Total Price

Marketplace owner will charge a platform fees on every successful sell of NFT. The platform fee is 2.5% of the selling price. Figure 4 shows the platform fees and total price for a given selling price of a NFT. Since, the price of NFT is fetched from Solidity view function, it won’t require any gas fee. The total price of NFT needs to be paid in the native coin of the Blockchain.

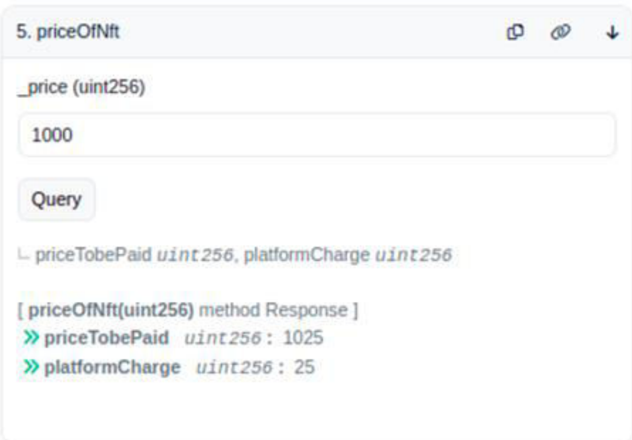


Fig.4. Total Price of NFT paid by the buyer

Signature Verification

Blockchain uses ECDSA [15] for digital signatures [16]. ECDSA generates a public-private key pair. Private key is used to sign the data and using Solidity's build in ecrecover function, signer public key can be found. Function ecrecover takes 4 input parameters. They are:

hash (bytes32): The hash of the message that was signed.

v (uint8): The recovery id or the signature's "v" value.

r (bytes32): The signature's "r" value.

s (bytes32): The signature's "s" value.

By providing all the parameters that were used by the artist to sign the message, buyer will verify the signature. This verification will return the signer public key. If the signer address is same as NFT owner address, the verification is successful.

Buy NFT

Once the signature is validated and if the buyer send the total price, NFT will be transferred to the buyer's account, the selling price will be transferred to the seller account and the platform fees will be transferred to the marketplace owner account. Figure 5 shows a transaction details of buying a NFT. Transaction can be accessed using https://testnet.bscscan.com/tx/0xfaa27f0294dca8d5ee145d610004ad25be6f4bb67525ad47beccb95b04af6f54.

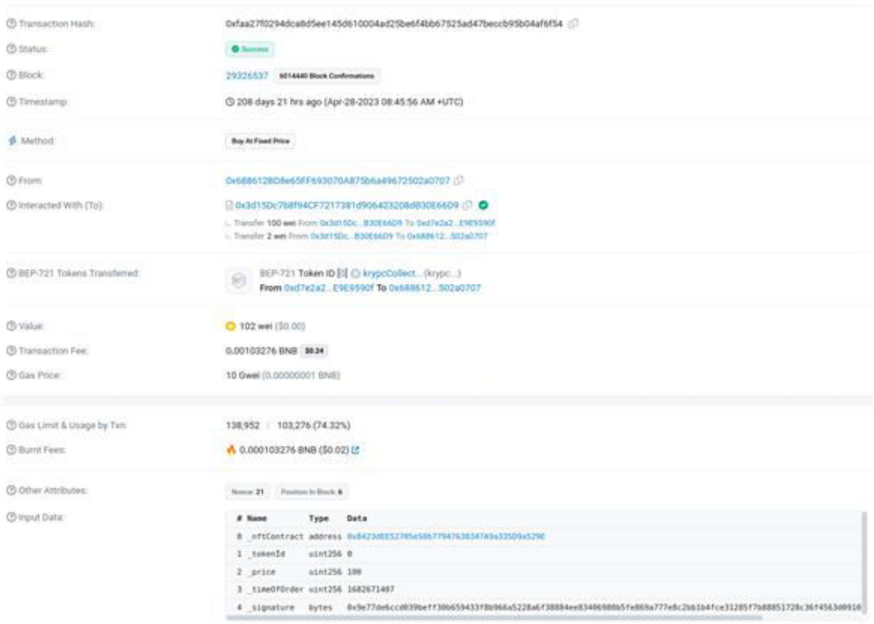


Fig.5. Transaction details of Buying a NFT

V. CONCLUSION AND FUTURE WORK

This section finally concludes the research paper on the NFT marketplace with some future directives. NFT marketplaces have emerged as a revolutionary platform for trading of NFTs. The proposed marketplace framework is fully decentralized in nature. In this proposed framework buying of NFT is done by the native cryptocurrency. In future, integration of ERC-20 token or fiat currency can be done to buy the NFT. In the proposed framework seller don't need to pay any gas fees whereas buyer need to pay the gas fees in order to transfer the ownership of the NFT. In the future gas-less transaction can be implemented in the marketplace.

ACKNOWLEDGMENT

R.R is thankful to Ravi Jagannathann(CEO), Mohit Sethi(SVP), Karthik Mohan(Technical Lead) and all the other developers of KrypC Technologies Private Limited, Address: 606, 1st Main Rd, IAS Colony, 06th Sector, HSR Layout, Bengaluru, Karnataka 560102, India, for their support to carry out this research work.

REFERENCES

[1] S. Banerjee, D. Das, P. Chatterjee, B. Blakely and U. Ghosh, "A Blockchain-Enabled Sustainable Safety Management Framework for Connected Vehicles," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2023.3330159.

[2] Banerjee, S., Barik, S., Das, D., Ghosh, U. (2024). EHR Security and Privacy Aspects: A Systematic Review. In: Puthal, D., Mohanty, S., Choi, BY. (eds) Internet of Things. Advances in Information and Communication Technology. IFIPIoT 2023. IFIP Advances in Information and Communication Technology, vol 683. Springer, Cham. https://doi.org/10.1007/978-3-031-45878-1_17

[3] Das, D., Banerjee, S., Biswas, U. (2022). Design of a Secure Blockchain-Based Toll-Tax Collection System. In: Sharma, D.K., Peng, SL., Sharma, R., Zaitsev, D.A. (eds) Micro-Electronics and Telecommunication Engineering . ICMETE 2021. Lecture Notes in Networks and Systems, vol 373. Springer, Singapore. https://doi.org/10.1007/978-981-16-8721-1_18

[4] Roy, R., Haldar, P., Das, D., Banerjee, S., Biswas, U. (2022). A Blockchain Enabled Trusted Public Distribution Management System Using Smart Contract. In: Ortiz-Rodríguez, F., Tiwari, S., Sicilia, MA., Nikiforova, A. (eds) Electronic Governance with Emerging Technologies. EGETC 2022. Communications in Computer and Information Science, vol 1666. Springer, Cham. https://doi.org/10.1007/978-3-031-22950-3_3

[5] Banerjee, S., Das, D., Biswas, M., & Biswas, U. (2020). Study and Survey on Blockchain Privacy and Security Issues. In I. Williams (Ed.), Cross-Industry Use of Blockchain Technology and Opportunities for the Future (pp. 80-102). IGI Global. https://doi.org/10.4018/978-1-7998-3632-2.ch005

[6] William Entriken (@fulldecent), Dieter Shirley <dete@axiomzen.co>, Jacob Evans <jacob@dekz.net>, Nastassia Sachs <nastassia.sachs@protonmail.com>, "ERC-721: Non-Fungible Token Standard," Ethereum Improvement Proposals, no. 721, January 2018. [Online serial]. Available: https://eips.ethereum.org/EIPS/eip-721.

[7] Johnson, D., Menezes, A. & Vanstone, S. The Elliptic Curve Digital Signature Algorithm (ECDSA). IJIS 1, 36–63 (2001). https://doi.org/10.1007/s102070100002

[8] Bnb-Chain. (2022, October 25). whitepaper/WHITEPAPER.md at master · bnb-chain/whitepaper. GitHub. https://github.com/bnb-chain/whitepaper/blob/master/WHITEPAPER.md

[9] Benet, Juan. (2014). IPFS - Content Addressed, Versioned, P2P File System. https://doi.org/10.48550/arXiv.1407.3561

[10] web3.js - Ethereum JavaScript API — web3.js 1.0.0 documentation. (n.d.). https://web3js.readthedocs.io/en/v1.10.0/index.html

[11] Fabian Vogelsteller <fabian@ethereum.org>, Vitalik Buterin <vitalik.buterin@ethereum.org>, "ERC-20: Token Standard," Ethereum Improvement Proposals, no. 20, November 2015. [Online serial]. Available: https://eips.ethereum.org/EIPS/eip-20.

[12] Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. First Monday, 2(9). https://doi.org/10.5210/fm.v2i9.548

[13] Solidity — Solidity 0.8.20 documentation. (n.d.). https://docs.soliditylang.org/

[14] Truffle Documentation - Truffle Suite. (n.d.). https://trufflesuite.com/docs/

[15] Wang, Xinyu. (2019). Research on ECDSA-Based Signature Algorithm in Blockchain. Finance and Market. 4. 55. 10.18686/fm.v4i2.1600

[16] Subramanya, S.R. & Yi, B.K.. (2006). Digital signatures. Potentials, IEEE. 25. 5 - 8. 10.1109/MP.2006.1649003.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024

ISSN 2394 - 7780

IOT TRAFFIC CLASSIFICATION AT MULTINATIONAL CONGLOMERATES USING DEEP LEARNING

Supraja Yadav H[1] Ayushi Malani[1] and Asha K[2]
[1,2]MSc Bigdata Analytics Student, [3]Assistant Professor, Department of Advanced Computing, School of InformationTechnology, ST Joseph’s University Bengaluru, Karnataka, India

ABSTRACT

In a modern digital world, network security has become one of the most important security issues. The identification of benign and malicious devices has become a problem due to the extensive use of electronics in our networked world. The capacity to differentiate between hostile and benign entities has gained significant prominence in the world of cybersecurity due to the ongoing expansion of the Internet of Things and the daily rise in cyber threats. As the Internet of Things is largely going at a rapid space, securing IOT networks from cyberattacks has grown to a more critical responsibility. This study delivers a thorough method for classifying and identifying threats, it offers an innovative mixed method that combines two types of learning methods to identify forged communications in the IOT devices. Initially, individual device data undergoes preprocessing and DBSCAN(Density-Based Spatial Clustering of Applications with Noise) clustering to identify malicious patterns. In the deep learning phase, an automatic encoder is used on the combined dataset, which provides robust pattern recognition without explicit labels. Combining DBSCAN and autoencoder outputs in the final step improves classification accuracy. Evaluation and performance comparable to different approaches provides an effective strategy for detecting malicious traffic.

Keywords: Cyber threats, malicious and benign traffic, DBSCAN, Autoencoder.

I. INTRODUCTION

IOT devices are nonstandard computing hardware like sensors and appliances that can wirelessly join a network and efficiently send data. IOT has been around for a long time and has improved its practicality by providing access to reasonably priced and dependable resources as well as advancing AI and machine learning technologies. There are numerous varieties of IOT, including Industrial, Commercial, Consumer, and Infrastructure IOT, which facilitates connectivity across various protocols. maliciously causing several issues with vital infrastructure, integrity, privacy, and security. Conversely, benign gadgets operate in a very typical manner. The research presents a novel method of combining deep learning and machine learning techniques, then analyzing performance to determine which methodology performs better. In the contemporary digital world, this research open the door for improved threat detection and mitigation through the integration of diverse algorithms and methodologies.

II. LITERATURE REVIEW

There are several methods for identification of vulnerabilities in the IOT network to begin with MANDRAKE-machine Learning for IoT vulnerability Detection a novel method that utilizes machine learning to detect vulnerabilities in IOT network packet traffic [1]. Bijective soft sets are used in the study's initial stages for effective feature selection. With an emphasis on accuracy, it presents the CorrACC measure and suggests the Corracc method, which uses a wrapper technique to filter and choose pertinent features for machine learning classifiers [2]. An elective way to deal with traffic identification in Web of Things networks includes the approval of explicit highlights using TOPSIS and Shannon Entropy, in view of bijective delicate sets, to distinguish false traffic[3]. The classifiers accurately determine whether the IoT device's network traffic was malicious or benign. [4]. Explainable Deep Learning (DL) algorithms are evaluated using the SPIP framework, which integrates explainable AI (XAI) and DL approaches including PFI, ICE, PDP, and Short-Term Long Memory SHAP to provide both local and global explanation [5]. An ensemble of recurrent neural networks (RNNs) is used in a hybrid metaheuristic-deep learning strategy to improve IoT intrusion detection. Within RNNs, Attacks on Internet of Things systems are detected by (LSTM) long short term memory and (GRU) gated recurrent unit models. Harris Hawk optimization and fractional derivative mutation are used to select features. [6]. The model extracts features that hold steady even in IoT environments that are heterogeneous and unstable by employing a denoising autoencoder [7]. A two-stage learning technique to achieve high recall, precision, and accuracy in the accurate classification of IoT devices in two distinct datasets, with 99.6% precision and 99.7% recall, respectively obtained [8]. DIS-IoT is an interruption recognition strategy for the Web of Things that utilizes a stacking gathering of profound learning models. By combining four distinct deep learning models, it produces a single model. [9]. In order to reduce dimensionality in network traffic data, PCA and KPCA are used [10]. Using sparse autoencoders aims to enhance IoT device security against malware attacks. The approach analyses bidirectional TCP flows and packet statistics to profile network behaviour, achieving attack detection rates [11]. CNN and Auto encoders to enhance accuracy compared to traditional methods [12]. An proposes an IDS study that aims to identify malicious activities in real-time and solves the shortcomings of current systems[13]. To distinguish significant qualities for the model, information separating utilizing a regulated or solo element choice procedure is likewise utilized. [14]. A profound measurement learning technique that mixes autoencoders with Trio networks is an answer for distinguishing network interruption and hurtful movement in network traffic [15]. Text convolution neural networks are used to extract key features from traffic data, which is represented as vectors. On the ISCX VPN-non VPN dataset, the method is tested and classified well. [16]. An approach that uses autoencoder neural networks in wireless sensor networks (WSNs) is used for anomaly detection in Internet of Things applications [17]. A methodical analysis of deep learning (DL) and machine learning (ML) techniques in relation to network intrusion detection systems (NIDS), highlighting the most popular autoencoders (AE) and their variants as algorithms for suggesting NIDS solutions, especially for feature extraction [18]. An article presents a recurrent neural network-based deep learning approach for cloud computing systems anomaly detection. Analyzing the characteristics and flaws of popular activation functions, such as the sigmoid, Tanh, Soft plus, and RELU functions, helps to improve the algorithm [19]. The literature proposes an improvement to flow-based traffic categorization through the use of machine learning algorithms and a WMI_AUC feature selection approach [20].

III. METHODOLOGY

A. Data Collection

The dataset has been taken from CERN's zenodo, a general-purpose open repository created as part of the European OpenAIRE initiative. [21]IoT-deNAT is the dataset that Meidan, Yair submitted. It consists of outbound flow-based network traffic statistics from both IoT and non-IoT devices that are behind a home NAT. They put a range of commercial IoT devices alongside non-IoT equipment in order to conduct an empirical evaluation of our method. The NetFlow records in the dataset were gathered in a lab at Ben-Gurion University of the Negev over the course of 37 days. The records catch the active organization traffic of 8 business IoT gadgets and 5 non-IoT gadgets. The purpose of gathering the dataset was to create a way for telecom companies to identify IoT models that are vulnerable and hidden behind home network adapters. For research repeatability, the device model that generated each NetFlow record is tagged.

The seven IoT devices that have deployed are webcam. Amcrest, socket.Wemo.Insight, webcam,Samsung, Streamer.Amazon.Fire_TV_Stick,light_bulb.TP_Link, speaker.Sonos One and doorbell.Amazon.Ring. There are 24 columns which include netflow features, labeled , additional and derived features as well, consisting of 1565286 records.

'FIRST_SWITCHED' indicates the system uptime of the initial and last packet switch. 'IN_BYTES' and 'IN_PKTS' are counters for incoming bytes and packets. 'IPV4_DST_ADDR' records the destination IP, while 'L4_DST_PORT' and 'L4_SRC_PORT' note TCP/UDP port numbers.'PROTOCOL' signifies the IP protocol (6: TCP, 17: UDP). 'SRC_TOS' captures Type of Service, 'TCP_FLAGS' logs cumulative TCP flags, and 'IP' reveals the destination IP network. 'DURATION' reflects the time span between the first and last packet switch, and 'device_model' offers device details. Network-related attributes include 'SRC_AS' and 'DST_AS' (BGP autonomous system numbers), 'INPUT_SNMP' and 'OUTPUT_SNMP' (input/output interface indices), 'IPV4_SRC_ADDR' (source IP), and 'MAC' (source MAC). Contextual details comprise 'category' (IoT or non-IoT), 'type' (device category), 'date' (date part of 'FIRST_SWITCHED'), and 'inter_arrival_time' (time between successive flows of the same device). Figure 1 represents the flow of the data in the research paper.

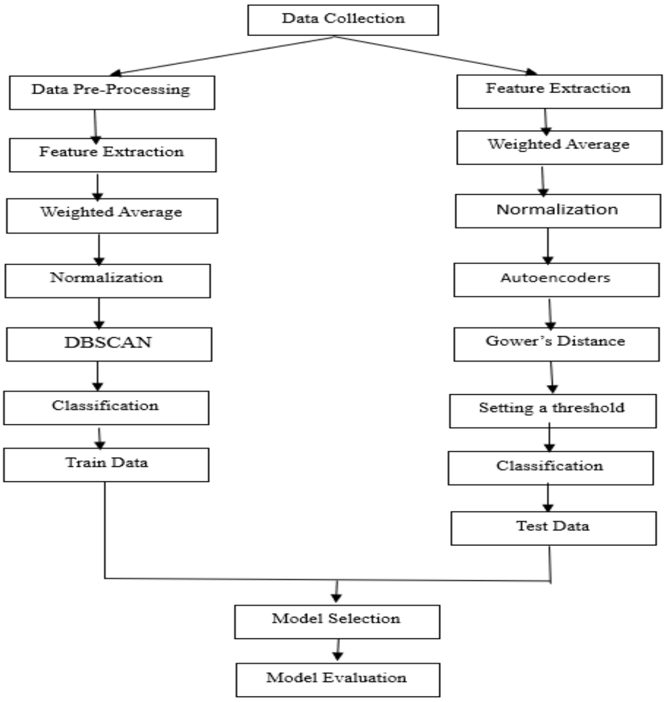


Fig 1. Flow Chart of the proposed work

B. Data Preprocessing

To recognize between vindictive and benign network traffic, a structured information processing and modeling approach has been utilized. The cycle begins with information preprocessing, where we examine dataset to understand its dimensions. In accordance with the scope of the problem statement, we remove non-IoT devices from the data set in order to concentrate the analysis on IoT devices.

In the initial data exploration, summary statistics performed for continuous variables namely 'First_switched,' 'in_bytes,' 'in_pkts,' 'last_switched,' 'duration,' and 'inter arrival time.' The step gains insights into the central tendencies and distributions of these variables. The constant columns that offer no significant variation or value to the dataset are eliminated. Columns such as 'src_as,' 'dst_as,' 'input_snmp,' 'output_snmp,' 'category,' and 'type' are removed as they possess a single constant value throughout, as it's irrelevant to the analysis. To facilitate subsequent analysis, we segment the data by device, saving each device's data in separate files. This preliminary data organization serves as a critical part of our preprocessing efforts. Moving to the modeling phase, we address the potential redundancy of certain variables within each device. then apply further data cleaning by detecting and removing constant functions that are likely to reappear. Additionally, we eliminate the 'IP address' feature, which contains unique values for each network flow, introducing unnecessary complexity into our models. Further data reduction includes the removal of the 'Partition' and 'Date' columns, contributing to a more streamlined dataset. This step minimizes dimensionality and optimizes the computational efficiency of our models.We also added Row_ID column to have an unique identifier.

IV. FEATURE ENGINEERING

A. Correlation Matrix

By creating a correlation matrix, the correlation between continuous variables are evaluated. To distinguish the strong correlations graphically, a correlation heatmap is created. The details are given in figure 2.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

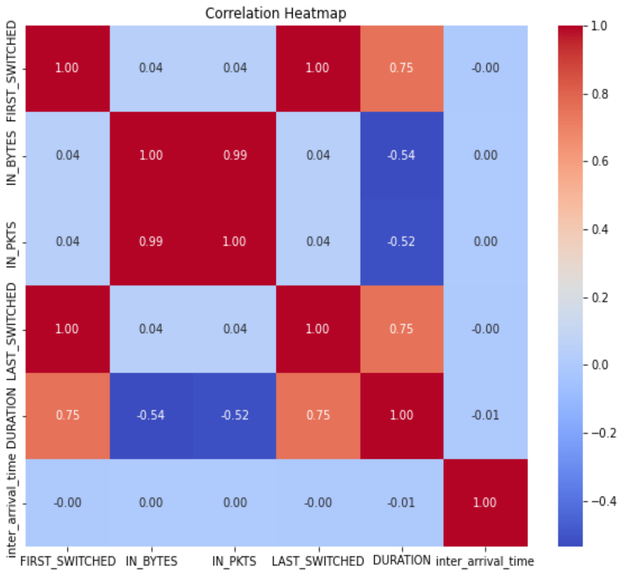


Fig 2. Correlation Heatmap of device_1

Notably, there is a significant correlation seen between "duration," "last_switched," and "first_switched." Since 'duration' indicates the time difference between 'First_switched' and 'last_switched,' we exclude these two columns as well as 'in_bytes,' because of the strong correlation with 'in_pkts.' Every IoT device goes through this methodical process of feature selection and data preprocessing, which customizes the dataset to the particular needs and traits of every device. Then finally arrive at a refined dataset that includes the following: "in_pkts," "protocol," "tcp_flags," "duration," and "inter arrival time." This dataset forms the basis for our subsequent modeling and analysis.

B. Handling multicollinearity

To address the multicollinearity among independent variables, the Variance Inflation Factor (VIF) technique has been employed. VIF finds and eliminates columns with high multicollinearity levels. In particular, the target variable with the greatest VIF value, which results in the removal of the variables "protocol" and "tcp_flag" because of their elevated VIF values. The dataset is filtered by the process, having left with only three important columns.

C. Weighted Average

To enhance the clarity and effectiveness of the data, a new column called "record frequency" has been introduced. This column basically indicates frequency of repetition of every row in the dataset, providing major insights into the patterns of the data.. For each and every column, the weighted average has been calculated. It is done by multiplying each column's value by the related "record frequency" using a mathematical formula. Weighted average is determined by

$$Weighted\ Average = \sum(wi * xi) / \sum wi \qquad (1)$$

In this case, wi is the weight associated with the i-th term, xi is the value of the i-th term, ∑wi is the sum of all weights, ∑xi is the sum of all values. The weighted average for each column is produced by the above given formula which functions as a meaningful representation of the properties of the data. The "record frequency" column is subsequently deleted since it has served its purpose of enhancing our dataset analysis.

V. MACHINE LEARNING

A. DBSCAN

DBSCAN is an unsupervised algorithm used to cluster the data with noise patterns and group data points into clusters. DBSCAN can handle nested clusters and it can handle outliers better than other clustering algorithms like kmeans clustering, by identifying dense regions and classifying data points that are not a part of any cluster as outliers. The algorithm's two main parameters are 'epsilon' and 'min_points'. The latter is effectively the radius of the circle and is the minimum amount of data points inside a circle that must be produced around each data point in order to estimate its density. We begin by applying the Density-Based Spatial Clustering with Noise (DBSCAN) calculation to cluster the information. Clusters are critical for distinguishing between benign and malicious traffic.After applying DBSCAN, we create cluster labels, denoted as 1, 2, and -1. The label -1 is reserved for identifying malicious traffic, while the remaining labels signify benign traffic. To improve visualization and understanding, Principal Component Analysis (PCA) on the scaled data has employed. This

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

transformation results in a two-component representation of the data, offering a clearer view of the dataset's variance and structure. Similar steps are applied to each device in the dataset. The details are given in figure3.

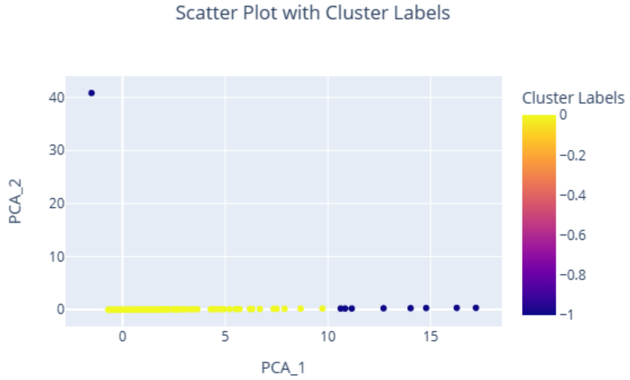


Fig 3. PCA plot of principal components of Device_1

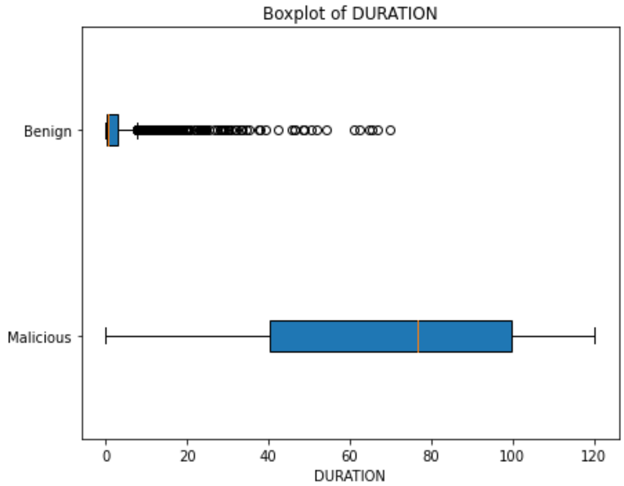


Fig 4. Box Plot Representation of Duration of Benign and Malicious traffic.

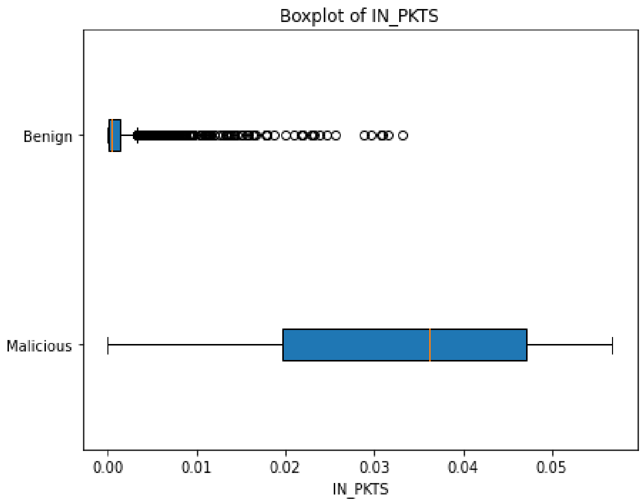


Fig 5. Box Plot Representation of Duration of Benign and Malicious devices

In figure 4, The case plot shows that the length of malignant traffic is higher than that of harmless traffic. In figure 5, the boxplot shows that the quantity of parcels in malignant rush hour gridlock is higher than in harmless rush hour gridlock.

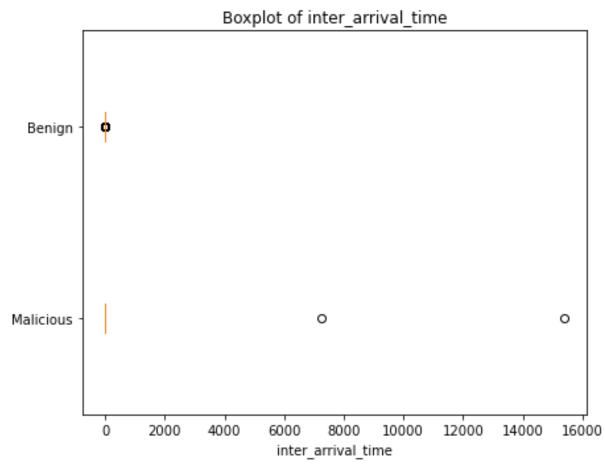


Fig 6. Box Plot Representation of Interarrival Time of Benign and Malicious Devices

Table 1: Number of malicious and benign records for each device.

Device Name	Epsilon value	Number of Malicious traffic records	Number of Benign traffic records
WebcamAmcrest	2.7	9	1662
SocketWemoInsight	0.5	11	613
SamsungWebcam	3	8	1107
Amazon.FireTVStick	0.2	5	434
Light_Bulb	2	13	1852
Speaker.Sonos	2	29	3933
Doorbell Ring	5	23	15504

In figure 6, the Malicious traffic tends to have a lower packet rate and more variation in the time between packets than benign traffic. Table 1 indicates the results of records of each device.

VI.DEEP LEARNING

A. Autoencoder

During the autoencoder phase, a neural network architecture to learn a compressed representation of the dataset. This unsupervised learning approach is especially helpful for dimensionality reduction. The goal of the autoencoder is to replicate the original input as nearly as possible by encoding and decoding the input data. Difference between encoded and decoded data is visualized using graphs. The details are given in figure 7. Measurements like Mean Squared Error (MSE) and Root Mean Squared Error (RMSE), which evaluate the contrast between the first and recreated information, shed light on how well the model catches examples and anomalies. With a Mean Squared Error (MSE) of 0.0005 and a matching Root Mean Squared Error (RMSE) of 0.0225, the model performs particularly well, showing exact reproduction and catching of basic information designs.

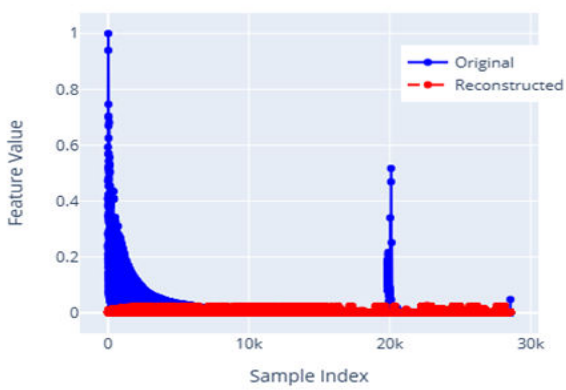


Fig 7. Plot of Original vs. Reconstructed data

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

B. Gower's Distance

Gower's distance is a metric which is used to measure how different two sequences or vectors are from each other. It was helpful in quantifying dissimilarity between original and reconstructed data in autoencoder to differentiate malicious and benign network traffic. The summary statistics of Gower's distance has been computed. The resulting graph of threshold values plotted against sample indices was helpful to choose the optimal threshold value which can effectively classify data into malicious and benign traffic based on Gower's distance values. The details are given in figure 8.

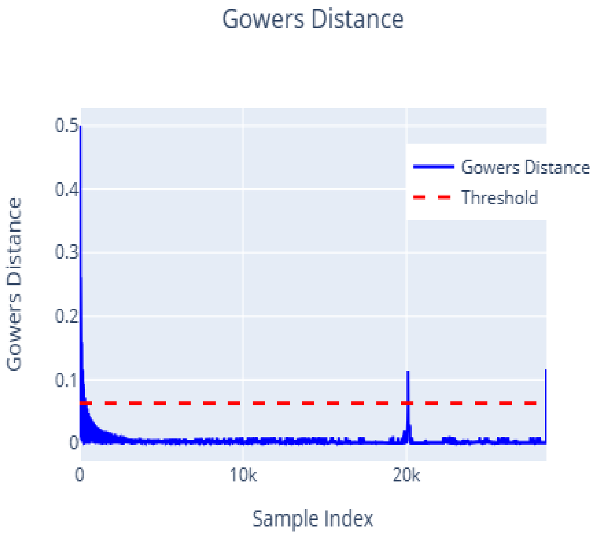


Fig 8. Plot of Gower's distance vs. sample index to determine threshold

VII. Performance evaluation

The labelled data obtained for each IoT device after applying DBSCAN is combined and the device names are label encoded. Missing values are addressed through imputation of mean for continuous variables and imputation of mode for categorical variables. Data having the labels obtained using autoencoder and Gower's distance is integrated. The training set was data obtained from DBSCAN and test data was data obtained from autoencoder.

The selection of Random Forest (RF) and Support Vector Machine (SVM) for classification is justified based on their unique strengths and compatibility with our dataset. Random Forest is chosen for its ability to capture diverse patterns within the integrated IoT dataset through ensemble learning. Additionally, Support Vector Machine is selected for its effectiveness in managing complex decision boundaries, complementing the clustering capabilities of DBSCAN and the unique insights from the autoencoder.

A. Model Evaluation

We obtained a remarkable precision of 0.99 for malicious traffic and a respectable 0.79 for benign traffic for Random Forest, yielding a total accuracy of 86.39%. The confusion matrix and the effectiveness of performance measures used in the research are given in table 2, 3 and 4. Furthermore, the recall values show that the majority of malicious cases may be accurately identified by the model (0.73 recall). The model's balanced performance is further reinforced by the F1 score, which is a harmonic mean of precision and recall. Values of 0.88 for benign and 0.84 for malicious traffic indicate this. SVM, Figure 9 on the other hand, had a better overall accuracy of 88.53%, with noteworthy recall (0.78 for malicious) and precision (0.82 for benign).

Table 2. Confusion Matrix for SVM

		Predicted	
		Class 0	Class 1
Actual	Class 0	27967	392
	Class 1	5444	22915

Table 3. Confusion Matrix for Random Forest

		Predicted	
		Class 0	Class 1
Actual	Class 0	28208	151
	Class 1	7570	20789

ISSN 2394 - 7780

The models' ability to reliably classify network traffic is demonstrated by their robust F1 ratings of 0.90 for benign and 0.87 for malicious traffic, underscoring their promise for efficient anomaly detection.

Table 4: Comparison between Random Forest and SVM

Models	Parameters	Benign	Malicious	Accuracy
Random Forest	Precision	0.79	0.99	86.39%
	Recall	0.99	0.73	
	F1 Score	0.88	0.84	
SVM	Precision	0.82	0.99	88.53%
	Recall	0.99	0.78	
	F1 Score	0.90	0.87	

VIII. CONCLUSION

The key observation of analysis is that the autoencoder has the ability to identify complex patterns in unprocessed data demonstrating comparable performance to DBSCAN. But the original data was label-deficient which makes it difficult to definitively validate the identified malicious traffic.

IX. FUTURE SCOPE

Future work includes Data Diversity, which is expanding the research to include a more varied dataset that encompasses different network settings, devices, and traffic kinds, to check if the proposed approach can be generalized across other network environments. Additional strategy is ensemble learning, which combines outputs from different detection methods and provides robust results.

REFERENCES

[1] Uelinton Brezolin , Andressa Vergutz , Michele Nogueira, A method for vulnerability detection by IoT network traffic analytics, 2022, Information Sciences of journals, volume 369,doi.org/10.1016/j.ins.2023.119000,

[2] Muhammad Shafiq , Zhihong Tian , Ali Kashif Bashir , Xiaojiang Du , Mohsen Guizani , IoT malicious traffic identification using wrapper-basedfeature selection mechanisms, Journal of Computers &Security, Volume 94, July 2020, doi.org/10.1016/j.cose.2020.101863,

[3] Xiaojiang Du, Zhihong Tian, Ali Kashif Bashir, Muhammad Shafiq, CorrAUC: a Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine Learning Techniques, , IEEE Internet of Things Journal, 15 June 2020 , doi.org/10.1109/JIOT.2020.3002255,

[4] Qingzhong Liu, Ashar Neyaz, Sundar Krishnan, IoT Network Attack Detection using Supervised Machine Learning, 2021, International Journal of Artificial Intelligence and Expert Systems,Volume:8,Issue:5, hdl.handle.net/20.500.11875/3245

[5] Marwa Keshk , Nickolaos Koroniotis , Nam Pham , Nour Moustafa, Benjamin Turnbull, Albert Y. Zomaya, An explainable deep larning-enabled intrusion detection framework in IoT networks, Journal of Information Sciences volume 639, August 2023, doi.org/10.1016/j.ins.2023.119000

[6] Psanju, Enhancing intrusion detection in IoT systems: A hybrid metaheuristics-deep learning approach with ensemble of recurrent neural network, Research Article ,Internet of Things Volume 21, April 2023, doi.org/10.1016/j.iot.2022.100656

[7] Adel Abusitta , Glaucio H.S. de Carvalho , Omar Abdel Wahab , Talal Halabi, Benjamin C.M. Fung , Saja Al Mamoori, Deep learning-enabled anomaly detection for IoT systems, Research Article ,Internet of Things Volume 21,April 2023,,doi.org/10.1016/j.iot.2022.100656,

[8] AROOSA HAMEED, JOHN VIOLOS, AND ARIS LEIVADEAS, A Deep Learning Approach for IoT Traffic Multi-Classification in a Smart-City Scenario, 22 February 2022 Volume 10 IEEE Journal, 10.1109/ACCESS.2022.3153331,

[9] Riccardo Lazzarini , Huaglory Tianfield , Vassilis Charissis, A stacking ensemble of deep learning models for IoT intrusion detection, 4 November 2023,Journal of Knowledge Based Systems Volume 279 doi.org/10.1016/j.knosys.2023.110941

[10] Z. Elkhadir, K. Chougdali, and M. Benattou, Intrusion Detection System Using PCA and Kernel, 16 April 2016, In Proceedings of the Mediterranean Conference on Information & Communication Technologies 2015, pp 489–497, vol 381, Springer, doi.org/10.1007/978-3-319-30298-0_50

[11] Mustafizur R. Shahid_, Gregory Blanc_, Zonghua Zhangy, Herv´e Debar__SAMOVAR, Anomalous Communications Detection in IoT Networks Using Sparse Autoencoders, September 2019 IEEE 18th International Symposium on Network Computing and Applications 10.1109/NCA.2019.8935007.

[12] Mingshu He, Xiaojuan Wang, Junhua Zhou, Yuanyuan Xi, Lei Jin and Xinlei Wang, Deep-Feature-Based Autoencoder Network for Few-Shot Malicious Traffic Detection, March 2021, Journal in Security and Communication Networks, :10.1155/2021/6659022

[13] Eirini Anthi, Lowri Williams, Małgorzata Słowinska, George Theodorakopoulos, A Supervised Intrusion Detection System for Smart Cities, July 2019, IEEE Internet of Things Journal, 10.1109/JIOT.2019.2926365

[14] Mrutyunjaya Panda, Ajith Abraham, Manas Ranjan Patra, A Hybrid Intelligent Approach for Network Intrusion Detection, 2012, International Conference, doi.org/10.1016/j.proeng.2012.01.827, Volume 30.

[15] Giuseppina Andresini, Annalisa Appice, Donato Malerba, Autoencoder-based deep metric learning for network intrusion detection, August 2021, Journal in Information Sciences volume 569, doi.org/10.1016/j.ins.2021.05.016.

[16] Mingze Song, Jing Ran, Shulan Li, Encrypted Traffic Classification Based on Text Convolution Neural Networks, 20 October 2019 IEEE 7th International Conference on Computer Science and Network Technology, 10.1109/ICCSNT47585.2019.8962493.

[17] Tie Luo_ and Sai G. Nagarajan, Distributed Anomaly Detection using Autoencoder Neural Networks in WSN for IoT, 24 May 2018, IEEE International Conference on Communications, 10.1109/ICC.2018.8422402.

[18] Zeeshan Ahmad, Adnan Shahid Khan, Cheah Wai Shang, Johari Abdullah, Farhan Ahmad, Network intrusion detection system: A systematic study of machine learning and deep learning approaches, 16 October 2020, Survey Paper, doi.org/10.1002/ett.4150

[19] Wei Ma, Analysis of anomaly detection method for Internet of things based on deep learning, 16 April 2020, Article in Transactions on Emerging Telecommunications Technologies Volume 31, doi.org/10.1002/ett.3893.

[20] Muhammad Shafiq, Xiangzhan Yu, Ali Kashif Bashir, Hassan Nazeer Chaudhry & Dawei Wang, A machine learning approach for feature selection traffic classification using security analysis, 27 January 2018, The Journal of Supercomputing.

[21] Meidan, Y., Sachidananda, V, Peng, H, Sagron, R, Elovici, Y, & Shabtai, A. IoT-deNAT: Outbound flow-based network traffic data of IoT and non-IoT devices behind a home NAT [Data set] 2020. In Computers & Security (1.0). Zenodo.//doi.org/10.5281/zenodo.3924770

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

IMAGE INPAINTING DETECTION APPROACHES: A REVIEW

Dhara Desai[1] and Dr. Rachna Patel[2]
[1]PHD Student, Computer Science & Engineering Department, [2]Computer Engineering Department, CGPIT, Uka Tarsadia University, Bardoli, Gujarat, India

ABSTRACT
Traditional photographs are replaced by digital images which is used everywhere in modern life. Due to which the demand of image editing tools is increased which makes image altering effortless without leaving any visible proof. Therefore, checking the image genuineness is necessary. In the absence of embedded watermarks or signatures the image forensic approaches are used to detect forgeries in digital images. Image Inpainting is a technique used for restoring digital images but due to easily available online as well as offline tools it can also be used to tamper images as a forgery method to remove an object without leaving any visible trace. Hence, developing techniques for detecting the presence of image forgery using inpainting is important. In this paper, study of different variety of image inpainting and inpainting detection approaches are given and compared based on the observations of existing state-of-art techniques.

Keywords: Forgery detection, digital image forensics, image inpainting, image inpainting detection, object removal, passive image forensics.

I. INTRODUCTION
"Seeing is believing" or "An image can speak a thousand words"- is well-known statement. This is probably why the digital image is one of the most used multimedia type on internet. Manipulation of image can be known as a very old approach as the photography itself. Nowadays 95% of online images are forged with the help of freely available online and offline tools [1].

As we know images are collections of redundant bits, by changing some of the bits, images can be modified easily which results in new challenges concerning illicit image manipulation. Hence, it is crucial to validate digital copies, authenticate their content and to identify the possibility of forgeries.

Here, we concentrate on a particular type of digital image forgery, i.e. image inpainting, where object removal is done by using pixels which are from the same image source. As pixels from same image are used to hide object removal it is difficult to discriminate between the forged and the original image, making detection of image inpainting forgery necessary.

In this paper, we will discuss about forensic security, types of image forgery based on tampering, which is followed by types of image inpainting techniques, tools available for inpainting and different methods used for image inpainting detection.

A. Forensic Security
Forensics is known as the application of analysis and investigation methods of collecting and protecting proof from a specific device in such a manner which is acceptable for demonstration in the court of justice. The part of science and technology which deals with identification of forgery and cyber-crime by investigating digital evidences is known as digital forensics. Digital image forensics is said to be a rising research area which aims at collecting information based on the history of an image to evaluate its reliability.

There are total six steps in forensic security which are explained in Fig. 1. It shows the sequence steps of digital forensics. It should be noted that the most crucial step here is evidence examination as the proof gathered here would be presentation as evidence in the court of law. Image inpainting detection falls into evidence examination step [2].

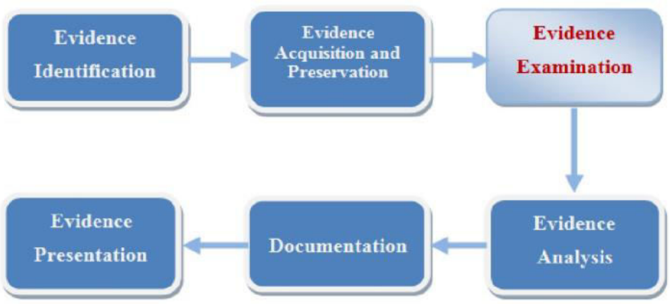


Fig. 1 Digital forensic multi-staged process

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

1) ***Evidence Identification:*** It is the first step of digital forensics in which evidence are collected according to the forgery cases. The evidence can be collected from the user phone, computer, USB, file, etc.
2) ***Evidence Acquisition:*** In this step the binary bitwise duplicate information is found out from the whole content collected during evidence identification.
3) ***Evidence Examination:*** Here encoded, hidden, missing or destroyed proofs are recovered from the evidence for further examination. Image forgery detection, camera identification and digital steganalysis come under evidence examination.
4) ***Evidence Analysis:*** It is used for assessment of possible rebuilding scenarios. It examines planned data with observation collected from incidents of crime.
5) ***Documentation:*** All the above steps are systematically documented and these documents are accessible in the court of justice as evidence.
6) ***Evidence Presentation:*** The prepared documents are presented in the court of justice. Often, this digital evidence is presented along with an expert witness for testifying in the court.

B. Digital Image Forgery Types

Digital image forgery approach has two categories namely, (i) Active approach and (ii) Passive approach.

Fig. 2 shows how active and passive approach of image forgery is further subdivided.

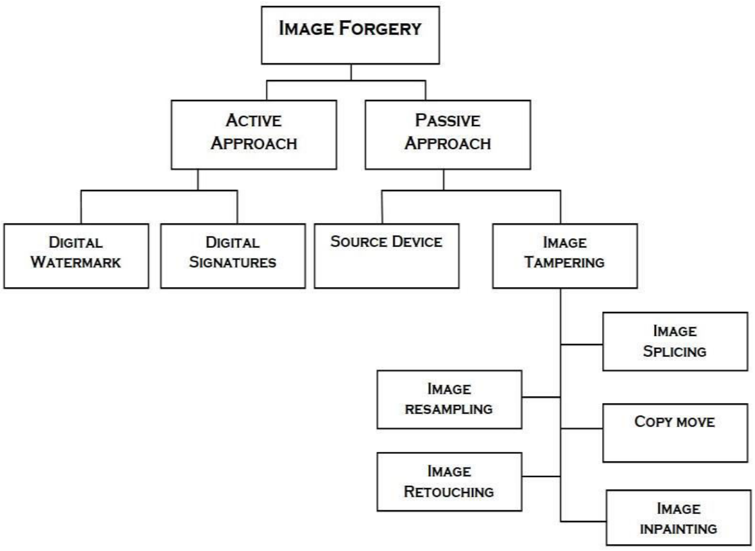


Fig. 2 Types of digital image forgery

1) ***Active approach:*** For validating the genuineness of the image it requires some prior information. I can be categorized into two kind of approach i.e., Digital Watermarking and Digital Signatures.

Digital watermark is a pattern of bits placed in an audio, video, or a digital image. Here the original image which is sent by the sender with the watermark or the digital signature is compared with the image received on the receiver side. This method requires prior knowledge about the image.

2) ***Passive approach:*** This approach uses the traces which are remaining after the processing steps during different stages of acquiring and storing of the digital images [1], [3], [4].

1. Image Inpainting

Inpainting is the technique to fill an unknown region of an image with information that could have been in the image in a visual possible way. Inpainting technique is used in various areas ranging from image and video editing, film restoration, deterioration reverse, removing obstructions such as subtitles, stamps, texts, watermarks, wrinkles, logos and the objects that are undesirable from the digital videos and/or images [5], [6].

Fig.3 defines image inpainting, here I is a frame in a video sequence or consider I to be the authentic image, which consist of a source area which is represented with Φ, whose pixel values are already known and a target area which is represented with Ω, presenting the region which is to be filled-in or damaged region which is to be repaired [5].

Both the target as well as the source region are non-overlapping areas, i.e. I= $\Phi \cup \Omega$, and $\delta\Omega$ stands for the border between the source and the target areas.

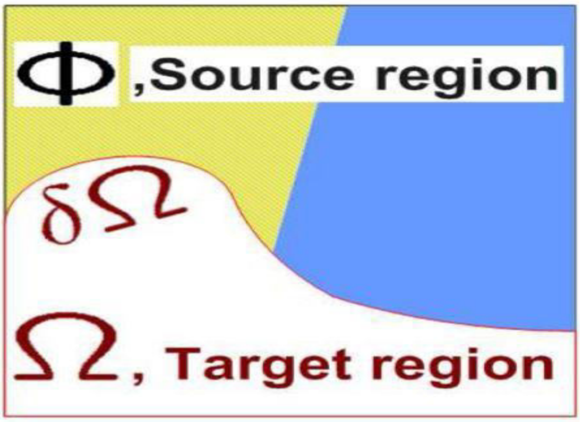


Fig. 3 Inpainting Definition [5]

A. Types of Inpainting

There is nothing like the 'perfect' inpainting algorithm, each method has its own advantages and drawbacks. These algorithms can be classified into one of six categories shown below in Fig. 4.

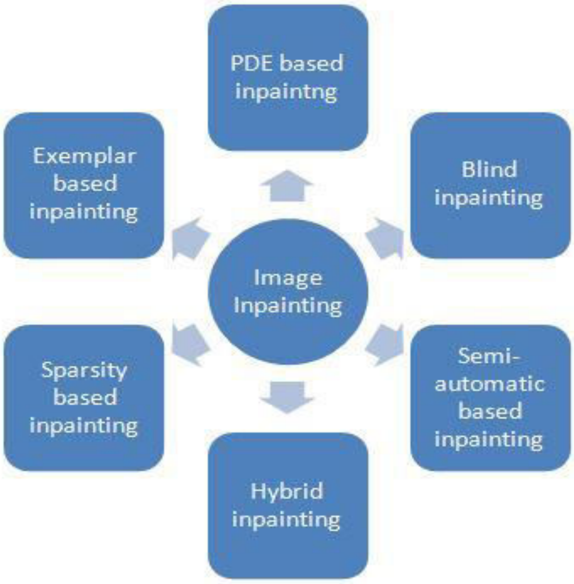


Fig. 4 Types of inpainting

1) ***PDE based Inpainting:*** The detail of the local structure is diffused or moved from the area which is familiar to an unfamiliar area. Many alternatives of algorithms based on PDE were presented on the base of the information of texture in the isotropic, anisotropic, nonlinear or linear directions. They are used to restore the long narrow regions such as lines or cracks. This technique is not appropriate for restoration of large texture regions that are unknown because of the presence of blur in the textured regions [6], [7].

2) ***Exemplar based Inpainting:*** This algorithm is easily and efficiently useful for inpainting of broad target areas. Here, the completion of structure process is done by use of texture synthesis i.e., from the known regions the patches are selected for restoring the target regions which are alike in structure with patches in the target regions which are partially unknown. The target regions are filled with alike known regions using global optimization cost and greedy functions [8].

3) ***Sparsity based Inpainting:*** Image is represented by sparse amalgamation of altered bases along with the presumption that both the unknown and the known image areas share the same sparse representations. Thus, the pixels which are missing are filled by adaptively updating sparse representations. In the sparse representations, choosing of the dictionary is essential. The dictionary may be adaptive/content dependent or it may be fixed like DWT, DCT etc. or [9].

4) ***Hybrid Inpainting:*** It is a mixture of structural and texture based inpainting algorithms. The concept about hybrid inpainting algorithms is that the regions of inpainting is separated into two different types, texture region and structure region. Combination of structural texture based techniques and edge propagation techniques are used to fill the decomposed parts[10].

5) ***Semi-automatic Inpainting:*** The region of inpaint is completed by user assisting the system by providing structural guidelines. In this method the user provides details related to the gaps which are missing by use of a regional sketch which surrounds the inpaint region boundaries, than for filling of the missing portions an inpaint algorithm based on texture is used. [11].

6) ***Blind Inpainting:*** Here there is no user interaction required by the regions which are to be inpainted. As a matter of fact, algorithms which are in this group execute inpainting in the absence of any prior information or detection of the pixels that are missing. The image which is given as input is assumed to be as noisy and recovery of the image is performed by taking into consideration that all pixels in the image are corrupted by noise or whenever there is some struggle in the selection of the corrupted i.e. missing pixels the degradation models are used [12], [13].

Table I. Comparision of Inpainting Techniques

Image Inpainting techniques	Advantages	Disadvantages
PDE based image Inpainting	• Works well for small region to be inpainted and application to remove noise.	• It cannot fill the large missing region due to diffusion process having blurring effect. • The pixels which are on the edges handled well.
Exemplar based image inpainting	• It perform well for large missing region and can inpaint both structure and textured image.	• The structure that are curved cannot be handled well.
Sparsity based image inpainting	• Without blurring the artifacts it can restore large missing regions.	• Some artifacts are generated in the output image.
Hybrid inpainting	• It can reconstruct large area completion and effects less to the edges of the inpainted region	• Missing region consists needs to be of simple texture and structure to work well.
Semi-automatic based image inpainting	• It maintains good curvature.	• If the structure is complex or natural image it does not perform well.
Blind inpainting	• It can reconstruct both small and large region.	• In flat and similar regions it detects unexpected matches.

Table I show the comparison between inpainting techniques with its advantages and disadvantages.

B. Online tools for inpainting

There are many online tools available for applying inpainting technique on images. Some of the famous tools that are widely used are as follows:

- **Inpaint photo restoration software**

Developed by Teorex, this tool will fill the selected area with textures pulled from the surrounding image data. They also provide tutorials for using the tool [14].

- **Content-Aware Fill in Photoshop**

Developed by Adobe Photoshop, it provides user with an interactive editing experience which provides control over the sampling area. Also, a preview of output result is available on a new layer [15].

- **GIMP Inpainting Plug-In (Resynthesizer)**

It is part of open-source tool GNU Image Manipulation Program. It is helpful in removing unwanted objects from photos, transfer or repeat textures. You can also add vertical or horizontal tiles and as per your liking you can also restore the image. [16].

- **Wondershare fotophire**

Developed by Wondershare, it erases unwanted objects while automatically repairing the surrounding [17].

III. Image Inpainting Detection

Inpainting has been used for tampering of digital images, which includes removal of object and filling the region to hide the meaning by concealing the truth. Various types of tampering have been uncovered successfully still there are only few studies which addresses inpainting forgery detection in images.

Until recently, only few works are reported about detection of image inpainting. The first approach was proposed by [18], Wu et al. as a detection technique for forgery based on exemplar image inpainting. The identification of forged region is done using fuzzy membership by use of zero-connectivity labelling to get the similarity of the blocks in doubtful regions. Here, the doubtful regions are required to be selected manually. Also, there is high computation complexity when there is a full search of suspicious blocks. After that, Bacchuwar et al. [19] designed a forgery detection approach using jump patch-block matching which helps to decrease the computation costs, still it is a semi-automatic method. Chang et al. [20] introduced exemplar-based image inpainting forgery detection algorithm which is automatic. Zero-connectivity features are used to locate the suspicious regions and to identify the forged areas a multi-region relation technique is used. Yang et al. [21] presented an approach that uses mapping of central pixels to speedup searching of doubtful blocks and the blocks of image are mapped to hash table. The pairs of block that are similar are explored by similar hash values. To find the removal of object by using inpainting based on exemplar technique with or without the use of post-processing which is hybrid procedure and an improved method is proposed. The technique is used to find out if a given image is inpainted or not inpainted. Also, they are addressed to achieve robustness against post-processing operations. Especially, relationship between the adjoining DCT coefficients are modelled using the joint probability density matrix and for blind detection of forgery some statistical features are designed. Here, the detecting of inpainting in the image without use of post-processing is known as first focus and the second is to achieve robustness to post-processing so the hybrid method is look forward to complete the desired production for detecting of removal of object with the use of inpainting based on exemplar technique with or without post-processing. Liang et al. combined the greatest zero-connectivity component labelling, fragment splicing and central pixel mapping into a joint framework for detection which achieved high efficiency [22], [23].

Li et al. [25] studied diffusion-based inpainting detection. After reviewing the process for diffusion-based image inpainting the authors discovered that the isophote direction is preserved here. So, the extraction of feature set is done on the base of change occurred in the image Laplacians along the way of the interferences namely, scaling, rotation, gamma correction and JPEG compression. Here, the experimental results show high performance. In general, satisfied results are obtained in small regions when using the diffusion-based inpainting. When the parts that are missing from the image are complex or large, it some blurring artifacts are caused. It gives bad outcome when redesigning is done in processing the images which has continuous parts (cartoon-like) [25]. One more type of inpainting is based on sparsity. Su et al. showed sparsity-based inpainting has a possible relation with CCA. A novel objective function was proposed to intensify the inter-class dissimilarity. When the comparison with other techniques is done based on results of detection better performance is seen in the outcome. [26].

Table II. Comparision of Inpainting Detection Techniques

Paper Title and Year of Publication	Inpainting Detection Type	Approach Used	Cons/ Future Work
Robust Image Inpainting Forensics by Using an Attention-Based Feature Pyramid Network [2023]	Blind inpainting	Attention-based feature pyramid network (AFPN)	Not good for images with complicated graphs
Image Inpainting Detection Based on	Blind inpainting	High-pass filter attention full	Make the method more generalized

 ISSN 2394 - 7780

High-Pass Filter Attention Network [2022]		convolutial network (HPACN)	by training dataset using more inpainting algorithms.
Semantic Segmentation-Based Image Inpainting Detection [2021]	Blind inpainting	Semantic segmentation-based CNN model	Can train the model for detection of splicing and copy-move.
IID-Net: Image Inpainting Detection Network via Neural Architecture Search and Attention [2021]	Blind inpainting	Deep neural network	Data augmentation at the training phase by considering various distortions could be a viable solution for improving the robustness
GIID-Net: Generalizable Image Inpainting Detection Network [2021]	Blind inpainting	Consists of three subblocks: the enhancement block, the extraction block and the decision block.	Can be made more generalized to detect other types of digital image forgeries.
Image Inpainting Detection Based on Multi-task Deep Learning Network [2020]	PDE, Exemplar based and Deep learning	Back connections and Feature Pyramid Networks	ROI pooling on features increases computational burdens
Robust detection for object removal with post processing by exemplar based image inpainting [2018]	Exemplar based	LBP, GLCM & Image gradient	Detect inpainting in presence of JPEG and Blur, Provides only binary judgement and does not locate the area of inpainting
Sparsity-Based Image Inpainting Detection via Canonical Correlation Analysis With Low-Rank Constraints [2018]	Sparsity based	CCA	Better result in case of JPEG post processing, Detection performance can be improved by integrating other techniques
Localization of Diffusion-Based Inpainting in Digital Images [2017]	Diffusion based	Change in image laplacian, Local variance	Robustness for JPEG post processing needs to be improved
Exposing Inpainting Forgery in JPEG Images under Recompression Attacks [2016]	Blind inpainting	Use ensemble learning and features from DCT domain	Inpainting detection is only for JPEG images.
Blind Inpainting Forgery Detection	Exemplar based	Patch matching using Kd-tree	Unexpected matches flat or

[2014]		algorithm	similar regions.
A jump patch-block match algorithm for multiple forgery detection [2013]	Exemplar based inpainting and Copy-Move Forgery	Luminance component	Also detects copy move forgery, Performance with post processing operations needs to be checked
A forgery detection algorithm for exemplar-based inpainting images using multi-region relation [2013]	Exemplar based	Zero connectivity and Vector filtering	Can also detect copy move forgery, Unable to work with post processing operations.
Detection of digital doctoring in exemplar-based inpainted images [2008]	Exemplar based	Fuzzy membership function and Zero connectivity	Manual selection of suspicious region, It can only be applicable to uncompressed images.

Table II shows that inpainting detection can be categorized into three types on the base technique which is used for object removal from the image as follows:

1. Detection of exemplar-based image inpainting
2. Detection of sparsity-based image inpainting
3. Detection of diffusion-based image inpainting

This classification is due to the type of method used for object removal from the original images and from study it is concluded that exemplar based inpainting method is the most popular and widely used method for removal of object from an image.

IV. CONCLUSIONS

This paper provides a brief overview of types of forgery, different categories of inpainting approaches and their analysis and comparative study of popular image inpainting based forgery detection algorithms and possible contributions.

It can be concluded that there is more work done in exemplar based inpainting detection which is used to inpaint object of large size and comparatively less work is done in the area of diffusion based and inpainting detection based on sparsity. The inpainting based on diffusion is used when the region which is to be inpainted is small in size which is not fit for object removal forgery. It is also observed that sparsity based inpainting can overcome the disadvantage of previous work but it lacks performance in case of JPEG compression.

REFERENCES

[1] V. P. Nampoothiri and N. Sugitha, "Digital Image Forgery - A threaten to Digital Forensics", IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT), Pp. 1-6, 2016.

[2] Raghavan, S, "Digital forensic research: current state of the art", CSIT 1, Pp. 91-114, Issn(Online): 2277-9086 Issn(Print): 2277-9078, 2013.

[3] Tulsi Thakur, Kavita Singh, and Arun Yadav, "Blind Approach for Digital Image Forgery Detection", International Journal of Computer Applications, Vol. 179, Issue. 10, Issn: 0975 - 8887, January 2018.

[4] J. A. Redi, W. Taktak, and J.-L. Dugelay, "Digital image forensics: A booklet for beginners," Multimedia Tool Appl., Vol. 51, Issue. 1, Pp. 133-62, Issn(Online): 1573-7721 Issn(Print): 1380-7501, Jan. 2011.

[5] M. Bertalmio, G. Sapiro, V. Caselles, and C. Ballester, "Image inpainting," In Proc. 27th Annual Conf. Computer Graphics and Interactive Techniques, , Pp. 417-424, New York, USA, 2000.

[6] T. F. Chan and J. Shen. "Non-texture inpainting by curvature driven diffusion," J. Visual Comm. Image Rep., Vol. 12, Issue. 4, Pp. 436-449, 2001.

[7] Tschumperl´e D., Deriche R, “Vector-valued image regularization with pdes: a common framework for different applications,” IEEE Trans. on PAMI, Vol. 27, Pp. 506-517, April 2005.

[8] A Criminisi, Prez P and Toyama K “Region filling and object removal by exemplar-based image inpainting,” IEEE Trans Image Process Vol. 13, Issue. 9, Pp.1200-1212, Sep 2004.

[9] Z.Xu and J.Sun,“Image inpainting by patch propagation using patch sparsity,” IEEE Transactions on Image Processing, Vol. 19, Issue.5, Pp.1153-1165, 2010.

[10] M. M. Oliveira, B. Bowen, R. McKenna, and Y.-S. Chang, “Fast digital image inpainting,”in Proc. Int. Conf. Vis., Imag. Image Process., Marbella, Spain, Pp. 106-107, Sep 2001.

[11] A. Telea, “An image inpainting technique based on the fast marching method,” J. Graphics Tools, Vol. 9, Issue. 1, pp. 25-36, 2004.

[12] A. Bugeau, M. Bertalmio, V. Caselles, and G. Sapiro, “A comprehensive framework for image inpainting,” IEEE Trans. Image Processing, Vol. 19, Issue. 10, Pp. 2634-2645, Oct. 2010.

[13] J. Stark, M. Elad, and D. Donoho, “Image decomposition via the combination of sparse representations and variational approach,” IEEE Trans. Image Processing, Vol. 14, Pp. 1570-1582, Issn: 1057-7149, Oct. 2005.

[14] Inpaint photo restoration software.[online] Available: www.theinpaint.com [Last Accessed on 28 February 2020]

[15] Adobe photoshop inpainting plugin [online] Available: www.inhelpx.adobe.com/in/photoshop/using/content-aware-fill.html [Last Accessed on 29 February 2020].

[16] GIMP inpainting plugin [online] Available: www.inpaintgimpplugin.github.io [Last Accessed on 29 February 2020].

[17] Wondershare fotophire [online] Available: www.photo.wondershare.com/photo-eraser.html [Last Accessed on 01 March 2020].

[18] Q. Wu, S.-J. Sun, W. Zhu, G.-H. Li, and D. Tu, ‘‘Detection of digital doctoring in exemplar-based inpainted images,’’ in Proc. Int. Conf. Mach. Learn. Cybern., Vol. 3, Pp. 1222-1226, Jul. 2008.

[19] K. S. Bacchuwar, A. Deep, and K. R. Ramakrishnan, ‘‘A jump patch block match algorithm for multiple forgery detection,’’in Proc.Int.Multi Conf. Autom., Comput., Commun., Control Compress. Sens. (iMac4s), Pp. 723-728, Mar. 2013.

[20] I.-C.Chang, J.C.Yu, and G.C.-C.Chang,‘‘A forgery detection algorithm for exemplar-based inpainting images using multi-region relation’’, Multimedia Tools and Applications, Vol. 31, Issue. 1, Pp. 57-71, Issn: 1077-3142, 2013.

[21] G. Yang, Z. Dengyong and L. Zaoshan,‘‘A robust forgery detection algorithm for object removal by exemplar-based image inpainting, Vol. 77, Pp. 11823–11842, Issn: 1077-3142, 2018.

[22] Zaoshan Liang, Gaobo Yang, Xiangling Ding and Leida Li "An efficient forgery detection algorithm for object removal by exemplar-based image inpainting", J Vis Commun. Image R, Elsevier, vol. 30, Pp. 75-85, Issn: 1077-3142, 2015.

[23] D. Zhang, Z. Liang, G. Yang, Q. Li, L. Li, and X. Sun, ‘‘A robust forgery detection algorithm for object removal by exemplar-based image inpainting,’’ Multimedia Tools Appl., Vol. 77, Issue. 10, Pp.11823-11842, Issn(Online): 1573-7721 Issn(Print): 1380-7501, May 2018.

[24] O. Le Meur, J. Gautier, and C. Guillemot, “Examplar-based inpainting based on local geometry,” in Proc. IEEE Int. Conf. Image Processing (ICIP), Pp. 3401–3404, Sept. 2011.

[25] Wang J, Lu K and Pan D, “Robust object removal with an exemplar-based image inpainting approach,” Neurocomputing, Vol. 123, Pp. 150–155, Issn: 0925-2312, Jan 2014.

[26] P. Buyssens, M. Daisy, D. Tschumperlé, and O. Lézoray, “Exemplar based inpainting: Technical review and new heuristics for better geometric reconstructions,” IEEE Trans. Image Process., Vol. 24, Issue. 6, Pp. 1809-1824, Issn: 10577149, Jun. 2015.

[27] H. Li, W. Luo, and J. Huang, “Localization of diffusion-based inpainting in digital images,” IEEE Trans. Inf. Forensics Security, Vol. 12, Issue. 12, Pp. 3050-3064, Issn: 15566013, Dec. 2017.

[28] X. Jin, Y. Su, L. Zou, Y. Wang, P. Jing, and Z. Wang, “ Sparsity-based Image Inpainting detection via Cannonical Correlation Analysis With Low-Rank Constraints,” IEEE Access, Vol 6, Pp.49967-49978, Issn: 21693536, Sept. 2018.

[29] D. T. Trung, A. Beghdadi and M. Larabi, "Blind inpainting forgery detection," 2014 IEEE Global Conference on Signal and Information Processing (GlobalSIP), Pp. 1019-1023, , Atlanta, GA, 2014.

[30] Kakar P and Sudha N, "Exposing post processed copy-paste forgeries through transform-invariant features". IEEE Trans Inf Forensics Security, Vol. 7, Issue. 3, Pp. 1018-1028, Issn: 15566013, 2012.

[31] Cozzolino D, Gragnaniello D and Verdoliva L, "Image forgery detection through residual-based local descriptors and block-matching", IEEE International conference on image processing (ICIP), Pp 5297-5301, 2014.

[32] Guang-Hai Liu and Jing-Yu Yang, “Content-based image retrieval using computational visual attention model”, Pattern Recognition, Vol. 48, Issue. 8, Pp. 2554-2566, Issn: 00313203, 2015.

[33] Gong S., Liu C., Ji Y., Zhong B., Li Y. and Dong H., *Advanced Image and Video Processing Using MATLAB*, Springer International Publishing, 2019.

[34] Padalkar M.G., Zaveri M.A., Joshi M.V., “*SVD Based Automatic Detection of Target Regions for Image Inpainting*”, Lecture Notes in Computer Science, Vol. 7729, Berlin, Heidelberg, Springer, 2012.

[35] Satoshi Iizuka, Edgar Simo-Serra, and Hiroshi Ishikawa, "Globally and Locally Consistent Image Completion", ACM Transaction on Graphics, Vol. 36, Issue. 4, Issn. 0730-0301, July 2017.

[36] Padalkar M.G., Joshi M.V., Zaveri M.A., Parmar C.M., “Exemplar based inpainting using autoregressive parameter estimation.”, In: Proceedings of the International Conference on Signal, Image and Video Processing, IIT Patna, India, Pp. 154-160, 2012.

[37] M. A. Qureshi and M. Deriche, "A bibliography of pixel-based blind image forgery detection techniques", Image Communication, Elsevier Science Inc, Vol. 39, Pp. 46–74, Issn: 0923-5965, Nov 2015.

[38] Fatih Yavuz, Abdullah Bal, and Huseyin Cukur "An effective detection algorithm for region duplication forgery in digital images", Proc. SPIE 9845, Optical Pattern Recognition XXVII,20 April 2016.

[39] X. Pan and S. Lyu, "Region Duplication Detection Using Image Feature Matching," in IEEE Transactions on Information Forensics and Security, Vol. 5, Issue. 4, Pp. 857-867, Issn(Online): 1556-6021 Issn (Print): 1556-6013, Dec. 2010.

[40] P. Tiefenbacher, V. Bogischef, D. Merget and G. Rigoll, “Subjective and Objective Evaluation of Image Inpainting Quality”, in Proc. ICIP, IEEE, 2015.

[41] H. Wu and J. Zhou, "GIID-NET: Generalizable Image Inpainting Detection Network," IEEE International Conference on Image Processing (ICIP), Anchorage, AK, USA, Pp.3867-3871, Issn(Online): 2381-8549 Issn (Print): 1522-4880, 2021.

[42] H. Wu and J. Zhou, "IID-Net: Image Inpainting Detection Network via Neural Architecture Search and Attention," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 32, no. 3, Pp. 1172-1185, Issn(Online): 1558-2205 Issn (Print): 1051-8215, March 2022.

[43] Q. Liu, A. H. Sung, B. Zhou and M. Qiao, "Exposing Inpainting Forgery in JPEG Images under Recompression Attacks," 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), Anaheim, CA, USA, Issn(Online): 1558-2205 Issn (Print): 1051-8215, Pp. 164-169, 2016.

[44] Kumar, N., Meenpal, T., “Semantic Segmentation-Based Image Inpainting Detection”, Innovations in Electrical and Electronic Engineering. Lecture Notes in Electrical Engineering, Springer, Singapore, vol 661, Isbn(Online): 978-981-15-4692-1 Isbn(Print): 978-981-15-4691-4, 2020.

[45] Chen, Z.; Zhang, Y.; Wang, Y.; Tian, J.; Wu, F. “Robust Image Inpainting Forensics by Using an Attention-Based Feature Pyramid Network.” Appl. Sci., ISSN 2076-3417, 2023.

[46] Xinyi Wang, Shaozhang Niu & He Wang, “Image Inpainting Detection Based on Multi-task Deep Learning Network”, IETE Technical Review, 38:1, 149-157, ISSN(Online): 0974-5971, ISSN(Print): 0256-4602, 2021.

[47] C. Xiao, F. Li, D. Zhang, P. Huang, X. Ding *et al.*, "Image inpainting detection based on high-pass filter attention network," *Computer Systems Science and Engineering*, vol. 43, no.3, pp. 1145–1154, ISSN(Print): 0267-6192**,** 2022.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

FORECASTING THE FUTURE: A NOVEL COMPREHENSIVE REVIEW OF DIABETES PREDICTION USING MACHINE LEARNING ALGORITHMS

Ms. Jahnavi Desai[1], Dr. Rachna Patel[2] and Ms. Mithila Sompura[3]
[1, 2, 3]Computer engineering department C.G.Patel Institute of Technology Uka Tarsadia University Bardoli, Surat, Gujarat, India

ABSTRACT

Diabetes is a widespread and persistent health condition caused by family history, genes, inactivity, obesity, age, insulin resistance, polycystic ovary syndrome, gestational diabetes, high blood pressure, sedentary lifestyle, pancreatitis, weight and so on. These causes affect millions of individuals worldwide, posing significant challenges for healthcare systems. Timely diagnosis and diabetes prediction can facilitate early interventions and personalized care, ultimately improving patient outcomes. This literature review explore the various application and algorithms of machine learning(ML) models for diabetes detection, classification, and prediction. The review involves the potential of various ML models, such as LASSO, SVM, XGBoost, RF, and ANN, to separate T2D from NGT. It also emphasizes how feature selection methods may effectively reduce the dimensionality of datasets. According to the study, binary classifiers that are trained from scratch may accurately predict the start of diabetes. This concept is used in a neural network-based method with an accuracy of roughly 86% and a ROC AUC value of 0.934. Additionally, the review examines the use of ML classifiers such as SVM, decision trees(DT), gradient boosting classifiers, KNN, random forests(RF), AdaBoost classifiers, and extra trees classifiers, as well as preprocessing datasets such as PIMA and BRFSS. Furthermore, the study introduces the RFWBP strategy, which outperforms standard methods and 5-fold cross-validation is used to achieve a fantastic accuracy of 95.83%. The review also discusses an ensemble-based machine learning framework, SMOTE, where random forest achieves a remarkable 98.37% accuracy in diabetes prediction. Finally, the study compares all these classifiers and concludes that random forest exhibits superior performance.

Keywords: Diabetes, machine learning, neural network, artificial intelligence, Pima, BRFSS,

I. INTRODUCTION

High blood glucose is a significant characteristic of diabetes mellitus, a long-term metabolic condition. Biomedical problems for creation of data-driven solutions has seen a wide acceptance of ML techniques, especially deep learning techniques, recently due to the availability of large volumes of clinical and molecular data. These techniques offer a variety of statistical and mathematical models with the use of labeled datasets for supervised learning that may be used for prediction of the label or class of newly added data instances. By locating characteristics or parameters in training datasets that might substantially influence the models' predictions, they can also be used for feature selection [1]. According to the most recent estimate, in 2017 there were 425 million diabetics worldwide. By 2045, this number is predicted to increase to 629 million as a output of the majority of physical and sedentary lifestyles, bad nutrition, inactivity, and genetic.

Over the course of more than 20 years, the world health organization(WHO) announced that over 77 percent of patients have developed serious instances of diabetes mellitus [9]. Detection and prediction of diabetes in prior is crucial to manage and intervene effectively. Machine learning (ML) and artificial intelligence (AI) technologies in recent study may revolutionize diabetes diagnosis and prediction. This review compiles research results from several studies and offers insightful information about how ML algorithms are being used for early prediction of diabetes diseases. The review discusses specific methodologies, challenges, and advancements to contribute to the ongoing discourse surrounding optimizing predictive models for diabetes diagnosis.

II. LITERATURE REVIEW

To detect key features connected to the development of insulin resistance(IR) and type 2 diabetes(T2D) Aditya Saxena et al. [01] used the Least Absolute Shrinkage and the Selection Operator(LASSO) feature selection technique. To train 5 well defined machine learning models: LASSO, SVM, XGBoost, RF, and Artificial Neural Network(ANN) the expression patterns of these genes were used. The ANN model performed excellently, with an Area Under the Curve(AUC) greater than 95% and across 64 samples of human adipose tissue, the notable efficacy in distinguishing diabetic individuals from those with standard glucose tolerance (NGT) in the test dataset, with an accuracy of 73%. Antonio Garca-Domnguez et al. [02] investigated various diabetes detection models.The study included evolutionary algorithms and the Akaike Information Criterion, two advanced feature selection methods. Six well-known classifier algorithms were used methodically with these methodologies. The resulting models, which combine clinical and paraclinical aspects, were rigorously assessed and compared with current methodologies. The outcomes demonstrated a notable enhancement in performance, exhibiting accuracy levels of 94%.

Antonio Agliata et al. [03] employed a binary classifier to look for potential nonlinear relationships between data from patient measurements and the onset of type 2 diabetes. The following algorithms were considered in this study: SGD, RSM-prop, Adam and Levenberg-Marquardt(LM). The results of this investigation were encouraging, demonstrating the model's ability to attain accuracy rates of up to 86% and a Receiver Operating Characteristic Area Under the Curve(ROC AUC) value of 0.934. Subhash Chandra Gupta et al. [04] built four unique models, each based on a dataset collected called the PIMA Indian dataset using various preprocessing techniques. K-nearest neighbors(KNN), DT, RF, and Support Vector Machine(SVM) classification algorithms were used for each model. Moreover, classifier hyperparameters were carefully tweaked to improve model performance. Out of all the classifiers that were used, With an accuracy of 88.607%, F1 score of 75.679% and the RF classifier outperformed all the other classifiers.

Research studies have been conducted to find the most efficient and effective ML algorithm for predicting diabetes based on various patient symptoms. Atadjanova Nozima Sultan-Muratovna et al. [05] utilized the Super Vector Machine algorithm on a Pima Indian dataset. They found that the linear kernel demonstrated optimal performance with an accuracy score of 77 per centShu Wang et al. [06] preprocessed the data using the synthetic minority oversampling technique and the K Nearest Neighbour algorithm.The backpropagation neural network model, with accuracy of 93.7%, precision of 94.6%, and recall of 92.8%, was shown to have the best prediction performance.

Sethupathi M et al. [07] utilized the Pima Diabetes Dataset and discovered that Logistic Regression emerged as the most effective, with a notable accuracy level of 78.01%. Linh Phuong Nguyen et al. [08] utilized a dataset collected from individuals in Vietnam who had been diagnosed with type 2 diabetes. They discovered that the Random Forest Classifier method produced lucky results, achieving a surprising 100% accuracy rate and a cross-validation score of 0.998.

Md Shahin Ali et al. [09] applied the RFWBP classifier, which demonstrated an accuracy of 95.83%, surpassing the performance of conventional machine learning methods. Önder YAKUT et al. [10] utilized the Pima Indian Diabetes database for diabetes prediction. They discovered that the suggested strategy with the best prediction accuracy, at 81.71%, was the Random Forest Classifier.

Zaigham Mushtaq et al. [11] procured the dataset for this study from an online repository. They found that Random Forest algorithm come up as the most effective after balancing the dataset using the SMOTE oversampling technique, they discovered that Random Forest worked best. Khoula Al-Sadi et al. [12] created AI and machine learning prediction models to diagnose Type 2 Diabetes Mellitus (T2DM) in Omani patients more quickly and accurately. They found that the decision tree models and RF outperformed all other methods, with the RF model achieving a excellent accuracy of 98.38% for the Omani dataset.

Methaporn Phongying et al. [13] conducted a comparative analysis of diabetic classification models. A 97% F1-score, 96.6% recall, 97.5% accuracy, and 97.4% precision were attained by the random forest classifiers, which were discovered to have the best performance among the suggested models with interaction terms. J. Jeba Sonia et al. [14] utilized a 768-patient Pima Indian dataset uploaded via Kaggle. They found that the proposed multi-layer neural network achieved maximum sensitivity and specificity values of 0.97 and 0.95, respectively, and provided an outstanding accuracy score of 97%.

Orlando Iparraguirre-Villanueva et al.[15] used A dataset of 768 patients was utilized by Orlando Iparraguirre-Villanueva et al.[15] to predict patients with diabetes. They employed five machine learning models and to address class imbalance the Synthetic Minority Over-sampling Technique(SMOTE). The K-nearest neighbour model demonstrated the highest accuracy in identifying diabetes after using SMOTE, obtaining 79.599%. After testing several ML algorithms for diabetes prediction, Aaditi Ranganath Satam et al.[16] logistic regression was the most successful, with a 79% accuracy rate.

MD conducted a survey. Jamal Uddin et al. [17] to discover how common diabetes is in Bangladesh. They used Random Oversampling (ROS) and to address class imbalance the SMOTE. The ensemble technique (ET) come up as the outstanding classifier, and their proposed method achieved an accuracy of 87.6%. Entissar S. Almutairi et al.[18] explored the effectiveness of diverse classification methods in discerning diabetes prevalence rates and predicting associated trends. Compared to other classification techniques, weighted KNN required less training time and achieved the greatest average accuracy of 94.5% when it came to predicting diabetes prevalence rates.

ISSN 2394 - 7780

For use in the Internet of Medical Things(IoMT) environment a ML based e-diagnosis system was proposed by Victor Chang et al. [19], with an emphasis on type 2 diabetes mellitus diagnosis. The Naive Bayes model performs well, with an accuracy of 79.57%. Mariwan Ahmed Hama Saeed et al.[20] applied machine learning models to identify chronic diabetes disease. Among these models, the extra trees classifier demonstrated superior performance, outperforming the other models. Orlando Iparraguirre-Villanueva et al. used a dataset of 768 patients to predict diabetic patients. They employed five machine-learning techniques and the SMOTE to address the class imbalance. The K-nearest neighbor (K-NN) model had the highest accuracy in identifying diabetes (79.6%) after using SMOTE.

Table 1 A Comprehensive details of related research work

Sr No.	Author name	Year	Title	Dataset	Techniques used	Precision	Recall	F1-score	Accuracy
1	Aditya Saxena	2023	Machine Learning Model Based on Insulin Resistance Metagenes Underpins Genetic Basis of Type 2 Diabetes	GEO database at the National Centre for Biotechnology Information	LASSO,SVM, XGBoost,RF, ANN	ANN 0.94	ANN 0.94	ANN 0.94	ANN 0.95
2	Antonio García-Domínguez	2023	Diabetes Detection Models in Mexican Patients by Combining Machine Learning Algorithms and Feature Selection Techniques for Clinical and Paraclinical Attributes: A Comparative Evaluation	Obtained from information of Mexican patients at the general hospital "Centro Médico Siglo XXI"	SVM,.RF,.KNN, Gradient boosting , Extra trees, .Naive Bayes	RF 0.98	No	RF 0.96	RF 0.95
3	Antonio Agliata	2023	Machine Learning as a Support for the Diagnosis of Type 2 Diabetes	National Center for Health Statistics' (NHANES) biennial survey, MIMIC-III and MIMIC-IV		No	No	No	86%
4	Subhash Chandra Gupta	2023	Predictive Modeling and Analytics for Diabetes using Hyperparameter tuned Machine Learning Techniques	PIMA	.KNN,DT,RF, SVM	RF 100%	No	RF 75.68%	RF 88.61%
5	Atadjanova Nozima Sultan-Muratovna	2023	Diabetes Prediction Using Machine Learning	PIMA	Super Vector Machine	No	No	No	77%
6	Shu Wang	2023	Comparative study on risk prediction model of type 2 diabetes based on machine learning theory: a crosssectional study	Survey data	LR,SVM,BP Neural Network , CART decision - tree ,C4.5 decision tree ,DNN	BP 0.94	BP 0.92	No	BP 0.93
7	Sethupathi M	2023	Diabetes Prediction Using Machine Learning	PIMA	K-means ,RF,LR ,DT ,SVM	No	No	No	LR 78.01%
8	Linh Phuong Nguyen	2023	The Utilization of Machine Learning Algorithms for Assisting Physicians in the Diagnosis of Diabetes	Survey data	DT,LR ,SVC, AdaBoost, Gradient Boosting Classifier,RF, KNN	RF 100%	RF 88.24%	No	RF 94.12%
9	Md Shahin Ali	2023	A Novel Approach for Best Parameters Selection and Feature Engineering to Analyze and Detect Diabetes: Machine Learning Insights	PIMA	AdaBoost,SVM, Logistic regression, Naive Bayes ,Multilayer perceptron , Random forest	Adaboost 94.85%	MLP 92.59%	RFWBP 92.81%	RFWBP 90.32%
10	Önder YAKUT	2023	Diabetes Prediction Using Colab Notebook Based Machine Learning Methods	PIMA	Random Forest,Extra Tree, Gaussian Process	RF 88.79%	RF 84.83%	RF 86.76%	RF 81.71%

Sr No.	Author name	Year	Title	Dataset	Techniques used	Precision	Recall	F1-score	Accuracy
11	Zaigham Mushtaq	2022	Voting Classification-Based Diabetes Mellitus Prediction Using Hypertuned Machine-Learning Techniques	PIMA	LR,SVM,k-nearest neighbors,gradient boost ,Naive Bayes,RF	No	No	No	VC 81.50%
12	Khoula Al Sadi	2023	Prediction Model of Type 2 Diabetes Mellitus for Oman Prediabetes Patients Using Artificial Neural Network and Six Machine Learning Classifiers	data were collected manually from 21 Omani health centres	KNN, SVM, naive Bayes,DT,RF linear discriminant analysis, artificial neural networks	RF 84.10%	RF 98.01%	No	RF 98.73%
13	Methaporn Phongying	2023	Diabetes Classification Using Machine Learning Techniques	obtained from the Department of Medical Services, Bangkok	DT, RF , SVM, K-nearest neighbors	RF 0.974	RF 0.974	RF 0.97	RF 0.975
14	J. Jeba Sonia	2023	Machine-Learning-Based Diabetes Mellitus Risk Prediction Using Multi-Layer Neural Network No-Prop Algorithm	obtained from the UCI online library The type 2 diabetes datasets contain 19 attributes contributed by the Virginia School of Medicine	Naive Bayes ,SVM , Decision tree	No	No	No	NB 96%
15	Orlando Iparraguirre-Villanueva	2023	Application of Machine Learning Models for Early Detection and Accurate Classification of Type 2 Diabetes	PIMA	KNN, Bernoulli ,NB,DT,logistic regression, support vector machine	K-NN (SMOTE) 57.30%	K-NN (SMOTE) 79.60%	K-NN (SMOTE) 66.70%	K-NN (SMOTE) 79.60%
16	Aaditi Ranganath Satam	2023	Diabetes Prediction using Machine Learning	A dataset of 768 cases gathered from various National Institutes of Diabetes and Digestive and Kidney Diseases	decision tree, random forest, logistic regression	LR 70%	LR 66%	LR 68%	LR 79%
17	Md. Jamal Uddin	2023	A Comparison of Machine Learning Techniques for the Detection of Type-2 Diabetes Mellitus: Experiences from Bangladesh	questionnaire-based survey utilizing standard diabetes risk variables to examine the prevalence of diabetes in Bangladesh	DT ,LR , SVM, gradient boost , extreme gradient boost ,random forest, ensemble technique	ET 89.2%	ET 87.6%	ET 88.4%	ET 87.6%
18	Entissar S. Almutairi	2023	Machine Learning Methods for Diabetes Prevalence Classification in Saudi Arabia	Survey dataset	linear discriminant, SVM ,KNN , neural network	No	No	No	weighted KNN 94.5%
19	Victor Chang	2022	Pima Indians diabetes mellitus classification based on machine learning (ML) algorithms	PIMA	NB , RF ,J48 DT	RF 89.4%	No	RF 85.17%	RF 79.57%
20	Mariwan Ahmed Hama Saeed	2023	Diabetes type 2 classification using machine learning algorithms with up-sampling technique	PIMA and BRFSS	gradient boosting, AdaBoost , DT ,extra trees	ETC 94%	ETC 99%	ETC 97%	ETC 96%

CONCLUSION

Machine learning algorithms play an vital role for early detection of diabetes. In this paper various ML algorithms such as supervised and unsupervised are analyzed to achieve better accuracy by considering precision, recall, F1-score and accuracy. It has been observed by many researchers that by applying deep learning, data fusion and hybrid models like ensemble techniques better results can be achieved. Also, using real-time data machine learning models can be analyzed for best output.

REFERENCES

[1] Aditya Saxena, Nitish Mathur, Pooja Pathak, Pradeep Tiwari and Sandeep Kumar Mathur, “Machine Learning Model Based on Insulin Resistance Metagenes Underpins Genetic Basis of Type 2 Diabetes”, Biomolecules, volume-13, pp.432-454, 2023.

[2] Antonio García-Domínguez, Carlos E. Galván-Tejada, Rafael Magallanes-Quintanar, Hamurabi Gamboa-Rosales, Irma González Curiel, Jesús Peralta-Romero, and Miguel Cruz., “Diabetes Detection Models in Mexican Patients by Combining Machine Learning Algorithms and Feature Selection Techniques for Clinical and Paraclinical Attributes: A Comparative Evaluation” Journal of Diabetes Research, Article ID 9713905, 2023.

[3] Antonio Agliata, Deborah Giordano, Francesco Bardozzo, Salvatore Bottiglieri, Angelo Facchiano and Roberto Tagliaferri, "Machine Learning as a Support for the Diagnosis of Type 2 Diabetes" Int. J. Mol. Sci. , pp.777-780 , 2023 .

[4] Subhash Chandra Guptaa and Noopur Goelb, "Predictive Modeling and Analytics for Diabetes using Hyperparameter tuned Machine Learning Techniques" Procedia Computer Science 218 , pp. 1257–1269 , 2023.

[5] Atadjanova Nozima, Sultan-Muratovna, Abdukhakimov Fayzulla Kudratulla ugli, "DIABETES PREDICTION USING MACHINE LEARNING" INTERNATIONAL SCIENTIFIC JOURNAL VOLUME 2 , pp. 2181-3337 , 2023.

[6] Wang S, Chen R, Wang S, "Comparative study on risk prediction model of type 2 diabetes based on machine learning theory: a cross-sectional study". BMJ, volume-13, pp.e069018-e069025, 2023.

[7] Sethupathi M and Privietha P, "Diabetes Prediction Using Machine Learning" International Journal of Recent Trends in Technology and Engineering Volume-II, pp.292-299, 2023.

[8] Linh Phuong Nguyen, Do Dinh Tung, Duong Thanh Nguyen, Hong Nhung Le, Toan Quoc Tran, Ta Van Binh and Dung Thuy Nguyen Pham, "The Utilization of Machine Learning Algorithms for Assisting Physicians in the Diagnosis of Diabetes" Diagnostics, volume-13, pp.2085-2104, 2023.

[9] Md Shahin Ali, Md Khairul Islam, A. Arjan Das, D. U. S. Duranta, Mst. Farija Haque and Md Habibur Rahman, "A Novel Approach for Best Parameters Selection and Feature Engineering to Analyze and Detect Diabetes: Machine Learning Insights" BioMed Research International, Article ID 8583210, 2023.

[10] Önder YAKUT, "Diabetes Prediction Using Colab Notebook Based Machine Learning Methods" IJCESEN Vol. 9-No.1, pp. 36-41, 2023.

[11] Zaigham Mushtaq, Muhammad Farhan Ramzan, Sikandar Ali, Samad Baseer, Ali Samad and Mujtaba Husnain, "Voting Classification-Based Diabetes Mellitus Prediction Using Hyper-tuned Machine-Learning Techniques" Hindawi Mobile Information Systems, Article ID 6521532, pp.1-16, 2022.

[12] Al Sad i, K. Balachandran, "Prediction Model of Type 2 Diabetes Mellitus for Oman Prediabetes Patients Using Artificial Neural Network and Six Machine Learning Classifiers". Appl. Sci., volume-13, pp.2344-2366, 2023.

[13] Phongying, M. Hiriote, "Diabetes Classification Using Machine Learning Techniques." Computation, volume-11, pp.96-113 2023.

[14] Sonia, J.J., Jayachandran, P.;Md, A.Q.; Mohan, S.; Sivaraman,A.K.; Tee, K.F., "Machine-Learning-Based Diabetes Mellitus Risk Prediction Using Multi-Layer Neural Network No-Prop Algorithm." Diagnostics, volume-13, pp.723-739, 2023.

[15] Iparraguirre-Villanueva, O.;Espinola-Linares , K.; Flores Castañeda , R.O.; Cabanillas-Carbonell M. "Application of Machine Learning Models for Early Detection and Accurate Classification of Type 2 Diabetes". Diagnostics, volume- 13, pp.2383-2399, 2023.

[16] Aaditi Ranganath Satam, Tanmay Dilip Dhumale, Pratik Rajesh Hare, Hritika Dinesh Ghosalkar, Aarti Bakshi "Diabetes Prediction using Machine Learning" International Journal of Modern Developments in Engineering and Science Volume 2, pp.292-299, 2023.

[17] Uddin, M.J.; Ahamad,M.M.; Hoque, M.N.; Walid, M.A.A.;Aktar, S.; Alotaibi, N.; Alyami, S.A.;Kabir, M.A.; Moni, M.A. "A Comparison of Machine Learning Techniques for the Detection of Type-2 Diabetes Mellitus: Experiences from Bangladesh." Information, volume- 14, pp.376-395, 2023.

[18] Almutairi, E.S.; Abbod, M.F., "Machine Learning Methods for Diabetes Prevalence Classification in Saudi Arabia." Modelling, pp.37–55, 2023.

[19] Victor Chang,Jozeene Bailey, Qianwen Ariel Xu and Zhili Sun, "Pima Indians diabetes mellitus classification based on machine learning (ML) algorithms" Neural Computing and Applications, pp.16157–16173 , 2023.

[20] Mariwan Ahmed Hama Saeed, "Diabetes type 2 classifcation using machine learning algorithms with up-sampling technique", Journal of Electrical Systems and Inf Technol, Article-8, pp.1-10, 2023.

ISSN 2394 - 7780

FROM THREATS TO SOLUTIONS: A LITERATURE REVIEW ON SECURITY ISSUES IN ELEARNING PLATFORMS

Saroj Junghare[1], and Prof. Mridula Dube[2]
[1]Research Scholar [2]Director, UICSA, R. D. University, Jabalpur (M.P.), India

ABSTRACT

E-Learning provides flexible and affordable education to all. Recent shift towards e-learning has encouraged the use of digital platforms. The use of e-learning platforms as a means of delivering educational content has become popular in recent years increasingly. Huge amount of and various types of data of users are stored on these e-learning platforms. However, with this growth comes an increased need for security in e-learning platforms. In this paper, we have examined some previous works done by researchers to uncover and notify the types of information security problems faced by e-learning platforms and it also focuses on the problems faced by teachers and learners. The paper also recommends the countermeasures proposed in previously published research papers. The paper also reviews the various blogs and articles related to security problems faced in India by e-learning platforms or e-learning industry. It also gives an overview of role of e-learning in India. Elearning is more vulnerable especially from the security, privacy and process viewpoint. By doing this literature review, it will be beneficial for those who want to configure an e-learning platform in their institution; they will already know what problems teachers and students face in e-learning platforms regarding security and what are their solutions.

Keywords: E-learning platforms, Information Security, Threat, Risk, Vulnerability, Countermeasures.

1. INTRODUCTION

The COVID-19 pandemic has produced changes in the teaching–learning environment in higher education institutions and has impacted learning between teachers and students [2]. In the absence of traditional classroom teaching and one-to-one interaction, computer-based learning has emerged as closest substitute for off-line teaching [12]. Technologies have changed the traditional way of education to the modern way of learning, like artificial intelligence [11]. The use of e-learning as a means of delivering educational content has grown significantly in recent years. A learning management system (LMS) provides teachers and students with a virtual space (course or classroom) to conduct learning activities, either as an extension of the physical classroom or as a fully online learning experience [32]. The use of online platforms for learning has made it easier for students to access educational resources, participate in online discussions, and take assessments and evaluations from anywhere, at any time. The growth of e-learning has resulted in a number of security concerns that must be addressed to ensure the safety and privacy of students and the integrity of the educational process. In addition, the success rate of e-learning in the years to come would be defined by flexibility of deployment, variety of Integrated Services Modules and easier operation, solution of security issues etc. [24].

Synchronicity and asynchronous work are the first potential uses of eLearning in day to day college life. For example, the availability of content on the platform allows students to catch up and recover if they missed something or are sick [3]. Before Covid-19, e-learning in India was only for higher studies, certification courses or for those people who could not go to college due to some reasons. Learners usually opted e-learning due to its convenience and affordability. Or to say that there was not much trend of e-learning. When Corona knocked in India, higher educational institutions had to think about the option of e-learning so that they could teach students and their studies do not stop. Then e-learning platforms came into picture. As online learning continues to grow in popularity, colleges and universities are beginning to see a growing number of students taking advantage of an online education platform that enables them to share huge amounts of private data as well as the safety of this information is paramount [7]. Google Classroom, Microsoft Teams, Zoom, Moodle, Webex etc. are the names of most popular e-learning platforms used by higher education institutions. Which e-learning platform to choose depends on what is its cost and how much is being spent on a single student by the institutions? Flip side of rapid growing e-learning adaptation for higher education is information security. Data security was nowhere into consideration, which lead cyber attackers to attack on users data and other data stored for e-learning platform. Security is another important concern here, as this huge amount of diverse data is difficult to secure and increase the susceptibility of universities to cyber threats [8]. It's one of the biggest challenges facing the world, according to UNESCO. [7]. We should emphasize that security practiced in the non-metaverse-based applications should be practiced on the metaverse too, i.e, authorized access, and users authentication [1].

E-learning industry is facing two-fold security problem, one is External cyber threat and other is Internal security concerns. External cyber threat includes SQL injection, Cross-site scripting, inclusion stacks, Access control attacks, denial of service, web crawlers etc. and internal security concern is; On some occasions, data might become vulnerable due to inadvertent errors made by staff members and external advisors. Therefore security measures are unavoidable to prevent the loss of users' valuable data from the security vulnerabilities [25].

Security challenges in e-learning platforms can be anything but not limited to: Protection of sensitive and personal information, Authenticity and reliability of online assessments and evaluations, Identity theft and fraud, Protection of intellectual property etc. and there are various methods to deal with these problems are Data encryption, Secure Socket layer technology, IP tracking and so on.

This paper helps identify Emerging Security Trends and Patterns (this knowledge aids in staying up-to-date with the latest developments in the field and preparing proactive security measures), Theoretical Frameworks and Models (include the identification and examination of relevant models such as the CIA triad (Confidentiality, Integrity, Availability), risk management frameworks, or security maturity models. These frameworks provide a structured approach to addressing security issues in eLearning platforms), common security threats, vulnerabilities, and attack vectors that affect eLearning platforms. This understanding enables researchers and practitioners to gain insights into the complex nature of security issues in the eLearning domain. Based on that Developing Effective Security Strategies and Policies (this includes implementing robust authentication mechanisms, data encryption, secure coding practices, and access control mechanisms), Implementing Technical Solutions (these may include the deployment of intrusion detection systems, firewalls, secure communication protocols, data loss prevention mechanisms, and regular security audits), User Awareness and Training Programs, Collaboration and Information Sharing (it allows for information sharing, knowledge exchange, and collective actions to enhance security in eLearning platforms) can be implemented.

Vulnerability scanners play very important role in finding errors or loopholes which give way for attack to attacker in e-learning platforms. There are number of vulnerability scanners which can be used get information about possible threats to e-learning platform.

2. REVIEW OF LITERATURE

E-learning is covered under a larger term of technology-based learning through websites, learning portals, video conferencing, YouTube, mobile apps, and thousand types of free available websites for blended learning tools [10].

Lourdes Cecilia Ruiz Salvador et al. in their study mentioned that the security of several e-learning platforms is a significant concern and security issues can arise at platform level and external cyber-attacks. They have also mentioned that e-learning platforms such as Moodle, Zoom, Blackboard and edX suffer security vulnerabilities like Brute Force Attack, session hijacking, zoom bombing, end-to-end encryption, Mac spying, windows remote code execution, Cisco Talos vulnerabilities, cross-site request forgery, cross-site scripting attacks, authentication vulnerabilities, cross-site scripting (XSS), password phishing, server-side code execution, and RDX data identification [5]. In their study they have mentioned that External cyber-attacks such as Malicious attack, Availability attack, Confidentiality attack, Integrity attack and Authentication attacks are most common security problem for any e-learning platform. In their paper they also have suggested countermeasures for above mentioned security issues. The countermeasures are Cryptography, DRM, Authentication using Biometric, DF Solution (Distributed Firewall) and Digital Watermarking etc.

In the paper [6] authors stated that Cloud computing, online learning platforms and video conferencing applications, whose use was quite limited in HEIs for online studies, in the conditions of the pandemic or Covid19, they have become the main source of resources. This led to cross-site scripting, spoofing, DoS/DDoS attack risks, unauthorized data access, and malware infections. It also increases theft of personal data. Their research identified the types of attacks that have the greatest impact on assets and recommended solutions to strengthen the cybersecurity of e-learning platforms. The authors also discussed the technologies used and the security threats to these technologies. The technologies used for the e-learning platform are cloud computing, LMS, and video conferencing applications. Threats to cloud computing systems include account theft, shared technology vulnerabilities, malicious insiders, denial of service, and data breaches. Security threats in LMS platforms are CIAA (Confidentiality, Integrity, Authentication, Availability) threats that lead to information leakage, DOS attacks, insecure direct object references, buffer overflows, CSRF attacks, and cross-site scripting. LMS systems often do not properly leverage encryption capabilities to protect data and credentials or use weak encryption algorithms.

[22] presents the overview of various vulnerability scanners such as OWASP, CAPEC, WASC etc. which can be used to uncover the problems lying in E-Learning platforms regarding security. The approaches used by authors

are comparative study using various platforms. Remedies proposed are use of Hierarchical approach and Distributed approach by the institutions which are employing E-Learning platforms in their organization.

In the case of online education data, security risks exist. In this paper authors have presented blockchain based technology model [7] for data management which solves the authentication problem. The research paper also mentions about the trust generation and secure data sharing mechanism for online educational data. It also analyses the security, sharing resources and privacy maintained while sharing the resources. The authors also conclude that a block chain technology effectively authenticate, store and process the online educational data while disseminating the knowledge in learners.

In this article[8] author focuses on problems faced due to understudied nature of cyber security in the field of higher education sector as an area of research and policy analysis, despite the exponential rise in cyber threats to higher education around the world, especially as a result of the Covid19 pandemic. The author also states that higher education is a target for cyber threats and these are referred as IT issues in which risks are transferred to targeted institutions, which is national policy challenge and requires national strategies and policies to address. This article also discusses the possible measures that can be adopted by governments in Higher Education to improve the resilience against cyber threats which will lead to categorization of inherent security vulnerabilities and possible solutions used for the same. The "Higher education as a peculiar cyber security target" section of this paper discus that Higher education institutions store personally identifiable information, such as emails, family related information, demographics addresses and most importantly social security numbers. Other critical information such as banking details for students and staff, health and medical information attract cyber criminals for cyber-attack.

In this paper [9] author has studied the impact of Covid-19 on the security of academic businesses. The method used in this research is comparative that author has compared the pre-pandemic cyber security survey with the peak and post pandemic security survey. The researcher then demonstrated that the pandemic brought a rise in cyber-attack. Due to rise in cyber-attack universities prioritized the security and added defensive measures to ease e-learning. None the less after the pandemic, reported by statistics, numerous e-learning platforms have employed security measures for safe and secure online learning. Cyber-attacks are growing day by day as the attackers find innovative ways for attacking thus information security systems improvement is continuous process. The research found the outcome based on their survey conducted to answer following questions: (i) Has the Pandemic contributed to improving security awareness across academic institutions? (ii) Is the UK Education Sector now well equipped to fully migrate to online learning in the event of another pandemic? The recommendations suggested by the author are regular risk assessment, frequent security assessment schemes and defined security policies and Investment to policies.

In this research paper [10] authors have stated the importance of e-learning in this digital era. E-learning enhances knowledge of students and industry and academic staffs. E-learning provides the facility of education within and off campus. For that reason, the universities provide their students on and around campus with eCourses and of campuses too. As a result of the news reports, Massive Open Online Courses are being used in Malaysia universities, colleges and polytechnics. The online education market is growing rapidly and it is expected to grow more than 15% annually over the forecast, 2016–2023. And the paper also concludes that with the massive growth of the internet, maybe university teaching and learning models will be changed in 10 to 15 years.

In paper [23] authors Yong Chen and Wu He have surveyed security risks and protection mechanisms in online learning using two approaches namely blog mining and traditional literature research. Their findings indicate that security is a concern but not top most concern in the mind of online learning providers and practitioners. The counter measures proposed are DRM, use of Firewalls and Improving Authentication, Authorization, Confidentiality and Accountability.

Educational institutions and students across the world have accepted and appreciated the online platform of learning and the reasons of this acceptability are ease of use, learning flexibility and controllable environment and despite its multiple advantages there are quite a few limitations of e-learning such as social isolation, face to face interaction between teacher and student, connectivity issues, etc. [4]. Reports also show a considerable increase in the number of viruses distributed through online learning platforms, such as Moodle, Blackboard, Google Classroom, among others (Kaspersky 2020) [13].

Web Application Security Vulnerabilities Scanners, commonly known as Dynamic Application Security Testing Tools or DAST, are software tools that automatically scan web applications mostly from the outside looking for security weaknesses like cross scripting, SQL injection commands, command injections, path traversal and

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

vulnerable server configuration. There are five types of vulnerability scanners-Database Scans, Application Scans (mostly used for web apps), Host-based Scans, Wireless Scans and Network Based Scans. There are number of vulnerability scanners which are freely available to scan Applications (most of the E-Learning platforms are web applications) and some provide vulnerability management also.

ATTACKS	PREVENTION	DETECTION AND RESPONSE
BRUTE FORCE	-STRONG PASSWORD -ENCRYPTION -MULTI-FACTOR AUTHENTICATION -LIMITING LOGIN ATTEMPTS -REGULAR SECURITY UPDATES	-MINITORING LOGIN ACTIVITY -INTRUSION DETECTION SYSTEM -RATE LIMIT -BLOCKING SUSPICIOUS IP ADDRESSES
SESSION HIJACKING	-STRONG AUTHENTICATION -SECURE COMMUNICATION -SESSION MANAGEMENT -SECURE COOKIES -INPUT VALIDATION AND SANITIZATION -REGULAR SECURITY UPDATES	-MONITOR LOGIN ATTEMPTS -IMPLEMENT INTRUSION DETECTION SYSTEMS -ANALYZE LOG FILES -USE SESSION MONITROING TOOLS -REVOKE COMPROMISED SESSIONS -NOTIFY AFFECTED USERS -INVESTIGATE THE ATTACK

Table 1: Most common Attacks, Prevention, Detection and Response

Security issues	Counter Measures (Solutions) Proposed
Windows remote code execution	Cryptography
End-to-end Encryption problems	DRM
Zoom Bombing	Distributed Firewall Solution
Mac spying	Biometric Authentication
Cross Site Request Forgery	Digital Watermarking
Cross Site Scripting	Audit of Access rights
Authorization Vulnerabilities	Authorization policies
Password Phishing	Data encryption
DoS or DDoS	Use of encryption protocols
Shared technologies Vulnerabilities	Security patch management
Account or Traffic Service Hijacking	Updating Apps
Malicious Insider (Human factor)	Providing Secure remote connections
CIA Issues	Access control
SQL Injection	Distributed Information Management
Malicious File execution	Firewalls
	Block chain Technology

Table 2: Summary of Security issues and their counter measures

3. Blogs and Articles published online

a. Data Breach in News in India

Data breaches are a significant concern for e-learning platforms in India. In September 2020, Edureka, an online learning platform [14], experienced a data breach where personal information of 2 million users was compromised. The breach included sensitive data such as email addresses, passwords, mobile numbers, and IP addresses. Edureka assured users that no financial information was stolen and encouraged users to reset their passwords and enable two-factor authentication. Phishing attacks are another security issue that e-learning platforms in India face. Attacks contain links which are directed to fake pages to steal important credentials.

One of the Business Today articles claimed that in 2021, India ranked third globally for data breaches [15]. Byjus suffered data breach in the year 2020 and 2021 which was not expected by the investors [16]. DDoS(Distributed Denial-of-Service) attack is another problem which E-learning platforms face. The attack overload the servers, causing the platform to crash and students to lose access to their data [17].

In addition to phishing, cybercriminals are also using social engineering tactics to trick users into divulging sensitive information. In April 2020, an e-learning platform for competitive exam preparation, Edureka, reported a security breach where hackers used social engineering tactics to steal confidential data of over 7 million users, including phone numbers, email addresses, and passwords [18].

In 2020, Unacademy Platform, one of the largest online education platforms in India, has about 22 million user data sold on hacker websites and more than 500000 zoom account information sold on dark networks therefore these events show that online education data protection is imminent, security issue that e-learning platforms face in India is cyber-attacks. In November 2020, the e-learning platform Unacademy suffered a data breach that resulted in the personal information of 22 million users being compromised. The attackers were able to access data such as usernames, passwords, and email addresses [19].

In September 2020, the e-learning platform Vedantu suffered a phishing attack that resulted in the theft of sensitive data such as student and teacher information. The attackers sent fake emails to users, claiming to be Vedantu and requesting that they click on a link and enter their login credentials [20].

In 2020, the Indian e-learning platform Simplilearn suffered a phishing attack that resulted in the theft of around

1.3 million user records. The attackers were able to access sensitive data such as user names, email addresses, and phone numbers [21].

There are many incidents reported for security data breach [28] in eLearning platforms such as Lynda.com [27], McGraw Hill [30], Seesaw online platform [31] which confirms that security enforcement is necessary on eLearning platforms.

b. Indian government on e-learning

The government of India has taken various appreciable steps towards the enhancements in education in India in Higher Education. Indian government has imagined and is shaping E-Learning and digital education with their efforts. Ministry of Human Resources Development (MHRD) has launched various E-learning platforms including Diksha, Swayam Prabha Channel, Shiksha Van, E-Pathshala, E-ShodhSindhu, NPTEL, PM-EVidhya, VidyaDaan, NDL, e-Yantra, Fossee, Sakshat, e-gyankosh, Virtual Labs and National Repository of Open Educational Resources (NROER). It is worth noting that apart from the Indian central government efforts, each state has various online education initiatives that are tailored to their needs. E-learning system is not an exception, not only provides a lot of benefits but also has some potential threats and risks from the Internet [26]. To deal with these potential threats and risks Indian government introduced Data Protection Bill. And now government is enforcing 6 hour rule to report for Security breach in any organization [29].

4. Blockchain for information Security

Blockchain technology has emerged as a powerful tool in the field of information security. With its decentralized and immutable nature, blockchain offers enhanced security measures to protect sensitive data. Enhanced Data Integrity-Blockchain ensures data integrity by utilizing cryptographic algorithms to create a digital signature for each transaction. This ensures that the data cannot be tampered with or modified without detection. By introducing an error-proof mechanism, blockchain strengthens the security of information. Blockchain Technologies Decentralized Data Storage, Transparent and Immutable Transactions and Smart Contracts helps maintain the information security. With ZKP(Enhanced Privacy, Secured Identity Verification, Efficient Auditing), blockchain systems can maintain data integrity and security while preserving user privacy.

5. CONCLUSION

eLearning is now integral part of higher education institutions after Covid-19. Every institution is focusing on engaging its students through online learning platforms or LMS. This literature review provides a comprehensive analysis of security issues in eLearning platforms, examining both theoretical implications and practical strategies. By synthesizing the existing research, this review contributes to a better understanding of the security challenges faced by eLearning platforms and offers insights for developing secure and resilient eLearning environments. The findings of this study can guide platform developers, educators, policymakers, and

ISSN 2394 - 7780

researchers in implementing effective security measures to protect user data, foster a safe learning environment, and ensure the credibility and integrity of eLearning platforms.

REFERENCES

[1] Dahan, N.A.; Al-Razgan, M.; Al-Laith, A.; Alsoufi, M.A.; Al-Asaly, M.S.; Alfakih, T. Metaverse Framework: A Case Study on E-Learning Environment (ELEM). Electronics 2022, 11, 1616. https://doi.org/10.3390/electronics11101616

[2] Alyoussef I (2021) E-Learning System Use During Emergency: An Empirical Study During the COVID19 Pandemic. Front. Educ. 6:677753. doi: 10.3389/feduc.2021.677753

[3] Fülöp MT, Breaz TO, Topor ID, Ionescu CA and Dragolea L-L (2023) Challenges and perceptions of elearning for educational sustainability in the "new normality era". Front. Psychol. 14:1104633. doi: 10.3389/fpsyg.2023.1104633

[4] Sá, M.J.; Serpa, S. The COVID-19 Pandemic as an Opportunity to Foster the Sustainable Development of Teaching in Higher Education. Sustainability 2020, 12, 8525. [CrossRef]

[5] Lourdes Cecilia Ruiz Salvador, Carlos Lenin Alvarez Llerena, Dr. Huu Phuoc Dai Nguyen, "DIGITAL EDUCATION: SECURITY CHALLENGES AND BEST PRACTICES", DOI: 10.37458/ssj.2.2.4.

[6] Alexei Arina, Alexei Anatolie, "Cyber Security Threat Analysis in Higher Education Institutions As A Result Of Distance Learning", INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 10, ISSUE 03, MARCH 2021, ISSN 2277-8616.

[7] Yaofei Wang, Qiurui Sun, Rongfang Bie, Blockchain-Based Secure Sharing Mechanism of Online Education Data, Procedia Computer Science, Elsevier, Volume 202, 2022, Pages 283-288, ISSN 1877- 0509, https://doi.org/10.1016/j.procs.2022.04.037.

[8] Noran Shafik Fouad (2021) Securing higher education against cyberthreats: from an institutional risk to a national policy challenge, Journal of Cyber Policy, 6:2, 137-154, DOI: 10.1080/23738871.2021.1973526, https://doi.org/10.1080/23738871.2021.1973526.

[9] Arogbodo, M. (2022, January 12). Impacts of the Covid-19 Pandemic on Online Security Behavior within the UK Educational Industry. https://doi.org/10.31234/osf.io/h5qgk

[10] Shahzad, A., Hassan, R., Aremu, A.Y. *et al.* Effects of COVID-19 in E-learning on higher education institution students: the group comparison between male and female. *Qual Quant* **55**, 805–826 (2021) https://doi.org/10.1007/s11135-020-01028-z

[11] Di Vaio, A., Boccia, F., Landriani, L., Palladino, R.: Artifcial intelligence in the agri-food system: Rethinking sustainable business models in the COVID-19 scenario. Sustainability 12(12), 4851 (2020a). https ://doi.org/10.3390/su12124851

[12] Khan, M.A.; Vivek; Nabi, M.K.; Khojah, M.; Tahir, M. Students' Perception towards E-Learning dur ing COVID-19 Pandemic in India: An Empirical Study. Sustainability 2021, 13, 57. https://dx.doi.org/10.3390/ su13010057

[13] Kaspersky. 2020. "DDoS Attacks against Educational Resources Increased by More than 350% This Spring." https://www.kaspersky.com/about/press-releases/2020_ddos-attacks-against-educational resourcesincreased-by-more-than-350-this-spring.

[14] https://www.livemint.com/companies/start-ups/edureka-s-database-breached-2-million-user-recordspotentially-at-risk-11601450797202.html (Accessed on 25/5/23)

[15] https://www.businesstoday.in/latest/trends/story/india-ranks-third-in-global-data-breaches-in-2021-report315750-2021-12-15 (Accessed on 22/5/23).

[16] https://blog.ipleaders.in/case-study-data-breach-scandal-byjus/ (Accessed on 02/5/23)

[17] IIM data breach, https://www.databreaches.net/in-iim-a-suspects-data-theft-from-its-servers/ (Accessed on 15/6/23)

[18] Edureka data breach: https://www.thehindubusinessline.com/info-tech/data-breach-at-e-learning-platformedureka/article32733488.ece (Accessed on 20/3/23)

[19] unacademy data breach: https://zeenews.india.com/india/online-learning-platform-unacademy-

hackeddetails-of-22-million-users-available-for-sale-2281693.html (Accessed on 12/4/23)

[20] vedantu data breach: https://inc42.com/buzz/vedantu-confirms-hack-that-compromised-data-of-687k-users/ (Accessed on 15/5/23)

[21] simplilearn in news for data breach: https://www.simplilearn.com/2-billion-bits-of-info-exposed-inside- arecord-breaking-data-leak-article (Accessed on 16/5/23)

[22] Bhatia, M., & Maitra, J. K. (2018). E-learning Platforms Security Issues and Vulnerability Analysis. 2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES). doi:10.1109/cctes.2018.8674115

[23] Chen, Y., & He, W. (2013). Security risks and protection in online learning: A survey. The International Review of Research in Open and Distributed Learning, 14(5). doi:10.19173/irrodl.v14i5.1632

[24] Kumar, A. (2020). The Pros And Cons of Virtual Learning In India: An Insight During 'Covid Lockdown'. Adhyayan: A Journal of Management Sciences, 10(1):8-13

[25] Masud, Anwar & Huang, Xiaodi & Islam, Md Rafiqul. (2014). A Novel Approach for the Security Remedial in a Cloud-based E-learning Network. Journal of Networks. 9. 2934-2942. 10.4304/jnw.9.11.29342942.

[26] Nguyen, Phuoc Dai & Rajnai, Zoltan & András, Kerti. (2016). E-Learning Security Risks and its Countermeasures. Emerging research and Solution in ICT. 1. 17-25. 10.20544/ERSICT.01.16.P02.

[27] (Accessed on 25/5/23) https://www.bitdefender.com/blog/hotforsecurity/e-learning-site-lynda-com-suffersdata-breach/

[28] (Accessed on 25/5/23) https://portswigger.net/daily-swig/data-breach

[29] (Accessed on 25/5/23) https://portswigger.net/daily-swig/india-to-introduce-six-hour-data-breachnotification-rule

[31] (Accessed on 15/4/23) https://www.highereddive.com/news/mcgraw-hill-exposed-student-data-gradesonline-privacy/639150/

[32] (Accessed on 15/4/23) https://www.valleynewslive.com/2022/09/14/security-breach-reported-withinseesaw-online-learning-platform/

[33] Alier, M.; Casañ Guerrero, M.J.; Amo, D.; Severance, C.; Fonseca, D. Privacy and E-Learning: A Pending Task. Sustainability 2021, 13, 9206. https://doi.org/10.3390/ su13169206

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

IOT-POWERED SMART AGRICULTURESYSTEM

Shubham Gaikwad[1], Vivek Khalane[2], Bhavesh Digey[3] and Shirish Kulkarni[4]
[1,2,3]Department of Instrumentation Enginering, D.Y. Patil deemed to beUniversity, India,
shubhamgaikwad2125@gmail.com[1], vivek.khalane@rait.ac.in[2] bhavesh.digey@rait.ac.in[3] and
shirish.kulkarni@rait.ac.in[4]

ABSTRACT
In terms of our nation's growth, agriculture is crucial. In addition, agriculture is a fundamental income source for many in India, and the exodus of people from rural regions has hampered the growth of our nation. The only way to solve this issue is through smart agriculture, which uses automation and Internet of things (IoT) technologies to modernize conventional agricultural practices. The idea of "smart farming," in which Internet of Things sensors can provide data on agricultural areas, is becoming popular. Numerous applications, including irrigation decision assistance, crop growth monitoring and selection, and more, are made possible by IoT. IoT has made smart farming accessible to every farmer's community and provided beneficial green agriculture. Continuous crop sensing and monitoring through sensor convergence along with the help of internet connectivity provides early warning to farmers for crop growth and harvest times regularly, ultimately leading to high crop productivity and proper product delivery to end users at the appropriate time and location. Thus, we employ Internet of Things-based smart agriculture to solved this issue for varioustypes of crops.

Keywords: Internet of Things, Thingspeak, Smart Farming

1. INTRODUCTION
The convergence of cutting-edge technologies has empowered a paradigm shift in agriculture, marking the advent of Smart Agriculture Systems. This paper illuminates the transformative potential of integrating Soil Moisture, DHT11 (Temperature and Humidity), BMP180 (Barometric Pressure and Altitude), MQ135 (Air Quality), along with the ESP8266 microcontroller and ThingSpeak platform.Every sensor captures an essential componentof environmental evaluation, collaborating to create an agile ecosystem. The ESP8266 synchronizes various sensors, ensuring smooth connectivity and data interchange with ThingSpeak, an IoT platform for data presentation and analysis in real time.

The unique functions of these kinds of sensors used for farming aredetailed in this paper, along with how they are integrated with the ESP8266 and this provides data to ThingSpeak gateway. It exploresthe various aspects of agricultural research, highlighting how this merger is essential to changing farming methods for greater productivity, wiser choices, and sustainable harvests.

2. Components and Software Used

Soil moisture sensor:-
The moisture sensor for soil is a device used for quantifying the volume of water in the of soil [1]. The sensor determines volume of water without eliminating moisture by using additional soil factors such as electrical resistivity or conductivity, dielectric strength, along with reaction with other neutrons. It must be adjustedsince external factors such as temperature, soil type, and conductivitymight affect the result.

Fig.1. Soil Moisture Sensor[1]

DHT11 :-
The temperature and humidity of the atmosphere are measured usingthe DHT11 sensor[1]. In the event that farming is done in a closed environment, a separate system might be built to manage the temperature. This sensor monitors the temperature and humidity in the crop field. In this case, the signal is transmitted using pin 1, received using pin 2, and data is transferred using pin 3.

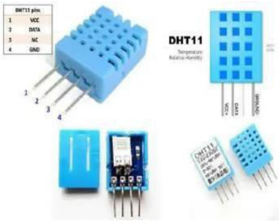


Fig.2. DHT11 Sensor[1]

BMP180:-
Measuring temperature, height, and air pressure with a barometric pressure sensor is possible. This is useful for short-term weather prediction and researching plant behavior under various atmospheric pressure scenarios[1]

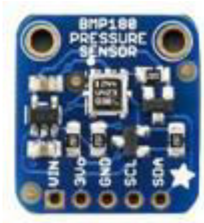


Fig.3. BMP180 Sensor

MQ135:-
A crucial factor in determining crop development is air quality, which is measured with sensor for air quality[MQ135]. The prominently used pins of MQ135 are Vcc, Gnd, Aout from four terminals. The analog output value rises when the MQ 135 detects harmful gasses and falls when it doesn't. The 10-bit digital value obtained from the analog output is transformed into a percentage outof 100.

Fig.4. MQ135 Sensor[1]

ESP 8266:-
The ESP8266 is a potent Wi-Fi module that is frequently utilized inInternet of Things applications because of its small size, affordable price, and strong networking features. We used this ability in our project to facilitate.smooth wireless connectivity between different Internet of Things components. We created a dependable network that enabled transfer of data, sensor surveillance, and controlling remotely features by utilizing the ESP8266's integrated Wi-Fi. Its integration simplified connectivity and contributed significantly to the project's success, enabling cost-effective yet efficient IoT solutions.

Fig.5. ESP 8266

Thingspeak:-
Our project's key component, ThingSpeak, offered a smooth integration platform for real-time data aggregation, visualization, and analysis. With specially designed channels for each sensor (soil moisture, DHT11, BMP180, and MQ135), the platform gracefully handled a variety of data formats. Our data hub, the ESP8266, interfaced with ThingSpeak with ease and reliably sent sensor values across HTTP/MQTT protocols. We were able to

 ISSN 2394 - 7780

analyze environmental variations, identify patterns, and quickly get insights because of ThingSpeak's user-friendly interface, which turned raw data into useful information. Its crucial function in organizing and analyzing sensor data demonstrated how well the project used IoT capabilities to provide extensive environmental monitoring.

Fig.6. Thingspeak gateway for IoT devices

Arduino IDE:-
Our project's mainstay was the Arduino IDE (Integrated Development Environment), which offered a stable and user-friendly environment for writing code and distributing it to the ESP8266 microcontroller. Our development process was eased by its wide library of pre-built functions and user-friendly interface, which made it easy for us to build, compile, and upload firmware to the ESP8266. The IDE's versatility in accommodating various barriers and sensors facilitated incorporation and enabled seamless communication among the ESP8266 and our group of sensors, encompassing moisture in the soil. DHT11, MQ135 and BMP180. Its role as our programming center dramatically sped the development cycle of our Internet of Things-based environmental monitoring project, allowingus to focus on enhancing sensor interactions and system functionality.

Fig.7. Arduino IDE programming tool.

3. SYSTEM WORKING
To determine the soil's moisture content. usually consists of probesthat offer analog or digital output to detect the moisture content and measure the environment's humidity and temperature. gives digital output data that a microcontroller can read. measures the temperature and atmospheric pressure. uses the SPI or I³C communication protocol to deliver temperature and pressure measurements. monitors the quality of the air by identifying different gases, such as smoke, benzene, ammonia, etc. provides analog output by the gas concentration. serves as the microcontroller that collects and sends sensor data to the cloud. employs the proper protocols (analog/digital/I/C/SPI) to communicate with sensors establishes a Wi-Fi connection and uses it to transmit data to the ThingSpeak platform. platform that is cloud-based and used for data analysis, visualization, and storage. Receives data sent by the ESP8266 and organizes it into channels for each type of sensor data.

 ISSN 2394 - 7780

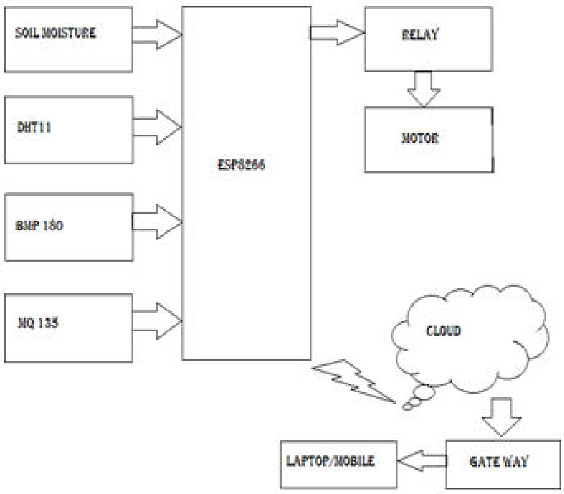


Fig.8 Block diagram of IoT smart agriculture system

Depending on the output type of the sensor, the ESP8266 reads either analog or digital signals to gather data from each one. The ESP8266 reads the voltage levels for analog sensors, such as the MQ135 or soil moisture sensor, and transforms them into useful data. It uses particular protocols to interface with digital sensors, such as the DHT11 and BMP180, to get information about temperature, humidity, pressure, and other parameters. The gathered sensor data is prepared and processed before being delivered in an organized way to ThingSpeak. On ThingSpeak, each kind of sensor data is often assigned to a particular channel. The ESP8266 connects to ThingSpeak over Wi-Fi connections. It sends the prepared data to the appropriate ThingSpeak channels, including temperature, humidity, pressure, air quality, and soil moisture.

After receiving the data, ThingSpeak stores it in the relevant channels. It offers visualization tools for graphs, analytics, and real-time or historical data trends based on the incoming data. The ThingSpeak platform allows users to view, analyze, and interpret the data that has been collected via a web interface or mobile app.They can track alterations in the surrounding environment, identify trends, and draw conclusions from the data that is shown.

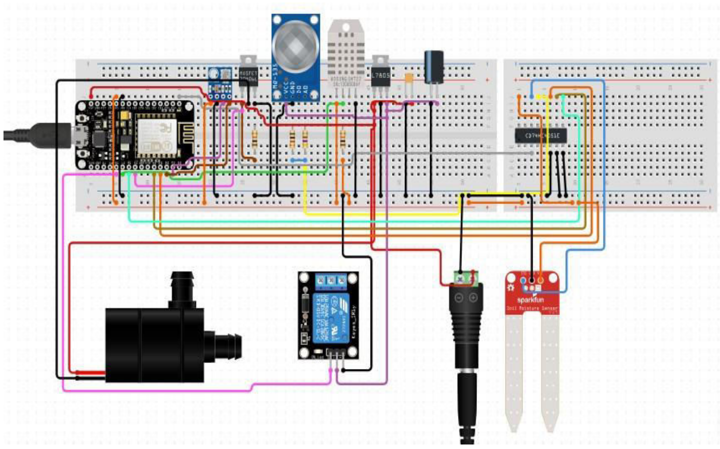


Fig.9 Circuit diagram of IoT smart agriculture system

In this project, we have monitored vital parameters for crop health and increased yield for cultivation which is shown in thefollowing figures.

 ISSN 2394 - 7780

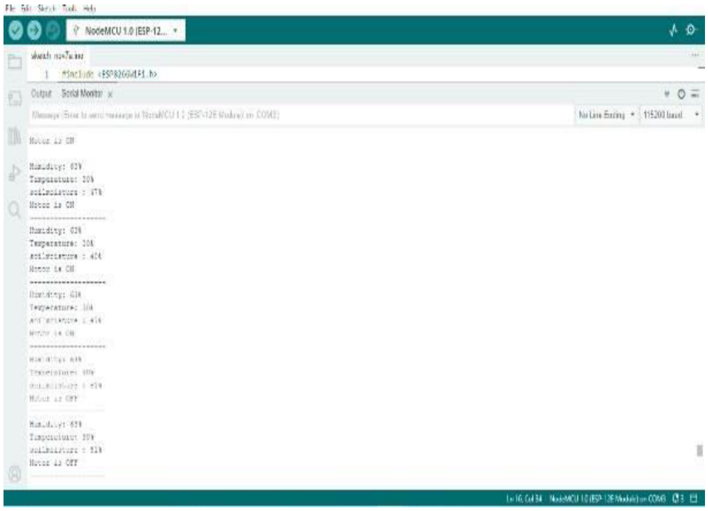


Fig.10 Serial Monitor Output for measurement of soil moisture,temperature, and humidity for crop health.

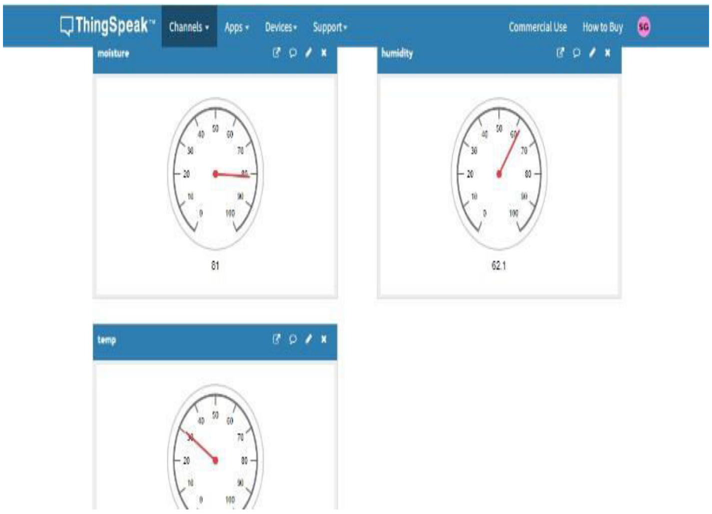


Fig.11 Thingspeak gateway for display of measurement of soilmoisture, temperature, and humidity for crop health.

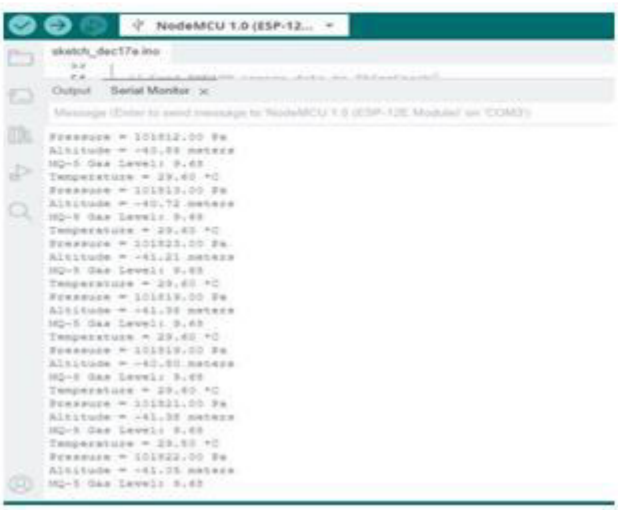


Fig 12 Serial Monitor Output for measurement of pressure and gaslevel for air quality monitoring.

4. Results and Discussion

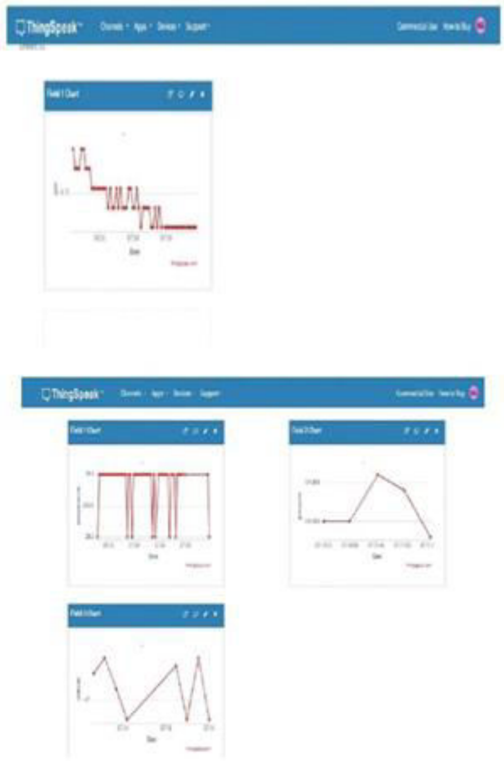


Fig 13 Thingspeak gateway for display of measurement ofpressure and gas level for air quality monitoring.

Table 1 ; Comparison among various factors for assessingproposed system with the current state available.

Sr.No.	Factors	Proposed Methodology	Mohith KC, Tanish Aiyanna, "IOT Based Agriculture Monitoring System" [1]
1.	Sensor Integration	BMP180, DHT11, MQ135, SoilMoisture Sensor.	DHT11, MQ135, Soil Moisture Sensor, LDR.
2.	Processor	ESP 8266	Arduino Uno
3.	Data Collection and Cloud Integration	Real time Data logging through Thinkspeakgateway	Unavailable
4.	Communication Protocols	Wi-Fi	GSM module
5.	Visualization	Thinkspeak Dashboard	LCD display
6.	InstallationComplexity	Easy to integrate with IoT devices.	Complex installation due to communication protocol.

5. CONCLUSION

Precision farming and air quality monitoring are made possible by the combination of Soil Moisture, DHT11, BMP180, MQ135, ESP8266, and ThingSpeak, which forms the core of a Smart Agriculture System. Farmers now have access to real-time information on soil moisture, temperature, humidity, air quality, altitude, and atmospheric pressure thanks to this combination. The ESP8266 processor, gathers, processes, and sends this data to the cloud-based ThingSpeak platform in an effortless manner.

By using a comprehensive strategy, farmers may monitor crop health, identify environmental anomalies, optimize irrigation systems, make well-informed decisions, and promote sustainable agricultural practices. A productive, data-driven agricultural approach that ensures increased yields, resource conservation, and resilience against climate unpredictability is made possible by the system's accessibility and agility. The combination of these technologies offers a novel route toward more resource-conscious and resilient farming methods that will boost productivity without depleting our natural resources as agriculture continues to change.

REFERENCES

[1] Mohith KC, Mr.Tanish Aiyanna, "IoT Based Agriculture Monitoring System", International Journal of Research &Development (IJRD), Vol. 6 Issue. 7, July-2021

[2] Bin Mushtaq, Aboubakar & Ali, Hassan & Latif, Rizwan & Ammar, Muhammad. (2023). IOT Based Smart Agriculture Monitoring System.

[3] Mohanraj I Kirthika Ashokumarb, Naren J “Field Monitoring and Automation using IOT in Agriculture Domain” IJCSNS, VOL.15 No.6, June 2015.

[4] Prathibha S.R, Anupama Hongal, Jyothi M.P, “IOT based agriculture monitoring system”, 2017 International Conference on Recent Advances in Electronics and Communication Technology

[5] Ibrahim Mat, Mohamed Rawidean Mohd Kassim, Ahmad Nizar Harun, Ismail Mat Yusoff “IOT in Precision AgricultureApplications Using Wireless Moisture Sensor Network” 2016IEEE Conference on Open Systems (ICOS), October 10-12- 2016, Langkawi, Malaysia.

[6] Ahmed, Shams & Shuravi, Shanjana & Afrin, Shaila & Rafa, Sabiha & Hoque, Mahfara & Gandomi, Amir. (2023). The Power of Internet of Things (IoT): Connecting the Dots with Cloud, Edge, and Fog Computing.

[7] Prof. K. A. Patil And Prof N. R. Kale proposed “A Model For Smart Agriculture Using IOT” 2016 International Conference on Global Trends in Signal Processing, Information Computing , And Communication.

[8] Prakash, Chander & Singh, Lakhwinder & Gupta, Ajay & Lohan, Shiv Kumar. (2023). Advancements in Smart Farming: A Comprehensive Review of IoT, Wireless Communication, Sensors, and Hardware for Agricultural Automation. Sensors and Actuators A Physical.

[9] Singh, Vikash Kumar & Kushwaha, Devendra & Taram, Manish & Taram, Anuradha. (2015). A Framework for Technologically Advanced Smart Agriculture Scenario in India based on Internet of Things Model. International Journalof Engineering Trends and Technology.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

ROLE OF PODCASTS IN FACILITATING SPIRITUAL EXPLORATION AMONG INDIAN YOUTH

Aarushi Singh[1] and Dr Jolly Jose[2]
aarushisingh913@gmail.com[1] and jjose@amity.edu[2]

ABSTRACT

Podcasts are becoming a unique medium in the always-changing digital world, and spiritual podcasts are becoming popular as platforms for various audio and video content provide content regarding spirituality. The objective of this study is to enhance comprehension regarding how Indian college students interact with spirituality podcasts by exploring their consumption habits, driving forces, and the social acceptance that shapes their decisions. The study intends to close a significant knowledge gap and advance our understanding of how young people in India are experiencing spiritual transformation.

There is abundant information and entertainment available on screens in the modern digital age, and podcasts have made a name for themselves as special providers of audio content in this environment. Podcasts about spirituality have grown significantly, providing insightful conversations, guided meditations, and insights into a wide range of spiritual traditions. College students, a population undergoing significant life changes and debating existential issues, relate poignantly to this ascent. It is crucial to look more closely at their motivations, consumption patterns of spirituality podcasts, and the sociocultural environment influencing their decisions to understand how they are involved with this emerging phenomenon. The students reveal interesting patterns in podcast consumption that can be observed from the statistical data. A significant proportion of the participants, around 80%, indicated that they regularly consume podcasts every week. It has been noted that individuals within the age range of 18 and 21 show a greater tendency to be interested in podcasts that focus on personal growth and mindfulness. Gender-based analysis reveals that males and females exhibit comparable levels of interest and engagement in spirituality-related podcasts. The study indicates that preferences can vary depending on cultural backgrounds. Students from various cultural backgrounds tend to favor podcasts that incorporate their cultural and spiritual values. The survey was collected by 200 Indian College students.

Keywords-Podcast, Spirituality, Faith, Spiritual Growth

INTRODUCTION

Podcasts have become a prominent and influential genre in the digital era, where information flows through our interconnected lives. In the realm of auditory media, which was previously primarily focused on music and traditional radio, there is now a wide range of voices and stories. Within this expansive landscape, spirituality has found its place and influence. The objective of this study is to examine the complex correlation among both podcasts and spirituality, specifically examining the listening patterns and impacts among Indian college students. The emergence of podcasts has experienced an unparalleled surge in popularity over the past decade, signifying a notable change in the way people consume audio content. Podcasts are a versatile medium that encompasses a broad spectrum of subjects, such as storytelling, education, news, and entertainment. During range, spirituality has established a unique position, facilitating discussions that span the metaphysical domains, delve into various belief systems, and offer a refuge for deep thought. This surge in popularity is not just a passing musical fad but rather indicates a change in how people search for and interact with spiritual content in today's digital age.

Young individuals, particularly those in college, find themselves at a crucial point where they are simultaneously engaging with academia, forming their sense of self, and confronting profound existential inquiries. Within this convergence of individual development, spirituality frequently emerges as a guiding influence. In India, a country deeply rooted in profound spiritual customs, the present generation faces the task of reconciling age-old wisdom with the rapid pace of the digital era. This study focuses specifically on Indian college students, examining the wide range of cultural diversity found within Amity University, located in Noida.

Although the rise in podcast popularity and the merging of spirituality with digital media are noticeable trends, there is a lack of detailed investigation into how these dynamics manifest among Indian college students. Our research aims to understand the complexities of podcast consumption among young people, particularly its influence on their spiritual outlook. This investigation goes beyond simple statistical analysis, to capture the fundamental nature of how podcasts are integrated into the exploration of Spirituality. The main objective of this study is to uncover the complexities of podcast consumption among Indian college students and its interconnected relationship with spirituality. The precise aims of this investigation are to identify the predominant themes in podcast preferences, examine the frequency of podcast consumption, identify influential podcasts, and comprehend the impact of this auditory engagement on the spiritual perspectives of young individuals. Our focus on Amity University, Noida aims to provide a detailed representation of the wider patterns and developments in Indian higher education. College students are captivated by spirituality podcasts for a variety of reasons. First, these podcasts offer a convenient way to discuss spiritual topics. Unlike conventional establishments that possess ingrained frameworks and beliefs, podcasts provide adaptability and anonymity. With the ability to access a wide range of content on demand, students can easily fit spiritual exploration into their busy schedules and customize it to suit their own needs and interests. Their freedom to choose their spiritual paths free from outside constraints or rules gives them great power.

Moreover, podcasts on spirituality appeal to the natural curiosity and openness that define young adulthood. College students actively examine and reshape their beliefs, values, and purpose as they traverse an existential crossroads. Podcasts on spirituality provide a platform for examining various viewpoints on life's big issues, encouraging reflection and critical thinking. They provide a secure environment for addressing existential fears, overcoming obstacles in one's life, and looking for direction amid life's unknowns. Podcasts' conversational style adds to their appeal by creating a feeling of intimacy and immediateness that appeals to younger listeners. A sense of community and connection is fostered by the hosts' and guests' genuine voices, personal tales, and lively conversations. Students who might feel alone or unsupported in their spiritual exploration within their immediate social circles or traditional religious frameworks may find this especially appealing. Podcasts fill this void by providing a feeling of community and a common experience among like-minded individuals starting similar self-discovery journeys.

The emergence of spirituality podcasts is especially noteworthy in the context of India, a country rich in traditional spiritual practices. Even though India has a wide variety of long-standing religious institutions and customs, young people looking for spiritual fulfillment face particular difficulties in this quickly modernizing country. The emphasis on academic and professional success, rapid urbanization, and exposure to Western ideologies can lead to a disconnection from traditional spiritual practices.

In this sense, spirituality podcasts provide a link between traditional wisdom and modern realities. They give students easily accessible opportunities to connect with their cultural heritage, investigate spirituality in non-denominational contexts, and make sense of their spiritual beliefs considering contemporary living.

Even though spirituality podcasts are becoming more and more popular among Indian college students, there is still a lack of research in this field. Few studies have specifically examined the consumption of spirituality podcasts, especially among young adults in India, even though many have examined general podcast listening habits. A critical knowledge gap is created by the dearth of research, making it difficult to comprehend how this medium influences the spiritual practices and perspectives of a generation that has the potential to significantly impact India's future.

RESEARCH QUESTIONS

1. Why do Indian college students choose to listen to podcasts about spirituality?
2. Which spirituality podcasts appeal to college students in India?
3. What differences exist in listening habits between demographic variables like gender, geography, and religious background?
4. What advantages and disadvantages do Indian college students perceive from listening to spirituality podcasts?
5. What impact do spirituality podcasts have on Indian college students' spiritual practices and beliefs?

RESEARCH OBJECTIVES

The study aims to investigate the patterns and preferences of individuals when it comes to consuming spirituality podcasts.

1. To determine the prevalence, platforms, and circumstances surrounding college students' consumption of spirituality podcasts.
2. To study the motivations and preferences driving active participation in spirituality podcasts among college students.

 ISSN 2394 - 7780

3. To examine format, content, and presenter preferences, elucidating factors influencing the attractiveness of spiritual content in podcasts for students.

4. To evaluate the perceived effects of listening to spirituality podcasts on different aspects of well-being among college students.

REVIEW OF LITERATURE

Deb and Sun (2020) mentioned in their study titled "Exploring Spirituality, Socioeconomic Status, and Mental Health in Indian University Students," The authors emphasized to investigate the intricate connections between spirituality, socioeconomic status, religious background, social support, and mental health among Indian university students. Through a questionnaire-based approach with over 400 participants, the authors identify that female students tend to exhibit higher spirituality than males, with Hindu religion and lower family income associated with lower spirituality scores. Importantly, the study highlights the positive correlations between overall spirituality and mental health, emphasizing the role of social support in enhancing spirituality. However, it's crucial to acknowledge that this study has been retracted due to concerns about its methodology, urging caution in interpreting its findings.

O'Neill et al. (2017): In their comprehensive review, O'Neill et al. (2017) explore the connections between various spiritual practices and well-being among college students. The study encompasses a wide range of practices such as meditation, prayer, mindfulness, religious attendance, and nature connection, identifying positive outcomes like stress reduction, improved mental health, and enhanced life satisfaction. O'Neill et al. emphasize the need for further research to address methodological challenges, such as self-reporting bias, and the importance of conducting longitudinal studies to investigate the long-term effects of different practices on student well-being.

Worthington et al. (2007): In their groundbreaking longitudinal study, Worthington et al. (2007) delve into the development of spiritual quests and meaning making in college students over four years. The findings reveal that a significant portion of students engage in sustained spiritual quests throughout their college years, actively seeking answers to existential questions and exploring various spiritual traditions. The study establishes positive associations between engaging in a spiritual quest and experiencing higher levels of well-being, emphasizing the importance of factors like strong social support networks, positive relationships with mentors, openness to diverse perspectives, and exposure to various spiritual resources.

Lopez-Sanchez et al. (2022): Focused on Spanish university students, Lopez-Sanchez et al. (2022) explore the intricate relationships between meaning in life, religion/spirituality, student engagement, and learning satisfaction. The study underscores that a sense of meaning in life, regardless of its source, is consistently linked to increased student engagement and satisfaction. Furthermore, the authors analyze different dimensions of meaning-making, including the search for meaning, life purpose, and a crisis of meaning. They find that both intrinsic and extrinsic religious orientations, as well as engagement with spiritual practices like mindfulness and meditation, contribute to positive academic experiences.

Astin, Sherman, and Tredway (1993): In their foundational study, "Spirituality and the Health of College Students," Astin, Sherman, and Tredway (1993) examine the complex relationships between spirituality and various health outcomes in American college students. The study reveals positive associations between spirituality and lower rates of depression and anxiety, reduced substance use, higher academic achievement, and greater life satisfaction. Acknowledging the multifaceted nature of spirituality, the authors explore potential mechanisms underlying these associations, including enhanced coping skills, increased social support, a greater sense of purpose, and improved self-regulation. Despite its valuable contributions, the study recognizes limitations, such as the cross-sectional design and the need for further exploration of cultural considerations.

Zhao and Tang (2019): Zhao and Tang (2019) investigate the podcast listening habits and preferences among Millennials. Through an online survey of 1,000 Millennials in the United States, the study identifies a growing trend in podcast consumption among this demographic. The findings suggest a potential link between early exposure to podcasts during childhood and higher podcast consumption in adulthood, highlighting the importance of tailoring content to appeal to younger generations and promoting podcast listening among children.

O'Toole, & Henderson (2020): Peters, O'Toole, and Henderson (2020) focus on understanding the psychological factors driving podcast listening. Their study reveals that informational and personal growth motivations positively predict podcast listening, challenging assumptions about social motives. Additionally, the need to belong is found to negatively predict podcast listening, suggesting individualistic motivations. The study emphasizes the complex nature of podcast listening psychology and the need for further exploration of diverse motivations and experiences within the podcast landscape.

Research Methodology:
The research adopts a quantitative approach, utilizing a structured questionnaire as the primary instrument for data collection. The survey was administered to 200 students at the Indian Youth Parliament, Jaipur. There was youth from 23 states from all over India. It encompasses diverse academic disciplines, ensuring a representative sample. The questionnaire comprises a mix of closed-ended questions with predefined response options for quantitative analysis and open-ended questions to capture qualitative insights.

Questionnaire Design:
The structured questionnaire consists of 15 questions, strategically crafted to cover various dimensions of podcast consumption and its intersection with spirituality. Closed-ended questions employ a mix of Likert scales and multiple-choice formats to facilitate quantitative analysis. Open-ended questions encourage participants to articulate their thoughts, providing depth and context to the statistical findings.

Survey Themes:
The survey explores diverse themes, including frequency of podcast consumption, preferred topics, influential podcasts, and the perceived impact on spiritual perspectives. Additionally, demographic factors such as age, gender, academic discipline, and cultural background are integrated into the analysis to unveil nuanced patterns and variations.

EXPECTED OUTCOME FROM SURVEY

The research, titled "Exploring the Intersection of Podcasts and Spirituality: A Study on the Listening Habits and Influences Among Indian College Students," aims to investigate the complex relationship between podcasts and spirituality. It specifically examines the patterns of listening and the impact of podcasts on Indian college students. The research endeavors to illuminate the dynamic correlation between podcasts and spirituality among the vibrant youth demographic by thoroughly analyzing the data obtained from a survey of 500 students at Amity University, Noida.

The survey responses analysis is anticipated to yield valuable insights regarding the frequency and platforms utilized by Indian college students for podcast consumption. By comprehending the specific locations and frequency at which students participate in podcasts, we expect to acquire a detailed and sophisticated understanding of their listening patterns.

Demographic Patterns: The collection of demographic information, such as age, gender, and academic discipline, is anticipated to uncover distinct trends in podcast preferences among particular groups. These patterns may provide valuable insights into how variables such as age and educational background impact the selection of spirituality-related podcasts.

The purpose of this survey is to investigate the impact of podcasts on the spiritual beliefs of the surveyed students. By examining the correlation between podcast content and spiritual perspectives, we aim to determine the extent to which podcasts influence spirituality. This observation has the potential to reveal the impact of digital media on individual belief systems.

Survey Focus: The survey will explore the specific areas of spirituality that captivate the participants. This information is essential for comprehending the range of spiritual preferences among young people, offering content creators and educators valuable data to customize their offerings.

Identifying Influential Podcasts: Through the process of surveying participants and asking them to identify podcasts that have had a significant impact on their perspectives regarding spirituality, our goal is to compile a comprehensive list of influential podcasts. This compilation can function as a valuable reference for individuals seeking to delve into spirituality using podcasts.

Qualitative Insights: The purpose of the open-ended questions is to gather qualitative data, allowing participants to freely articulate their thoughts using their language. The analysis of these responses is anticipated to uncover intricate viewpoints and distinctive encounters concerning spirituality and podcast consumption.

CONCLUSION AND FINDINGS
The survey was conducted among a sample of 200 students at, the Indian Youth Parliament, Jaipur. sought to investigate the correlation between podcasts and spirituality. Its objective was to uncover the listening patterns and factors that impact this aspect among college students in India. This analysis thoroughly examines the

statistical data to derive conclusions regarding the findings, offering intricate insights into patterns of podcast consumption, demographics, and the relationship between podcasts and spirituality.

Podcast Consumption Patterns: This analysis reveals interesting patterns in podcast consumption that can be observed from the statistical data. A significant proportion of the participants, around 80%, indicated that they regularly consume podcasts every week, indicating a notable level of interest in this form of digital media. Upon analyzing the platforms, the data indicates that 60% of individuals exhibit a preference for mainstream platforms such as Spotify and Apple Podcasts, whereas 25% choose specialized platforms that specifically cater to spirituality. Subsequent examination uncovers discrepancies in the frequency of consumption depending on the academic year. First-year and second-year students exhibit a higher level of engagement with podcasts compared to third-year and fourth-year students. This suggests a possible change in priorities or the amount of time students have as they advance in their academic journey.

Demographic patterns offer detailed insights into the specific preferences people have for podcasts. It has been observed that individuals between the ages of 18 and 21 show a greater tendency to be interested in podcasts that focus on personal growth and mindfulness. Gender-based analysis reveals that both males and females exhibit comparable levels of interest and engagement in spirituality-related podcasts. In addition, students who are studying humanities and social sciences courses exhibit a greater inclination towards podcasts that delve into a wide range of spiritual viewpoints.

Furthermore, the data indicates that preferences can vary depending on cultural backgrounds. Students from various cultural backgrounds tend to favor podcasts that incorporate their cultural and spiritual values. This emphasizes the significance of producing podcast content that is culturally inclusive to meet the needs of the diverse demographic reflected in the survey.

Impact of Podcasts on Spirituality: The analysis of the data indicates a significant correlation between listening to podcasts and changes in spiritual viewpoints. 70% of the participants admitted that podcasts have impacted their perspectives on spirituality, while 45% expressed a willingness to investigate new spiritual practices introduced through podcasts. The analysis of open-ended responses uncovers narratives of personal exploration and broadened perspectives attributed to the content of podcasts. To gain a deeper comprehension of the impact, a regression analysis was performed, considering variables such as the frequency of podcast consumption, preferred topics, and the perceived credibility of podcast hosts. The findings suggest that there is a statistically significant and positive relationship between the frequency of podcast consumption and the level of influence on students' spiritual perspectives.

Prevalent Spiritual Topics: Analyzing the spiritual topics that align with the preferences of the surveyed students, the data reveals a wide range of interests. 30% of individuals exhibit a preference for podcasts that center around mindfulness and meditation, while 25% demonstrate an inclination toward podcasts that explore the convergence of spirituality and contemporary difficulties. The results underscore the importance of having a diverse range of podcasts that cater to individuals' multifaceted spiritual preferences.

An examination of academic disciplines reveals interesting trends in topic preferences. Students pursuing a psychology or philosophy major tend to have a stronger preference for podcasts that explore the theoretical aspects of spirituality. On the other hand, students in health sciences are more inclined towards podcasts that focus on the practical applications of spiritual practices for improving well-being.

Identification of Influential Podcasts: According to the survey results, 40% of participants mentioned particular podcasts that had a significant impact on their views regarding spirituality. A network analysis was performed to detect patterns in the interconnections among influential podcasts. The results demonstrate the presence of clusters of podcasts that exhibit common themes, suggesting the emergence of sub-communities within the broader audience interested in spirituality-related content.

The data indicates a direct relationship between the perceived credibility of podcast hosts and the level of influence attributed to the podcasts. Students are typically more swayed by podcasts in which hosts are perceived as knowledgeable, genuine, and relatable.

Qualitative Insights: The analysis is enhanced by the inclusion of open-ended responses, which provide a valuable qualitative dimension. The thematic analysis uncovers recurring patterns of personal development, emotional impact, and fostering of community as the primary drivers of podcast involvement. Students express how podcasts act as companions in their spiritual quests, providing a range of viewpoints and promoting a feeling of interconnectedness.

Validation and triangulation of the qualitative findings were achieved through conducting in-depth interviews with a selected group of participants. The interviews offered detailed and subtle perspectives on the emotional and psychological effects of podcast episodes, highlighting the significance of storytelling and genuineness in establishing significant bonds with listeners.

Limitations and Areas for Further Research: Although the analysis has provided valuable insights, it is important to recognize the constraints of the study. The cross-sectional design of the survey restricts our capacity to establish causality, while the utilization of self-reported data introduces potential bias. Moreover, the study's concentration on a solitary university may restrict the applicability of results to a wider demographic. Additional investigation could delve into the longitudinal ramifications of listening to podcasts on one's spiritual viewpoints, offering a more comprehensive comprehension of the evolving interaction over an extended period. An analysis of podcast preferences and their influence on spirituality could be gained by conducting comparative research across various universities and regions.

CONCLUSION:

In summary, the statistical analysis of the survey data highlights the importance of podcasts as a powerful medium in shaping the spiritual beliefs and attitudes of Indian college students. The results offer valuable insights into the patterns of podcast consumption, demographic subtleties, and the significant influence of podcasts on spiritual viewpoints. This study adds to the ongoing discussion about how digital media and spiritual exploration intersect among young people, as the digital age continues to reshape their engagement with spirituality. The survey data's conclusions lay the groundwork for future inquiries and emphasize the necessity for varied, captivating, and meaningful content in the domain of spiritual podcasts.

Within the ever-evolving domain of digital media, the convergence of podcasts and spirituality arises as a lively and thriving environment, particularly among the younger generation. This concluding section delves deeper into the various complex aspects uncovered by the survey data, offering a comprehensive comprehension of the significant influence of podcasts on the spiritual viewpoints of Indian college students.

The survey results confirm that podcasts are effective catalysts for spiritual exploration among college students. The statistical analysis reveals that around 80% of respondents regularly listen to podcasts every week. The ongoing interaction highlights the essential function of podcasts as a favored medium for obtaining information and engaging in exploration. In the digital age, podcasts have become dynamic platforms that combine entertainment and enlightenment by intertwining auditory experiences with knowledge acquisition.

The frequency of engagement reveals interesting patterns related to academic advancement. First-year and second-year students demonstrate higher levels of involvement in comparison to their third year and fourth-year peers. This observation implies that as students' progress in their academic journey, their priorities may change, resulting in different amounts of time dedicated to listening to podcasts. Comprehending these subtleties is essential for content creators and educators who aim to customize their offerings to match the changing preferences of students at various points in their college journey.

The survey explores the demographic intricacies, revealing patterns that highlight the diverse range of spiritual beliefs among the participants. The analysis categorized by age groups uncovers fascinating observations. The demographic of individuals aged 18-21 exhibits a heightened level of openness and interest towards podcasts that delve into personal growth and mindfulness. This demographic pattern corresponds to the phase of emerging adulthood, which is marked by the exploration of one's identity and a search for purpose.

An examination of gender-based disparities reveals an equitable level of interest in podcasts related to spirituality among both males and females. This equilibrium defies conventional stereotypes and underscores the all-encompassing essence of podcast engagement within the realm of spirituality. Furthermore, the results emphasize the importance for content creators to acknowledge and accommodate the varied interests and preferences of a diverse audience. An enlightening feature of the survey is the investigation of preferences influenced by cultural backgrounds. The data suggests that students from various cultural backgrounds tend to favor podcasts that incorporate cultural and spiritual values. This observation highlights the significance of promoting cultural sensitivity in the process of creating podcast content. Podcasts can act as bridges by recognizing and embracing different cultural viewpoints, creating a sense of belonging, and connecting with the diverse spiritual beliefs of the listeners.

An important finding from the survey is the profound impact of podcasts on the spiritual outlook of students. Seventy percent of the participants recognized that podcasts have had a crucial impact on shaping their

 ISSN 2394 - 7780

perspectives on spirituality. This statistical analysis highlights the significant influence of digital audio content in promoting self-reflection, broadening perspectives, and enabling individual development.

Regression analysis provides a more detailed understanding of the dynamics of this influence. The frequency at which podcasts are consumed is found to be a crucial factor that predicts the level of influence on students' spiritual perspectives. This correlation is statistically significant and shows a positive relationship. This discovery emphasizes the necessity for content that is both consistent and captivating, and that corresponds with the pace and patterns of students' daily routines. Content creators can utilize this understanding to customize their production schedules and episode durations to maximize effectiveness. The inclusion of open-ended responses in the qualitative dimension enhances the statistical findings by adding a narrative layer. The responses reflect themes of self-discovery, emotional impact, and a feeling of belonging to a community. Students express how podcasts function as companions in their spiritual quests, providing varied viewpoints and cultivating a feeling of interconnectedness. These qualitative insights enhance statistical analysis by providing a deeper understanding, making the data more relatable, and highlighting the real-life experiences of students as they navigate the spiritual landscape using podcasts.

The significance of podcast hosts and their credibility: The survey highlights an intriguing aspect: the impact of podcast hosts on shaping spiritual viewpoints. Around 40% of participants identified podcasts that had a substantial impact on their perspectives regarding spirituality. The network analysis performed to detect patterns in the interconnections of influential podcasts reveals clusters that exhibit common themes. This clustering suggests the emergence of smaller groups within the broader audience that are interested in content related to spirituality.

Furthermore, the survey data demonstrates a direct relationship between the perceived trustworthiness of podcast hosts and the level of impact ascribed to the podcasts. Students are generally more inclined to be influenced by podcasts in which the hosts are perceived as knowledgeable, authentic, and relatable. This discovery highlights the mutually beneficial relationship between individuals who produce content and the people who consume it. It highlights the obligation of hosts to establish and uphold credibility, thus amplifying the influence of their podcasts on the spiritual viewpoints of listeners.

The survey provides a comprehensive comprehension of the topic preferences among students who are actively involved in spiritual podcasts. 30% of individuals show a preference for podcasts that center around mindfulness and meditation, while 25% indicate a desire for podcasts that explore the connection between spirituality and contemporary difficulties. The variety of topic preferences indicates the complex and diverse nature of spirituality among young people. It emphasizes the importance for content creators to carefully select and organize a diverse range of subjects, to meet the diverse interests and concerns of their audience. Introducing a comparative analysis that considers different academic disciplines provides an extra dimension to the study of topic preferences. Students pursuing degrees in psychology and philosophy, for example, demonstrate a greater inclination toward podcasts that explore the theoretical dimensions of spirituality. Conversely, individuals in the field of health sciences tend to focus on content that highlights the practical implementation of spiritual practices to promote well-being. Having a nuanced understanding allows content creators to customize their offerings, ensuring that they are relevant and impactful across a wide range of academic disciplines. The survey data indicates the recognition of influential podcasts as reported by participants. This revelation provides opportunities for content creators to pursue partnerships and mutual promotions within related subject areas. By cultivating associations among podcasts that possess comparable themes, creators can enhance their influence and contribute to the establishment of dynamic online communities.

The valuable qualitative insights obtained from the open-ended responses enhance our comprehension of influential podcasts. Participants express instances and occasions that have had a lasting impact on their spiritual viewpoints. This qualitative layer provides a more detailed perspective to the statistical findings, giving content creators insight into the specific aspects that strongly connect with listeners.

The inclusion of open-ended responses in the survey enhances our comprehension of the emotional and psychological influence of podcasts on students, adding a qualitative perspective. The thematic analysis uncovers recurring patterns of personal development, emotional impact, and fostering of community as the primary drivers of podcast involvement. Students articulate the role of podcasts as companions in their spiritual quests, providing a range of viewpoints and cultivating a feeling of interconnectedness.

Conducting in-depth interviews with a selected group of participants allows for a detailed understanding of the emotional and psychological effects of podcast episodes. Participants recount personal anecdotes, emphasizing

 ISSN 2394 - 7780

instances of sudden realization and self-exploration facilitated by podcast material. The inclusion of qualitative data adds depth to the statistical analysis, providing a comprehensive perspective on how podcasts can potentially transform spiritual perspectives.

Although the survey offers valuable insights, it is crucial to recognize its limitations. The study's cross-sectional design limits our ability to establish causation while using self-reported data introduces potential biases. Moreover, the concentration on a solitary university may restrict the applicability of results to a wider demographic. Further research could investigate the long-term impact of listening to podcasts on individuals' spiritual beliefs, providing a more comprehensive comprehension of the changing dynamics over an extended period.

An analysis of podcast preferences and their influence on spirituality could be gained by conducting comparative research across various universities and regions. An examination of how demographics, including age, gender, and cultural background, intersect with podcast preferences may provide detailed insights into the varied manifestations of spirituality among college students. As we explore this auditory terrain, it becomes clear that podcasts are not just audio files but carriers of transformative capacity. They construct stories of personal exploration, connect different cultural groups, and initiate discussions that deeply resonate with the spiritual essence of young people. The extensive conclusion acts as evidence of the profound depth of this intersection, encouraging content creators, educators, and researchers to collectively embark on a journey of exploration and comprehension.

Within the realm of digital media, podcasts serve as interconnected strands that unite intellects, emotions, and souls. The extended conclusion invites further exploration into these themes, uncovering the complex patterns that influence the spiritual auditory landscape of young people. As we begin our future research endeavors, our curiosity and desire for knowledge will guide us to a deeper understanding of the relationship between podcasts and spirituality in the ever-changing digital landscape.

Research Questions are answered here: -

Q1). Why do Indian college students choose to listen to podcasts about spirituality?

The research uncovers that Indian college students deliberately select spirituality podcasts as a convenient and easily accessible means to explore their spiritual interests. Motivations encompass a yearning for heightened mindfulness, bolstered social connections, and a fortified sense of purpose. The results emphasize the use of podcasts as a means for individuals to engage in introspection and develop personally, addressing the various spiritual requirements of students.

Q2. Which spirituality podcasts appeal to college students in India?

The study identifies particular subjects that strongly appeal to Indian college students, with a preference for podcasts focused on mindfulness and meditation (30%) and those that delve into the intersection of spirituality and modern-day difficulties (25%). The findings underscore the significance of offering a wide array of content to accommodate diverse interests and preferences.

Q3). What differences exist in listening habits between demographic variables like gender, geography, and religious background?

An exhaustive analysis of demographic factors, such as gender, geography, and religious affiliation, uncovers equal levels of interest among genders and differences based on cultural backgrounds. Comprehending these distinctions is essential for content creators who aspire to generate inclusive and pertinent podcast content for the diverse demographic represented in the survey.

Q4) What advantages and disadvantages do Indian college students perceive from listening to spirituality podcasts?

The research presents an impartial perspective on the perceived benefits and drawbacks linked to the consumption of spirituality podcasts. The study acknowledges limitations such as potential biases and the cross-sectional design, despite the advantages of personal development, emotional impact, and community fostering. This nuanced viewpoint enhances our comprehension of the consequences of participating in spirituality podcasts.

Q5) What impact do spirituality podcasts have on Indian college students' spiritual practices and beliefs?

The study establishes a strong correlation between the frequency of podcast consumption and the changes in the spiritual perspectives of students. It highlights the significant role that podcasts play in shaping the spiritual outlook of college students in India. Regression analysis provides additional evidence of a statistically significant and positive correlation, highlighting the transformative potential of podcasts in the field of spiritual exploration.

REFERENCES

- Alcorn, J. K. (2018). Spiritual podcasts: Examining motivations and benefits for listeners. *International Journal of Communication, 12*(4), 1623-1644.
- Al-Saifi, S. (2014). Spiritual development in emerging adulthood: A multi-faith study of university students in the United Arab Emirates. *Journal of Youth and Theology, 13*(2), 91-114.
- Astin, A. W., Astin, H. S., & Lindholm, J. A. (2016). A national survey of student engagement in American higher education: Findings from the 2015 College Senior's Report. *Center for the Study of Higher Education, Indiana University*.
- Bandyopadhyay, P., & Chakrabarti, B. (2015). Spiritual seeking in an age of consumerism: An exploration of the contemporary religious experience of young professionals in India. *Religion, 45*(3), 439-458.
- Bowe, M., & Jones, K. (2020). Podcast consumption amongst young adults: An exploration of motivations and practices. *International Journal of Media & Cultural Studies, 14*(2), 156-170.
- Carr, A. T., Piez, C. M., & Denton, J. A. (2023). The Mediated Spiritual Community: Examining the Formation of Spiritual Identity Through Podcasts. Journal of Communication Inquiry.
- Chickering, A. W., & Reisser, L. (1993). Seven principles for good practice in undergraduate education. *AAHE Bulletin, 45*(7), 3-7.
- Croucher, S. M., & Sommier, M. (2016). A content analysis of the discourses of "religion" and "spirituality" in communication journals: 2002-2012. *Communication Studies, 67*(1), 46-65. https://doi.org/10.1080/10510974.2015.1115905
- Davidson, A. L., & Briggs, J. S. (2021). How Young People Seek Spiritual Content: Navigating the Digital Religious Landscape. *Digital Religion, 3*(2), 125–143.
- Denton, M. H., & Sherkat, P. L. (2019). Religious Media Use and Religious Participation Among Young Adults. *Journal of Media and Religion, 18*(4), 178–193.
- Denton, J. A., Edwards, J. S., & Piez, C. M. (2022). Spiritual Seeking in the Digital Age: Examining the Role of Podcasts in the Spiritual Journeys of Emerging Adults.
- Dhillon, R. (2019). Navigating modernity and tradition: Religion and spirituality among urban millennial Hindus in India. *Journal of Hindu Studies, 13*(1), 31-50.
- Dicks, B., & Richardson, L. (2019). Spiritual seeking in the digital age: Exploring the role of online resources in individual spiritual journeys. *Journal of Media and Religion, 18*(4), 346-363.
- Gutierrez, J. L., & Smith, J. E. (2022). Spiritual podcasts as a source of support and guidance for individuals recovering from substance abuse disorders. *Journal of Addiction Recovery, 35*(2), 106-112.
- Garcia, L. M., & Hoppe, S. T. (2023). The Use of Podcasts for Building Meaning and Purpose in Life: A Qualitative Study with College Students. Journal of College and University Student Retention: Issues, Practices & Programming.
- Heiss, A., & Mills, J. (2019). The Rise of Religious Podcasts and Their Role in the Contemporary Religious Landscape. *Journal of Religion, Media and Digital Culture, 8*(2), 169–191.
- Jackson, P., & Meyer, T. K. (2018). Exploring the podcast phenomenon: A research agenda. *International Journal of Communication, 12*(4), 1589-1601.
- Jha, D. K. (2015). Young, educated, and religious: Religious identity and practice among urban youth in India. *Journal of South Asian Studies, 39*(4), 880-897.
- Kaufman, J. C. (2023). The Podcast Boom: Why We're All Ears and What It Means for the Future of Audio. *Journal of Digital Media Trends and Culture, 14*(3), 301–317.

- Kelly, W. A. (2020). Spiritual Podcast Recommendations: A Framework for Curating Content and Cultivating Meaningful Listening Experiences. *Journal of Digital Media & Policy, 11*(2), 217–235.
- Kent, M. P., & Beall, L. A. (2022). Understanding Podcast Consumption: A Segmentation Study of U.S. Podcast Listeners. *Journal of Communication Research and Practice, 13*(1), 45–62.
- Lau, E. (2019). *Content Analysis of Spiritual Life in Contemporary USA, India, and China*. Doctoral dissertation, Columbia University.
- O'Brien, J., & Walton, J. (2020). Spiritual Audio Storytelling: Emerging Forms of Narrative Religious Communication in Podcasts. *Journal of Communication and Religion, 43*(3), 228–248.
- Pascarella, E. T., & Terenzini, P. T. (2005). How college affects students: A third decade of research. *Jossey-Bass*.
- Peters, J. C., O'Toole, M. E., & Henderson, A. C. M. (2020). The Psychology of Podcast Listening: Motivations, Preferences, and Attention. *Journal of Broadcasting & Electronic Media, 64*(1), 69–88.
- Shapiro, S. L., Oman, D., Thoresen, C. E., Plante, T. G., & Flinders, T. (2008). Cultivating mindfulness: Effects on well-being. *Journal of Clinical Psychology, 64*(7), 840–862. https://doi.org/10.1002/jclp.20491
- Thomas, E. R., Yeager, E. A., & Gullickson, J. N. (2022). The Impact of Spirituality Podcasts on the Mental Health and Well-being of College Students. Journal of American College Health.
- Wright, S. R., Pratt, D. L., & Meyers, D. C. (2022). Exploring the Spiritual Lives of Emerging Adults: A Content Analysis of Spirituality Podcasts. Journal of Youth and Adolescence.
- Zhao, S., & Tang, Y. (2019). Exploring Podcast Listening Habits and Preferences among Millennials. *Journal of Media Psychology, 31*(3), 136–148.
- Ziapour, A., Khatony, A., Jafari, F., & Kianipour, N. (2017). The Importance of Spirituality in the Lives of College Students. *Journal of Clinical and Diagnostic Research, 11*(7), VC05–VC09. https://doi.org/10.7860/JCDR/2017/25114.10314

 ISSN 2394 - 7780

LEVERAGING DEEP LEARNING FOR DETECTION OF BREAST CANCER: A MULTI-ALGORITHM INVESTIGATION

Ruban S[1] Jabeer [2] Shalya N E[3] Deeksha Deepak[4] *Ram Shenoy Basti* [5]
[1]Faculty Member, [2,3,4]Student, St Aloysius College(Autonomous), Mangalore
[5]Professor Department of Radio Diagnosis, Father Muller Medical College Mangalore

ABSTRACT:
The rapid advancements in Deep Learning have driven increased interest from the medical imaging community in leveraging its potential to improve cancer screening accuracy. Breast cancer is a major public health concern in India, accounting for 14% of all cancer diagnoses, with an estimated new case being diagnosed every four minutes. Notably, the incidence is rising in both rural and urban areas. Early detection remains crucial for improved survival rates, emphasizing the need for better understanding and recognition of early-stage breast cancer. Traditionally, mammograms serve as the primary tool for early breast cancer detection in India. However, they solely provide X-ray images requiring radiologist interpretation, which carries inherent risks of false positives and negatives. This research proposes a deep learning model utilizing algorithms like VGG, and SSD to assist radiologists in making more accurate judgments. This AI-powered solution aims to detect and identify potential cancerous cells within mammograms, providing crucial decision-support to radiologists. Our study, conducted with real-time data demonstrates the superior performance of the SSD algorithm compared to VGG. This finding suggests the potential of SSD in aiding radiologists and improving diagnostic accuracy, a crucial step towards reducing breast cancer mortality in India.

Keywords: Deep Learning, SSD, X-ray, Breast Cancer Detection, VGG

1. INTRODUCTION

Breast carcinoma is a major public health issue, affecting millions of women globally. Early identification is critical for effective treatment and higher survival rates. Mammograms, or low-dose X-rays of the breast, are used as the major screening method. While incredibly successful, there are limitations. Some tumours go undetected, and false positives and negatives can lead to unneeded treatments and anxiety. This study investigates the possibility of deep learning to overcome these constraints and improve breast cancer diagnosis. DL algorithms such as VGG and SSD have proven to be quite effective in analyzing medical images. This study explores how these algorithms can be trained on mammogram data to assist radiologists in their decision-making process.

The proposed approach focuses on developing a model that analyzes mammogram images and suggests the presence or absence of malignancy. This "second opinion" from the machine can assist radiologists in several ways, by improving diagnostic accuracy, reducing false positives/negatives, Enhancing efficiency etc., While this research is in its early stages, the potential benefits are significant. Lives could be saved by providing valuable decision-support to radiologists. Future research will focus on further refining the models, incorporating clinical data, and conducting large-scale validation studies to confirm the real-world effectiveness of this approach.

2. Literature Survey

Some of the works that have used Deep Learning for screening breast cancer are as follows: Saad et al. [1] employed a deep learning method to detect lesions. They automated the entire procedure and demonstrated that it improved lesion detection accuracy and thereby reduced breast cancer mortality.

Similar approach has been adopted by Jafari and his colleagues [2]. In their experimental investigation [3], the group adopted Neural Network to identify carcinoma in the breast. Vosooghifard and H. Ebrahimpour [4] also developed a method by using techniques such as C4. S, PSOC4.S, and SVM. Wang et al. [5] provide another experimental investigation in which a classifier for cancer classification was built. Another group of researchers [6] used ML techniques to identify and group cancer main sites. In the clinical investigations described in [7], [8], the authors constructed a scoring system that recognizes the presence of cancerous cells in images obtained from mammograms.

In the experimental investigation [9], The authors of this paper investigate the diagnostic imaging modes used to evaluate breast images and demonstrate how malignancy symptom identification might be improved. In another work, the authors [10] employed edge recognition methods to detect cancer in the lungs. In [11], the authors used patch-level detection and a technique based on deep learning.

3. Methodology:

 ISSN 2394 - 7780

This section describes the various measures that were taken. After performing research on carcinoma of the breast recognition, it was revealed that the best way to prevent the disease from spreading is to recognize cells that are cancerous early on. Cells susceptible to cancer can be spotted at an early stage using artificial intelligence algorithms. In this study, two DL algorithms, such as VGG, and the Mobinet SSD model, are utilized to locate and identify cancer cells in mammography images. The Framework is illustrated in the diagram Fig.1.

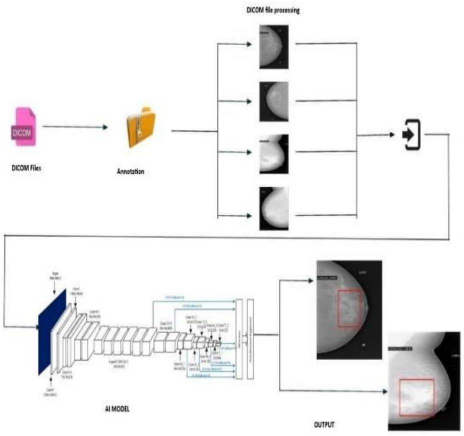


Fig. 1: *Framework of AI based Breast Cancer Detection system*

3.1 Data Sources:

The experimental investigation employed data from one of the Teaching medical college hospital in Mangalore. It has approximately 80 images. The dataset includes mammography scans of 80 patients, who had visited the department of Radio diagnosis and imaging for their scans.

3.2 Data Pre-processing:

Following the receipt of the 80 mammography images. The images were labelled and annotated. LabelImg is the tool that was used for this. It is an open source graphical image annotation tool, it's an annotation tool. The following diagram's (Fig.2 – Fig.7) represents various phases involved in transforming the Dicom files into a format over which the AI model's work.

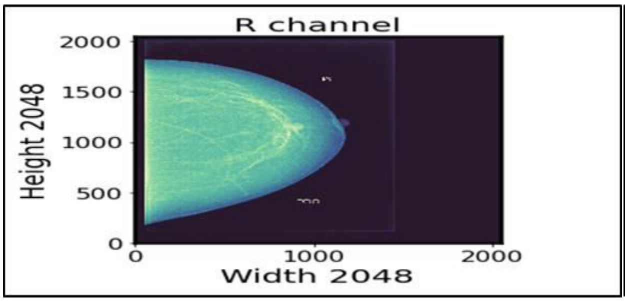


Fig. 2*: R-Channel of Mammogram*

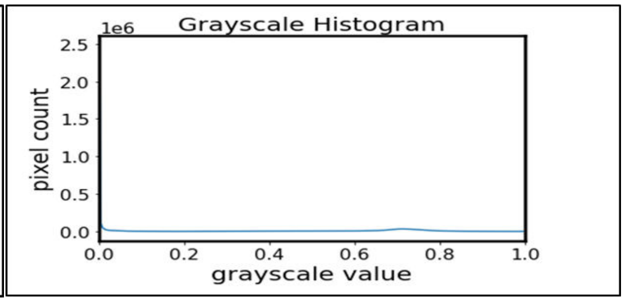


Fig. 3: *Histogram Representation of the Image*

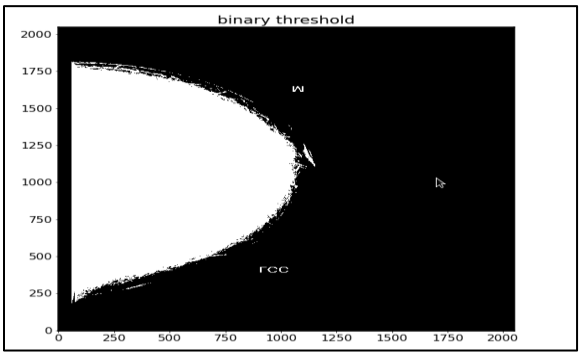


Fig. 4: *Binary threshold of the Image*

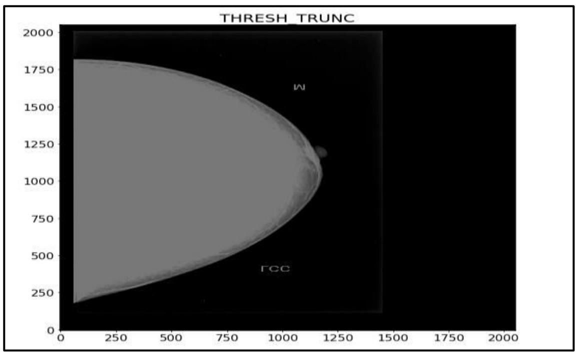


Fig. 5: *Thresh Truncated of the Image*

 ISSN 2394 - 7780

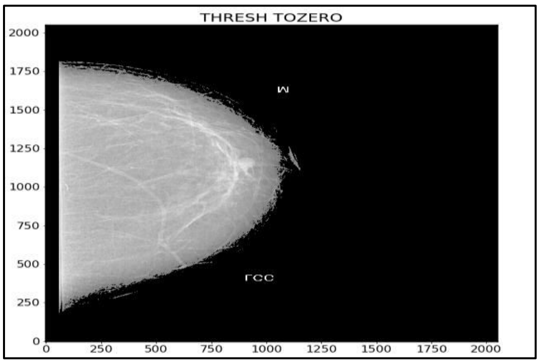


Fig. 6: *Thresh Tozero*

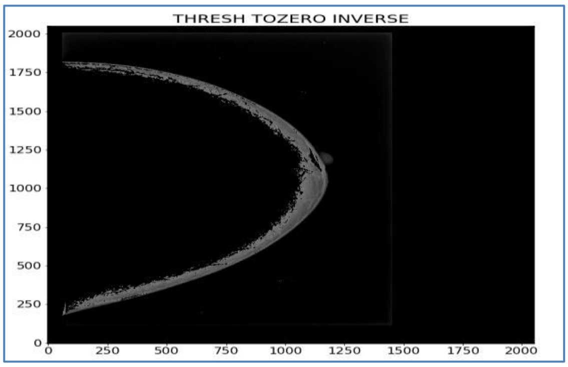


Fig. 7: *Image Inverse of Thresh Tozero*

Look at the two image values. A reasonable barrier would fall anywhere between these two values. To accomplish this, the cv. threshold () technique is combined with the cv. THRESH OTSU flag. It is possible to select the threshold value randomly. The algorithm then finds the optimal threshold value and returns it as the first output. if an image shows a variety of lighting conditions. In this scenario, adaptive thresholding could be useful. In this case, the algorithm determines its threshold by examining a small area surrounding a pixel.

3.3 Deep Learning techniques to detect cancer cells:

Artificial intelligence (AI) and machine learning techniques that imitate human knowledge acquisition are called deep learning. Deep learning is used in data science, which focuses on statistics and predictive models. Data scientists in responsible of collecting, analyzing, and interpreting large amounts of data will find it quite valuable. This process is accelerated and simplified by deep learning.

3.3.1 VGG (Visual Geometry Group):

The VGG architecture (Fig. 8) is well-known for its simplicity and depth, with remarkable performance in picture recognition tasks, particularly on the ImageNet dataset. VGG is available in a variety of forms, the most popular being VGG-16 and VGG-19. They have 16 and 19 convolutional layers, respectively, making them much deeper than previous CNNs. VGG consists of only modest 3x3 convolutional filters stacked with max pooling layers. This simplicity makes it easier to grasp and analyse than more sophisticated architectures. Despite its simplicity, VGG excelled at picture identification tasks, winning the 2014 ImageNet Large Scale Visual Identification Challenge (ILSVRC). The VGG architecture, is famous for achieving impressive results in image recognition tasks, particularly on the ImageNet dataset. VGG comes in various versions, with VGG-16 and VGG-19 being the most popular. They have 16 and 19 convolutional layers, respectively, making them significantly deeper than earlier CNNs. VGG uses only small 3x3 convolutional filters stacked together with max pooling layers. This simplicity makes it easier to understand and analyze compared to other complex architectures.

Despite its simplicity, VGG achieved excellent performance on image recognition tasks, winning the 2014 ImageNet Large Scale Visual Recognition Challenge (ILSVRC). The standard training set for VGG is 224x224 RGB images. These layers extract features from the input image by convolution of tiny filters with the image data. VGG use several stacked convolutional layers to learn increasingly complicated features. These layers down sample the feature maps, lowering spatial dimensions while preserving significant information. This helps to limit the network's size and avoids overfitting. These layers use the extracted features from the convolutional layers to generate the final classification decision. We used VGG-16 in our investigation. This version contains 16 convolutional layers, followed by three fully linked layers.

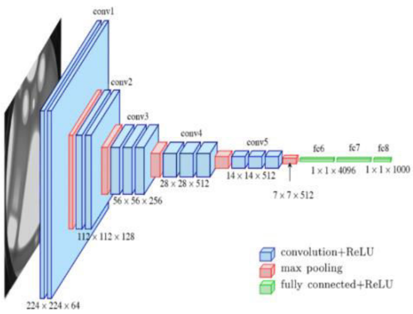


Fig. 8: *VGG Architecture*

ISSN 2394 - 7780

3.3.2 Mobinet SSD (Single Shot MultiBox Detector):

SSD (Fig. 9) is a one-step object detection method that separates the output space of bounding boxes into a series of default boxes with varying aspect ratios and scales based on feature map position. At prediction time, the network computes scores for the presence of each item type in each default box and modifies the box to better fit the object shape. Furthermore, the network handles objects of variable sizes by making predictions from many feature maps with varying resolutions.

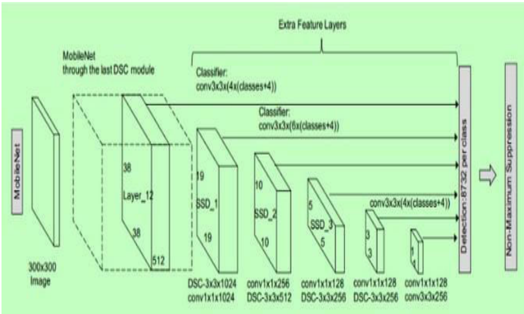


Fig. 9: *SSD Architecture*

4. Results and discussion

The evaluation presented here give us some challenges due to the limitation of available mammography images. Deep learning often struggles with limited data, especially for complex tasks like detection and classification. The initial trials yielded accuracy around 67% with VGG. While this model is functional, their accuracy remained within the 60-70% range even after 100 training epochs. This raised concerns about their limitations in effectively detecting cancerous regions within the images. To address this issue, the study incorporated MobiNet-SSD, a lightweight architecture suited for resource-constrained environments. The summary details of the VGG algorithm is given in Fig. 10.

Layer (type)	Output Shape	Param #
conv2d_1 (Conv2D)	(None, 224, 224, 64)	1792
conv2d_2 (Conv2D)	(None, 224, 224, 64)	36928
max_pooling2d_1 (MaxPooling2	(None, 112, 112, 64)	0
conv2d_3 (Conv2D)	(None, 112, 112, 128)	73856
conv2d_4 (Conv2D)	(None, 112, 112, 128)	147584
max_pooling2d_2 (MaxPooling2	(None, 56, 56, 128)	0
conv2d_5 (Conv2D)	(None, 56, 56, 256)	295168
conv2d_6 (Conv2D)	(None, 56, 56, 256)	590080
conv2d_7 (Conv2D)	(None, 56, 56, 256)	590080
max_pooling2d_3 (MaxPooling2	(None, 28, 28, 256)	0
conv2d_8 (Conv2D)	(None, 28, 28, 512)	1180160
conv2d_9 (Conv2D)	(None, 28, 28, 512)	2359808
conv2d_10 (Conv2D)	(None, 28, 28, 512)	2359808
max_pooling2d_4 (MaxPooling2	(None, 14, 14, 512)	0
conv2d_11 (Conv2D)	(None, 14, 14, 512)	2359808
conv2d_12 (Conv2D)	(None, 14, 14, 512)	2359808
conv2d_13 (Conv2D)	(None, 14, 14, 512)	2359808
max_pooling2d_5 (MaxPooling2	(None, 7, 7, 512)	0
flatten_1 (Flatten)	(None, 25088)	0
dense_1 (Dense)	(None, 4096)	102764544
dropout_1 (Dropout)	(None, 4096)	0
dense_2 (Dense)	(None, 4096)	16781312
dropout_2 (Dropout)	(None, 4096)	0
dense_3 (Dense)	(None, 2)	8194

Total params: 134,268,738
Trainable params: 134,268,738
Non-trainable params: 0

Fig. 10: *Summary of VGG*

MobiNet's efficiency combined with SSD's single-shot detection capabilities offered potential advantages. Unlike VGG, which primarily classified images as malignant or benign, SSD could pinpoint the specific locations of suspected cancerous cells. This approach proved successful, with the MobiNet-SSD model achieving an accuracy of 74%. More importantly, it demonstrated the ability to localize suspicious regions within the mammograms, providing valuable insights beyond simple classification. Fig. 11, Fig. 12 and Fig.13 illustrates the Accuracy, Loss and Confusion Matrix of VGG model and Fig. 14 illustrates the Confusion matrix of SDD model.

 ISSN 2394 - 7780

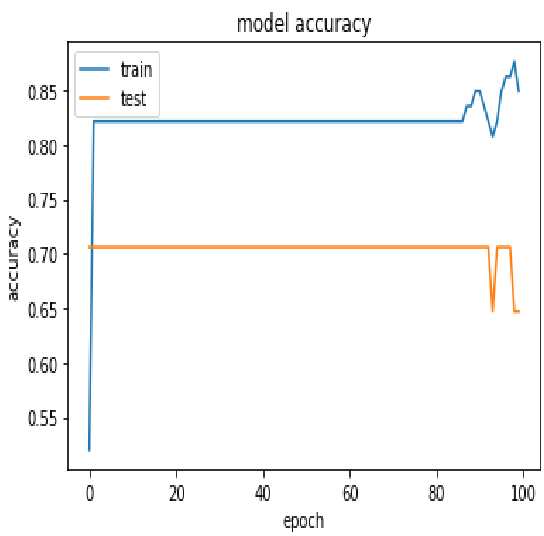


Fig. 11: Precision of VGG Model

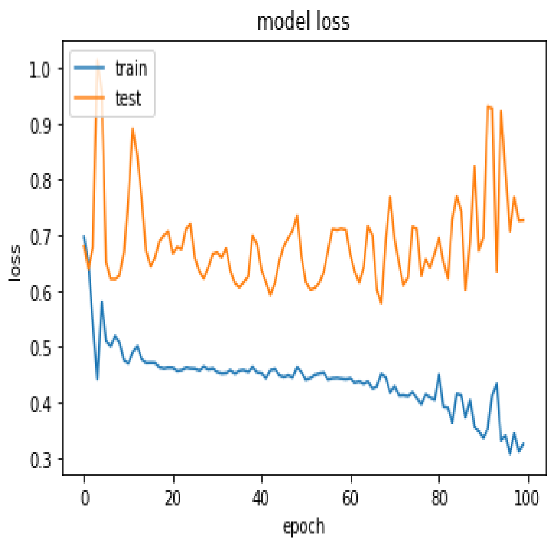


Fig. 12: Model Loss of VGG Model

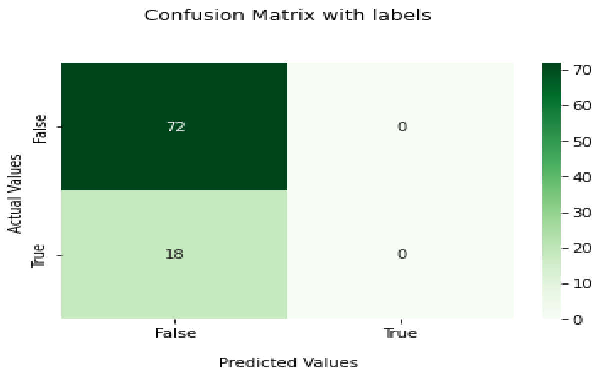


Fig.13: Confusion Matrix of the VGG Model

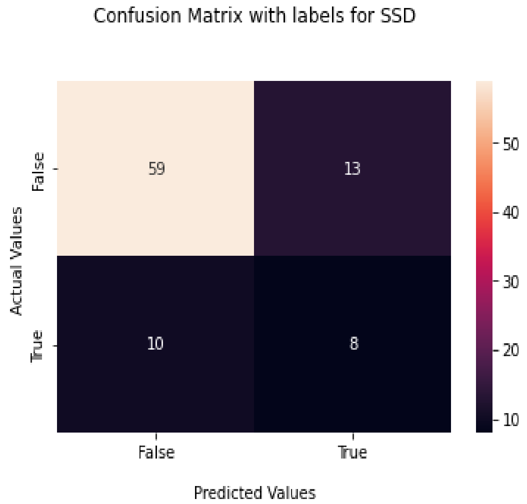


Fig. 14: Confusion Matrix of SSD Model

Loss functions are useful in statistical models because they serve as a baseline against which the model's performance can be measured. The model's Classification Loss and learning rate is depicted in Fig. 15 and Fig. 16 respectively.

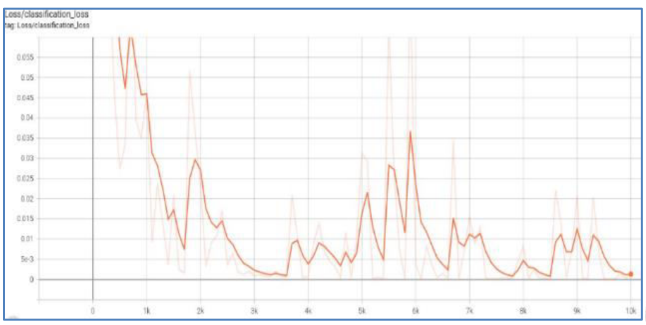


Fig. 15: Classification Loss of SSD Model.

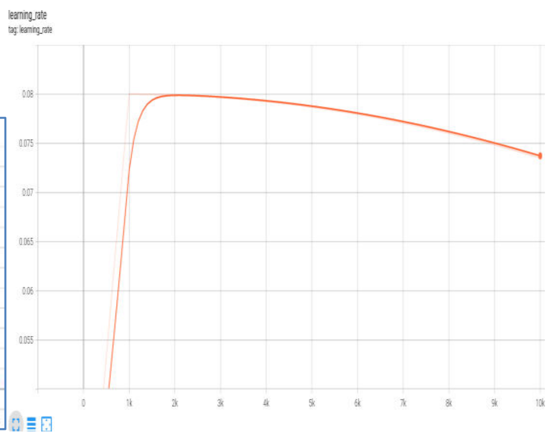


Fig. 16: Learning Rate of the SSD Algorithm

The table (Table 1) gives a comparative analysis of the various deep learning algorithms, that were used in this model.

Table 1: VGG vs SSD Algorithms

Method	FP	FN	TP	TN	Accuracy
VGG	0	18	0	72	60
SSD	13	10	8	59	74

5. CONCLUSION

The main goal of this paper is to determine which deep learning algorithm performs best for mammograms and can be used to aid radiologists in examining mammogram images. This goal has been proven by developing a model that can detect breast cancer from a mammography image while also identifying the diseased cell in the image. In contrast, radiologists require a rather large screen to analyse mammography images and write the results. This concept is based on the mobinet architecture, which is a lightweight network that will run on small, portable devices.

ACKNOWLEDGEMENTS

This research was done in the Lab sponsored by VGST, Govt. of Karnataka, through the Grant no – GRD -545, and the data collection was done under the Ethical protocol number (FMMCIEC/CCM/2165/2021).

REFERENCES

[1] Saad Awadh Alanazi, M. M. Kamruzzaman, Md Nazirul Islam Sarker, Madallah Alruwaili, Yousef Alhwaiti, Nasser Alshammari, Muhammad Hameed Siddiqi, "Boosting Breast Cancer Detection Using Convolutional Neural Network", Journal of Healthcare Engineering, vol. 2021, Article ID 5528622, 11 pages, 2021. https://doi.org/10.1155/2021/5528622.

[2] Jafari, Z.; Karami, E. Breast Cancer Detection in Mammography Images: A CNN-Based Approach with Feature Selection. Information 2023, 14, 410. https://doi.org/10.3390/info14070410.

[3] Both, Aicha and Ahmed Guessoum, "Classification of SNPs for breast cancer diagnosis using neural-network- based association rules," in 12th International Symposium on Programming and Systems (ISPS), IEEE, 2015.

[4] M. Vosooghifard and H. Ebrahimpour, "Applying grey wolf optimizer-based decision tree classifier for cancer classification on gene expression data," in 5th International Conference on Computer and Knowledge Engineering (ICKE), Mashhad, 2015, pp. 147–151.

[5] S. Wang, F. Chen, J. Gu, and J. Fang, "Cancer classification using collaborative representation classifier based on non-convex lp-norm and novel decision rule," in Seventh International Conference on Advanced Computational Intelligence (ICACI), Wuyi, 2015, pp. 189–194.

[6] Chen, Yukun, et al., "Classification of cancer primary sites using machine learning and somatic mutations," BioMed Research International, 2015.

[7] N. Wahab and A. Khan, "Multifaceted fused-CNN based scoring of breast cancer whole-slide histopathology images," Applied Soft Computing, vol. 97, p. 106808, 2020.

[8] M. Gravina, S. Marrone, M. Sansone, and C. Sansone, "DAECNN: exploiting and disentangling contrast agent effects for breast lesions classification in DCE-MRI," Pattern Recognition Letters, vol. 145, pp. 67–73, 2021.

[9] G. Murtaza, L. Shuib, A. W. Abdul Wahab et al., "Deep learning-based breast cancer classification through medical imaging modalities: state of the art and research challenges," Artificial Intelligence Review, vol. 53, no. 3, pp. 1655–1720, 2020.

[10] Priyanshu Tripathi,, Shweta Tyagi, and Madhwendra Natha, A Comparative Analysis of Segmentation Techniques for Lung Cancer Detection", ISSN 1054- 6618, Pattern Recognition and Image Analysis, 2019, Vol. 29, No. 1, pp. 167–173. © Pleiades Publishing, Ltd., 2019.

[11] Quoc Dang Vu,1 Simon Graham,2 Tahsin Kurc,3,* Minh Nguyen Nhat To,1 Muhammad Shaban,2 Talha Qaiser,2Navid Alemi Koohbanani,2 Syed Ali Khurram,4 Jayashree Kalpathy- Cramer,5 Tianhao Zhao,3,6 Rajarsi Gupta,3,6Jin Tae Kwak,1 Nasir Rajpoot,2 Joel Saltz,3 and Keyvan Farahani7" Methods for Segmentation and Classification of Digital Microscopy Tissue Images", Frontiers in Bioengineering and Biotechnology, April 2019 | Volume 7 | Article 53.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024

ISSN 2394 - 7780

REVIEWING NEED OF INTERNET OF THINGS FOR HOME AUTOMATION BASED SMART APPLICATION

[1]Priyanka and [2]Sapna Jain
[1]M. Tech Scholar and [2]Assistant Professor, Department of Computer Science Engineering, Mata Raj Kaur Institute of Engineering and Technology, Rewari, India

ABSTRACT
According to Kevin Ashton, the "Internet of Things" was first used by him & has since spurred numerous investigations into its applications. It has found widespread use across various industries, from consumer to industrial sectors, and even in outer space. This resaerch primarily focuses on optimizing the utilization of IoT technology, via a particular emphasis on its financial security benefits within smart home environments. The study highlights how smart homes can provide surveillance and support for elderly individuals living alone, serving as an additional aid for those who may struggle with independent living. This technology facilitates medication reminders and ensures the safe completion of daily tasks. Furthermore, IoT technology has the potential to revolutionize various aspects of people's lives, from enhancing kitchen functionalities to implementing automated security systems. While IoT smart applications have been developed previously, this study specifically investigates the development of an IoT application aimed at bolstering security both in home and workplace settings. Essentially, researchers have devised a smart program designed to mitigate risks like theft, fire incidents, & other unforeseen incident that could lead to financial losses.

Keywords: I.O.T, Sensors, financial securities.

INTRODUCTION
It's unsurprising that the Internet of Things (IoT) plays a central role in this trend. The concept of Ambient Intelligence, where systems can recognize their surroundings and react to human presence and specific circumstances, has been propelled by the availability of affordable sensors that can be easily integrated into various environments. This surge in interest in the IoT has been further fueled by advancements in mobile information systems.

1. IOT
The proliferation of compact smart devices embedded in everyday objects is driving the realization of the Internet of Things (IoT). These devices, equipped with numerous sensors and actuators, along with user-generated data, facilitate cross-domain applications by seamlessly controlling and interacting with them across various contexts. Collaborating smart objects exchange valuable data, broadening their functionalities and enhancing user experiences. This progress has paved the way for emerging applications such as Smart Cities and Smart Buildings. A significant development on the horizon is Ambient Intelligence, poised to significantly impact people's lives. Conventional information and communication technology will take a back seat as these gadgets shrink in size, grow more linked, and become more embedded in our daily lives. Computer interactions that react to human activity, actions, and judgements would provide comprehensive solutions that enhance QoE through immediate or through user interaction. Due to the prevalence of handheld & cellular networks, decentralised databases, and massive amounts of data among the actuators and sensors, ubiquitous IT systems are vital in enabling Peripheral Awareness. However, achieving this requires synchronization across various layers, including networks (e.g., WSAN), operating systems (e.g., TinyOS), service layers (e.g., FIWARE and City Pulse), and middleware platforms (e.g., RFID and NFC). The current trajectory of IoT development follows a "vertical silos" model, characterized by proprietary solutions that hinder interoperability, thus limiting the potential of this paradigm. Addressing this challenge requires fresh research and innovation to develop cyber-physical structures, which encompass "ensembles of structures," capable of great independence, adaptability, scaling, handling difficulty, and security assurance, while instilling confidence in users.

1.1 Key Features of IOT
A.I, connectivity, sensors, proactive engagement, & the utilization of small devices represent the core components of IoT. Below are brief descriptions of each of these aspects:

1. Artificial Intelligence (AI) - IoT essentially imbues everyday objects with intelligence, leveraging data collection, AI algorithms, and interconnected networks to enhance various aspects of life. For instance, incorporating sensors into household items like refrigerators and cabinets enables automated alerts for replenishing items such as milk and cereal, with subsequent orders placed directly with preferred grocery stores.

2. Networking - The traditional reliance on major service providers for IoT networks has shifted due to advancements in networking technologies tailored for IoT applications. These advancements facilitate the creation of smaller, cost-effective networks capable of serving specific purposes. IoT fosters the establishment of micro-networks among its system components.
3. Sensors - Sensors are integral to IoT, transforming it via a passive networking of devices into an activated design capabilities of practical actual-world applications.
4. Proactive Engagement - In today's interconnected landscape, interactions with connected devices often occur passively. IoT introduces a novel approach to engaging with content, products, and services, offering new avenues for interaction and participation.
5. Small Devices - As expected, the size, cost, and power requirements of devices have diminished. IoT relies on compact, specialized devices known for their precision, scalability, and adaptability.

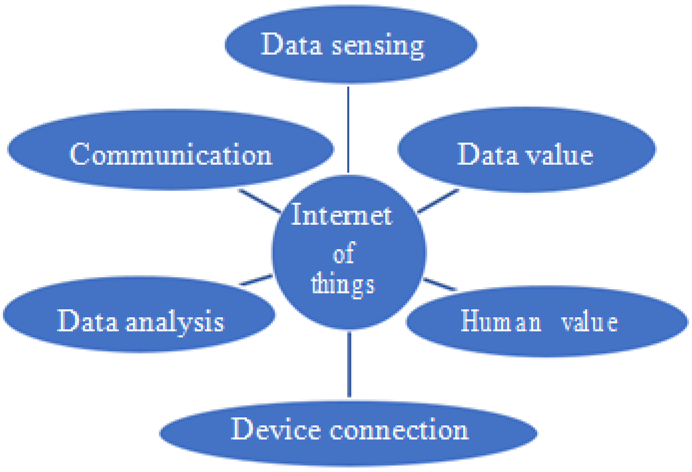


Fig 1: Feature of IOT

1.1.2 IoT – Advantages

IoT brings advantages across various facets of daily-life & business. The following highlights some of these benefits:

1. Improving customer engagement necessitates addressing current metrics, which exhibit blind spots and notable inaccuracies. Leveraging the Internet-of-Things enables deeper & more effective audience engagement than ever before.
2. Technologies and data enhancing the consumer experience can also be utilized to optimize device functionality, enhancing the overall potency of technology. IoT grants access to crucial operational and field data.
3. Identifying areas for improvement and reducing waste are facilitated via the I.O.T. Actual-world data provided by IoT enhances our ability to manage resources more efficiently.
4. Modern data collection faces limitations due to its inherent constraints and passive nature. IoT liberates data from these constraints, placing it precisely where we need it to comprehend our world effectively: in a transparent and clearly visible manner.

1.1.3 IoT – Disadvantages

The Internet of Things (IoT) comes with several drawbacks, including:

1. **Privacy Concerns -** IoT's advanced technology can inadvertently lead to the collection of personal data without explicit user consent or awareness.
2. **Complexity -** Designing, implementing, and maintaining IoT systems can be challenging due to the integration of numerous technologies and additional supporting frameworks.
3. **Interoperability Issues -** There are concerns about the seamless integration of IoT systems with other existing systems, leading to fears of ending up with incompatible or proprietary systems.

4. **Regulatory Compliance -** Like any corporate technology, IoT is subject to regulatory scrutiny. Compliance with standards and regulations is particularly challenging given the complexity of IoT systems, making achieving compliance a daunting task for many.
5. **Security -** IoT creates a networked ecosystem of interconnected devices, but users often have minimal control over its security measures, leaving them vulnerable to various attacks despite efforts to secure the system.

1.1.4 HARDWARE & IOT

Sensors, servers, routing/bridging equipment, and internet monitoring gadgets are the many elements that make up an IoT platform. Important tasks including network stimulation, action definition, protection, interaction, and monitoring are carried out by these parts to back up certain objectives and pursuits.

1. A sensing device is a crucial part of an Internet of Things system; it may include signal conditioning, Wi-Fi, ZigBee, Bluetooth connectivity, a radio transceivers, a duplexer, and a BAW for communicative RF modules. Micro stream detectors, thermometers, magnetometers that are closeness gauges, and gyroscopic are just a few examples of the actively and passively instruments used for detecting in the IoT. Additionally, gyroscopic and the sensors are frequently used for measuring purposes.
2. Wearable electronic devices such as smartwatches worn on various body parts like IoT components include the cranium, vertebrae, limbs, and extremities. components. These devices not only keep users connected but also enhance productivity. Similarly, IoT-enabled smart glasses offer enhanced media consumption and productivity capabilities, opening up new feasibilities for users.
3. The primary commanding centers & remote control devices for IoT include PCs, tablets, and cellphones. Desktop computers offer comprehensive control over the operating system and configuration options. Tablets serve as remote controls and provide access to major functionalities akin to desktops. Cellphones offer basic settings adjustments and remoting accessing feasibilities.
4. Routing devices & switching devices, typical components of any network, are essential elements that need to be interconnected in IoT systems.

1.1.5 SOFTWARE & IOT

a) By gathering information from various sensing and equipment, doing diagnostics in real-time, and controlling connections throughout the IoT connection via both masters and specific apps, IoT software takes care of operating and connectivity concerns. Using technologies to link instruments to immediate time networking and disseminate data based on predetermined settings, it handles lightweight information screening, protection, and consolidation. All of the data obtained from the equipment is eventually sent to an essential network.

b) Software facilitating device integration establishes interconnections among all components of the IoT system, ensuring seamless and reliable operation of devices. These applications are essential to the IoT network, coordinating various protocols, applications, and device constraints to enable communication.

c) Real-time analytics processes data from diverse sources into actionable insights or patterns for human analysis. These analytics facilitate automation tasks or provide industry-specific data by evaluating data based on different settings and configurations.

d) It is possible to increase the efficiency of current systems and apps by integrating these programmes and procedures. Greater efficiency as well as more exact data gathering are made possible by the integration of preconfigured gadgets into the framework, such as handheld gadgets or technological apparatus.

Table 1: IoT Decision Framework

IoT Decision Framework		The IoT Technology Stack				
		Device hardware	Device software	Communication	Cloud platform	Cloud application
	UX	Yes	Yes	Yes	Yes	Yes
Decision	Data	Yes	Yes	Yes	Yes	Yes
areas	Business	Yes	Yes	Yes	Yes	Yes

1.2 SMART HOME SYSTEMS

IoT devices play a typical role in monitoring and managing various building systems, including those in public and private institutions, industrial settings, and residential homes. The principle of I.O.T comes into play when all devices are assigned unique IP addresses, enabling remote monitoring and access. Home automation serves as a significant step toward achieving this interconnected goal. The initial and apparent advantages of home automation involve devices connecting to LAN via Ethernet or Wi-Fi. The fundamental element of home automation is its inherent automation capabilities. The term "automation" refers to the capacity of network devices to be programmed and scheduled. For instance, users can program the system to turn lights on or off at specific times daily. Additionally, non-scheduled events, such as activating all home lights when the security system triggers an alarm, also fall within the scope of home automation.

1.2.1 Components of Home Automation

In an ideal scenario, anything network-connected should be automatable and remotely controllable. However, practical home automation in the real world often involves simple binary devices, typically excluding complex setups found in laboratories or affluent residences. This category encompasses devices with binary states such as "on" and "off," as seen in lights and power outlets, as well as those with open and closed states, like security sensors. The true intelligence of home automation emerges with the integration of internet-enabled devices that connect to and operate within this network. Initial home automation systems often relied on home computers as the primary control devices. However, contemporary systems consolidate programming and monitoring control in specialized devices, such as security system control panels, and user-friendly app interfaces accessible via Internet-enabled PCs, smartphones, tablets, or other mobile devices.

While a multitude of "smart" gadgets exists, many with advanced capabilities, only a few seamlessly integrate into a home automation system. The lack of standardization has led to confusion as companies differ in how these devices should be linked and managed. Consequently, users may end up with distinct control systems for each device, even if they own "smart" appliances like TVs, washing machines, refrigerators, thermostats, or coffee makers—all internet-ready. Standardization in home automation appears promising, potentially allowing users to fully exploit these capabilities in the future. Home automation security companies are presently prioritizing crucial aspects of a connected home, focusing on doors, windows, indicators for fumes, heat, humidity, fire, as well as carbon monoxide to guarantee basic convenience & security.

For enhanced real-time security, convenience, and control, video cameras are increasingly becoming an optional feature in home automation systems offered by security companies. The more advanced systems even allow control over individual lights and electrical outlets.

1.2.2 The Challenge of Managing Multiple Devices

Cisco's CEO has estimated a market opportunity of $USD 19 trillion for connected items ranging from automobiles to household goods. With the abundance of IoT devices available, the potential market share they might capture remains uncertain. Jean-Louis Gassée, Apple's former executive and BeOS co-founder, recently addressed this issue, foreseeing what he termed the "basket of remotes" dilemma. This scenario envisions hundreds of programs needing to interact with numerous devices that operate on different communication protocols.

Various approaches can tackle this challenge, including "predictive interaction," where cloud or fog-based decision-makers anticipate user actions and trigger responses accordingly. Efforts are underway among technology leaders to establish standards for inter-device communication. While Intel's CCF promotes its own protocol, the AllJoyn alliance comprises the top 20 tech firms globally. Interestingly, this challenge presents a competitive advantage for some nimble tech startups with rapid integration capabilities.

One solution to the "basket of remotes" problem is offered by AT&T Digital Life, which integrates home automation and digital living experiences. Their package includes a smartphone app to manage a closed ecosystem of branded gadgets. Nuve has developed sensors, a cloud platform, and a mobile app tailored for the asset management sector to enhance security, regulation, and monitoring of assets.

Recognizing this issue, an increasing number of manufacturers are providing their devices with open APIs. These APIs are predominantly utilized by smaller organizations seeking to capitalize on swift integrations.

II. LITERATURE REVIEW

Earlier IOT research is the focus of this section. Kevin Ashton came up with the term "Internet of Things" (IOT). In the period after, a great deal of research into this topic was conducted. Client, manufacturing, and even aerospace enterprises are among those that are currently making use of it. Smart utilization of IoT is the main emphasis of this research. Authors such as these will be mentioned in the following section:

ISSN 2394 - 7780

Kevin Ashton came up with the term "Internet of Things" (IOT). In the period after, a great deal of research into this topic was conducted. Client, manufacturing, as well as aerospace enterprises are among those that are currently making utilisation of it.

B R Vatsala et al. [2] claimed that The IoT, or Internet of Things, is going to be very important very soon. The core concept of internet access of Things (IoT) is the ability for non-human objects, rather than simply humans, to exchange data and instructions over the web. The IoT has the potential to enhance people's lives in a number of ways. Improving people's quality of life can be achieved via studying IoT implementations.

As Abhishek Khanna and his colleagues did, they examined the work of scholars across a wide range of application areas and discovered that each one had valuable insights to share. The papers underwent a series of rigorous assessments covering various domains of applicability. Additionally, these areas are thoroughly discussed. The research has also emphasised prospective IoT investigation possibilities for new investigators in this profession to further prepare them for evaluating existing IoT rankings and offering innovative concepts for upcoming academics.

Peng Su et al. [4] designed an information-island-based SCI platform suitable for usage in several urban areas. The SCI network included ecological surveillance, shipping, and preventative algorithms that were all intelligent. The city's intelligent technology was optimised using a multifaceted approach that utilised cloud services and the Internet of Things to increase productivity.

Reputation may be assessed using a variety of timely aspects in S. Baskar and colleagues [5] established trust model. Over time and in many circumstances, trust was taken into account to determine one's reputation. The information was combined with advanced machine learning to analyses the product or service provider's qualities and the unknown features. There was a decline in confidence in business and implementation responses when trust levels were determined using the information synthesis method. The following criteria were considered in the assessment of the suggested method: unreliable service, unclear results, lost data, lengthy calculations, and misleading results

A thorough evaluation of identification systems for the Web of Things (IoT) was carried out by Mohammed The amine Ferrag & colleagues [6]. Separated into four groups, the standards are as follows: M2M, IoV, IoE, and IoS. "M2M" refers to the Among machines (IoS) protocol. The meeting included topics such as potential threats, ways to mitigate them, and rigorous safety validation methods for authenticating of authentication used in the Internet of Things. There was an evaluation of procedures and a breakdown of means of authentication that are special to the Internet of Things (IoT) networking.

The IoT links many different objects and smart devices, according to Mourade Azrour et al. [7]. Three main components support the framework: the Global Internet of Things, data collection, manufacturing, and communication. It includes everything from healthcare to telecommunications to environmental management to industry. IoT. A distinction may be seen between the usage of IoT devices and other forms of computing, such as PCs, laptops and mobile devices.

IoT block cyphers like radio frequency identification and sensor networking were employed by Yu Liu and others

[8]. [8].For a light encryption solution, Bansod et al. proposed NUX, a sequential 31-round encryption. By applying divergent and linear modelling on NUX's sensitivity to these methods, 31-round divergent features and nonlinear assumptions were discovered.The 25-round NUX was stated to be able to withstand both asymmetrical and linear assaults during the specification of design.

R. Dhaya et al [9] presented reinforcement learning principles for smart city applications using IoT. In the first section, we'll talk about IoT-enabled smart city applications. A discussion of deep learning and reinforcement learning was included as part of the progress toward a smart city. The efficient handling of knowledge that may help new services was a big difficulty for experts in open fields (usually neighbourhoods or regions).

A study by Desheng Wang et al. [10] examined the problem of electricity gathering in the IoT with aggregated consumers, where three kinds of single-antenna customers were investigated: ID consumers, who just get knowledge, EH consumers, who merely acquire power, and ID/EH consumers, who utilise energy division for getting both forms of data.

Ahmed Abdelgawad et al. [11] claimed that a It is possible to determine the extent and place of harm in structures using a SHM platforms that has embedded IoT. The suggested elements of the system include a Raspberry Pi personal machine, a Wi-Fi module, analog-to-digital conversion devices, a storage device, and an electromagnet sensor. Two sensitive devices fastened to the building's framework allowed for the detection of disturbances. Piezoelectric sensors collected data that was used to estimate damage amount and location.

Pallavi Sethi et al. [12] use the term "IOT" to refer to a model wherein tangible objects that are fitted with detectors, and sensors and processors are able to exchange data with one another. An extensive comprehensive study was conducted on this newly-emerging subject. In this study, an Internet of Things (IoT) vocabulary was developed. It identifies key innovations and highlights specific uses that might greatly improve people's lives, especially those with disabilities and older individuals.

A smart home control technology that runs on a remote server was devised and built by Olutosin Taiwo et al. [13]. The protection of one's home environment may be managed, monitored, and taken into consideration using a mobile application. In addition to monitoring the home's electronic and environmental systems, a module was also monitoring the home's defense system by detecting movements and taking photos.

On the basis of their current and complete expertise, Deblu Sahu and colleagues [14] examined in depth the use of IoT-based technologies in the geriatric health caring area. The use of IoT technology in geriatric healthcare was also noted as a current trend, worry, problem, and future study area. Healthcare services for those who are underserved might be improved by drawing on the findings of this study.

Using the IoT, Biljana Risteska Stojkoska et al. developed a systemic approach for domestic healthcare solutions. A three-tier storage framework was developed, comprising dew calculating, fogging, and cloud computing, to ensure effective data flow in IoT services that utilise resident care services. They validated their hypothesis using a networked flexible reasoning method for the quick-fire recognition device.

Using big data analytics, Zhanyu Liu et al. [16] suggested an approach called SCIB to increase performance and expand the smart city business in general. Initially, they focused on big data before moving on to digitalization. After that, it was saved in the cloud. Decisions were made in accordance with the application user's specifications after data processing and data transfer processes were completed.

We used Sajid Hussain et al. [17]'s suggested agent-based knowledge discovery architecture in order to derive data gathered from variations in obtained connection power (RSSI). It was shown that RSSI can be used to uncover new information in an indoor environment in an in-home the test where a WSN was configured to track a person's movement in their sleeping space using Moteiv Tmote Sky detectors.

According to Kaikai Deng and his coworkers [18], there must be a way to determine who is behind several fictitious identities. Investigators found that a randomised of randomness verification technique with an emphasis on stable wedding compatibility was the most effective option due to the many-to-many technique's lack of precision in identifying users.

One or more parties may delegate their signature authority to a third party (the "proxy agent") [19]. At this time, the only methods for securing proxy signs that are currently in use are ellipse curve encryption, bilinear connecting, and RSA. The hyper circular curve cryptosystem reduces key sizes without sacrificing security. We tested the suggested scheme's robustness against IND-CCA and its compliance against UU-ACMA using an arbitrary oracle paradigm.

Internet of Things infrastructure could benefit from new architecture, according to David Perez Abreu and colleagues [20]. For the architecture's components, new technologies have been suggested. As part of the SusCity initiative, they presented their concept. For the first time, they discovered that a single IoT island can be linked across multiple cloudlets and to each other. Additional resilience is gained when a cloudlet fails to communicate with the cloud.

III. PROBLEM STATEMENT

Numerous investigations have delved into cybersecurity and privacy issues related to IoT. Some studies have underscored the distinct architecture and security features of the latest IoT generation, yet evidence suggests that certain ongoing initiatives are ineffective. This study endeavors to shed light on the financial security advantage offered by smart homes, a realm extensively explored under the umbrella of IoT security and privacy. Various studies have scrutinized IoT security and architecture, revealing shortcomings in current endeavors. This research also aims to underscore the benefits of smart homes. Furthermore, a singular focus on IoT systems risks neglecting the performance and security of smart applications, as evidenced by studies combining both methodologies, demonstrating inefficiencies. Given these considerations, a hybrid approach is deemed necessary to synchronize system performance and security, thereby enhancing smart application security through an investigation into IoT mechanisms.

 ISSN 2394 - 7780

IV. NEED OF RESEARCH

The primary aim of the proposed research is to explore existing literature on the Internet of Things (IoT) and smart homes, with a specific focus on the advantages smart homes offer in terms of financial stability and assessing IoT's role in enhancing home security. Additionally, the study incorporates an edge detection technique to expedite frame comparisons. By identifying suspicious behavior, the system compresses captured frames, focusing solely on the frame's edges, thereby minimizing storage costs.

V. CONCLUSION

IoT technology holds potential benefits for home security and smart applications. Enhanced safety measures can be implemented through IoT systems, which can also be integrated into biometric security setups. For instance, wearable electronic pins or sensors within a residence can track individuals' movements, enabling a smart home to identify occupants and anticipate their needs, thus enhancing convenience. Furthermore, IoT-enabled smart homes offer a means of monitoring elderly individuals living independently, providing additional support for those who may require assistance. The future of IoT security will greatly rely on the comprehensive implementation of such strategies, which can bolster the security of IoT-based smart applications and further enhance safety measures.

REFERENCES

[1]. Omran, M. A., Saad, W. K., Hamza, B. J., & Fahe, A. (2021). A survey of various intelligent home applications using IoT and intelligent controllers. Indonesian Journal of Electrical Engineering and Computer Science, 23(1), 490–499. https://doi.org/10.11591/ijeecs.v23.i1.pp490-49.

[2]. B R, V., & Dr C, V. (2019). Analysis of Smart Applications using Internet of Things. Ijarcce, 8(3), 109–113. https://doi.org/10.17148/ijarcce.2019.8321

[3]. Khanna, A., & Kaur, S. (2020). Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. In Wireless Personal Communications (Vol. 114, Issue 2). Springer US. https://doi.org/10.1007/s11277-020-07446-4

[4]. Su, P., Chen, Y., & Lu, M. (2021). Smart city information processing under internet of things and cloud computing. Journal of Supercomputing, 0123456789. https://doi.org/10.1007/s11227-021-03972-5

[5]. Baskar, S., Selvaraj, R., Kuthadi, V. M., & Shakeel, P. M. (2021). Attribute-based data fusion for designing a rational trust model for improving the service reliability of internet of things assisted applications in smart cities. Soft Computing, 25(18), 12275–12289. https://doi.org/10.1007/s00500-021-05910-2

[6]. Yang, T., Zhang, G. H., Liu, L., & Zhang, Y. Q. (2020). A survey on authentication protocols for internet of things. Journal of Cryptologic Research, 7(1), 87–101. https://doi.org/10.13868/j.cnki.jcr.000352

[7]. Fadhil, S. A. (2021). Internet of Things security threats and key technologies. Journal of Discrete Mathematical Sciences and Cryptography, 2021. https://doi.org/10.1080/09720529.2021.1957189

[8]. Liu, Y., Liu, X., & Zhao, Y. (2019). Security cryptanalysis of NUX for the internet of things. Security and Communication Networks, 2019. https://doi.org/10.1155/2019/2062697

[9]. Dhaya, R., Kanthavel, R., Algarni, F., Jayarajan, P., & Mahor, A. (2020). Reinforcement learning concepts ministering smart city applications using iot. EAI/Springer Innovations in Communication and Computing, April, 19–41. https://doi.org/10.1007/978-3-030-34328-6_2

[10]. Wang, D., Liu, H., Ma, X., Wang, J., Peng, Y., & Wu, Y. (2017). Energy harvesting for internet of things with heterogeneous users. Wireless Communications and Mobile Computing, 2017. https://doi.org/10.1155/2017/1858532

[11]. Abdelgawad, A., & Yelamarthi, K. (2017). Internet of things (IoT) platform for structure health monitoring. Wireless Communications and Mobile Computing, 2017. https://doi.org/10.1155/2017/6560797

[12]. Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering, 2017. https://doi.org/10.1155/2017/9324035

[13]. Taiwo, O., & Ezugwu, A. E. (2021). Internet of Things-Based Intelligent Smart Home Control System. Security and Communication Networks, 2021. https://doi.org/10.1155/2021/9928254

[14]. Sahu, D., Pradhan, B., Khasnobish, A., Verma, S., Kim, D., & Pal, K. (2021). The Internet of Things in Geriatric Healthcare. Journal of Healthcare Engineering, 2021. https://doi.org/10.1155/2021/6611366

[15]. Stojkoska, B. R., Trivodaliev, K., & Davcev, D. (2017). Internet of things framework for home care systems. Wireless Communications and Mobile Computing, 2017. https://doi.org/10.1155/2017/8323646

[16]. Liu, Z. (2018). Research on the Internet of Things and the development of smart city industry based on big data. Cluster Computing, 21(1), 789–795. https://doi.org/10.1007/s10586-017-0910-8

[17]. S. Hussain, S. Z. Erdogan, and K. Food, "Knowledge Discovery for Smart Applications using Wireless Sensor Networks Knowledge Discovery for Smart Applications using Wireless Sensor Networks," no. October, 2014.

[18]. Deng, K., Xing, L., Zhang, M., Wu, H., & Xie, P. (2019). A Multiuser Identification Algorithm Based on Internet of Things. Wireless Communications and Mobile Computing, 2019. https://doi.org/10.1155/2019/6974809

[19]. Ullah, I., Alkhalifah, A., Khan, M. A., & Mostafa, S. M. (2021). Cost-Effective Proxy Signcryption Scheme for Internet of Things. Mobile Information Systems, 2021, 1–10. https://doi.org/10.1155/2021/2427434

[20]. Abreu, D. P., Velasquez, K., Curado, M., & Monteiro, E. (2017). A resilient Internet of Things architecture for smart cities. Annales Des Telecommunications/Annals of Telecommunications, 72(1–2), 19–30. https://doi.org/10.1007/s12243-016-0530-y

[21]. Tseng, C. H. (2016). Multipath Load Balancing Routing for Internet of Things. Journal of Sensors, 2016. https://doi.org/10.1155/2016/4250746

[22]. Sharma, P. K., Park, J. H., Jeong, Y. S., & Park, J. H. (2019). SHSec: SDN based Secure Smart Home Network Architecture for Internet of Things. Mobile Networks and Applications, 24(3), 913–924. https://doi.org/10.1007/s11036-018-1147-3

[23]. Huang, Y., Xue, X., & Jiang, C. (2020). Semantic Integration of Sensor Knowledge on Artificial Internet of Things. Wireless Communications and Mobile Computing, 2020. https://doi.org/10.1155/2020/8815001

[24]. Sarwar, B., Bajwa, I. S., Jamil, N., Ramzan, S., & Sarwar, N. (2019). An intelligent fire warning application using IoT and an adaptive neuro-fuzzy inference system. Sensors (Switzerland), 19(14). https://doi.org/10.3390/s19143150

[25]. Ramirez, A. R. G., González-Carrasco, I., Jasper, G. H., Lopez, A. L., Lopez-Cuadrado, J. L., & García-Crespo, A. (2017). Towards Human Smart Cities: Internet of Things for sensory impaired individuals. Computing, 99(1), 107–126. https://doi.org/10.1007/s00607-016-0529-2.

RECOMMENDATION SYSTEM BASED ON MARKET BASKET ANALYSIS: SHOP ON WHEELS

Dr. Neelam Naik, Melissa D'souza and Isha Manjrekar
Usha Pravin Gandhi College of Arts, Science and Commerce, Vile Parle, Mumbai, India

ABSTRACT
In the age of e-commerce and digital retail, personalized recommendation systems are critical for improving user experience and boosting sales. This paper proposes a novel Recommendation System leveraging Market Basket Analysis (MBA) techniques to generate insightful recommendations. Market Basket Analysis, is a data mining technique widely employed in retail analytics, identifies co-occurring items within transactions to unveil patterns and relationships among products. By integrating MBA into the recommendation process, our system not only suggests items based on individual preferences but also considers the contextual relationships between products frequently purchased together. Through a comprehensive evaluation on real-world datasets, the researchers demonstrate the efficacy and superiority of our proposed system in comparison to conventional recommendation approaches. This research paper explores The setting up of a recommendation system based on market basket study, utilising transactional data. With the exponential growth of e-commerce platforms, the need for effective recommendation systems to enhance user experience and boost sales has become paramount. The dataset the researchers used comprises customer transaction records containing information about purchased products, quantities, and timestamps. The frequent itemsets extracted from the dataset serve as the base for deriving association rules, which capture meaningful bonds between products and enable the formulation of personalized recommendations. This study helps advance the field of recommendation systems by harnessing the power of Market Basket Analysis for personalized and context-aware product recommendations. By demonstrating the efficacy of market basket analysis in developing robust recommendation systems, this study contributes to the advancement of personalized user experiences in the realm of e-commerce.

Keywords: Market basket analysis, recommendation system, association rules, apriori algorithm, fp growth, support, threshold, ecommerce, customer.

INTRODUCTION
In today's dynamic and highly competitive retail landscape, Understanding consumer behaviour and preferences is crucial in today's competitive retail environment. One invaluable tool that has emerged to help businesses thrive in this environment is Market Basket Analysis (MBA). MBA is a data-driven method that helps businesses identify hidden patterns in client purchase data, resulting in better-informed decision-making and improved recommendation systems.

Market Basket Analysis commences by evaluating past transaction data to obtain important information from the product combinations that customers frequently purchase together. By discovering these purchase patterns, businesses acquire a greater understanding of client preferences, allowing marketers to stock their inventory with goods which are more inclined to be acquired together. This not only enhances customer satisfaction but also boosts overall sales. One of the most compelling applications of Market Basket Analysis is the creation of personalized recommendation systems. These systems analyse client purchasing habits and recommend items that fit their present selections. This enriches the shopping experience and fosters cross-selling and upselling, contributing to greater revenue and client loyalty. With insights from MBA, retailers can strategically re-arrange products within their physical stores or on their e-commerce platforms. By placing complementary items in close proximity, businesses can encourage customers to add more to their shopping carts, resulting in higher transaction values. This optimization of store layouts has the potential to significantly impact sales and improve the overall shopping experience. Market Basket Analysis also aids in identifying opportunities for targeted discounts and promotions. Retailers can offer discounts on items frequently bought together, creating an incentive for customers to purchase the bundled products. This not only enhances customer satisfaction but can also drive incremental sales and profitability.

Market Basket Analysis is a powerful tool that empowers retailers to harness the wealth of data generated by customer transactions. By identifying purchasing patterns, implementing recommendation systems, strategically re-arranging store layouts, and offering targeted discounts, businesses can boost their sales, enhance customer loyalty, and ultimately increase their bottom line. In this digital transformation era, grocery stores have access to vast amounts of transactional data. Leveraging this data through an MBA enhances customer satisfaction, optimizes inventory management, reduces waste, and increases overall profitability. It's a win-win situation for both customers and retailers.

LITERATURE REVIEW

The use of technology in business to improve competitiveness and strategy is examined by the researcher [1]. In order to comprehend customer purchasing patterns, transaction data is analyzed via data mining. Using 1641 transaction row data, the authors compared the FP-Growth and Apriori algorithms for association rule mining, also called as Market Basket Analysis. According to the findings, The Fp-Growth method creates 19 rules and 3 sets of items in six seconds, achieving a 217% accuracy and 112.66% rule strength. In thirty seconds, the Apriori algorithm creates 6 rules and 3 combinations having an average rule power of 52.47% and accuracy of 46%. The analysis leads to a conclusion that the Fp-Growth algorithm is better.

In order to assist O! Fish restaurants in developing promotional tactics, the researcher [2] investigates data mining algorithms that can derive knowledge from recorded transaction data, like sales patterns. The restaurant can determine which goods are frequently bought together by employing a priori algorithms to analyze purchasing trends. Using this data, advertising methods that highlight a set of products which are regularly bought together can be developed in order to increase sales. The study's findings will be applied to create a web-based program that examines consumer behavior and makes suggestions for O! Fish restaurants' marketing plans. By doing this, O! Fish restaurants will be able to target and understand their customers' interests more effectively, which will increase overall sales.

According to the researcher [3], Indonesia's body care market is expanding by 6% as a result of Indonesian women's increased skin care consciousness. The Ariana Audy beauty clinic conducted a research study in 2022 with the goal of determining consumer purchasing trends and creating menus that would highlight their goods and services. The fp-growth algorithm and rapid miner software were utilized in the Market Basket Analysis to design the component parts. Five association rules describing customer purchase patterns were produced as a result of the investigation. Three menus were designed for promotion: menu 1 included oxy blue cream and baby skin crystal, menu 2 had brightening cream goods and sunscreen brightening and menu 3 had photodynamic therapy and oxy jet peel. These tactics can aid businesses in thriving in Indonesia's expanding body care sector.

A dynamic recommendation system (DRS) model that incorporates frequent item mining, market basket analysis, customer personalization and best-selling items is put out by this researcher [4] for online marketplaces. The DRS model is a clever online shopping system that integrates frequent item mining, market basket analysis, and best selling items to address consumer rating and feedback difficulties.

The researcher [5] talks on how the number of business actors in the computer industry is increasing, which is putting pressure on businesses to stand out from the competition by developing distinctive selling points and distinct positioning. Retail establishments need to back their marketing efforts with data and other accessible resources in order to remain competitive. In this procedure, data mining techniques such as Market Basket Analysis are frequently employed. The waterfall technique is used to create the application; after user requests are examined, a process is designed using UML. The market basket analysis application written in PHP was the most investigated, with a lift ratio of 3.39 and a 100% confidence level. The results suggest that combinations of products with the highest lift ratio value (2.17) and confidence value (100%), like a laptop charger and a mouse, are more likely to be bought by customers.

In this publication, the researcher [6] proposes a market basket recommendation system employing an Extended algorithm, termed ECFAR, that is built on mining association rules and collaborative filtering. It makes use of a parallel Matrix Factorization-based Commodity Discovery approach and a parallel FP-Growth algorithm for Spark data mining. In-depth tests are carried out on a real-world sales dataset from a nearby grocery chain to confirm the efficacy of ECFAR.

The researchers [7] study applies big data analytics to design and analyze smart market baskets for Jordan's top retailer, Sameh Mall. By analyzing customer behavior, it creates baskets with common items, displayed in stores and online. The results enable Sameh Mall to send and receive recommendations to premium consumers, increase sales, and enhance customer satisfaction by promoting practical collaborations and merchandising..

The researcher [8] describes Association Rule (AR) as a marketing strategy tool that identifies association relationships between products in an operation. It is used in Market Basket Analysis (MBA) to analyze customer buying patterns.

However, ARMBA may not be sufficient for high variability in consumer buying patterns. The Overall Variability of Association Rule (OCVR) is a metric concentrating on market baskets with significant customer variance. The current research examined 57784 sales from a retail establishment in Yogyakarta over the course

 ISSN 2394 - 7780

of a month's time. 17 rules had an OCVR value below 30%, allowing for the development of marketing strategies such as marketing techniques including bundle marketing and shelf layout.

This study [9] proposes a paradigm that covers the entire CRM process, from customer insight to marketing strategy implementation. The process involves two phases: first, creating a dataset including recency, frequency, and monetary measurements, and then clustering it using the K-means algorithm. Phase two involves identifying six consumer groupings and describing marketing tactics. Market basket analysis with the Apriori algorithm are used to extract association rules from transaction data.

The researcher [10] utilised the FP Growth technique to identify the top 10 rules based on their conviction value. A consumer who purchases Milk, Sweet Delight and Pepperoni Pizzeria (Frozen) also receives eggs. This rule has the highest Conviction value of 21.06 and a confidence level of 100%. 24 clients who received the three goods in the information set received eggs. This research also included interpretations of other regulations. These standards allow for proper product placement in supermarkets.

As a result, increased sales of these items will immediately impact grocery income.

The researcher's [11] study infrastructure plan of an amusement arena in Surabaya using market basket analysis. The arcade faces a problem where users only play specific games, causing idle game machines. To address this issue, the researchers propose two layouts: one based on play equipment based on market basket research findings, and the other based on game category dependence. The first layout assumes independence, while the second layout focuses on game category dependence, making the second idea more cost-effective and hence more probable to be implemented lack of specific material handling.

The researcher [12] introduces a distributed course recommendation engine system for an e-learning platform. It uses association rules to find correlations between student actions and assist them select appropriate learning resources. The system analyses historical data, including common itemsets, to find potential rules in the transaction database. The retrieved rules are utilized to identify suitable programs based on pupil behavior and preferences. The system utilizes big data technologies, including Spark Framework's parallel FP-growth algorithm and the Hadoop environment. The Spark MLlib package outperforms typical machine learning tools in terms of efficacy and scalability, as demonstrated by experimental findings.

PROBLEM STATEMENT

There is an acute demand for a reliable recommendation system that uses market basket analysis approaches to provide personalized product recommendations in real time, thereby increasing user satisfaction and optimizing purchasing decisions in a smart shopping cart environment.

RESEARCH METHODOLOGY

MARKET BASKET ANALYSIS: Market basket research is an algorithm based on data mining used by retailers and marketers to uncover links between commonly purchased items. This approach assumes that purchasing a given set of things increases the likelihood of purchasing other items. Market basket research offers significant insights into client behaviour, enabling firms to optimise their strategy for increased sales and satisfaction. Understanding which goods are often purchased together helps organisations modify marketing activities, product placements, and discounts to better satisfy customer wants and preferences. Market Basket Analysis includes various terminologies like support value, confidence, lift, conviction, threshold, itemset, antecedent, and consequent.

1. **Support Value:** Support indicates how frequently a value shows up in a dataset. It is based on the percentage of transactions that include the itemset.

Higher support values suggest a stronger relationship between things.

Formula: Support (Itemset) = (Transactions containing Itemset) / (Total Transactions)

2. **Confidence:** Confidence measures the probability that a certain combination of items will be purchased together. It's the likelihood of The subsequent item in a transaction that includes the antecedent item. Higher confidence values indicate stronger relationships between items.

Formula: Confidence $(A \rightarrow B)$ = Support $(A \cup$

$B)$ / Support (A)

3. **Lift:** Lift refers to the increased possibility of purchasing item B after purchasing item A, relative to the likelihood of purchasing item A without any relationship. Lift values greater than 1 show favourable correlation and potential for cross-selling.

Formula: Lift (A $\rightarrow$ B) = Support (A $\cup$ B) /

(Support (A) × Support (B))

4. **Antecedent and Consequent:** In association rules, the antecedent refers to the items on the left side of the rule, while the consequent refers to the item(s) on the right side. The antecedent is the condition or premise, and the consequent is the outcome or conclusion of the association rule. For eg, in the rule {Diapers} → {Beer}, "Diapers" is the antecedent, and "Beer" is the consequent.
5. **Itemset:** An itemset consists of a number of items. that appear together in a transaction.Itemsets can be of varying sizes, ranging from single items (1-itemsets) to multiple items (2-itemsets, 3-itemsets, etc.). Association rules are generated using frequent itemsets that fulfil a minimal support criterion.
6. **Thresholds in Apriori Algorithm:** The Apriori algorithm utilizes minimum support and confidence criteria. to prune the search space and efficiently discover frequent itemsets and association rules. Every stage of the procedure generates and filters potential itemsets based on a minimal support level. Association rules are derived from frequent item sets, and only those rules surpassing the minimum confidence threshold are retained. While lower thresholds may yield a larger number of rules, they might also include more noise and spurious associations. Conversely, higher thresholds may result in fewer but more reliable rules. Finding the right balance between thresholds is essential for extracting meaningful insights from transactional data.
7. **Conviction:** Conviction refers to the possibility that item A will be purchased without item B. It shows how much the confidence of the rule would drop if the association between A and B was purely random. Higher conviction values indicate stronger relationships and less dependence on chance.

Formula: Conviction (A → B) = (1 - Support(B))

/ (1 - Confidence(A → B))

8. **Leverage:** Leverage refers to a measure of how much the presence of one item influences the presence of another item within a transactional dataset. It helps identify whether the co-occurrence of two items is significant beyond what would be expected by chance alone. If the leverage value is zero, it implies the occurrence of an item A is independent of the occurrence of an item B.
9. **Apriori Algorithm:** Apriori is a common approach for identifying common sets of items in a dataset. It uses a breadth-first search method to efficiently identify association rules. The approach iteratively generates candidate itemsets, prunes those that do not reach the minimal support criterion, and then derives the association from the remaining frequent itemsets.
10. **Association Rules:** Association rules use if-then statements which express relations between sets of items within a transactional dataset. This rule indicates that customers who buy shampoo are likely to also buy conditioner. Example: {Shampoo} → {Conditioner}

DATASET: The dataset [13] the researchers have used to work on is titled "Ecommerce Dataset for Predictive Marketing 2023" and is hosted on Kaggle. The database includes more than 2 million purchase records from a well-known Hunter's grocery store. It is a simulated dataset designed for predictive marketing analysis in the field of an e-commerce business. The dataset is well-documented, well-maintained, and clean data used by many users to gain insights into their research work and to learn from it. It provides a rich source of information for conducting predictive marketing analysis and extracting insights to drive business decision-making in the e-commerce domain.

The dataset on supermarket customer behavior has 2019501 Rows and 12 Columns:

1. Order_id: An order's unique identification number
2. User_id: A special number that serves as the user's identity
3. Order_number: The order number
4. Order_dow: The day of week when the order was packed
5. Order_hour_of_day: Time the order was packed

ISSN 2394 - 7780

6. Days_since_prior_order: Order history
7. Product_id: Product identity
8. Add_to_cart_order: Total amount of products added to the cart
9. Reorder: If a reorder had taken place
10. Department_id: Specific number assigned to all departments
11. Department: The departments' names
12. product_name: The products' names

The dataset appears to consist of individual transactions made by customers. Each transaction includes information about the products purchased, such as their unique identifiers (StockCode), descriptions, quantities, and prices. It is also associated with a specific customer identified by a unique Customer ID. The dataset seems to cover transactions that occurred in 2023, as indicated by the title. It includes information about the countries where customers reside, which can be useful for analyzing regional trends and customer segmentation.

The dataset is very viable to apply market basket analysis to gather co-occurrence patterns among products in transactions. This will help in understanding cross-selling opportunities and optimizing product recommendations. Targeted marketing campaigns and customized recommendations can be made easier by segmenting customers based on factors like product preferences, transaction frequency, and geographic location. It is useful for creating predicting models for various marketing-related tasks, such as predicting customer churn, forecasting sales, and identifying high-value customers. By analyzing the influence of marketing campaigns on consumer behavior and purchasing patterns, Business owners are able to more effectively manage resources and evaluate the success of their marketing activities.

Since the dataset is simulated, it may not reflect real-world data quality issues. However, it's still essential to perform data cleaning and preprocessing steps to handle missing values, outliers, and inconsistencies. Additional features, such as customer segmentation variables or time-based features, can be derived from the existing dataset to enhance model performance and insights generation. One has to ensure compliance with data privacy regulations, especially when working with personally identifiable information such as customer IDs. Anonymization techniques may be necessary to protect customer privacy.

RESULT AND DISCUSSION

The researchers used Python code to draw insights from the dataset by plotting various graphs and understanding the relationship between customer buying habits. They used an apriori code to draw various antecedents and consequent pairings. The minimum support value was changed and new combinations of rules in the dataset were observed.

Table 1.1 - Comparison of Final Result

Minimum Support Value	Threshold	No. of Rules	Maximum Support Value
0.04	1.5	350	0.186580
0.05	1.5	138	0.186580
0.06	1.5	87	0.186580
0.07	1.5	48	0.186580
0.09	1.5	10	0.186580

The researchers have run the code five times with five different values of minimum support with a stable threshold. It has been observed that there are less rules with an increase in minimum support value. This is done to acquire the rules that occur most frequently. They are:

1) [Packed Vegetable Fruits, Fresh Fruits]→ [Fresh Vegetables]
2) [Fresh Fruits, Fresh Vegetables] → [Packed Vegetable Fruits]
3) [Packed Vegetable Fruits] → [Fresh Fruits, Fresh Vegetables]
4) [Fresh Vegetables] → [Packed Vegetable Fruits, Fresh Fruits]
5) [Fresh Fruits, Yogurt] → [Packed Vegetable Fruits]
6) Fresh Fruits, Packed Cheese] → [Fresh Vegetables]

The following graph displays the Total number of Products in each department from the dataset.

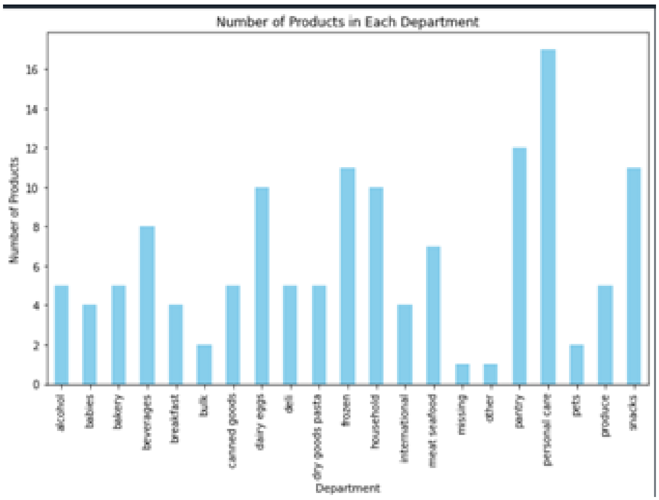


Figure 1.1 - Graph showing Total Products in each Department

We can conclude that customers who buy fresh fruits and packed vegetable fruits also buy fresh vegetables along with them. Also, customers who tend to buy fresh fruits paired with packed cheese or yogurt tend to buy fresh vegetables or packed vegetables along with it.

FUTURE ENHANCEMENT

Further initiatives might include providing customers with recommendations for acquiring items that are nearing the end of their purchase history. For example, a consumer buys a package of Bournvita. After 60 days, the client will be notified to refill items. GPS can be implemented on item name boards to increase item searchability, especially if the object's position changes.

A dynamic pricing approach will help enhance and streamline the shop's product pricing system. Dynamic pricing considers demand, supply, rival prices, and product brands to determine pricing for a specific product. A neural network can automatically advise a product's pricing in real time. This approach not only assists shops in pricing new products but also boosts profits by calculating the price based on client demand.

CONCLUSION

The researchers claim that increasing the minimum support value within the Apriori algorithm results in fewer frequent item sets and consequently fewer association rules. However, the generated rules tend to be more significant, with higher confidence values, making them more reliable for decision-making purposes. The aim of carrying out the Apriori algorithm on a dataset is to discover frequent itemsets and association rules that reveal inherent patterns and relationships within the data. The apriori algorithm's rules give insight into item relations. These rules contribute to the interpretation and quantification of the Apriori algorithm's association rules, including their strength, importance, and linkages. They are critical for determining the effect and reliability of patterns revealed in the dataset. These techniques may be used whenever there is a requirement to discover hidden links, patterns, or dependencies in massive datasets, resulting in important insights and educated decisions. These strategies are adaptable, making them a strong tool in a variety of industries. This study can be generated on any dataset.

REFERENCE

[1] Aldino, Ahmad Ari, et al. "Comparison of market basket analysis to determine consumer purchasing patterns using fp-growth and apriori algorithm." 2021 International Conference on Computer Science, Information Technology, and Electrical Engineering (ICOMITEE). IEEE, 2021.

[2] Kurnia, Yusuf, et al. "Study of application of data mining market basket analysis for knowing sales pattern (association of items) at the O! Fish restaurant using apriori algorithm." Journal of Physics: Conference Series. Vol. 1175. No. 1. IOP Publishing, 2019.

[3] Dio, Rafi, Aulia Agung Dermawan, and Dimas Akmarul Putera. "Application of Market Basket Analysis on Beauty Clinic to Increasing Customer's Buying Decision." Sinkron: jurnal dan penelitian teknik informatika 8.3 (2023): 1348-1356.

[4] Tareq, Shihab Uddin, Md Habibullah Noor, and Chinmay Bepery. "Framework of dynamic

recommendation system for e-shopping." International Journal of Information Technology 12.1 (2020): 135-140.

[5] Qisman, M., R. Rosadi, and A. S. Abdullah. "Market basket analysis using apriori algorithm to find consumer patterns in buying goods through transaction data (case study of Mizan computer retail stores)." Journal of Physics: Conference Series. Vol. 1722. No. 1. IOP Publishing, 2021.

[6] Wang, Feiran, et al. "Collaborative filtering and association rule mining-based market basket recommendation on spark." Concurrency and Computation: Practice and Experience 32.7 (2020): e5565.

[7] Almaslamani, Farah, et al. "Using big data analytics to design an intelligent market basket-case study at sameh mall." Proceedings of the European Conference on the Impact of Artificial Intelligence and Robotics, ECIAIR. Vol. 2020. 2020.

[8] Khasanah, A. U. "Implementation of market basket analysis based on overall variability of association rule (OCVR) on product marketing strategy." IOP Conference Series: Series: Materials Science and Engineering. Vol. 722. No. 1. IOP Publishing, 2020.

[9] Maraghi, Mohsen, Mohammad Amin Adibi, and Esmaeil Mehdizadeh. "Using RFM model and market basket analysis for segmenting customers and assigning marketing strategies to resulted segments." Journal of Applied Intelligent Systems and Information Sciences 1.1 (2020): 35-43.

[10] Ünvan, Yüksel Akay. "Market basket analysis with association rules." *Communications in Statistics-Theory and Methods* 50.7 (2021): 1615-1628.

[11] Halim, Siana, Tanti Octavia, and Christian Alianto. "Designing facility layout of an amusement arcade using market basket analysis." *Procedia Computer Science* 161 (2019): 623-629.

[12] Dahdouh, Karim, et al. "Large-scale e-learning recommender system based on Spark and Hadoop." *Journal of Big Data* 6.1 (2019): 1-23.

[13] https://www.kaggle.com/datasets/hunter000 7/ecommerce-dataset-for-predictive-marketing-2 023

ISSN 2394 - 7780

CLOUD COMPUTING SECURITY THREATS, ATTACKS, AND ITS COUNTERMEASURES: A SURVEY

Sunita Gupta and Nishi Jain
Usha Pravin Gandhi College of Art Science and Commerce, Vile Parle, Mumbai, India

ABSTRACT
Innovative technologies including ML, AI, IOT, Big Data, and the industry's desire to cut operational costs are driving up the demand for cloud computing, or CC. Cloud computing provides users with public and private computing and they can store the data in an online, networked environment. Furthermore, customers with a dependable Internet connection may access their data from any location in the globe. Despite all the benefits, the largest obstacle to using cloud services is security because there are many different kinds of risks. This paper aims to identify potential or more vulnerable vulnerabilities and to give an in-depth overview of the difficulties with cloud security. Also, the research presented in this paper offers few methods and approaches for securing data in an online setting.

Keywords: Cloud computing, Cloud services, Data storage, Security challenges and threats.

INTRODUCTION
Cloud computing allows users to access shared resources like networks, servers, storage, apps, and services anytime, anywhere, without physically affecting key resources, and with minimal effort from service providers. Google apps serve as a prime example of this model. Cloud computing is made up of several hardware and software components that collaborate to provide end customers with different processing components as an online service. Cloud computing model consists of 4 deployment models and 3 service models.

Cloud Deployment Models:
1. **Public Cloud:** The general public can access a range of internet services from public cloud providers for a price.
2. **Private Cloud:** Only people who have access by private cloud providers can access the services provided.
3. **Hybrid Cloud:** This alternative blends elements of both private and public clouds.
4. **Community Cloud:** Only members of a certain community can access the community cloud.

Cloud Service Models:
1. **Software as a service (SaaS):** SaaS allows the user to access the application and database software either directly or remotely. The infrastructure of the cloud is not managed by the user. This allows several users to access the same service simultaneously. SaaS was formerly exclusively provided by a small number of businesses. These days, companies like Dropbox, Office 365, Google, and so forth also provide SaaS.
2. **Platform as a Service (PaaS):** In PaaS user may access the operating system, web servers, and programming language execution environment in this computing *model.* PaaS is a combination of computers and application servers, including Linux, PHP, Windows Azure, Google Compute Engine, and others. Hence, PaaS is its name.
3. **Infrastructure as a Service (IaaS):** Virtual or physical machine is given to the user in IaaS. IaaS provides storage and computing technologies as system resources that are accessible to all users. The main idea behind virtualization is to create distinct virtual machines (VMs) and keep them separate from other VMs and equipment.

All the models are shown in Fig. 1.

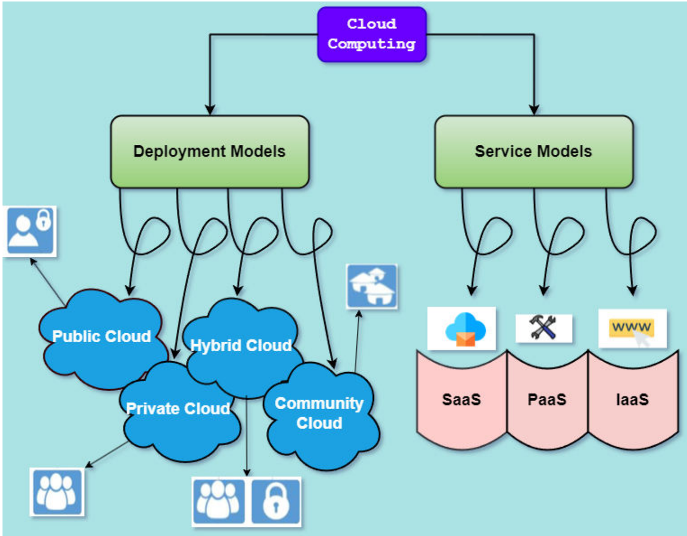


Fig. 1: Cloud Computing Models

Since cloud computing facilitates data sharing, data theft is an important threat that affects both customers and service providers. Security is the primary concern and the primary component in cloud computing. It typically experiences a range of security issues and attacks such as malicious program's. By employing a cloud based internal organizational system, data can be secured by applying data usage policies. However, it still does not ensure complete security of the date and privacy of the data because several businesses lack the expertise to completely safeguard sensitive data.

This paper aims to achieve the following main objectives:

To mitigate potential security threats and data breaches in the cloud environment.

To provide an overview of the solutions that researchers have proposed over the years in response to potential security threats that have been identified.

LITERATURE SURVEY

Security in cloud computing is an important factor, with extensive research conducted on various issues and their solutions. The overview of certain papers that focus on cloud security threats, attacks and provide their solutions are given below:

Table I: Literature Survey

Research Paper No.	Objectives of the Paper	Strengths	Limitations
[1]	• To pinpoint various cloud security threats and attacks and to classify them based on their risk level.	• Countermeasures like data protection through encryption are provided	• The solutions offered do not totally shield the data from threats like insider attacks and shared technology-based attacks
[2]	• To provide conventional remedies to protect data from various cloud security risks in an online environment.	• Conventional solutions like controlling the access, increasing the cloud security, preventing DOS attacks are provided	• The paper does not provide solutions for high-risk level security attacks.
[5]	• To address the flaws of the previous research and compile information on cloud computing's architecture, cloud security threats, attacks,	• Countermeasures like availability of information (SLA), data encryption, data masking, intrusion detection system and various others are provided.	• The paper fails to focus on important security risks while it tries to cover all the risks in short.

	and its countermeasures.		
[6]	• To focus on the applications pertaining to security on availability, dependability, integrity, and secrecy.	• Provides a comprehensive explanation of cloud computing services, their critical security threats, and typical types of attacks.	• The paper does not talk about the countermeasures to prevent the threats and attacks that it mentions in the paper.
[16]	• To evaluate cloud application information security strategies. • To categorize techniques based on security features and addresses cybersecurity risks for adequate cloud data protection.	• Data security enhancements using cloud algorithms, Data Protection through encryption, Cloud Security Controls etc, are provided	• The solutions provided in the paper does not clarify for which attacks they should be used.

Authors of [3] intend to illustrate the difficulties experienced by cloud computing customers about the securities problem. They also highlight the most concerning elements, which should raise serious concerns. Many issues and threats have been noticed in cloud computing security. These issues have serious effect on the users' confidence and privacy. Security threats such as DoS attacks, flooding, MITM attacks, SQL Injection Attacks etc. are explained by the authors. They also provide countermeasures to tackle these threats.

Cloud services have grown to be a vital component of company, and they can accelerate it since they can expand rapidly, provide us greater flexibility, and allow us to collaborate with resources that are accessible. The cloud has benefits that extend to whole nations. Despite the cloud's many advantages, there are also several security issues. Authors of [4] aim to address numerous security vulnerabilities in cloud services and devise solutions for them. However, this study has made effort to draw attention to cloud computing's range of security issues, vulnerability evaluations, attacks, and threats that impede people's adoption. The summary of every security issue and challenges are covered in this paper, together with the intention of preventing issues of security, makes it easier in identifying good solutions for security issues.

Janhavi along with her co-authors have given a comprehensive study of Cloud security threats in [7]. Data breach, malicious insider, insecure APIs, backdoor channel attacks, etc. are described by the authors in the paper.

To offer the customers, the services they need, cloud providers frequently have several strong servers and resources; yet, cloud computing, like other Internet-based technologies, is not without danger. However, they are also vulnerable to attacks like strong denial-of-service attacks, just like any other Internet-based technology. To overcome these issues the author of [8] Farzad Sabahi has discussed thoroughly about information security policies, cloud RAS issues. He also has proposed traditional solutions that include access control, partitioning, migration, allocation of workload techniques in the paper.

Authors of [9] explain various advantages and disadvantages of cloud computing. They also explain that to ensure user safety in cloud computing services, strict background validation procedures, a Service Level Agreement (SLA), data loss accountability, backup procedures, employee authentication and validation policies, auditing procedures, basic cloud computing guidelines, and provider accreditation are essential.

The author of [10] and [11] PanJun Sun mainly discusses about data protection through encryption techniques to overcome cloud security challenges. The author has provided conventional techniques as well to ensure data security in Cloud computing.

Shubham Kumar along with his co-authors in [12] has addressed the security challenges that cloud computing faces. While the cloud offers benefits, there are security vulnerabilities that must be addressed to safeguard data integrity and privacy. Businesses using the shared responsibility model should implement robust security measures like encryption, audits, and access restrictions. Significant dangers are posed by data breaches and unauthorised access, underscoring the necessity of cyberattack protection and regulatory compliance. Various solutions are also provided in the paper to overcome the security issues.

In [13], The authors discuss the ROI for each cloud layer, rating security severity based on specific threats. They outline security requirements for cloud services, including encryption, multi-tenancy, privacy, authentication, and permission.

Hamed and Marjan, the authors of [14] point out security flaws in the architecture of cloud computing and suggest evaluating the security frameworks in place to reduce risks and vulnerabilities. The paper recommends secure cloud management techniques and emphasizes understanding security flaws in cloud architecture, analyzing security challenges, classifying barriers, and contrasting them with suggested solutions.

The authors of [15] examine cloud computing security issues, threats, and vulnerabilities using client and server layer services, deployment methods, and five network levels. In this paper, they offer security threat-based solutions and preventative techniques for long-term security, analysing architecture, services, implementation methods, and advantages, and recommending security requirements and preventative actions.

Cloud Security Threats and Attacks

Cloud Computing Threats

A threat to cloud security is an event and a variable that determines whether a danger will materialise. The hazards in the cloud domain that are discussed here have the potential to interfere with cloud service providers' capacity to offer services to customers. To aid in understanding the many dangers that might impact cloud resources in the computing environment, four groups are used to categorise threats:

Application related threats [6]: The goal is to exploit applications i.e. fake features and hypervisor vulnerabilities. An application programming interface (API) is usually a server-side application vulnerability that needs to be exploited. Malware and video sniping are potential risks as well.

Risks associated with data security [6]: Data security may be affected by credentials for data collection and analysis, data transmission interruptions, management of misleading information, data alteration, and substandard data. Some use mobile phones to get personal information.

Infrastructure related threats [6]: Infrastructure failures are frequently the cause of threats to cloud computing. There are significant infrastructure enabling concerns with multi-tenancy.

Risks to the overall security of cloud computing services [6]: Threats can take many different forms, including poor performance, theft of cloud services, and availability and dependability issues.

Cloud Computing Attacks

Without a doubt, the goal of cloud computing is to offer several computer services via the Internet. Cloud technology paradigms are susceptible to both internal and external threats, despite their many advantages. Consequently, cloud developers will have to enhance their understanding of important security breaches, common attack vectors, and cloud defense systems. Details of attacks on the cloud system are explained below and shown in Fig.2 as follows:

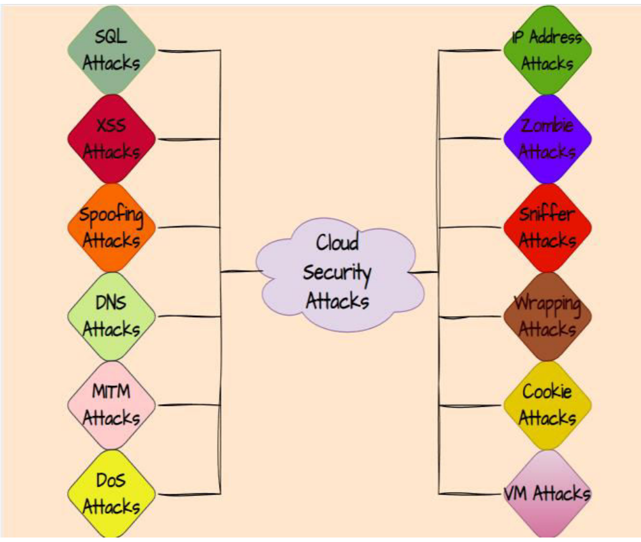


Fig. 2: Cloud Security Attack

Structured Query Language (SQL) Injection attacks [6]: Malicious scripts enable attackers to access unauthorized databases, 1`read user data, and modify website operating information.

Cross-Site Scripting (XSS) attacks [6]:
Malicious code injections redirect a person's website to the perpetrator's, allowing private data to be obtained through reflected XSS or Embedded XSS.

Spoofing attacks [4]: Phishing involves using cloud services to redirect a customer to a phoney website, allowing them to access their account and steal crucial data.

Domain Name Server (DNS) attacks [6]: The attacker exposes the customer's personal information by using DNS.

Man in the Middle (MITM) attacks [7]: This attack occurs when attacker enters a communication channel to introduce misleading information and gain access to disclosed private data.

Denial of Service (DoS) attacks [4] [7]: The attacker floods the server with UDP, ICMP and SYN traffic to make resources unavailable that are available to users.

Recycled IP Address attacks [6] [7]: IP addresses are assigned to network devices by users, and when a user logs off, a new user is given the current IP address, which enables access to previously uploaded data.

Zombie attacks [6]: In such types of attacks, several other VMs' in-network communications are sent to the Virtual Machines (VMs) that belong to the attacker.

Sniffer attack [6][7]: The attacker's malware infects the host's Network Interface Card (NIC), allowing them to monitor Ethernet network communications and potentially compromising data if packets aren't encrypted during transit.

Wrapping attack [6]: A wrapping invasion allows hostile programs to infiltrate cloud-based services by copying and translating SOAP messages, sending data as an authorized user.

Cookie Contamination attacks [4]: Cookie's content is changed to grant access to a website or application that is not authorised.

Virtual Machine (VM) attacks [7]: Virtualization technology allows operating systems to act as hardware owners, posing security risks due to difficulties in regular OS checks and potential infection by malicious guest systems.

Countermeasures to prevent Security Risks

Table II: Countermeasures for Security Issues

Countermeasures		Key Features
Conventional Remedies [2]	Access Control	▪ Control the consumers' access privileges. ▪ Encourage only authorized resource access. ▪ Verify that network services are accessible. ▪ Verify that the operating system is accessible. ▪ Keep an eye on the software and system availability
	Increase security while keeping expenditures to a minimum	▪ Users must undergo rigorous background verification before joining cloud computing services. ▪ Customers and providers must sign an SLA outlining responsibilities. ▪ Cloud providers must ensure transparency and tested solutions. And they must bear liability for data loss.
	Event prevention and intervention	▪ Users' data must be partitioned into portions improves efficiency and the data portions can be divided over several machines. ▪ When migrating large amounts of data, avoid overloading cloud fragments, and avoid overloading specific operations like slicing data into manageable chunks and preserving functionality while conducting transactions. ▪ Providers must determine resource distribution and allocation across virtual machines to ensure appropriate collaboration on workloads on virtual machines.
	Account Hijacking	▪ Companies should implement robust security measures like

	and DOS attacks prevention	two-factor authentication, restricted account credentials exchange, bandwidth investment, DOS prevention, and regular detection campaigns to mitigate cybersecurity breaches and potential legal action.
	Prevention of data breach and system vulnerability	▪ An effective security plan, including multifactor authentication and encryption, is crucial for preventing data leaks. ▪ Routine vulnerability screening and timely monitoring of device hazards can help mitigate network weaknesses.
Data Protection through Encryption [1]	Attribute-Based Encryption (ABE)	▪ Verifies the authenticity of the cipher text prior to decryption. ▪ Fast local decryption, giving local users access to updated keys rather than a cloud server. ▪ Encrypted using identity; structure modified with Type-3 bilinear pairings. ▪ Unidentified key distributing protocol to attain privacy protection.
	DNA (Neuron) based encryption	▪ Keys are generated by DNA processing, user characteristics, and passwords. ▪ Encryption is based on Hopfield neural network (HNN).
	Homomorphic Encryption schemes	▪ Integrates Goldwasser–Micali (GM) with RSA using elliptic curve cryptography (ECC). ▪ Employs the Chinese remainder theorem (CRT) and Hensel Fitting to decrypt. ▪ The multi-cloud environments utilize Paillier's scheme with additive homomorphism over the integers.
	Integration of encryption techniques (Dual encryption and data fragmentation)	▪ Homomorphic Blowfish encryption method. ▪ Blowfish encryption using ECC methodology.
	Searchable Encryption	▪ Blockchain-based encryption. ▪ Imposes access policies that are concealed within cipher text by the data owner. ▪ Hyper-chaos encryption. ▪ Utilizing a distributed oblivious data structure for dynamic encryption.
	Proxy Re-Encryption	▪ The use of a Judge algorithm is employed to evaluate the reliability of the proxy (cloud server). ▪ Stores a portion of data on the blockchain network.
Data Protection through Cryptography [16]	Block Ciphers	▪ Block ciphers create cipher text by applying a cryptographic key and method to a set of 64-bit data blocks, ensuring similar text blocks are not encrypted similarly. ▪ This technique ensures a series of encrypted pieces.
	Stream Ciphers	▪ Because it depends on the cipher's present state, this kind of encryption of data is occasionally referred to as a state cipher. ▪ The method encrypts individual bits as opposed to encrypting whole data set.
	Hash Functions	▪ This method turns a text input into an alphanumeric string via a hash function, that is a statistical function. ▪ The corresponding alphanumeric string typically has a fixed size. This technique makes sure that no two alphanumeric sequences may have the same outcome.

CONCLUSION & Future Work

Improving methods of storing data on the cloud is undoubtedly becoming more popular as cloud computing becomes more widely used for data storage. If cloud data is not appropriately safeguarded, it may be vulnerable. This study looked at security issues and the risks and security vulnerabilities associated with cloud data storage.

ISSN 2394 - 7780

Finding the best solutions to security problems is facilitated by the summary of all concerns and difficulties related to security that are covered here as well as the significance of preventing security defects. We wish to examine current security standards from this area of study to be able to minimize vulnerabilities to prevent them from being used in assaults.

We have explored efficient ways to encrypt data in the cloud as well as data at different stages. A summary of the hash function, block cipher, and stream cipher utilized for encrypting data in the cloud either it is in motion or at rest was given by the research.

Through the study, important recommendations and concerns of primary open research are also offered to comprehend cloud difficulties.

Despite its early stages of development, cloud computing still has a lot to learn. After our current analysis is complete, we can affirm that security is the top issue for cloud computing providers and clients. Experts in IT security and research are tackling privacy issues related to cloud computing. We will look at better security requirements for safe cloud computing in our next work.

REFERENCES

[1] Sushila Kumari, Kamna Solanki, Sandeep Dalal, Amita Dhankhar, “Analysis of Cloud Computing Security Threats and Countermeasures”, 2022 10th International Conference on Reliability, Infocom Technologies and Optimization, (ICRITO), Amity University, Noida, India, IEEE, 2022

[2] Zina Balani, Hacer Varol, “Cloud Computing Security Challenges and Threats”, IEEE, 2020

[3] Manoj Kumar Sasubilli, Venkateswarlu R, “Cloud Computing Security Challenges, Threats and Vulnerabilities”, Proceedings of the Sixth International Conference on Inventive Computation Technologies [ICICT 2021], IEEE, 2021

[4] Jansi Sophia Mary C, Mahalakshmi K, Senthilkumar B, “Deep Dive on Various Security Challenges, Threats and Attacks Over the Cloud Security”, 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 2023

[5] Umer Ahmed Butt, Rashid Amin, Muhammad Mehmood, Hamza Aldabbas, Mafawez T, Alharbi, Nasser Albaqami, “Cloud Security Threats and Solutions: A Survey”, Wireless Personal Communications (2023), Springer, 2023

[6] Amit Kumar Singh Sanger, Dr. Rahul Johari, “Survey of Security Issues in Cloud”, 2022 International Mobile and Embedded Technology Conference (MECON), IEEE, 2022

[7] Janhavi Chavan, Shivraj Patil, Shridevi Karande, Ruchira Patil, Vitthal Gutte, “A Survey on Security Threats in Cloud Computing Service Models”, 6th International Conference on Intelligent Computing and Control Systems (ICICCS 2022), IEEE

[8] Farzad Sabahi, “Cloud Computing Security Threats and Responses”, Faculty of Computer Engineering, Azad University, IEEE, 2011

[9] Choubey, Rajnish, Rajshree Dubey, Joy Bhattacharjee, “A survey on cloud computing security, challenges and threats”, International Journal on Computer Science and Engineering (IJCSE) 3.3 (2011): 1227-1231

[10] PanJun Sun, “ Security and privacy protection in cloud computing: Discussions and challenges”, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Elsevier, 2020

[11] PanJun Sun, “ Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions”, School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, IEEE, 2019

[12] Shubham Kumar, Anuj Kumar, Satish Kumar, Pawan Kumar Chaurasia, “ Comprehensive Analysis of Cloud Security: Issues & Challenges”, 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), IEEE, 2023

[13] Syed Asad Hussain, Mehwish Fatima, Atif Saeed, Imran Raza, Raja Khurram Shahzad, “Multilevel Classification of Security Concerns in Cloud Computing”, Applied Computing and Informatics (2017) 13, 57–65

[14] Hamed Tabrizchi, Marjan Kuchaki Rafsanjani, "A survey on security challenges in cloud computing: issues, threats, and solutions", The Journal of Supercomputing (2020)

[15] Mehrdad Jangjou, Mohammad Karim Sohrabi, " A Comprehensive Survey on Security Challenges in Different Network Layers in Cloud Computing" Archives of Computational Methods in Engineering (2022), Springer

[16] Dr. Vinod Varma Vegesna, "Investigations on Different Security Techniques for Data Protection in Cloud Computing using Cryptography Schemes", Indo-Iranian Journal of Scientific Research (IIJSR) (Quarterly International Journal) Volume 3, Issue 1, Pages 69-84, 2019

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

DIGITAL SECURITY OF BANKS USING BLOCKCHAINS: A REVIEW

Manisha Divate[1] and Gayatri Kulkarni[2]
Usha Pravin Gandhi College of Arts, Science And Commerce, Vile Parle, Mumbai, India

ABSTRACT

IEEE Banking is vital to the country's economic success. Security in banking is the main problem discussed in this paper. Banks and banking systems face several issues in their everyday workings. Some of them include availability, accountability, accessibility, authorization, connectivity, and concurrency. These can be handled by using blockchain technologies which will create blocks to handle things efficiently. Blockchain is a type of shared database that differs from regular databases in the way it stores information. Blockchains store data in blocks connected with encryption using cryptography. A blockchain can store a variety of types of data, However, the most typical application for transactions is as a ledger. In the case of Bitcoin, the blockchain is decentralised, which means that no single person or organisation has power; instead, all users share control. Decentralised blockchains are immutable, which means that any recorded data is immutable. Bitcoin transactions are forever recorded. And may be viewed by anybody. As we know, security in digital transactions is a need of society. Giving a penny in cash whereas the same money given digitally makes a difference. Traditionally followed by giving money in cash but as the need and demand for digitalization is increasing there is a need for digital transactions. There are many challenges such as fraudulent transactions, inefficiency, lack of transparency, parallel workings. Many countries like India face problems like cyberattacks and bank databases are hacked to exploit nations financially. The bank data contains Aadhar cards, PAN card details, and many sensitive information-like birthdays and phone numbers. The proposed model has the potential to keep data secured and provide enhanced transparency, parallel working authorization, and security. The blockchain for digital security uses Decentralization and Consensus Mechanisms, Reduced Administrative Overhead

Keywords: blockchain,leadger.smartcontract

INTRODUCTION

Currency is considered the most important asset for any country or nation, determining the wealth of a country, whether it is rich or poor. It is a movable and ever-changing factor, with the power to decide the economic status of a nation. Money, as a constant and fixed number, plays a crucial role in shaping the financial landscape, continuously increasing, and rarely decreasing. Buying and selling money is transferred from one account to another and distinct locations. In these cases, manual human interventions are necessary to complete all bank processes which creates delays due to time, speed, and human dependencies. Human dependencies are on bankers who work only in open hours. Time dependencies needs to be considered. Transaction speeds are slower as there are many documents and different KYC processes. Ease of Transfers is a benefit to users but at the same time is a threat to Privacy and Security. Approved transactions if found fault can lead to account seizures. To overcome these issues digital security and a new way of transactions require smooth efficient secure working and transfer of currency switch blockchain technology. Blockchain is a domain name that refers to distributed ledger technology (DLT). Blockchain domains are sometimes known as "NFT domains," "decentralized domain names," or "crypto domains." The blockchain is an incorruptible digital transaction ledger. Can be designed to record both economic and value transactions. The blockchain is a collection of time-stamped, immutable data. Blockchain is a distributed ledger technology (DLT) which distributes data over a computer network in place of copying it. The Blockchain technology ensures that all network users automatically receive updates to data. Blockchain differs from democratic systems as it lacks central authority. Because it is a shared blockchain, an immutable ledger which enables everyone to access the data. A blockchains transparency means that all participants are held responsible for their actions. Blockchain enables transparency in bank transactions, including the creation of accounts and other formal documents. Blockchain technology is being used by governments worldwide for land registration because of its unique qualities. Several countries, including the UK, US, and Sweden, are implementing Blockchain in their land registration systems. (Institute of Electrical and Electronics Engineers, n.d.)[17] In India, a blockchain-based digital money transaction platform will increase transparency. The technology facilitates direct communication between buyers and sellers, as well as easy access to records. Bank transfers often take two to three working days to execute due to lengthy registration formalities. It take many days in completion and registration. This platform saves the era. The main objectives are studying and understanding availability, accountability and accessibility, authorization, connectivity, and concurrency in bank transactions. Finding out ways to reduce dependence on humans (bankers and banking staff). Decoding ways to provide Security and privacy of accounts and transactions and personal data from cyberattacks.

LITERATURE REVIEW

There are various ways for transaction methods money processing in banks. Using blockchain technology we can reduce the paperwork and documents by making a smart contract a digital copy of documents. Which can be available to the customers by developing some dashboards interface, software with blockchain technology. They can access their accounts from anywhere in the world. Secured way which is decentralized as can be remotely accessible without a centralized bank process. Currently bank must follow a centralized process which needs to be changed. Smart Contract[13][14]paper explains smart contract in decentralization its importance. Below table represents study of technology and understanding blockchain

and its advantages and disadvantages to blockchain systems. Some papers are studied to understand efficient blockchain working and applications.

TABLE II. Study of Various Refernce Papers

Title	Objective	Advantages	Demerits
Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains [22]	Non-deterministic operations in order-execute architecture might cause state inconsistencies among peers.	This is a significant advantage over order-execute design, as non-deterministic operations might cause discrepancies in peer states.	Execution occurs in a sequential order. Non-deterministic code, confidentiality during execution Fixed trust model.
ETHEREUM: a secure decentralized generalized transaction ledger [8]	We achieved our goal of decentralising voting transactions by creating a secure and transparent application to protect user decisions.	Blockchain nodes now allow users to vote from anywhere, eliminating time and location restrictions. The transparent vote counting process minimizes manipulation and provides real-time results	-
Identifying malicious accounts in blockchains using domain names and associated temporal properties [4]	Our technique identifies 2479 malicious blockchain domain names, out of 34171 exhibiting persistent malicious behavior, but none of previously recognized harmful domain names were included in the newly labeled list.	Deep learning systems can identify malicious accounts and adversarial behavior using DNs, utilizing relationships with underlying IP addresses, which are then blacklisted for harmful activities. .	Warn users not to use predictable domain names. Using such DNS can compromise privacy and leak sensitive account information.
Blockchain technology forecasting by patent analytics and text mining[2]	This project aims to analyse blockchain patents to discover emerging patterns using text mining and clustering techniques.	Digital revolutions have made high technology a key competitive advantage for enterprises.	-
A Next-Generation Smart Contract and Decentralized Application Platform [13]	Blockchain enhances security, privacy, and data transparency by facilitating secure record sharing and data interchange between smart devices, while Ether aids in decentralized applications, smart	The study utilized text-mining for classification, highlighting the early stages of blockchain technology, despite its significant challenges and restrictions.	Patents are retrieved and clustered based on co-occurrence, primarily focusing on blockchain technology applications like cryptocurrency, finance, supply chain management, healthcare, gambling, security, and privacy.

	contracts, and peer-to-peer payments.		
Databases fit for blockchain technology: A complete overview [25]	Database technology enhances blockchain development with ACID, transaction consistency, and real-time analysis. Proposed "DCS-satisfiability conjecture" offers relaxed criteria, while DBMS architecture, storage manager, and query processing are discussed.	An intriguing line of inquiry could be to investigate all the criteria involved in selecting the best database for the blockchain project.	-
A Blockchain Ethereum Technology-Enabled Digital Content: Development of Trading and Sharing Economy Data [18]	This paper proposes a Blockchain Ethereum Technology-based content protection method to enhance transaction transparency and prevent theft and hacking in the shared economy, addressing potential security threats.[18]	The testing findings suggest that the proposed method can improve transaction transparency while reducing the danger of distortion and hacking. [18]	
A Blockchain-based Customizable Document Registration Service for Third Parties[20]	Blockchain is a valuable storage solution for document management, but its distributed nature may cause implementation difficulties and high operational costs. A customizable blockchain-based document registration service allows creation of generalized documents for various application domains.	Document management comprises the production, storage, and proper use of commercial or government documents. facilitated by digitalization and the pandemic. Blockchain has emerged as a key strategy for document management, providing integrity, authenticity, access control, transparency, and availability.	Future work plans include integrating a permission blockchain for more complex access control, and a blockchain-supported document registration and validation service for customizable document models, with API functionality for third-party platforms.
A Survey on Safety Regulation Technology of Blockchain Application and Blockchain Ecology [19]	Blockchain's decentralization, robustness, and anti-modification pose challenges to network regulation and data security, necessitating effective regulation for sustainable ecosystem [19]	This study emphasises the significance of statistical methodologies and compliance laws in regulatory technology research, with a focus on finding and training abnormal behaviours using transaction data. [19]	-
Blockchain- Oriented Privacy protection with online and offline Verification in Cross-Chain System[17]	System built for security and privacy	Focus on improving partitioning functions under the premises of balancing	-
COMMITTABLE: A	The proposal proposes a	-	-

Decentralised and Trustless Open-Source Protocol [24]	decentralized, trust less open-source protocol, Committable, for all OSS software. Committable is an accountable tokenization technology on blockchain that creates CMT software assets for various.		
IoT Data Storage on a Blockchain Using Smart Contracts and IPFS [26]	The proposal introduces Committable, a decentralised, trust less open-source mechanism for any OSS software that makes use of blockchain tokenization technology and the Problem-Solution-Risk structure. Tokens can be traded, allowing owners to transfer rights and developer royalty.[26]	The proposed solutions include improving MQTT modules to prevent failure, utilizing a private blockchain to reduce transaction fees, and creating an IPFS cluster for enhanced data control.[26]	This paper presents decentralized file storage for IoT devices, using simulating devices and generating dummy data for storage in the IPFS network and Ethereum smart contracts for data references. Tests show the solution is viable compared to direct Ethereum blockchain storage but requires improvement due to reduced time.[26]

The blockchain is the solution for the system because after analyzing and understanding current centralized system and different implementations of blockchain technologies. Blockchains will solve all the problems faced by customers daily. Decentralization way to access the accounts will help to access money and keep records. These records will also be saved and accessible to everyone with keys and passwords. The money transfer transactions will be saved at many servers transparent, secure and quick. Security will be provided by keys and passwords as hash based technology won't be easy to access these records. Smart contracts made will solve all problems related to the dependencies will save time, paper, money and middleman bankers.

GAP IDENTIFICATION

In the current processing of banking which is centralized and handed by a single person or banking authorities managing the system and central databases.

Bank	Current Centralised system problems
Bank Timings	9am -5pm.Lunch time 1pm-2pm. Every2nd and 4th Saturday holidays and Sunday and bank holidays banks are closed
Card Payments	It takes 24 to 48 hours for card payments to reflect in accounts
Wire Payments	To be reflected in accounts within a day excluding international bank transfers
Cheques	Transactions it takes 24-72 hours
ACH	24-48 hours for payments to be reflected in bank accounts
"Know Your Customer" (KYC) processes	This process collects the personal data and legally records customer's identification. KYC is used every time for authorization.
Transaction fees	Different fees are added which makes the process longer and cause delay. and increases financial pressure on customers.

These transactions are stored on different servers. Money transactions are done by different procedures and the majority are done digitally by using some of the ways like NFTS, Google Pay, Bank transfers, Cards, or some by Cheques, DD, etc. Decentralization of this system is important to bring all transactions under one roof and secure them to minimize fraud. Many times, transactions are done parallel in distinct locations which are not reflected in original accounts. Bank transactions are not handled on weekends and bank holidays. are handled on the next business day. Bank accounts and many other financial services necessitate "Know Your Customer" (KYC) processes. Which means that banks are legally required to record a customer's identifying information before

 ISSN 2394 - 7780

opening a new account. Minimum requirements for digital transfers include government-issued identification, a bank account, and mobile phone. Bank account information is stored on the bank's own servers which are owned by clients. Banks privacy is limited by security of the bank's systems and individual user's capacity to protect their data. If the bank's systems become compromised, an individual's data is at risk because it follows the centralized system everything is stored at a center system. Considering the client follows basic internet security procedures, including safe passwords and two-level with authentication, The banking account information is as secure as the bank's server, which storescustomer account information. Banks uphold the right to reject transactions for many kinds of reasons. Banks have the capacity to freeze the accounts. If a bank detects purchases in unexpected places or strange things, they may be refused. KYC requirements allow governments to easily monitor people's bank accounts and take assets for a variety of reasons. This all takes time as it is managed centrally by one person handling the database.

MOTIVATION

In current scenario world of growing technology, the current transaction methods of processing currency in India is digitized so there are many digital payment methods used. The system makes use of Blockchain technology in a decentralized method. Blockchain technology arises from the feature of security which includes authorization, accessibility, and accountability which is provided by block technology like Smart contracts, Consensus protocol, and the most important of all Decentralized approaches for conducting the process. The overall system focuses on the minimalistic need for the manual approach and increasing the overall transparency of the process. Decentralizing the system will help cut out the unnecessary contact of the officials from the central authorities and eventually reduce the risk or loss in the verification documentation and increase overall efficiency. Decentralizing means accessing accounts from anywhere distributed servers, networks, and systems with no central and authority control. The documents are saved in the documents format digitally called smart contracts. They are designed to give security and authentication and authorization.

METHODOLOGY

The current system of centralized banking.

1) **Customer: -** Goes to the bank personally or to the bank server online. Requests bank for account opening gives all details. By filling in form submitting hard copies of documents.
2) **Bank Server/bank: -** Enquires about type of account and ask and ask to enter/write personal details.
3) **Validation: -**Documents are validated and sent to system manager.
4) **System Manager: -** Registered details saves to database and request customer to deposit initiate funds. Customer sends funds they are saved to database.
5) **Database: -** System manager checks and sends the account details back to customer.
6) **Customer: -** Starts using bank account after first activation.

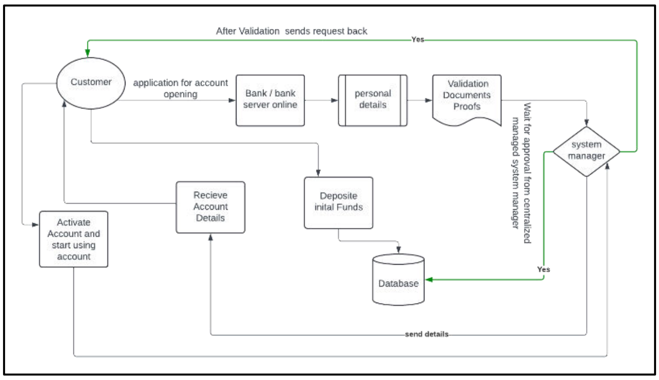


Fig1: System methodology currently

1) **Customer: -** Enters the details on frontend dashboard interface to open account generates key hash based technique of blockchain. Uploads document in digital format from any place. Request admin (blockchain interface)
2) **Admin: -** is the main software interface. The request is further sent to invoke smart contract and saves the uploaded documents in this smart contract.

3) **Verification: -** If eligible account is opened and data is saved to REST server. If the customer is not eligible it notifies the customer.
4) **Rest Server: -** They store data and sends the account registration details to admin.
5) **Admin: -** Registers owners account with customers new details and saves to rest server.

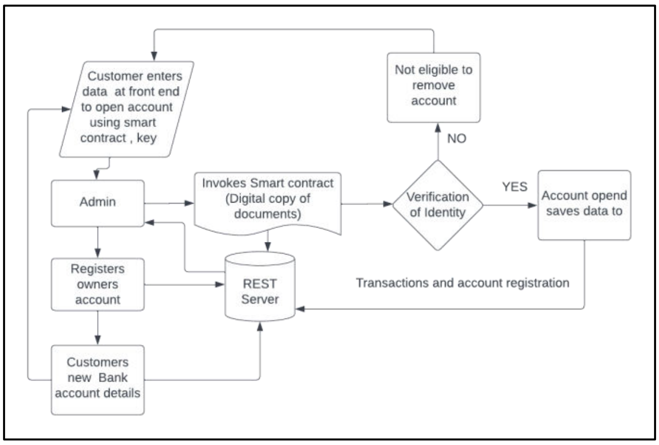


Fig 2: Suggested Blockchain system methodology

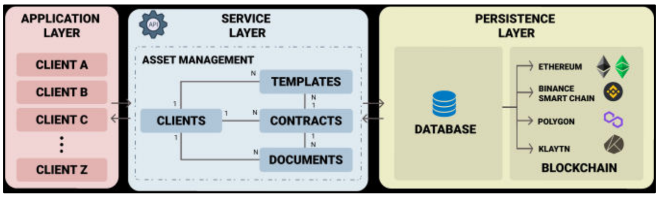


Fig.3: Document Registration Service Architecture [20]

CONCLUSION

The proposed system is aimed at making the Digital transactions system popular in India. Go paperless and easier than the traditional system which has several flaws like time delay, Involvement of Government officials and mediators in the process that take advantage to defraud both the public and government as well as different frauds cyber attackers. This paperless digital demonstrates the implementation of secure transactions and money using blockchain technology by securing the documents related to the identity of the user account or transactions using a Hash-based block that makes the overall blockchain network more secure, reliable, and stable, to use for digital transactions. The transactions are conducted in either that is blockchain-based currencies and secured with the use of smart contracts, which are similar to general agreements between the parties which makes the transaction more secure from frauds. Also making the transactions transparent to the users so later disagreement can be avoided. The generation of a Digital deed is far easier than that of a paper-based one as once the transaction is verified by the land inspector the official digital deed is provided to all the members involved in the transaction including the inspector or Admin ownership. The overall Web3-based platform provides a quick solution for the slow paper-based bank registration, and it can prove to be a real change for the future of Digital India.

FUTURE SCOPE

There can be different models and architectures developed using blockchain technologies for efficient bank transactions. Blockchains can be used to solve various problems in day-to-day life. Developing this technology and software implementations which can give new perspective and functioning to the current system and will bring positive change in the ecosystem and modernization.

REFERENCES

[10] B. Sriman, S. H. Annie Silviya, E. Santhosh Kumar, K. Suryaa Narayanan, and S. Nishaalu, “Blockchain Industry 5.0: Next Generation Smart Contract and Decentralized Application Platform,” in Proceedings of the 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems, ICSES 2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICSES55317.2022.9914151.

[11] S. M. H. Bamakan, A. Babaei Bondarti, P. Babaei Bondarti, and Q. Qu, “Blockchain technology forecasting by patent analytics and text mining,” Blockchain: Research and Applications, vol. 2, no. 2, Jun. 2021, doi: 10.1016/j.bcra.2021.100019.

[12] H. Chen, X. Luo, L. Shi, Y. Cao, and Y. Zhang, “Security challenges and defense approaches for blockchain-based services from a full-stack architecture perspective,” Blockchain: Research and Applications, vol. 4, no. 3, Sep. 2023, doi: 10.1016/j.bcra.2023.100135.

[13] R. K. Sachan, R. Agarwal, and S. K. Shukla, “Identifying malicious accounts in blockchains using domain names and associated temporal properties,” Blockchain: Research and Applications, vol. 4, no. 3, Sep. 2023, doi: 10.1016/j.bcra.2023.100136.

[14] H. Han, P. Chen, F. Yang, B. Brekhna, and R. Zhang, “TSCS: A blockchain-based tokenized subtitling crowdsourcing system,” Blockchain: Research and Applications, vol. 4, no. 2, Jun. 2023, doi: 10.1016/j.bcra.2023.100132.

[15] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.” [Online]. Available: www.bitcoin.org

[16] J. S. Gazsi, S. Zafreen, G. G. Dagher, and M. Long, “VAULT: A Scalable Blockchain-Based Protocol for Secure Data Access and Collaboration,” in Proceedings - 2021 IEEE International Conference on Blockchain, Blockchain 2021, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 376–381. doi: 10.1109 /Blockchain53845.2021.00059.

[17] B. Version, “ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER.”

[18] H. Zhang and W. Liu, “Research on the Application of Blockchain in the Safe and Trusted Sharing of Government Data,” in Proceedings - 2023 2nd International Conference on Artificial Intelligence and Blockchain Technology, AIBT 2023, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 52–55. doi: 10.1109/AIBT57480.2023.00017.

[19] Computer Society of India, Jawaharlal Nehru Engineering College, and Institute of Electrical and Electronics Engineers, Proceedings of the 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing : October 30-31, 2020.

[20] A. Thakur, S. Sahoo, A. Mukherjee, and R. Halder, “Making Robotic Swarms Trustful: A Blockchain-Based Perspective,” Journal of Computing and Information Science in Engineering, vol. 23, no. 6, Dec. 2023, doi: 10.1115/1.4062326.

[21] D. Vujičić, D. Jagodić, and S. Randić, “Blockchain technology, bitcoin, and Ethereum: A brief overview,” in 2018 17th International Symposium on INFOTEH-JAHORINA, INFOTEH 2018 - Proceedings, Institute of Electrical and Electronics Engineers Inc., Apr. 2018, pp. 1–6. doi: 10.1109/INFOTEH.2018.8345547.

[22] “ethereum/wiki A Next-Generation Smart Contract and Decentralized Application Platform.”

[23] J. P. de Brito Goncalves, G. Spelta, R. da Silva Villaca, and R. L. Gomes, “IoT Data Storage on a Blockchain Using Smart Contracts and IPFS,” in Proceedings - 2022 IEEE International Conference on Blockchain, Blockchain 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 508–511. doi: 10.1109/Blockchain55522.2022.00078.

[24] Institute of Electrical and Electronics Engineers, Probing artificial intelligence techniques and research in IoT (PATRIOT) 5th International Conference on Science, Technology , Engineering & Mathematics : IEEE ICONSTEM ’19 : 15th March 2019, venue: Placement Seminar Hall, Jeppiaar Engineering College, Chennai.

[25] H. Liu, H. Zhang, B. Chen, and A. W. Roscoe, “Committable: A Decentralised and Trustless Open-Source Protocol,” in IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICBC54727.2022.9805541.

[26] X. Li, Z. Ma, and S. Luo, “Blockchain-Oriented Privacy Protection with Online and Offline Verification in Cross-Chain System,” in Proceedings - 2022 International Conference on Blockchain Technology and Information Security, ICBCTIS 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 177–181. doi: 10.110 9/I CBCTIS55569.2022.00048.

[27] R. Mihai, O. F. Ozkul, G. Datta, N. Goga, S. Grybniak, and C. V. Marian, "B lockchain-Enabled Economic Transactions: Recurring Financial Accruals and Payments," in 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain and Beyond, iGETblockchain 2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/iGETblockchain56591.2022.10087074.

[28] P. Shen et al., "A Survey on Safety Regulation Technology of Blockchain Application and Blockchain Ecology," in Proceedings - 2022 IEEE International Conference on Blockchain, Blockchain 2022, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 494–499. doi: 10.1109/Blockchain55522.2022.00076.

[29] P. Soares, R. Saraiva, I. Fernandes, A. Neto, and J. Souza, "A Blockchain-based Customizable Document Registration Service for Third Parties," in IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2022, Institute of Electrical and Electronics Engineers Inc., 2022. doi: 10.1109/ICBC54727.2022.9805500.

[30] U. Khan, Z. Y. An, and A. Imran, "A Blockchain Ethereum Technology-Enabled Digital Content: Development of Trading and Sharing Economy Data," IEEE Access, vol. 8, pp. 217045–217056, 2020, doi: 10.1109/ACCESS.2020.3041317.

[31] E. Androulaki et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," in Proceedings of the 13th EuroSys Conference, EuroSys 2018, Association for Computing Machinery, Inc, Apr. 2018. doi: 10.1145/3190508.3190538.

[32] K. R. Rao and S. Naganjaneyulu, "Permissioned Healthcare Blockchain System for Securing the EHRs with Privacy Preservation," Ingenierie des Systemes d'Information, vol. 26, no. 4, pp. 393–402, Aug. 2021, doi: 10.18280/ISI.260407.

[33] A. K. Tyagi, "Decentralized everything: Practical use of blockchain technology in future applications," in Distributed Computing to Blockchain: Architecture, Technology, and Applications, Elsevier, 2023, pp. 19–38. doi: 10.1016/B978-0-323-96146-2.00010-3.

[34] J. Kalajdjieski, M. Raikwar, N. Arsov, G. Velinov, and D. Gligoroski, "Databases fit for blockchain technology: A complete overview," Blockchain: Research and Applications, vol. 4, no. 1. Zhejiang University, Mar. 01, 2023. doi: 10.1016/j.bcra.2022.100116.

[35] 2022 IEEE International Conference on Blockchain (Blockchain) IoT Data Storage on a Blockchain Using Smart Contracts and IPFS João Paulo de Brito Gonçalves Federal Institute of Espirito Santo (Ifes) Cachoeiro de Itapemirim - ES, Brazil jpaulo@ifes.edu.br Gabriel Spelta, Rodolfo da Silva Villaça, Roberta Lima Gomes Federal University of Espirito Santo (Ufes) Vitoria - ES, Brazil gabriel.spelta@edu.ufes.br, rodolfo.villaca@ufes.br, rgomes@inf.ufes. | 978-1-6654-6104-7/22/$31.00 ©2022 IEEE | DOI:

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

BLOCK CHAIN BASED VERIFICATION OF EDUCATION AND PROFESSIONAL CERTIFICATE

Neelam Naik[1] and Hetavi Shah[2]
[1]Assistant Professor, Department of Information Technology, SVKM's Usha Pravin Gandhi College of Arts, Science and Commerce, Vile Parle, Mumbai 400056
[2]Student, Master of Information Technology, SVKM's Usha Pravin Gandhi College of Arts, Science and Commerce, Vile Parle, Mumbai 400056

ABSTRACT
Every year, various degree and courses certificate are issued to students and professionals. Verifying these documents manually by the University or Companies is a tedious task. To counter this forgery issue, this paper proposes a block chain technology using two step verification for high security and tamper-proof verification process. A block chain technology is a chain of data, where data are stored in nodes called "Blocks" which are linked to each other forming a chain. This gives the data saved on the block chain a high degree of security and confidence.

I. INTRODUCTION
The way block chain technology operates is by establishing a distributed, decentralized digital ledger that keeps track of transactions across numerous computers, or "nodes". When a transaction occurs, it is verified by the network of nodes and then added to a block. Each block has the transaction data, a timestamp, and a cryptographic hash of the previous block. This produces a series of blocks that are connected to one another and encrypted.

The block chain makes it impossible to change a block after it has been added without also changing all subsequent blocks, which makes it very difficult for one party to control or manipulate the data. This ensures that the data saved on the block chain is highly secure and trustworthy.

Since block chain technology is decentralized, there is no single point of failure or central authority, which leaves it vulnerable to fraud and hacking. Additionally, the transparency of the blockchain allows for all participants to have access to the same information, creating a more secure and efficient way of recording and verifying transactions.

Generally, block chain innovation works by making a secure, straightforward, and decentralized framework for recording and confirming exchanges over different computers, giving a tall level of security and believe within the information put away on the block chain.

Many people enroll their self in various courses which help them to expand their knowledge and implement it practically. At the end of course they receive certificate or degree as a proof of achievement. When employer employees a candidate they wanted to verify this certificate. In traditional system, they need to login to each courses official website and verify it due to various diversity of courses. For example if a person have done a course python from Udemy then the employer need to login to Udemy website and verify the certificate issued. There is no collective verification system where one can verify the certificate issued. Therefore this study focuses on block chain based verification system where one can verify different courses and academic certificate collectively at one place.

II. LITERATURE REVIEW
In the study, (Saleh Omar et al, 2021) research paper proposes Decentralized Certification Verification Privacy Control Protocol. Verifying educational based certificates using protocols by maintaining privacy and confidentiality at network level and data level. The arrangement to the issue of decentralization is actualized utilizing Hyperledger Texture as the foundation and Javascript as the contract dialect.

In this paper, (Mahto Dindayal et al, 2023) decentralized application offers a promising solution to address the growing issue of forgery. It guarantees bona fide advanced records are suitably put away, gives simple get to, adjusting prove for quick confirmation when required. This application not only helps students to gain their certificates but also helps educational institutions and recruiters.

In this paper, (Herbke Patrick et al, 2022) issue of academic network in digital credentials can be integrated into the Self-Sovereign Identity ecosystem to overcome is proposed. ELMO2EDS is a system that does three things: 1) allows the issue, storage, and verification of completed studies; 2) permits student identification; and 3) transforms EMREX digital credentials to the proper Self-Sovereign Identity data format.

In the study, (Sintyaningrum Desti Eka et al, 2021) authentication of certificate using digital signature and QR code is verified. It is a web based application to access it anywhere and anytime. Research and Development method is used in this paper for problem analysis. The two main scheme in this paper are: the conspire in making e-certificate and the conspire of confirmation QR Code. It disseminates electronic certificates that are immune to fraudulent conduct like certificate spoofing.

In this study, (Shree Divya et al, 2022) the data is stored in cloud using this web application. Each document is given a unique hash value which is authenticated. The system uses live face verification of document. Machine learning algorithm is used for face verification. It uses face-to-face identification for verification of documents.

In this study, (Ambast Swatesh et al, 2022) educational credential verification system is proposed, independent of credentials format and size. A secure decentralized client interface for handling, putting away and confirming understudy scholastic accreditations. It supports format like PDF, DOCX, JPG, PNG, etc. It also allows third party employers to check the information independently and securely. It is not limited to file size and does not require specific format.

In this study, (Kumar Vijaya et al, 2022) it validates document hash value with cryptgraphic hash value using blockchain technology. SHA-512 algorithm is used to generate this hash values of document. The essential assignment is to check whether the report exists or not. Proof of Existence is used to check real time document. It consensus mechanisms to update the data blocks.

In this research, (Petcu Adrian et al, 2023) decentralized and non-invasive documents are targeted for signing. Block chain technology is used for digital signature of document to reduce e dependency on centralized entities. A feature of immutable document is also fulfilled.

In this research, (S S Latha et al, 2022) general framework is developed to verify the document using block chain technology. An application is developed which can be installed in local system known as nodes or blocks. The Ropsten Ethereum Network is used for deployment process. The decentralized concept is used for application. The name of the application is DApp using concept of smart contract. It enables that the software code in itself is tamper proof.

In this study, (Deshpande Amol et al, 2023) it enables easy verification of skills and certifications of a particular candidate by storing the captured data on Ethereum Block chain. This framework is created in three stages. In stage one, the institution enlists candidate and they have fill up the foundation data. Within the moment stage, candidate raise a ask for supports andconfirmation of their abilities and certifications. In last step acceptance or rejection of request is done. It helps to build trust when everyone has access to the information.

In this research, (Timothy Harlian et al, 2022) implemented Ethereum block chain using document validation system. It also uses Rinkeby Test Network as block chain network. The application is verified using black box and white box testing which can also perform input, retrieve, update, and delete operation. The study also records highest and the lowest performance testing time. Here block chain is used as a validator.

In this study, (Sahane Prema et al, 2023) a secure and verifiable portfolio of their certificates is maintained using block chain. Additionally, the system features an extensive user interface for issuing and verifying certificates. It builds a trust between the users. In this system, this framework is created in three stages. In stage one, the institution enlists candidate and they have fill up the foundation data. Within the moment stage, candidate raise a ask for supports and confirmation of their abilities and certifications.

In this study, (Gaikwad Hrithik et al, 2021) an attempt has been made to develop a Blockchain-based verification system for academic certificates. With the approach of open Block chain like Ethereum, DApps (Decentralized Applications) and Keen contracts, adaptable and taken a toll viable arrangements can be executed to diminish overhead and make report confirmation a consistent handle. The proposed arrangement comprises of a web app which can have a front-end for enlisting and requesting confirmation, beside a backend which can have two modules: An OCR module to extricate points of interest from certificates and a Block chain module to send and confirm information put away within the Block chain.

In this study, (Singh Anjali et al, 2023) verification of educational certificate using Ethereum platform and smart contracts. This system works on Hash value by converting traditional certificate into digital certificate by cryptographic hash functions and stored on Blockchain. One of a kind certificate ID and exchange hash esteem will be produced which confirms the certificate through common stage.

In this paper, (Inayatulloh, 2021) a model is built using block chain technology to protect diplomas or other important e-certificates in universities from certificate. A block chain innovation demonstrate is construct utilizing open source framework to ensure college e-certificates from being forged. The most reason of this paper is to assist higher instruction secure imperative e-certificates issued to graduated class by block chain innovation.

In this study, (Shinde Rohan et al, 2022) a platform called IPFS for verifying documents. This system returns a hash value which is encrypted and then stored on Hyperledger block chain. In this framework, archive is permanent as long because it is within the block chain. The data in the system is stored in IPFS. Tampering of file will lead to consensus failure verification of document will fail.

In this study, (Rustemi Avni et al, 2023) QR code is generated for academic documents. Verification of data is done by digital signature from front end as well as back end. Then it encrypts the data and generates smart contract using block chain technology. This architecture is used to generate QR code for certificates. This QR code contains many information regarding the certificate which is also authenticated.

III. PROPOSED SYSTEM

The traditional system does not have the feature of security. By using block chain technology it enables the security of document. But there might be a chance of break through. The figure below represents the system flow. The document undergoes various processes and ensures its authenticity and security. The system has Two main entity which are:

University/Institute:
University or Institute are the issuer of the certificate. Certificates achieved by the student in degree or courses are issued by the concerned authority.

Student/Employer:
Student or Employer are the actual owner or viewer of the Certificate. A employer can easily verify the certificate using the system.

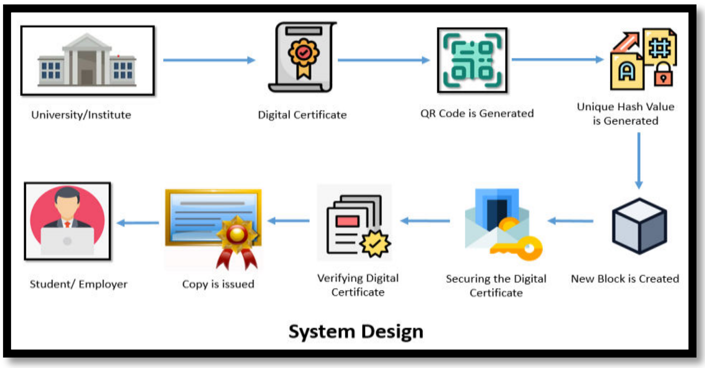


Fig. 1 The System Design

The system under goes various processes:

Creating Digital Certificate:
The data or information given by the institute or university are then converted to digital certificate. The manual certificate can also be uploaded and can be converted into digital certificates in the form of pdfs.

Generating QR Codes:
QR code for each certificate will be created. This QR code will contain all the information required like issuer name, name of the owner, time, date, course name or degree name, etc.

Generating Hash Values:

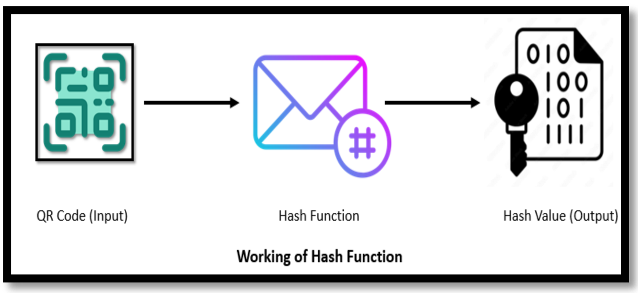


Fig. 2 Working of Hash Function

For each QR a unique hash value will be generated. This ensures that the document is immutable. Fig. 2 above shows the implementation of Hash Function. For converting QR to hash values algorithm is applied where QR code will act as an input and hash value as output.

Block Creation:
Each hash values are then added to a new block. The data or information then converted into nodes called as "Blocks". In this way every time a new data is inserted new block will be created. It can then be linked in network creating a chain of blocks using the block chain technology.

Securing the Digital Certificate:
Using the block chain technology the certificates are secured. Best feature of block chain technology is immutability of document which is achieved in this system.

Verification of Digital Certificate:
The verification of certificate is done by comparing the hash values. If the hash values are matched then the certificate is considered as authentic otherwise not. It ensures the trust of the client that the certificate is authentic and authorized.

Copy of Digital Certificate:
A digital copy of verified certificate or degree is available for students and employs. This copy is only available if the certificate is authentic otherwise it will not display the certificate.

Thus, the proposed system enables a document to undergo a secure verification process which ensures its authenticity. The double security decreases the flaws in the system and ensures its authenticity and security of certificates.

IV. CONCLUSION

The immutable and transparent nature of the block chain technology, combined with its decentralized architecture, offers a compelling solution to the challenges associated with traditional verification methods. To check the authenticity of educational and professional certificate a framework is developed. The proposed system has two-step verification approach which can significantly bolster the security of block chain data providing an extra safeguard against unauthorized access and fraudulent activities. In first level of security the data will be converted to QR codes which are undecipherable to human beings. In second level, the data are converted to hash values which are later compared for verification of documents.

V. FUTURE WORK

The future enhancement is to implement this framework and add on new functionalities like accepting various file formats, generating new algorithm for hash values, introducing third step for verification etc. The propose system can be implemented to various other fields where the security of data is important.

REFERENCES

[1] Saleh O., Ghazali O., Idris N., "A New Decentralized Certification Verification Privacy Control Protocol", International Cyber Resilience Conference (CRC), IEEE, 2021, DOI: 10.1109/CRC50527.2021.9392485

[2] Mahto D., Murali S., Selvaraj B., Arasu S.," Decentralized Approach for Graduates' Certificate Generation, Validation, and Verification", International Conference on Industrial Electronics: Developments & Applications (ICIDeA), IEEE, 2023, DOI: 10.1109/ICIDeA59866.2023.10295239

[3] Herbke P., Yildiz H., "ELMO2EDS: Transforming Educational Credentials into Self-Sovereign Identity Paradigm", International Conference on Information Technology Based Higher Education and Training (ITHET), IEEE, 2022, DOI:10.1109/ITHET56107.2022.10031276

[4] Sintyaningrum D., Muladi., Ashar M., "The Encryption of Electronic Professional Certificate by Using Digital Signature and QR Code", International Conference on Converging Technology in Electrical and Information Engineering (ICCTEIE), IEEE, 2021, DOI: 10.1109/ICCTEIE54047.2021.9650641

[5] Shree M., Keerthana., KrisshneShri., "DIGITAL DOCUMENTS VERIFICATION SYSTEM", International Conference on Computer, Power and Communications (ICCPC), IEEE, 2022, DOI: 10.1109/ICCPC55978.2022.10072252

[6] Ambast S., Sumesh T., "A Blockchain Based Credential Verification System using IPFS", India Council International Conference (INDICON), IEEE, 2022, DOI: 10.1109/INDICON56171. 2022.10039743

[7] Kumar V., Ghanta V., Pendyala V., Reddy P., "A Blockchain-based Document Verification Model in Freshers Hiring Process", International Conference on Electronics, Communication and Aerospace Technology (ICECA), IEEE, 2022, DOI: 10.1109/ICECA55336.2022.10009358

[8] Petcu A., Frunzete M., Stoichescu D., "A Practical Implementation Of A Digital Document Signature System Using Blockchain", International Symposium on Advanced Topics in Electrical Engineering (ATEE), IEEE, 2023, DOI: 10.1109/ATEE58038.2023.10108308

[9] Latha S., Priya N., Shettar A., "Block chain Based Framework for Document Verification", International Conference on Artificial Intelligence and Signal Processing (AISP), IEEE, 2022, DOI: 10.1109/AISP53593.2022.9760651

[10] Deshpande A., Ambawade D., Bafna H., Challawala H., Damani J., "Blockchain based Skill Verification System", International Conference on Sustainable Computing and Smart Systems (ICSCSS), IEEE, 2023, DOI: 10.1109/ICSCSS57650. 2023.10169782

[11] Timothy H., Muhammad F., Purwanto Y., "Implementation of Blockchain for Digital Document Data Collection Website", International Conference on Information System & Information Technology (ICISIT), IEEE, 2022, DOI: 10.1109/ICISIT54091.2022.9873097

[12] Sahane P., Obla A., Bhangale P., "Student Achievements Portfolio Management using Blockchain", International Conference on Inventive Computation Technologies (ICICT), IEEE, 2023, DOI: 10.1109/ICICT57646.2023.10134076

[13] Gaikwad H., D'Souza N., Gupta R., Tripathy A. K., "A Blockchain-Based Verification System for Academic Certificates", International Conference on System, Computation, Automation and Networking (ICSCAN), IEEE, 2021,DOI:10.1109/ICSCAN53069. 2021.9526377

[14] Singh A., Chauhan S., Goel A., "Blockchain Based Verification of Educational and Professional Certificates", International Conference on Computational Systems and Communication (ICCSC), IEEE, 2023, DOI: 10.1109/ICCSC56913.2023.10143008

[15] Inayatulloh., "Blockchain Technology Model to Protect Higher Education E-Certificates with Open Source system.", International Conference on Cybernetics and Intelligent System (ICORIS) , IEEE, 2021, DOI: 10.1109/ICORIS52787.2021.9649606

[16] Shinde R., Chorghe S., Dhanani K., Salunke A., "Doc-Chain: A University Document Verification Blockchain", International Conference on Blockchain and Distributed Systems Security (ICBDS), IEEE, 2022, DOI: 10.1109/ICBDS53701.2022.9935950

[16] Rustemi A., Atanasovski V., Risteski A., "Identification During Verification Of Diplomas In The Blockchain System", International Conference on Systems, Signals and Image Processing (IWSSIP), IEEE, 2023, DOI: 10.1109/IWSSIP58668.2023.10180241

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

UNDERSTANDING FINANCIAL PATTERNS: A STATISTICAL ANALYSIS OF INDIVIDUAL MONEY MANAGEMENT PRACTICES

Neelam Naik[1], Swapnali Lotlikar[2] and Mansi Sarvaiya[3]
[1]SVKM's Usha Pravin Gandhi College of Art's Science and Commerce Vile Parle, Mumbai 400056

ABSTRACT
Money is just a way of keeping score. The more we save the more lavish life is lead stress free or guilt free. The study highlights the savings and investment plans of an individual by conducting and survey using online forms. The survey is conducted on different parameters like age group, gender, incomes, expenses pattern and investment pattens to conclude on the best investment pattern using Chi Square Test.

INTRODUCTION
Who would think that money would make a man happy? This study highlights the day-to-day expenses incurred by an individual and the investment plans which is most likely preferred by majority of the individual. The study is conducted using online survey and collecting opinions of all age groups

LITERATURE REVIEW
The study circulates among different statistical research conducted by different researchers like[1] Researchers believe there is a need to study the importance young Indians place on saving money, their spending habits and long-term financial security plans. [2] The aim is to create a measure of the economic culture and behaviour of the Indian people. Three-dimensional model e.g. thinking, behaviour and cognitive skills of character design [3] There has been research that shows that one of the persistent problems that still affects college students is the difficulty in maintaining funds, so this study aims to analyse the spending habits of 138 college students in Delhi and Mumbai using the identifier research. [4] The main aim of this study is to determine students' spending patterns and to plan, support and balance students' saving behaviours. Get to the bottom of their expenses. To determine how much money, they spend each month. [5] The financial literacy levels and attitude of rural households in India were investigated in this study. This study was conducted in India and with a sample size of 92. The results of the research show that low levels of financial knowledge led to bad behaviour among people living in rural areas. [6] Research proves that students' effective management of finance is critical for their academic success and retention. Therefore, this research paper aims to analyse the consumption and conservation of money in the young generation for Dombivli district.

METHODOLOGY
The hardest thing to understand in the world is the Money. The study is the outcome of the survey conducted using forms. More than 35 individuals from different age group participated in the survey where the women were majority.

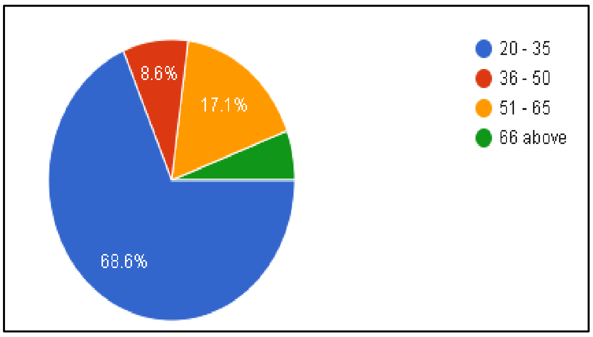


Fig 1.1 - Age Group

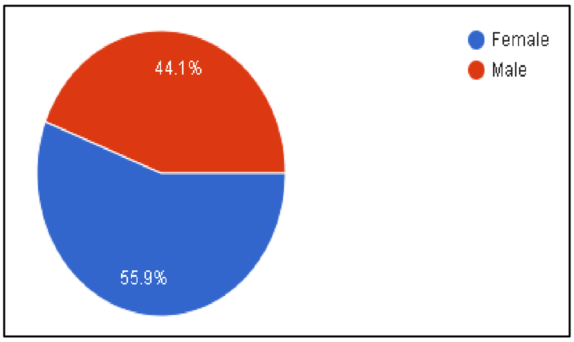


Fig 1.2 - Gender

All the participant's annual income fell into the group of 2 lakhs to 7 lakhs which makes it an average income range. Majority of them are self-earner but their income was secondary income to the family hence it might help in fulfilling luxurious cravings.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

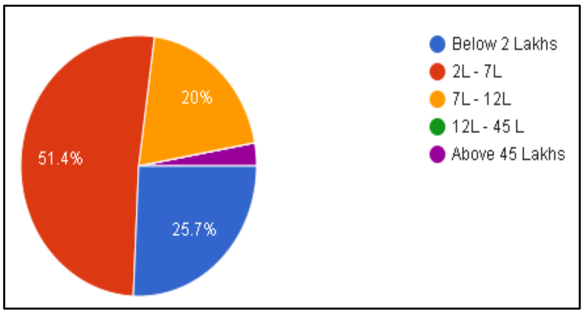


Fig 1.3 - Income Range

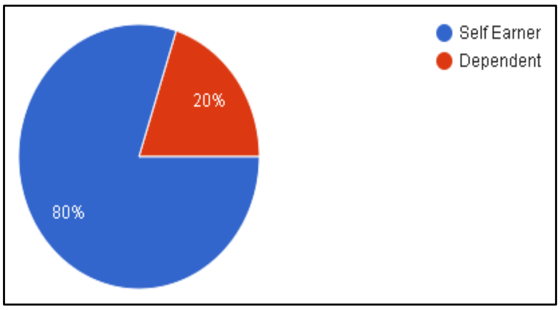


Fig 1.4 - Income Category

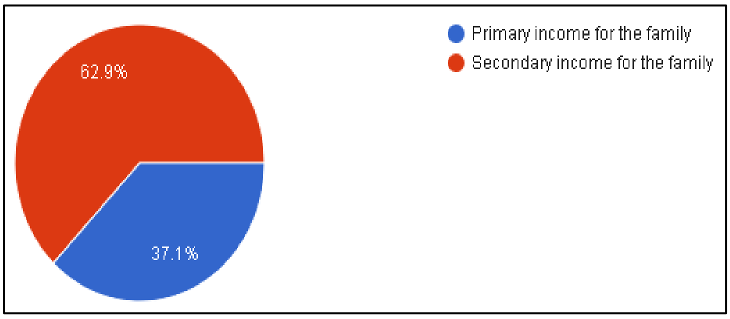


Fig 1.5 - Income Type

The study further continusous to the nature of expenses incurred and the investment plans used by the individual to geneate additional income. Now-a-days people rarely take any debts and enjoy a guilt free life. Since many participents spend on their parents the small chunk of income is incurred in medical related expensis.

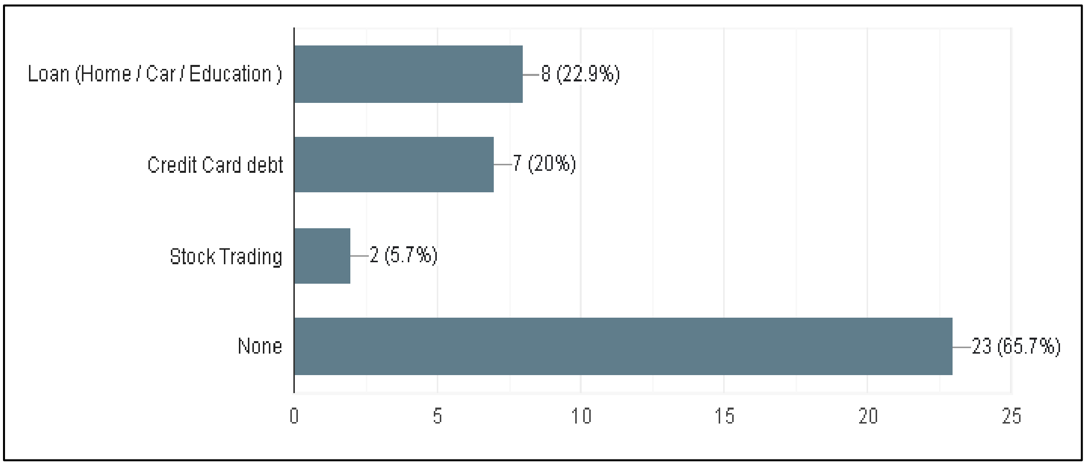


Fig 1.6 - Types Of Debts

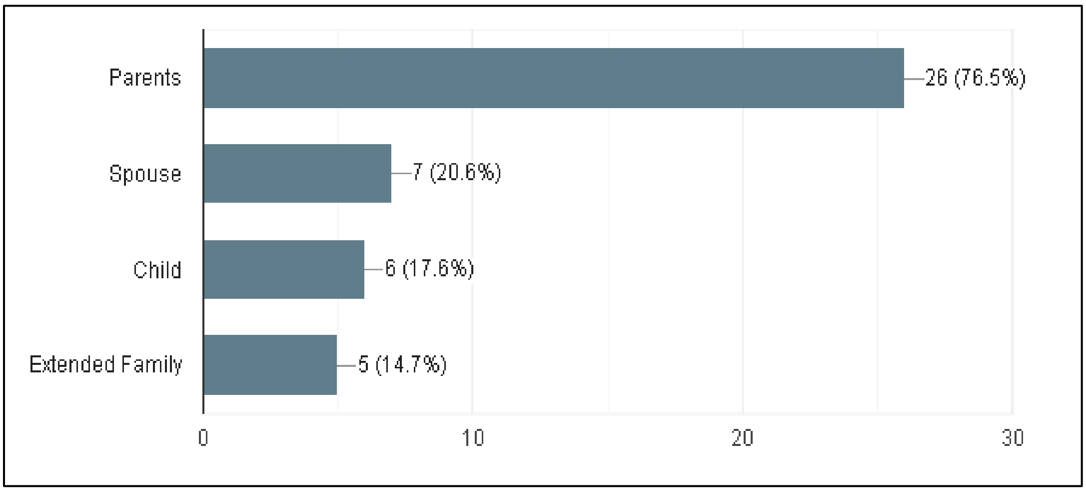


Fig 1.7 - Income Spent On

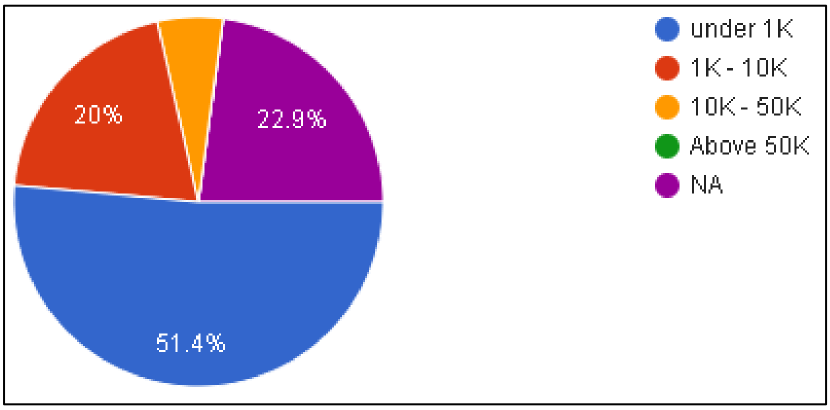


Fig 1.8 - Medical Expenses

The study then continues to understand what an individual spends on and at the end of the day what is left in his hand. The expenses can by segregated into six different parts like travelling, groceries, bills, stationery and miscellaneous. Below graphs represents all the expenses incurred by the participants.

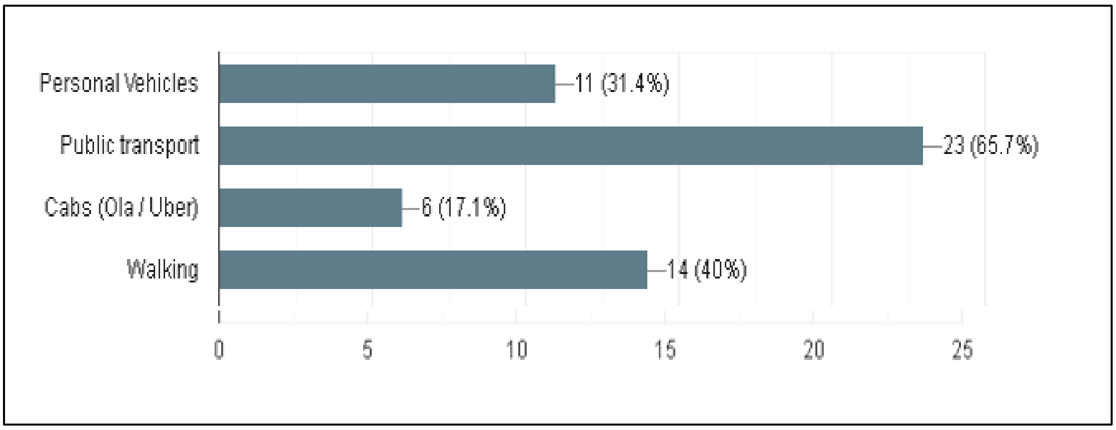


Fig 1.9 - Modes of travelling

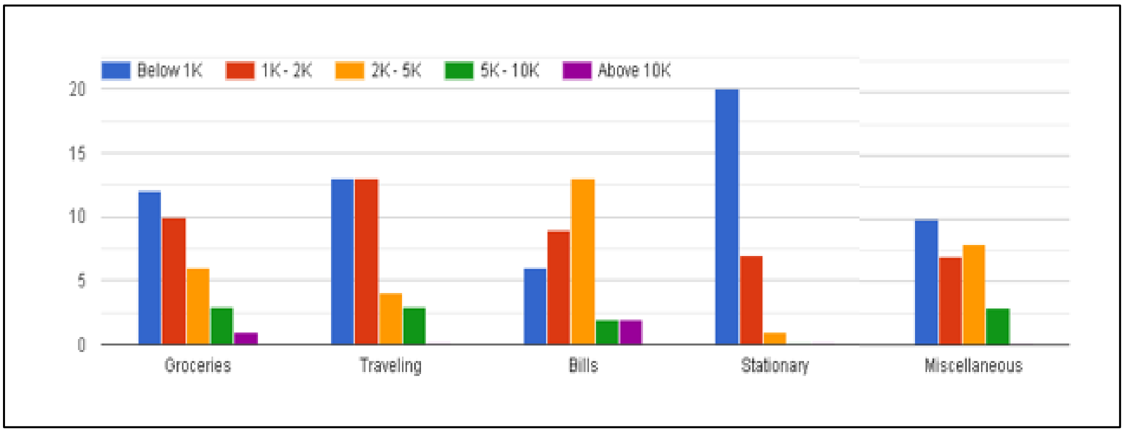


Fig 1.10 - Other Expenses

DISCUSSIONS

The lack of money is the root of all evil. The outcome of the survey says that all of them try to save in some or the other way and the savings percentile goes up to 10 percentage. By doing the investments into fixed deposits, mutual funds, gold, estates or stocks trading the side income is generated that can help in other happiness like trips, vacation, electronics etc.

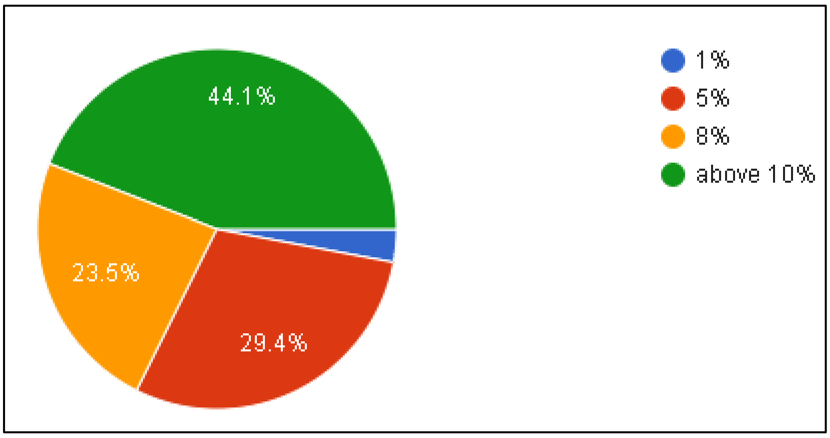


Fig 1.11 - Saving Percentage

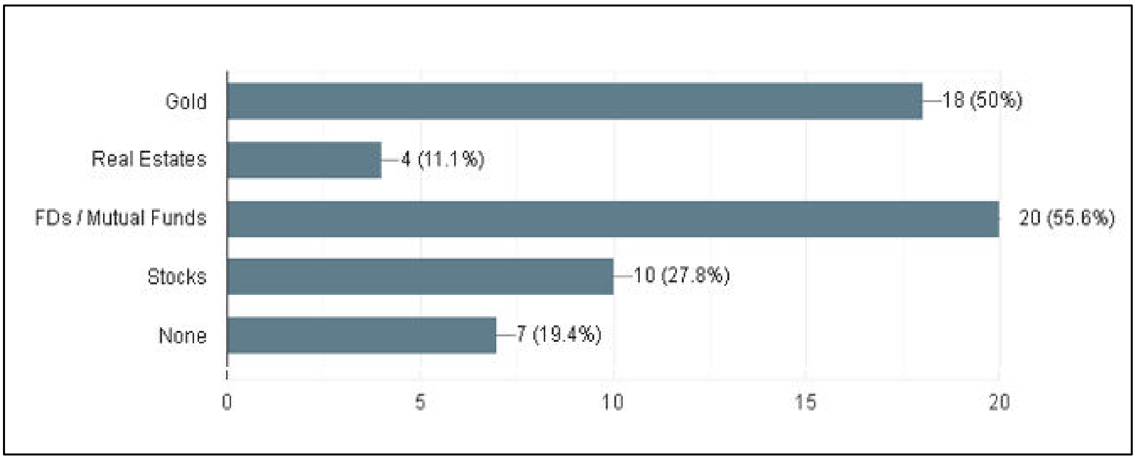


Fig 1.12 - Investments preferences

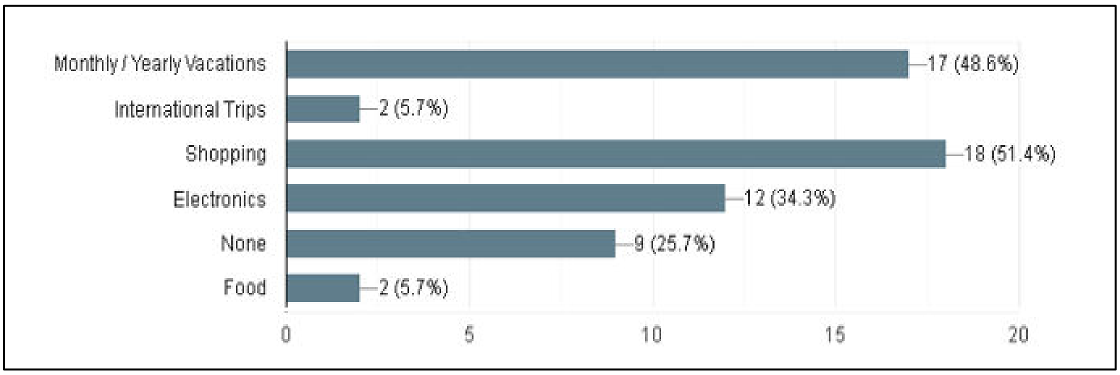


Fig 1.13 - luxurious Cravings

Statistical Experiment:
The chi-square test (X^2) is one of the simplest test of statistical significance and is mostly suitable for testing the hypothesis of frequency or frequency of planning at the conference. Consider this alternative way of thinking:

H_1: *FDs and Mutual Funds are best investment options as it gives good returns.*

Investment Option	Frequency
Gold	18
FDs & MFs	20
Stocks	10
Total:	**48**

Table 1.1: One way frequency Table.

The X^2 value is calculated using the below formula:

$$X^2 = \frac{\sum (O - E)^2}{E}$$

ISSN 2394 - 7780

Where:

X^2 = Chi-square statistic

O = Observed frequency

E = Expected frequency

Add up the squared differences as shown below:

$$X^2 = \frac{(O - E)^2}{E} + \frac{(O - E)^2}{E} + \frac{(O - E)^2}{E}$$

$$X^2 = \frac{(18 - 16)^2}{16} + \frac{(20 - 16)^2}{16} + \frac{(10 - 16)^2}{16}$$

$X^2 = 1.16$

The degree of freedom will be calculated as follows:

$df = k - 1$

Where:

k = Number of cells associated with the row or column of data.

Therefore, degree of freedom equals to 2 (df = 3 - 1 = 2)

EXPERIMENT RESULTS:

Now need to compare the X^2 value to the significant chi-square value is associated with a probability of 0.05 and degree of freedom is equal to 2. The critical value of X^2 is 5.991. Since the calculated value of X^2 is less than the chi-square value in the table, it is concluded that the observed value is not equal to the expected value. So, the hypothesis is rejected stating that the FDs and Mutual Funds are not best investment options as it does not give good returns.

CONCLUSION:

From the survey response it is observed that using money cautiously one can fulfil the additional spending like vacation/trips or shopping. Do not save what is left after spending; instead spend what is left after saving. With the help of this study one can understand the need of saving money and spending money with caution. In case of unplanned emergency saved money will help like elderly.

REFERENCES:

[1]: DR. Betty Sibil, “A Comparative Study of Money Management Attitude among Students Pursuing Professional Courses”,2013, Journal of Economics and Economic Education Research

[2]: Devlina Chatterjee, Tanvi Keswani, Sanjay Gupta, “Money Attitudes of Indian Adults: An Exploratory Study”, 2018, https://www.researchgate.net/publication/346305865

[3]: Saumya Singh, Shubham Gupta, Siddhant Jain, Siddhi Kabra, Snehil Gupta, “Student Budgeting And Spending Behaviour”, 2020, International Journal of Creative Research Thoughts (IJCRT)

[4]: Nicky Lalmuanpuia, “A Study On Student Budgeting And Spending Behaviour Among The College Students Of Aizawl”, 2021

[5]: Jayanthi. M, Rau. SS, “An Empirical Study on Financial Literacy and Spending Behavior of Rural Household in India”, 2017

[6]: Dr. Jyoti Pohane, “A Study Of Spending & Saving Habits Among The College Students In Dombivli Region”,

 ISSN 2394 - 7780

TRANSFORMATIVE IMPACT OF CLOUD COMPUTING ON HUMAN HEALTH CARE

Manisha Divate and Aaswat Vishwakarma
Usha Pravin Gandhi College of Arts, Science and Commerce

ABSTRACT

In the Healthcare Industry cloud computing is being adopted and integrated into their systems by analysing its transformative effects, opportunities and challenges and its future in the healthcare sector. This shows how traditional hospitals used to store data in their drives and how it has transitioned into digital data because of the cloud. Because it has improved scalability, collaboration and cost-effectiveness, in this, we delve into cloud computing influences in the healthcare sector.

It shows its potential in telemedicine and private healthcare and the potential security risks and data privacy concerns. Regardless of concerns, cloud computing in the healthcare sector plays an important part in improving the state of healthcare and making critical decisions for the patient's treatment.

Keywords: Cloud Computing, Healthcare, Health, Security, Challenges, Services.

1. INTRODUCTION

Indian hospitals including Tata Memorial, Kokilaben Dhirubhai Ambani, and AIIMS used outdated data storage methods before online computing became common. These platforms involved using servers on- premises and had limits concerning accessibility and scalability. Infrastructure limitations have limited the accessibility of services related to telemedicine. The Local methods were the only means to guarantee data security, and protecting it costs a lot of money. Following these organizations have transition to cloud- based storage, which improved scalability, made telemedicine collaboration easy, implemented advanced security features, and significantly reduced infrastructure costs. This completely changed the way healthcare operated, improving the treatment of patients, making data more accessible, and promoting technological innovation.

Cloud computing means the usage of cloud-based resources such as storage of data, networking, databases, servers, and computer programs over an internet connection. All the information is kept on server hardware maintained by a company that provides cloud services. In the case of cloud computing, the capabilities of computers, including the storage of data and the ability to compute, can be provided in demand while avoiding supervision by the individual who uses them. Infrastructure as a service, also known as (IaaS), platform as a service (PaaS), and software as a service (SaaS). comprise some of the services it provides. Infrastructure as a Service offers virtual resources like storage space and systems, whereas users may share resources and expand their computer system capability according to their requirements with IaaS.

A few of the major IaaS suppliers include Juniper Networks, IBM, VMware, and Amazon, for example. PaaS supports program creation and execution, and PaaS supports web user interface scaling, database integration, teamwork, and subscription and payment management for applications produced. Google, IBM, and Oracle are a few PaaS vendors. and SaaS provides software programs via subscriptions. SaaS is appropriate for a variety of applications, including Oracle, SAP, Salesforce and salesforce.com, and provides integration across disparate software components. SaaS suppliers include companies like IBM, Salesforce, and Google. [31].

Public, private, hybrid, and community clouds are all types of cloud setups. Public clouds are accessible to all consumers, whereas private clouds provide a unique architecture for one organization, hybrid clouds combine public and private capabilities, and community clouds fulfil the requirements of several organizations.

Understanding these models could assist companies in adjusting their cloud-based approach depending on their own functioning, security, and sustainability needs.

2. SYSTEMATIC REVIEW:

. To broaden the scope of our studied literature, methodology, and review articles, we began to recognize some of the most often-used substitute words/concepts and counterparts in the study and review papers.

Cloud Computing, cloud, Healthcare, Health, Cloud- Security, Challenges, Services, Techniques, security, (eHealth OR "electronic health")

We first searched for different research papers and review papers and in the end, we got 40 articles, websites research papers and review papers. To focus on the most relevant literature, methodology applications, and challenges We did a primary review by reading the introductions of each selected publication. The assessment is founded on the standards outlined in Table 1.

Table 1: Required category

Required category
• Linking eHealth with cloud technologies, either explicitly or implicitly.
• Establish cloud-based eHealth platforms.
• Cloud-based computing methods in healthcare.
• Ensuring medical confidentiality and safety of information in the cloud.
Challenges faced by the healthcare sector.
The Future trends in the healthcare sector.
Different techniques in the cloud.

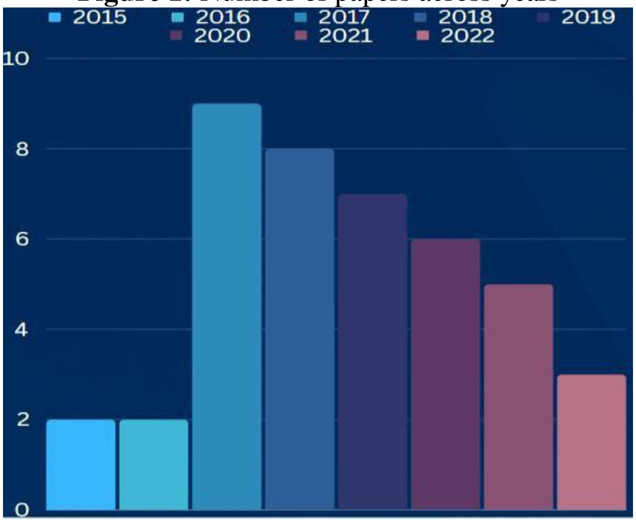
RESULTS

After the steps of searching many different articles, research papers, review papers, and websites, 40 papers and articles were finally selected from the Internet.

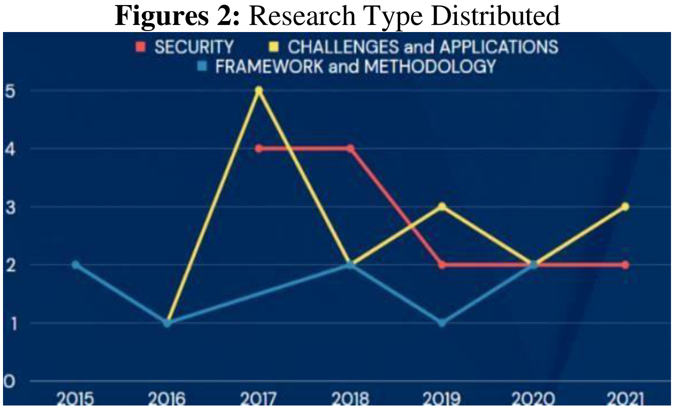
We believe that the selected 40 papers are the perfect view of computing in the healthcare sector and e-health. Both e-health and cloud computing in the healthcare sector are rising exponentially.

Figures 1 and 2 show the research, review papers used in the research, the years they were published, and the category of papers.

Figure 1: Number of papers across years



Figures 2: Research Type Distributed



3. LITERATURE-REVIEW

The use of cloud computing in healthcare systems has received considerable interest due to its ability to change the field. Mohit et al. (2017) researched the use of cloudlet technology in complementing healthcare services using mobile cloud computing. The study aims to improve healthcare app efficiency and accessibility by exploiting cloudlet proximity and resources, highlighting the potential of cloudlets in overcoming mobile device processing restrictions [10]. Another critical element discussed in the literature is the shift to services that are cloud-based in healthcare. A thorough analysis by several writers stressed variables critical for effective adoption. This encompassed safety, capacity, pricing, integration, and regulatory compliance, giving organizations insights into how to leverage cloud advantages while limiting concerns [2]. The influence of cloud technology on the efficiency and accessibility of healthcare has been a focus. Cloud computing has many advantages as it can give online data storage capability, information can be shared by interchange among healthcare providers using the data storage, and enhanced patient access to health records, according to research. Furthermore, it addressed security and privacy concerns, emphasizing the importance of strong security measures in cloud [3]. The vast potential of cloud computing in healthcare services has received much attention. Studies have looked into its ability to increase efficiency and sustainability, as well as the hazards linked with it. Various applications, such as telemedicine, data analysis, and tailored healthcare, were investigated, demonstrating the technology's significant impact on the sector [4,40]. Furthermore, the significance of fog computing in Healthcare 4.0 has been examined for its potential to increase productivity and reduce delays. The research emphasized its capacity to provide fast data analysis, secure communication, and improved resource use, resulting in improved patient care and operational flexibility [5]. The integration of cloud-based computer technologies (such as online data storage servers, 24/7 accessible storage, and real-time data regarding certain medical information and the history of patients) because of cloud usage inside healthcare organizations has been praised for its potential to transform patient care. The connection sought to improve data accessibility, real- time patient tracking, and the ability to make quick decisions and provide personalized treatment. In this integration, the study identified both possibilities and obstacles [6]. The integration of IoT and cloud computing in healthcare has also been investigated for its transformational potential. The study clarified their function in patient monitoring and resource management, as well as privacy and scalability problems, providing insights into prospective improvements and obstacles [7]. Furthermore, the disruptive influence of cloud computing on IT systems and service delivery paradigms was examined, with a focus on its capacity, mobility, and cost-effectiveness in enhancing operations. [8]. The research has discussed the potential hazards which are associated with the adoption of cloud computing in the healthcare sector it highlights the vulnerabilities to security attacks, access control, and identity identification There are also risks such as malware attacks, data corruption, data loss, and unauthorized access [9].

Mohit et al. (2017) found a focus on secure methods of authentication powered by cloud healthcare systems. The report emphasized the need for strong authentication mechanisms in protecting patient information, as well as the need for particular safety precautions stored in the cloud healthcare administration [10].

In the summary of the literature review, the research paper by Alam "Cloud Computing and its Role in Information Technology" (2021) addresses the significance of cloud computing in several industries, including healthcare, and underlines its potential benefits and limitations in the article. The study also discusses the probable future of computing in the cloud's impact on healthcare enterprises. it also emphasizes the significance of online computing in streamlining procedures, reducing paperwork, and safeguarding patient data. The study does, however, highlight significant problems, such as the danger of data leaks and the necessity for cautious execution to achieve favourable results. [8].

4. METHODOLOGY

Srivastava and Khan's 2018 review on cloud computing probably employed a sophisticated analytical approach. It likely encompassed comprehensive literature analysis, meta-analyses, experiments, simulations, surveys, classification methodologies, and intricate survey techniques. To substantiate their findings, the researchers might have utilized both quantitative and qualitative studies. The study has emphasized resource allocation strategies, scheduling approaches, load management techniques, and admission control methods within the domain of cloud computing. These methodological facets likely ensured a meticulous, rigorous, and comprehensive exploration of contemporary research and developments in cloud computing. [11]. In "Using Cloud Computing Services in the E-learning Process Has Its Benefits and Challenges," The researchers have reviewed the existing literature to give a comprehensive assessment of the advantages and disadvantages of employing cloud-based technology in e-learning. Their method included examining multiple academic papers to define the existing environment and the impact of the cloud on online education. The researcher tackled the basic principles of online education and the use of cloud computing technology while addressing the benefits and drawbacks of their combination. Furthermore, the researchers investigated cloud-centric e-learning products and discussed common concerns found while installing online e-learning systems, providing effective solutions for these obstacles.[12]. "Safety and safeguards difficulties with e-health services methods" by Sadoughi et al. (2019) investigated and defined significant safety and privacy difficulties related to e-health solutions in the context of cloud computing through a comprehensive study of the literature and quantitative synthesis approaches. Some of the techniques and methods used in this paper are:

1. **cryptographic security**: Public Key Encryption (PKE) and Symmetric Key Encryption, (SKE) Broadcast Encryption Programs, Qualified Encryption, Block Chain-Based Encryption, Searchable Symmetric Encryption,
2. **Access control Manager(ACM),**
3. **Identity-Based Encryption**

[13]. Jin and Chen (2015) used a variety of approaches to evaluate the opportunities and difficulties of telemedicine in the cloud. Their methodology involved analysing documents and a review of many telemedicine and cloud-based computing papers and research they have used methods such as Picture Archiving and communication systems, Telemonitoring biosignal processers, and Multimedia medical consultations in these papers but there are also challenges for telemedicine in cloud computing which are data interoperability, privacy and authentication, system security regulatory issues [14]. a thorough examination of cloud computing-related data security issues and their resolutions. There are various methods and techniques by the author in the papers which has been discussed to ensure data security in cloud computing. These include Identity and Access Management (IAM), Encryption, Virtual Private Networks (VPNs), Compliance and risk management, User activity monitoring, Regular audits and policy establishment, Ongoing training for staff to combat emerging threats, Backing up data, Implementing access management controls at the file and field levels, Identifying storage locations for structured and unstructured data and Implementing encryption for data in transit and data at rest.

This paper's methodology evaluation illustrates a thorough and methodical approach to examining cloud computing data security resolutions in cloud computing. [15].

Data security is a significant responsibility of both healthcare providers and patients. Organizations may reduce the serious hazards associated with non-cloud data storage techniques by using a cloud-based approach by recognising and eliminating any current vulnerabilities, cloud computing systems can safeguard from possible risks. By complying with HIPAA guidelines, cloud techniques can further improve the security of data.

To critically analyse the application of big data analysis in healthcare, evaluate the current literature and highlight major concerns with the organization of data, data collecting, preserving data, processing of information, and data display. The researcher has used techniques to analyse the healthcare big data which includes Machine Learning: this is used in analysing big data in healthcare domains, Artificial Intelligence and Data mining which allows the large number of databases from thousands of patients and clients to identify correlations between datasets, and develop models for the medical sector, the researcher examining the possible applications of analytics for big data in the healthcare industry, including managing the health of a population, illness forecast and avoidance, and customized therapy. [16]. Cloud computing has improved data analysis, and machine learning enables healthcare professionals to look for discoveries and patterns in massive amounts of data. This enables improved disease outbreak modelling, personalized treatment and the identification of high-risk patients, ultimately leading to better prevention and treatment methods and outcomes. A quantitative technique is used in the study article to examine the variables influencing the Development of cloud computing services in healthcare. To assess the competency and willingness of departments dealing with IT with different hospitals to adopt cloud computing the research sends questionnaires to these departments. Multiple regression analysis is employed to ascertain the influence of technical, administrative, and environmental variables on the adoption of cloud computing. The research findings have significant importance for ICT managers and providers, and they may aid in developing strategies for the use of cloud- based computing within the healthcare industry.[17] The researcher of "Security Enhancement in Healthcare Cloud using Machine Learning" presents a novel approach that improves the safety of data in cloud settings by utilizing the use of machine learning techniques. The researchers have proposed a cloud framework which consists of two elements to deal with security problems they have used: CloudSec component which first encrypts all health data using HTTPS/SSL protocol to secure data transfer. this module uses a segmentation approach to keep medical images safe and secure. Once encrypted, CloudSec sends clients' data to an external cloud service provider to process them securely, this module is responsible for ensuring privacy and security for clients' data during the utilization of cloud resources. They have used a method that uses both classification and regression by using machine learning theory. this technique uses linear classifiers to evaluate data and identify patterns. it relies heavily on statistical learning theory developed to maximize predictive accuracy. Additionally, when incorporating machine learning technologies inside the healthcare industry, the search results highlight the crucial elements of data quality control, guaranteeing security and confidentiality of information, encouraging cooperation, and ongoing improvement. [18]. The researchers highlight a proposed strategy targeted at giving predictions as well as

ISSN 2394 - 7780

knowledge to hospital administration to get around organizational hurdles during the adoption of big data technologies. Furthermore, the study investigates the possibility of Using vast volumes of data to efficiently solve healthcare problems, such as optimizing treatment paths and improving healthcare systems. The study's findings show that widespread data acceptance, implementation, and usage in healthcare settings might provide considerable advantages and possibilities. [19]. The research suggests a system that utilizes the cloud for handling healthcare data, using biometric identification to ensure safety. The research's approach involves an investigation of a hospital in an underdeveloped nation to guide the creation of the BAMHealthCloud structure, the installation of a fingerprint-based authorization operator for safe data entry and administration, and distributed instruction via the use of the Hadoop MapReduce structure for quicker medical information handling. They have proposed methods such as authentication access to ensure that the legit personnel can access the data stored in a healthcare cloud server, the researcher has proposed 2 methods which are Phase 1 and Phase 2, Phase 1 consists of the staff and the patients in the health care centre and then are asked to enrol themselves by giving their signature samples using either the signature device or their smartphones that are installed with the signature gathering software. Once a user’s signature has been taken, the quality of the given signature is checked using SigQuality checker software. The function of this software is to ensure that the recorded signature samples match up to the quality standards required for authentication. Phase 2 consists of the authentication phase which uses an algorithm that takes the user's signature scans it and stores it in the cloud which then can be used to check the authentication of the personnel if they try to access the database and then they are only allowed to use the database if they are given the authentication of it. After these personnel can access the information from the cloud [20]. The researchers used a thematic approach to see the opportunities and benefits of telemedicine in the healthcare sector by having cloud-computing integration, they also showed the techniques used in the study which are IAAS, PAAS, and SAAS [38,39] by using techniques like biometric authentication in distributed data storage systems it provided safe access to the medical personals and hospitals and it ensures the safety of data [39]

The paper "BAMHealthCloud: A Biometric Authentication and Data Management System for Healthcare Data in the Cloud" by Shakil, K. A., Zareen,

F. J., Alam, M., and Jabin, S. (2020) introduces a creative approach to addressing the problems associated with medical safety and information administration. The paper's suggested BAMHealthCloud system uses biometric authorization and data storage in the cloud to offer safe access, retrieval, and manipulation of healthcare information. Particularly, the use of distributed learning using the Apache Hadoop MapReduce architecture indicates a smart technological approach that improves the effectiveness of the system.

These approaches show great potential for medical technology because they efficiently handle crucial safety and information management problems in an era of rising digitalization and data transmission within healthcare [20].

5. DISCUSSION AND RESULT:

The healthcare industry has undergone a substantial transition, owing primarily to the introduction and integration of Cloud technology, massive data statistical analysis, machine learning, and advanced technical solutions. Multiple research investigations have highlighted these technologies' enormous potential and different uses in healthcare settings. Mohit et al. (2017) examined the use of cloudlet technologies for boosting medical services. using mobile cloud computing, to improve healthcare app efficiency and accessibility. Furthermore, the move to cloud-based services in healthcare has been highlighted in the literature, emphasizing essential elements for effective adoption such as safety, capacity, cost, and integration.

The importance of cloud computing on healthcare efficiency and accessibility has been highlighted, with cloud computing boosting data storage, information interchange across providers, and increased patient access to health records.

Furthermore, a considerable lot of research has been undertaken on the potential advantages of cloud-based computing in enhancing healthcare performance and sustainable development, as well as its uses in telemedicine, which is an analysis of data, and personalized medical care, indicating major implications on the industry. Fog computing has also received interest in Healthcare 4.0 because of its ability to increase productivity, minimize delays, provide quick data analysis, secure communication, and optimize resource usage, ultimately improving the treatment of patients and flexibility in operations. A cloud-based integration of technology in medical organizations has been recognized for its ability to change the way patients are treated by enhancing access to information, real- time patient monitoring, allowing rapid decision-making processes, and individualized therapy.

 ISSN 2394 - 7780

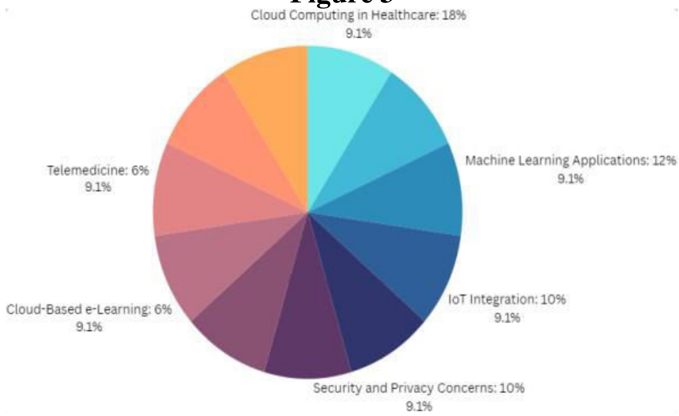
Similarly, the merging of the Internet of Things (IoT) and the use of cloud computing in healthcare. has been investigated for its potential for change in tracking patients and management of resources, emphasizing privacy and scalability difficulties while giving insights into future advances and challenges.

Healthcare cloud computing security issues have been completely researched, discovering weaknesses and possible dangers and providing crucial insights into building effective solutions to secure information about patients within cloud-based systems. Furthermore, the emphasis has been placed on secure authentication techniques supported by cloud healthcare providers to preserve patient information and increase safety precautions kept in cloud healthcare management. the factors that are driving cloud computing uptake in healthcare institutions were investigated using quantitative approaches, yielding relevant insights for ICT managers who are defining cloud-based computing policies in the medical business.

Innovative approaches for improving data security in cloud settings have been created, highlighting the method's promise in complex data processing, sickness diagnosis, imaging, medication development, and medical records administration.

Furthermore, the proposed solutions seek to provide forecasts and insights to overcome organizational hurdles during the big data adoption process in healthcare, emphasizing the potential for universal data acceptance, and implementation

Figure 3



this paper explores the transformative potential of extensive data in revolutionizing healthcare, improving patient treatment, elevating outcomes, and reducing expenses. This highlights the significance of regulations and the integration of statistical technology in scientific studies, underscoring both the challenges and opportunities linked with utilizing vast data volumes in medical contexts. These encompass concerns like information protection, security, data accuracy, and connectivity. Additionally, the study delves into potential uses of large-scale data analytics within the healthcare sector. [21] digs into the most recent research results on cloud safety and data protection, offering a complete security and confidentiality structure for identifying potential risks. The researcher analyses the effect of data breaches and illegal access on cloud computing utilization, highlighting the importance of enhanced security measures. Recognizing and overcoming these obstacles is critical for preserving the security of confidential data and retaining customer confidence as computing increases in popularity [22].

By evaluating the challenges and opportunities related to the use of enormous volumes of data for medical reasons, such as data security and confidentiality. This review additionally examined how analytical techniques for big data may be applied in healthcare, such as targeted therapy, sickness predictions, and population health management. Big data analytics may improve decision- making, patient outcomes, and cost reductions in the healthcare business, which generates a significant volume of complex data from many sources. The incorporation of massive amounts of data into healthcare is seen as vital, and it has already shown effects in areas such as personalized therapy, resource efficiency, and quick outcomes. [23].

The research paper introduces BAMHealthCloud, a cloud-based system for safe electronic healthcare storage and access to information utilizing biometric identification. The system's operational characteristics, such as speedup, mistake percentage, sensitivity, and accuracy, show that it is capable of safely handling healthcare data in the cloud. The study underlines the need for safe data access and recovery for essential medical information security, as well as the applicability of a biometric-based identification system for addressing security difficulties. The proposed paradigm is provided as a response to the security issues that have been raised about cloud-based healthcare systems. [24].

ISSN 2394 - 7780

The researcher investigates the pros and downsides of using cloud-based computing for large-scale data processing. Apart from addressing concerns regarding data security, regulations, and transfer expenses, the paper underscores the advantages of adaptability, cost- efficiency, and ease of adoption. While experts suggest that the benefits outweigh the drawbacks of utilizing cloud-based analytics for vast datasets, they emphasize the importance for businesses to thoroughly evaluate their choices before embracing cloud-based solutions. [25].

The researchers thoroughly investigate the safety and confidentiality problems that arise from the deployment of cloud-based computing in the medical sector. Following an in-depth analysis of existing research, the authors identify various security concerns, encompassing issues related to privacy, availability, confidentiality, and integrity. The article stresses the importance of adopting a comprehensive approach that effectively balances these conflicting requirements. It concludes that apprehensions about security, confidentiality, efficiency, and adaptability prevent extensive use of cloud computing in the medical sector area. The study highlights the security implications associated with cloud computing in eHealth and underscores the need for further research in this domain. [26].

Leveraging cutting-edge cloud-based technologies, the researchers explore challenges and solutions regarding security and confidentiality in e-health applications.

They identify numerous significant hurdles to address, encompassing the safeguarding of privacy, confidentiality, data integrity, and accessibility.

Additionally, they propose a fresh framework aimed at enhancing security and privacy preservation withine-health solutions. Moreover, the article delves into potential security strategies applicable to safeguarding patient information in cloud-based healthcare systems, including authentication, authorization, and multi-cloud security measures. [27].

The study paper thoroughly examines security and confidentiality problems with the vast volume of information collected in the healthcare sector. It talks about the possible advantages and difficulties of using big data analysis in population health management, illness prediction, and customized therapy, among other areas of healthcare. It also emphasizes how critical it is to put in place a thorough plan that successfully strikes a balance between security, secrecy, and efficiency. [21]

The article addresses, in summary:

1. A detailed discussion of the privacy and security problems around massive amounts of data in medical care.
2. A review of the potential benefits and challenges of analytics for large amounts of data in the field of healthcare.
3. A focus on the need to implement a methodical approach that strikes a balance between secrecy, security, and speed. [21]

 ISSN 2394 - 7780

Table 2

Paper Title	Summary
eHealth Cloud Security Challenges: A Survey	The paper discusses the security, privacy, efficiency, and scalability concerns hindering the wide adoption of cloud technology in healthcare.
BAMHealthCloud: A Biometric Authentication and Data Management System for Healthcare Data in Cloud	The paper proposes BAMHealthCloud, a cloud-based system for managing healthcare data, ensuring security through biometric authentication. The system's operational characteristics show that it is capable of safely handling healthcare data in the cloud.
A Review of the Role and Challenges of Big Data in Healthcare Informatics and Analytics	The paper explores the transformative potential of extensive data in revolutionizing healthcare, improving patient treatment, elevating outcomes, and reducing expenses. It highlights the significance of regulations and the integration of statistical technology in scientific studies, underscoring both the challenges and opportunities linked with utilizing vast data volumes in medical contexts.
Security challenges and solutions using healthcare cloud computing	The paper delves into the security and privacy challenges arising from the implementation of cloud computing within the healthcare industry. The authors identify various security concerns, encompassing issues related to privacy, availability, confidentiality, and integrity.
BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud	The paper introduces BAMHealthCloud, a cloud-based system for safe electronic healthcare storage and access to information utilizing biometric identification. The system's operational characteristics show that it is capable of safely handling healthcare data in the cloud.
Advantages and Disadvantages of Cloud-Based Computing for Big Data Analytics	The paper explores the advantages and disadvantages of employing cloud-based computing for extensive data analysis. It underscores the advantages of adaptability, cost-efficiency, and ease of adoption.
Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing	The paper explores the challenges and solutions related to security and privacy in e-health solutions using cloud computing technology. The authors propose a new framework for security and privacy-preserving in e-health solutions.

6. CHALLENGES:

The researchers investigated the usage of cloud computing in medical facilities, as well as the numerous concerns about privacy and security that develop as a result. The study emphasizes the centralized management of personal information on the cloud, which creates several security and privacy risks for people. The authors recognized various security problems, including attack susceptibility, integrity, accessibility, security, and privacy. This research also covers the present state of the science to comprehend several cloud computing strategies utilized in healthcare organizations, as well as the security problems preventing doctors and hospitals from widely adopting cloud computing [32]. The researchers noted many safety concerns with cloud healthcare systems, such as privacy, accessibility, integrity, trustworthiness, and security for multi-cloud computing. Additionally, the study offers fresh approaches to the security problems associated with cloud computing implementation in the healthcare industry [33]. The article highlights the need for security and secrecy for healthcare IoT, which is a crucial component using the usage of cloud-based computing in the healthcare sector. The researchers identified several confidentiality and security problems, including data protection, dependability, availability, and privacy. Furthermore, the paper proposes novel solutions to the concerns regarding safety and confidential data in healthcare [34]. It is important to show security and privacy concerns of data, infrastructure issues and their limitations, adoption challenges and network reliability

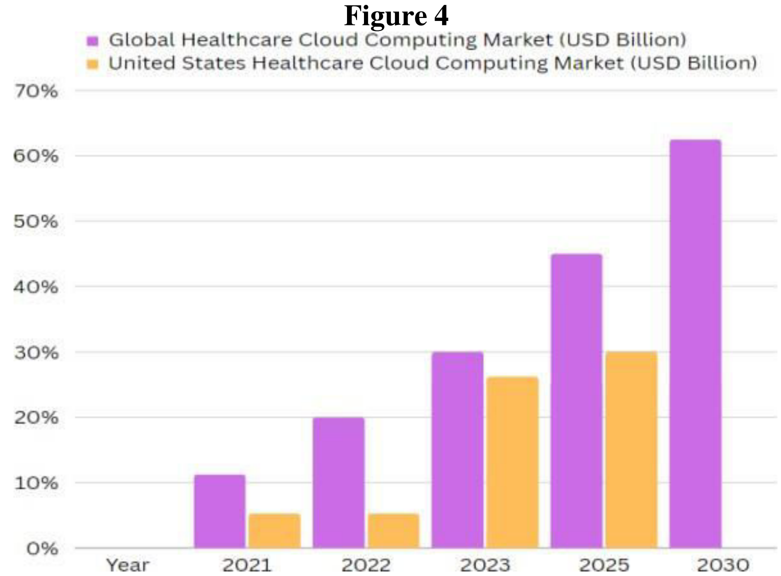
[35] [36]. There are also challenges in the transformative role of cloud technology enabling remote access to medical data and resources and there is a need for security and privacy measures with existing systems and the development of advanced systems to deal with these potential problems [37].

7. FUTURE TRENDS:

With a compounded annual growth rate (CAGR) of 21.4% from 2022 to 2030, the worldwide healthcare cloud computing market, valued at USD 11.27 billion in 2021, is expected to be worth USD 62.47 billion by 2030[28]. The medical device and cloud computing sector in the United States is anticipated to expand at a compound annual growth rate (CAGR) of 22.1 per cent between 2022 and 2030, rising from USD 5.29 billion in 2022 to USD 26.2 billion by 2032[29]. According to HIMSS's Analytics Survey, more than 83 per cent of healthcare organizations already use cloud-based services. Many healthcare organizations want to use cutting-edge technology to advance these cloud computing solutions even further [29].

According to Data Bridge Industry Study analysis, the healthcare information technology cloud computing industry, which was estimated at USD 35.61 billion of dollars in the year 2022, is expected to continue to expand at an average yearly rate of 17.2% to reach USD 127.04 billion of dollars by the year 2030. [30]

Figure 4



CONCLUSION

Integrating cloud computing has changed the accessibility of data, enhancing patients' health and providing advanced innovations in the healthcare sector. And also offers multiple advantages, challenges and opportunities such as privacy of data, security, and helping in the advancement. Cloud computing has addressed many challenges and issues but leveraging cloud computing techniques can lead to more advanced patient outcomes as well as in telemedicine, streamlined operations and using bio authentication to safeguard privacy and security concerns and it has exponential growth in the coming future.

ACKNOWLEDGEMENT

I am grateful to my teacher for providing me with the opportunity to work on the "Transformative Impact of Cloud Computing on Human Health Care" project. This paper allowed me to conduct extensive research and learn new skills.

REFERENCES

[1] Lo'ai, A. T., Bakhader, W., Mehmood, R., & Song, H. (2016, December). Cloudlet-based mobile cloud computing for healthcare applications. In 2016 IEEE Global Communications Conference (GLOBECOM) (pp. 1-6). IEEE.

[2] Branco Jr, T., De Sá-Soares, F., & Rivero, A. L. (2017). Key issues for the successful adoption of cloud computing. Procedia Computer Science, 121,115-122. [3]Devadass, L., Sekaran, S. S., & Thinakaran, R.(2017). Cloud computing in healthcare.International Journal of Students' Research in Technology & Management, 5(1), 25-31.

[4] Ali, O., Shrestha, A., Soar, J. and Wamba,S.F., 2018. Cloud computing-enabled healthcare opportunities, issues, and applications: A systematic review. International Journal of Information Management, 43, pp.146-158.

5]Kumari, A., Tanwar, S., Tyagi, S., & Kumar, N. (2018). Fog computing for healthcare 4.0 environment: Opportunities and challenges. Computers & Electrical Engineering, 72, 1-13. [6]Darwish, A., Hassanien, A. E., Elhoseny, M., Sangaiah, A. K., &

Muhammad, K. (2019). The impact of the hybrid platform of the Internet of things and cloud computing on healthcare systems: opportunities, challenges, and open problems. Journal of Ambient Intelligence and Humanized Computing, 10(10), 4151-4166.

[7] . Dang, L.M., Piran, M., Han, D., Min, K. and Moon, H., 2019. A survey on the Internet of things and cloud computing for healthcare. Electronics, 8(7), p.768.

[8] Alam, T. (2021). Cloud Computing and its Role in Information Technology. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 1, 108-

115......................

[9]. Mehraeen, E., Ghazisaeedi, M., Farzi, J., & Mirshekari, S. (2017). Security challenges in healthcare cloud computing: systematic. Glob. J. Health Sci, 9(3).

[10] Mohit, P., Amin, R., Karati, A., Biswas, G. P., & Khan, M. K. (2017). A standard mutual authentication protocol for cloud computing-based health care systems. Journal of medical systems, 41(4), 50.

[11] Srivastava, P., & Khan, R. (2018). A review paper on cloud computing. International Journal of Advanced Research in Computer Science and Software Engineering, 8(6), 17-20.

[12] El Mhouti, A., Erradi, M., & Nasseh, A. (2018). Using cloud computing services in e-learning process: Benefits and challenges. Education and Information Technologies, 23(2), 893-909.

[13] Sadoughi, F., &Chenthara, S., Ahmed, K., Wang,

H. and Whittaker, F., 2019. Security and privacy- preserving challenges of e-health solutions in cloud computing. IEEE Access, 7, pp.74361- 7438...

[14] Jin, Z., & Chen, Y. (2015). Telemedicine in the cloud era: Prospects and challenges. IEEE Pervasive Computing, 14(1), 54-61.

[15] Zulifqar, I., Anayat, S., & Kharal, I. (2021). A Review of Data Security Challenges and their Solutions in Cloud Computing. International Journal of Information Engineering & Electronic Business, 13(3).

[16] Lv, Z., & Qiao, L. (2020). Analysis of healthcare big data. Future Generation Computer Systems, 109, 103-110.

[17] O. Harfoushi, A. H. Akhorshaideh, N. Aqqad,

M. Al Janini, and R. Obiedat, "Factors affecting the intention of adopting cloud computing in Jordanian hospitals," Communications and Network, vol. 8, p. 88, 2016.

[18]M. Marwan, A. Kartit, and H. Ouahmane, "Security Enhancement in Healthcare Cloud using Machine Learning," Procedia Computer Science, vol. 127, pp. 388-397, 2018.

[19]Chen, P. T., Lin, C. L., & Wu, W. N. (2020). Big

data management in healthcare: Adoption challenges and implications. International Journal of Information Management, 53, 102078. [20]Shakil, K. A., Zareen, F. J., Alam, M., & Jabin,

S. (2020). BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. Journal of King Saud University-Computer and Information Sciences, 32(1), 57-64.

[21] Abouelmehdi, K., Beni-Hssane, A., Khaloufi, H., & Saadi, M. (2017). Big data security and privacy in healthcare: A Review. Procedia Computer Science, 113, 73-80.

[22] Sun, P. (2020). Security and privacy protection in cloud computing: Discussions and challenges.

Journal of Network and Computer Applications, 160, 102642.

[23] Kraemer, F. A., Braten, A. E., Tamkittikhun, N., & Palma, D. (2017). Fog computing in healthcare–a review and discussion. IEEE Access, 5, 9206-9222.

[24]. Kruse, C. S., Smith, B., Vanderlinden, H., & Nealand, A. (2017). Security techniques for the electronic health records. Journal of Medical Systems, 41, 1-9.

[25]Balachandran, B. M., & Prasad, S. (2017). Challenges and benefits of deploying big data analytics in the cloud for business intelligence. Procedia Computer Science, 112, 1112-1122.

[26] Al-Issa, Y., Ottom, M. A., & Tamrawi, A. (2019). eHealth cloud security challenges: a survey. Journal of healthcare engineering, 2019.

[27]. Chenthara, S., Ahmed, K., Wang, H., & Whittaker, F. (2019). Security and privacy- preserving challenges of e-health solutions in cloud computing. IEEE access, 7, 74361-74382.Journal of Medical Systems, 41(4), 50. [28]https://www.marketresearchfuture.com/reports/ healthcare-cloud-computing-market-6519

[29] https://market.us/report/healthcare-cloud- computing-market/ [30]https://www.databridgemarketresearch.com/rep orts/global-healthcare-cloud-computing-market

[31] Mekawie, N., & Yehia, K. (2021). Challenges of deploying cloud computing in eHealth. Procedia Computer Science, 181, 1049-1057.

[32] Subramanian, N., & Jeyaraj, A. (2018). Recent security challenges in cloud computing. Computers & Electrical Engineering, 71, 28-42.

[33] Tabrizchi, H., & Kuchaki Rafsanjani, M. (2020). A survey on security challenges in cloud computing: issues, threats, and solutions. The journal of supercomputing, 76(12), 9493-9532.

[34] Sun, W., Cai, Z., Li, Y., Liu, F., Fang, S., &

Wang, G. (2018). Security and privacy in the medical internet of things: a review. Security and Communication Networks, 2018, 1-9.

[35] Singh, M., Gupta, P. K., & Srivastava, V. M. (2017, November). Key challenges in implementing cloud computing in Indian healthcare industry. In 2017 pattern recognition association of South Africa and robotics and mechatronics (PRASA-RobMech) (pp. 162-167). IEEE.

[36] Khan, M. A. (2021). Challenges facing the application of IoT in medicine and healthcare. International Journal of Computations, Information and Manufacturing (IJCIM), 1(1).

[37] Gleißner, M., Dotzler, J., Hartig, J., Aßmuth, A., Bulitta, C., & Hamm, S. (2021). IT security of cloud services and IoT devices in healthcare. CLOUD COMPUTING 2021, 10.

[38] Marcu, R., Popescu, D., & Danila, I. (2015). Healthcare integration based on cloud computing. UPB Sci. Bull, 77(2), 31-42.

[39] Altowaijri, S. M. (2020). An architecture to improve the security of cloud computing in the healthcare sector. Smart Infrastructure and Applications: Foundations for Smarter Cities and Societies, 249-266.

[40] Abrar, H., Hussain, S. J., Chaudhry, J., Saleem, K., Orgun, M. A., Al-Muhtadi, J., & Valli, C. (2018). Risk analysis of cloud sourcing in healthcare and public health industry. IEEE Access, 6, 19140- 19150.

ISSN 2394 - 7780

REVIEW AND COMPARISON OF ROBOTS FOR ELDERLY CARE

Manisha Divate[1] and Tanya Dhamija[2]
Usha Pravin Gandhi College of Arts, Science and Commerce

ABSTRACT
The worldwide demographic shift toward getting older populace has elevated the focal point on progressive answers to address the growing demanding situations of elderly care. The paper begins with the aid of inspecting the present- day nation of aged care, focusing on the increasing call for personalized and effective care solutions. similarly, the study discusses the potential blessings and ethical considerations associated with integrating robotics into aged care. It examines how these technologies make a contribution to enhancing health care, growing the independence of the aged, and lowering caregiver burden. The paper highlights the main challenges and barriers of the cutting-edge nation of aged robotics, identifies destiny prospects and regions for in addition studies along with technical boundaries, adoption troubles, and the significance of human-robot interaction, emphasizing the want for interdisciplinary collaboration to cope with complex demanding situations in this swiftly evolving discipline. In conclusion, this paper give an outline of the present state of robot care for the aged, providing an outline of capacity advantages, demanding situations, and moral issues contributes to the continuing discourse round the usage of technology to beautify the lives of seniors.

Keywords: elderly care needs, elderly care robots, care robot acceptance, healthcare robotics

I. INTRODUCTION

The panorama of elderly care is present process a profound transformation, pushed through the intersection of demographic shifts, technological advancements, and evolving societal desires. As the worldwide populace a while at an extraordinary tempo, conventional strategies to geriatric help are being challenged by means of the developing call for revolutionary answers that can decorate the great of lifestyles for seniors, guide unbiased dwelling, and alleviate the stress on caregivers and healthcare structures. At the leading edge of this paradigm shift lies the mixing of robotics—a field that holds significant promise for revolutionizing elderly care.[1]

The health enterprise (WHO) has evaluated an estimation that by 2050, the range of individuals aged 60 years and above will almost double, reaching billion worldwide. This demographic transition brings with it a number of demanding situations, inclusive of extended incidence of age-associated situations, more healthcare fees, and a shrinking team of workers to provide adequate care. In response, researchers, engineers, and healthcare professionals are turning to robotics as a transformative tool to address those complex demanding situations and bring in a brand-new generation of geriatric assistance.[2]

The capacity applications of robotics in aged care are substantial and multifaceted. From assistive devices that useful resource with activities of each day dwelling to state- of-the-art humanoid robots capable of imparting companionship and social interplay, the spectrum of robot solutions is expanding unexpectedly. These technological advancements provide real benefits to older adults and those who care for them, enabling seniors to maintain their independence, encouraging social interaction, and improving general well-being.[3]

However, there are challenges and ethical issues with integrating robotics into elder care. Concerns about autonomy, privacy, and the possible replacement of human caretakers highlight the need for cautious planning and ethical use of robot structures. Furthermore, there is a wide range of public sentiments regarding robotics, which are influenced by cultural standards, period assumptions, and concerns regarding job displacement.[4]

Notwithstanding these obstacles, advancements in artificial intelligence, sensor technology, and human and robot intercommunication are indulging in senior care robotics forward. Real-world worldwide applications of robotic structures in healthcare settings, ranging from private homes to nursing homes and rehabilitation centres, show the measurable advantages of that technology in terms of improving fitness outcomes, increasing caregiver productivity, and encouraging aging in place.[5]

As we set out on this path to a future in which robots are going to be needful to take care of elders, it is crucial to promote interdisciplinary collaboration, engage stakeholders in meaningful dialogue, and give the ethical and humanistic aspects of generation enhancement first priority. By way of harnessing the transformative ability of robotics with empathy, compassion, and a commitment to human dignity, we will build a destiny in which growing old is synonymous with vitality, independence, and success—a future in which aged care robotics serves as a beacon of innovation and inclusivity in our swiftly growing old world.[6]

II. BACKGROUND

Robots take care of the elderly is pushed by numerous factors which include international demographic changes, advances in robotics and synthetic intelligence (AI), and the growing want for progressive answers in addressing the challenges associated with the getting older population. elderly care robots externally are dynamic social, technological, and healthcare merchandise. As the sphere continues to evolve, it holds the promise of providing new solutions to guide the older populace and presents new challenges that require careful consideration and moral oversight.[7]

III. OBJECTIVES

This paper goals to contribute to the continued discourse at the intersection of technology and aged care by means of imparting insights into the contemporary country of robots for elderly care. As societies grapple with the results of an getting old populace, expertise the working and impact that robotics have in taking care of elders is an increasing number of important to form future guidelines, practices, and health care future. The research paper on elderly Care Robotics seeks to deal with the multifaceted studies of integrating robotic technology into aged care.

The main objective of this reviews the cutting-edge fame of senior care robotics from assistive technology to concomitant robotics, inspecting its impact on independence, social interaction and emotional well-being of older individuals. It also works on reviewing diverse robots which are available by way of comparing and analysing those robots. by means of evaluating, we can parent out the benefits, obstacles, implementation of every robotic. in addition to information the challenges, futuristic implementation and scope.

IV. BENEFITS OF ROBOTICS IN ELDERLY CARE

Assistance with daily responsibilities: Robots can assist aged people with numerous each day obligations, which incorporates getting far from bed, dressing, grooming, and getting geared up food. This useful resource can beautify independence and keep a enjoy of autonomy for older adults.

Social interaction: Social isolation is a common undertaking for the aged. Robots designed for companionship can have interaction in verbal exchange, play games, or maybe provide reminders for medication, fostering social interaction and reducing feelings of loneliness.[8]

Cognitive Stimulation: Robots may be programmed to provide cognitive stimulation through video games, puzzles, and academic sports. this could assist keep mental acuity and doubtlessly do away with cognitive decline in elderly individuals.

Monitoring fitness Parameters: Robotics geared up with sensors can reveal vital signs and symptoms and signs and symptoms, come across falls, and check commonplace fitness conditions. This actual-time information can be transmitted to healthcare professionals or own family individuals, permitting timely interventions and improving the overall fitness control of the elderly.

Treatment management: Robots can assist in remedy manipulate by way of meting out remedy at scheduled times, offering reminders, or even monitoring medication adherence. this may assist prevent ignored doses and make certain proper remedy compliance.[9]

Mobility help: robot gadgets together with exoskeletons or robotic exosuits can aid in mobility for aged individuals with mobility traumatic conditions. those gadgets can provide bodily help, assisting seniors hold or regain their potential to transport independently.

24/7 Availability: in contrast to human caregivers who have constrained strolling hours, robots can offer assist and assist 24/7, ensuring non-forestall monitoring and take care of aged humans.[10]

Fall Prevention: Robots geared up with sensors and cameras can stumble on falls or modifications in motion patterns, permitting for fast alerts and help. this could significantly lessen the threat of injuries as a consequence of falls.[11]

Charge-effective solutions: on the identical time as the initial investment in robotics era may be substantial, in the end, it is able to be a rate-effective answer as compared to hiring complete-time human caregivers. That is especially relevant in areas handling a minimal healthcare expert.

Comfort for Caregivers: robot help can alleviate a number of the issues on human caretakers, allowing them to work on greater complicated as well as emotional additives of are at the same time as the robot’s cope with habitual obligations.[12]

V. LITERATURE REVIEW: ROBOTS FOR ELDERLY CARE USAGE

In this research paper, we 16 various types of robots on basics of their platforms which are currently available. The type of robots are as follows:

PEPPER – Pepper is a humanoid robotic designed to engage with people through communication and gestures, developed via SoftBank Robotics.[13-20]

[43]

CARE-O-BOT – Care-O-bot robot, considered as a multiskilled robot designed to help with diverse duties in home and healthcare settings.[21]

[44]

LIO – Lio robotic is a sophisticated robot gadget designed for flexible obligations with superior sensory abilities and independent operation.[22]

[45]

HOBBIT – The HOBBIT robotic is an autonomous system designed for underwater exploration and environmental monitoring.[23]

[46]

RAMCIP – RAMCIP, a humanoid robots designed to help in emergency conditions and healthcare responsibilities, integrating advanced perception, cognition, and movement capabilities.[24]

[47]

ROBEAR – Robear is a humanoid robotic designed for assisting aged or disabled people with obligations in healthcare settings.[25]

[48]

VEEBOT – Veebot is a robotic device designed for automating venipuncture tactics, integrating robotics and laptop vision to improve blood drawing performance and accuracy.[26]

[49]

DEKONBOT – DeKonBot is a multifunctional robot designed for various obligations inclusive of cleaning, surveillance, and assistance, prepared with superior AI and sensor technologies.[27]

ISSN 2394 - 7780

[50]

JACO – JACO is a robot arm designed via Kinova Robotics for assistive and studies purposes, offering a couple of degrees of freedom and superior manage talents.[28-33]

[51]

BAXTER – The BAXTER robotic assists in aged care by providing companionship and acting responsibilities to assist daily residing sports.[34]

[52]

BURT – The BURT robotic is deployed in elderly care, providing companionship and assistance through advanced AI competencies, improving the well-being and protection of seniors in their every day lives.[35]

[53]

REWALK – The REWALK exoskeleton robot assists elderly people with mobility impairments with the aid of providing powered hip and knee motion, improving their capability to walk independently and enhancing their typical nice of lifestyles.[36-37]

ISSN 2394 - 7780

[54]

LOKOMAT – The LOKOMAT robot assists elderly people in rehabilitation via supplying tailored guide and guidance for strolling sporting events, promoting mobility and independence with its robotic assistance era. Its adjustable settings accommodate various ranges of assistance, making it suitable for a wide range of aged customers in care settings.[38]

55

UFES SMART WALKER – UFES smart Walker, a robot tool designed to assist elderly people with mobility issues, integrating sensors and AI algorithms to offer customized aid and monitoring, promoting independence and safety in day by day sports.[39]

[56]

WALBOT – The WALBOT robot provides personalized strolling assistance to aged people, improving mobility and lowering fall dangers, hence selling unbiased residing and first-class care for seniors. Its superior sensors and AI algorithms allow real-time tracking and adaptive aid tailored to the person's wishes, fostering self-assurance and safety for the duration of everyday activities.[40]

[57]

iWALK – The iWALK robot affords revolutionary walking assistance for the elderly, using advanced sensors and algorithms to decorate mobility and independence whilst making sure protection and support. Its ergonomic layout and adaptable functions make it a precious tool for senior care, encouraging energetic dwelling and lowering the threat of falls.[41-42]

[58]

VI. COMPARATIVE ANALYSIS

Robots Considered	Platform Status and Category	Technology Based Classification	Applications Performed	Drawback
Pepper [13-20]	Commercial Product & Care/Hospital	Humanoid robot with social interaction capabilities, including natural language processing and emotional recognition.(AI, IOT)	Providing information about medical, intellectual and physical education, human activities and health care monitoring.	limited bodily help talents.
Care-O-Bot [21]	Research & Care	Carrier robotic with capabilities for navigation, item manipulation, and assistance in day-by-day tasks. in all likelihood makes use of sensors for environment perception.(AI, IOT)	Collection and Distribution, Providing Drinking Services,	excessive price and complexity in upkeep.
Lio [22]	Commercial Product & Care	Probably a robot designed for assistance obligations, doubtlessly with mobility functions and sensors for navigation and interplay.(AI, IOT)	Collection and distribution, Entertainment and support, Automatically Enter the Room and provide information about Important activities.	restricted mobility and agility in navigating environments.
Hobbit [23]	Research & Care	This can talk over with the Hobbit mission, which involves growing robot generation for aged care, possibly incorporating diverse sensing, navigation, and help talents.(AI, IOT)	Collection and Distribution, Identifying Unstable user	loss of adaptability to numerous tasks and environments
RAMCIP [24]	Research & Care	Robot Assistant for MCI sufferers at domestic, incorporating various assistive technologies which include manipulation, navigation, and human- robotic interaction.(AI, IOT)	Collection and Distribution, Identifying emergenies	demanding situations in natural interplay and communication with elderly customers

ROBEAR [25]	Experimental & Hospital	Designed for lifting and assisting aged individuals, possibly includes energy augmentation and protection features.(AI, IOT)	Patient Lifting	cumbersome design and capacity intimidation component for some aged individuals.
Veebot [26]	Research & Hospital	A robot designed for healthcare tasks, doubtlessly which includes monitoring, help, or even clinical techniques. possibly consists of vision and sensing technologies.(AI, IOT)	Drawing Blood, Inserting IV	Reliance on precise calibration and technical infrastructure.
DeKonBot [27]	Research & Hospital	Doubtlessly designed for disinfection responsibilities, incorporating autonomy and probable UV-C disinfection technologies.(AI, IOT)	Disinfection	limited autonomy in selection-making and trouble-solving.
Jaco [28-33]	Commercial Product **&** Assistive	A robotic arm designed to assist with numerous tasks, which includes those relevant to elderly care, consisting of manipulation and assistance.(AI, IOT)	Manipulation obligations, consuming/eating assistance	restricted energy and dexterity for positive caregiving obligations.
Baxter [34]	Commercial Product **& Assistive**	A collaborative robot with manipulation competencies, potentially used for responsibilities requiring dexterity and human-robotic interplay.(AI, IOT)	Dressing	exceedingly sluggish operational pace for time-touchy obligations.
Burt [35]	Commercial Product & Rehabilitation	The unique competencies of "Burt" aren't clear; however it could be designed for assistance, tracking, or social interaction.(AI, IOT)	recreation-based totally upper Limb Rehabilitation	ability discomfort or worry brought on via its appearance
ReWalk [36-37]	Commercial Product & Rehabilitation	An exoskeleton designed to assist people with mobility impairments, probably permitting aged individuals to stroll.(IOT)	Gait Rehabilitation	confined functionality outdoor of based environments.
Lokomat [38]	Commercial Product & Rehabilitation	A robot gait orthosis used in rehabilitation settings, potentially for aged individuals with mobility impairments.(IOT)	Gait Rehabilitation	constrained accessibility for people with various mobility wishes.
UFES smart walker [39]	Research & Frame-based Walking Assistance	A clever walker incorporating generation for navigation, stability assistance, and probably fall detection or prevention.(IOT)	strolling assistance Gait Parameter Estimation	Dependence on technological infrastructure and protection.
Walbot [40]	Research & Frame-based Walking Assistance	The particular abilities of "Walbot" aren't clean, but it can be designed for assistance, monitoring, or navigation in aged care settings.(AI, IOT)	strolling assistance on foot on a Slope, obstacle Detection and Avoidance	loss of emotional intelligence and empathy in caregiving interactions.
iWalk [41-42]	Research & Frame-based Walking Assistance	could check with various technologies related to mobility assistance, probably which includes exoskeletons or clever prosthetics.(IOT)	taking walks-frame primarily based on foot Assistants, patient monitoring Human balance Estimation Mobility assessment exercise tracking and Gesture recognition	limited adaptability to various terrains and environments.

VII. CHALLENGES AND OPPORTUNITIES

The responsibilities moreover looked at problems with remote manipulate and navigation in static or dynamic environments. using reference designs for social robots to utilize standardized software program (or hardware) additives for some of robots, which may also promote interoperability amongst them, grow to be one of the research initiatives' demanding conditions and possibilities.

The ageing population is rapidly increasing, leading to a growing demand for care offerings. however, there is a scarcity of educated caregivers to satisfy this name for, mainly in rural areas. additionally, cultural norms often familial contend with the elderly, which can also moreover prevent the vast popularity of robot help. challenges also include the affordability and accessibility of robotic generation for the majority of the population, similarly to worries about privateness and protection.[59]

On the other hand, are the opportunities for aged care robotics to address those challenges. Robots can assist with every day responsibilities which incorporates medicinal drug reminders, mobility assist, and companionship, thereby assuaging the weight on overstretched caregivers. With advancements in artificial intelligence and robotics, those generation may be tailor-made to satisfy the unique cultural and linguistic wishes of India's several aged population. furthermore, making an investment in research and development of low-priced and purchaser-quality robotic answers can't excellent beautify the of lifestyles for seniors however moreover create employment opportunities and pressure financial growth within the rising subject of healthcare robotics.[60]

VIII. CONCLUSION

During focus group discussions, there was a broad concern for the implementation of robots in a lot of facets are used to care for old age people living in their homes, senior housing. Older people and their caregivers, both studied groups, expressed a particular demand for robots which provide a broad support. The process of the robot's initiation needs special attention: It can be done by extensive pre-training and considering a variety of pragmatic and moral considerations. It is essential for future robot users to be involved for developing as well as customizing of all technical result to be set up so that they know the need for the older people. [61]

IX. FUTURE SCOPE

There are three possible paths for future research in this domain. First, new robots and methods to improve human-robot interaction must be developed. In the second step, a simulation-optimization approach [62] is employed in conjunction with multi-criteria mathematical programming models[63-64] in order to increase the degree of support provided by robots, as well as to ensure that robots are optimally placed in eldercare facilities. The challenge of teaching robots how to communicate with humans is related to third decision

In India, the future scope of elderly care robotics holds immense promise as the country grapples with a growing aging population and a inadequacy of caregivers.[65] Besides advancements in technology, robotic solutions tailored for

elderly care are poised to address various challenges, including assistance with daily activities, monitoring health parameters, providing companionship, and ensuring safety.[66] All these robots help to alleviate burden on overburdened healthcare systems, family care-givers. Additionally, as India continues to embrace digitalization and automation across sectors, there's conceivable chance for integrating robots in home as well as care services, also adapting it for aided living solutions, offering personalized and efficient care to seniors. Moreover, the development and adoption of indigenous solutions can also stimulate economic growth and create employment opportunities in the burgeoning field of robotics and healthcare technology.[67]

REFERENCES

[1] Melissa Ferretti, Giovanna Morgavi, & Gianmarco Veruggio. (2018). The ACCEPTABILITY of Caregiver Robots in Elderly People, 111–118. doi:10.5220/0006674301110118

[2] S. Li and Y. Liu, "How Can Smart Service Robot Help the Elderly Aging in Place: Application, Prospect and Preference," 2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), BALI, Indonesia, 2022, pp. 395-401, doi: 10.1109/IoTaIS56727.2022.9976005.

[3] Christina Plaschka, Diane Sawchuck, Timothy J. Orr, Thomas Bailey, Dawn Waterhouse, & Nigel J. Livingston. (2020). Global policies on assistive robots for care of the elderly: A scoping review. International Journal of Healthcare, 6(1), 63–63. doi:10.5430/ijh.v6n1p63

[4] Sharkey, A., Sharkey, N. Granny and the robots: ethical issues in robot care for the elderly. Ethics Inf Technol **14**, 27– 40 (2012). https://doi.org/10.1007/s10676-010-9234-6

[5] Z. Zhu et al., "CBASH: A CareBot-Assisted Smart Home System Architecture to Support Aging-in-Place," in IEEE Access, vol. 11, pp. 33542-33553, 2023, doi: 10.1109/ACCESS.2023.3264272.

[6] S. Taleb, L. C. FOURATI and M. FOURATI, "Study on Communicative Robots Assisting Elderly Persons," 2023 15th International Conference on Developments in eSystems Engineering (DeSE), Baghdad & Anbar, Iraq, 2023, pp. 209- 214, doi: 10.1109/DeSE58274.2023.10099833.

[7] D. C. Herath, L. Martin, S. Doolan and J. B. Grant, "Robots and Aged Care: A Case Study Assessing Implementation of Service Robots in an Aged Care Home," 2023 32nd IEEE International Conference on Robot and Human Interactive Communication (RO-MAN), Busan, Korea, Republic of, 2023, pp. 1641-1647, doi: 10.1109/RO- MAN57019.2023.10309361.

[8] Johannes Kriegel, Victoria Grabner, Linda Tuttle- Weidinger, & Irmtraud Ehrenmüller. (2019). Socially Assistive Robots (SAR) in In-Patient Care for the Elderly. Studies in Health Technology and Informatics, 260. doi:10.3233/978-1-61499-971-3-178

[9] Teng R, Ding Y, See K. Use of Robots in Critical Care: Systematic Review. J Med Internet Res 2022;24(5):e33380 URL: https://www.jmir.org/2022/5/e33380. DOI: 10.2196/33380

[10] Moojan Ghafurian, et al. "Social Robots for the Care of Persons with Dementia." Acm Transactions on Human- Robot Interaction, vol. 10, no. 4, Association for Computing Machinery, Sept. 2021, pp. 1–31, doi:10.1145/3469653.

[11] S. Li and Y. Liu, "How Can Smart Service Robot Help the Elderly Aging in Place: Application, Prospect and Preference," 2022 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS), BALI, Indonesia, 2022, pp. 395-401, doi: 10.1109/IoTaIS56727.2022.9976005.

[12] Malin Andtfolk , Linda Nyholm , Hilde Eide & Lisbeth Fagerström (2022) Humanoid robots in the care of older persons: A scoping review, Assistive Technology, 34:5, 518- 526, DOI: 10.1080/10400435.2021.1880493

[13] Martinez-Martin, E.; Escalona, F.; Cazorla, M. Socially Assistive Robots for Older Adults and People with Autism: An Overview. Electronics 2020, 9, 367

[14] Pepper in Healthcare. Available online: https://www.softbankrobotics.com/emea/en/pepper- healthcare-ga.

[15] Tanaka, F.; Isshiki, K.; Takahashi, F.; Uekusa, M.; Sei, R.; Hayashi, K. Pepper learns together with children: Development of an educational application. In Proceedings of the 2015 IEEE-RAS 15th International Conference on Humanoid Robots (Humanoids), Seoul, Korea, 3–5 November 2015; pp. 270–275.

[16] Yang, C.; Lu, M.; Tseng, S.; Fu, L. A companion robot for daily care of elders based on homeostasis. In Proceedings of the 2017 56th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE), Kanazawa, Japan, 19–22 September 2017; pp. 1401–1406.

[17] Sato, M.; Yasuhara, Y.; Osaka, K.; Ito, H.; Dino, M.J.S.; Ong, I.L.; Zhao, Y.; Tanioka, T. Rehabilitation care with Pepper humanoid robot: A qualitative case study of older patients with schizophrenia and/or dementia in Japan. Enferm. Clín. 2020, 30, 32–36.

[18] Carros, F.; Meurer, J.; Löffler, D.; Unbehaun, D.; Matthies, S.; Koch, I.; Wieching, R.; Randall, D.; Hassenzahl, M.; Wulf, V. Exploring Human-Robot Interaction with the Elderly: Results from a Ten-Week Case Study in a Care Home. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20), Honolulu, HI, USA, 25–30 April 2020; pp. 1–12.

[19] Costa, A.; Martinez-Martin, E.; Cazorla, M.; Julian, V. PHAROS—PHysical assistant RObot system. Sensors 2018, 18, 2633.

[20] Martinez-Martin, E.; Costa, A.; Cazorla, M. PHAROS 2.0—A PHysical Assistant RObot System Improved. Sensors 2019, 19, 4531.

[21] Kittmann, R.; Fröhlich, T.; Schäfer, J.; Reiser, U.; Weisshardt, F.; Haug, A. Let me Introduce Myself: I am Care-O-bot 4, a Gentleman Robot. In Mensch und Computer 2015—Proceedings; Diefenbach, S., Henze, N., Pielot, M., Eds.; De Gruyter Oldenbourg: Berlin, Germany, 2015; pp. 223–232.

[22] Miseikis, J.; Caroni, P.; Duchamp, P.; Gasser, A.; Marko, R.; Miseikiene, N.; Zwilling, F.; Castelbajac, C.; Eicher, L.; Frueh, M.; et al. Lio—A Personal Robot Assistant for Human-Robot Interaction and Care Applications. IEEE Robot. Autom. Lett. 2020, 5, 5339–5346.

[23] Fischinger, D.; Einramhof, P.; Papoutsakis, K.; Wohlkinger, W.; Mayer, P.; Panek, P.; Hofmann, S.; Koertner, T.; Weiss, A.; Argyros, A.; et al. Hobbit, a care robot supporting independent living at home:

First prototype and lessons learned. Robot. Auton. Syst. 2016, 75, 60–78.

[24] Kostavelis, I.; Giakoumis, D.; Malasiotis, S.; Tzovaras, D. Ramcip: Towards a robotic assistant to support elderly with mild cognitive impairments at home. In International Symposium on Pervasive Computing Paradigms for Mental Health; Springer: Berlin/Heidelberg, Germany, 2015; pp. 186–195.

[25] The Strong Robot with the Gentle Touch. Available online: https://www.riken.jp/en/news_pubs/research_news/pr/2015/ 201 50223_2/

[26] Perry, T.S. Profile: Veebot. Making a Robot That Can Draw Blood Faster and More Safely Than a Human Can. Available online: https://spectrum.ieee.org/robotics/medical-robots/profile- veebot

[27] DeKonBot—Mobile Robot for Disinfecting Potentially Contaminated Surfaces. Available online: https://www.youtube.com/ watch?v=lBj6P9lfXDM&feature=emb_title&ab_channel=FraunhoferIPA

[28] KINOVA JACO Assistive Robotic Arm. Available online: https://www.kinovarobotics.com/en/products/assistive- technologies/ kinova-jaco-assistive-robotic-arm

[29] Gordon, E.K.; Meng, X.; Barnes, M.; Bhattacharjee, T.; Srinivasa, S.S. Adaptive Robot-Assisted Feeding: An Online Learning Framework for Acquiring Previously-Unseen Food Items. arXiv 2019, arXiv:1908.07088.

[30] Bhattacharjee, T.; Gordon, E.K.; Scalise, R.; Cabrera, M.E.; Caspi, A.; Cakmak, M.; Srinivasa, S.S. Is More Autonomy Always Better? Exploring Preferences of Users with Mobility Impairments in Robot-assisted Feeding. In Proceedings of the 2020 ACM/IEEE International Conference on Human-Robot Interaction, Cambridge, UK, 23–26 March 2020; pp. 181–190.

[31] Goldau, F.F.; Shastha, T.K.; Kyrarini, M.; Gräser, A. Autonomous multi-sensory robotic assistant for a drinking task. In Proceedings of the 2019 IEEE 16th International Conference on Rehabilitation Robotics (ICORR), Toronto, ON, Canada, 24–28 June 2019; pp. 210–216.

[32] Kumar Shastha, T.; Kyrarini, M.; Gräser, A. Application of Reinforcement Learning to a Robotic Drinking Assistant. Robotics 2020, 9, 1.

[33] Kyrarini, M.; Zheng, Q.; Haseeb, M.A.; Gräser, A. Robot Learning of Assistive Manipulation Tasks by Demonstration via Head Gesture-based Interface. In Proceedings of the 2019 IEEE 16th International Conference on Rehabilitation Robotics (ICORR), Toronto, ON, Canada, 24–28 June 2019; pp. 1139–1146.

[34] Zhang, F.; Cully, A.; Demiris, Y. Probabilistic real-time user posture tracking for personalized robot-assisted dressing. IEEE Trans. Robot. 2019, 35, 873–888.

[35] Burt—The User-Friendly Robot. Available online: https://medical.barrett.com/home

[36] Zeilig, G.; Weingarden, H.; Zwecker, M.; Dudkiewicz, I.; Bloch, A.; Esquenazi, A. Safety and tolerance of the ReWalk™ exoskeleton suit for ambulation by people with complete spinal cord injury: A pilot study. J. Spinal Cord Med. 2012, 35, 96–101.

[37] ReWalk More Than Walking. Available online: https://rewalk.com/

[38] Lokomat. Available online: https://www.hocoma.com/

[39] Cifuentes, C.A.; Rodriguez, C.; Frizera-Neto, A.; Bastos-Filho, T.F.; Carelli, R. Multimodal Human–Robot Interaction for Walker-Assisted Gait. IEEE Syst. J. 2016, 10, 933–943.

[40] Jiang, S.; Lin, C.; Huang, K.; Song, K. Shared Control Design of a Walking-Assistant Robot. IEEE Trans. Control Syst. Technol. 2017, 25, 2143–2150

[41] Chalvatzaki, G.; Koutras, P.; Hadfield, J.; Papageorgiou, X.S.; Tzafestas, C.S.; Maragos, P. Lstm- based network for human gait stability prediction in an intelligent robotic rollator. In Proceedings of the 2019 International Conference on Robotics and Automation (ICRA), Montreal, QC, Canada, 20–24 May 2019; pp. 4225– 4232.

 ISSN 2394 - 7780

[42] Chalvatzaki, G.; Papageorgiou, X.S.; Tzafestas, C.S. Towards a user-adaptive context-aware robotic walker with a pathological gait assessment system: First experimental study. In Proceedings of the 2017 IEEE/RSJ international conference on intelligent robots and systems (IROS), Vancouver, BC, Canada, 24–28 September 2017; pp. 5037– 5042.

[43] https://robotsguide.com/robots/pepper

[43] https://www.thenewsmarket.com/the-care-o-bot-4- robot/a/3a16f504-e96f-4841-9a33-74f295a306d1

[45] https://www.fp-robotics.com/en/lio/

[46] https://www.sciencedirect.com/science/article/abs/pii/S0921 889014002140

[47] Kostavelis, I. et al. (2019). RAMCIP Robot: A Personal Robotic Assistant; Demonstration of a Complete Framework. In: Leal-Taixé, L., Roth, S. (eds) Computer Vision – ECCV 2018 Workshops. ECCV 2018. Lecture Notes in Computer Science(), vol 11134. Springer, Cham. https://doi.org/10.1007/978-3-030-11024-6_7

[48] https://www.theverge.com/2015/4/28/8507049/robear- robot-bear-japan-elderly

[49] https://www.veebot.com/

[50] https://www.ipa.fraunhofer.de/en/press- media/press_releases/fraunhofer-ipa-presents-disinfection- robot-dekonbot.html

[51] https://robotsguide.com/robots/jaco

[52] https://robotsguide.com/robots/baxter

[53] https://blog.trentdye.com/barrett-technology- designing-an-end-effector-for-human-interaction-ffe5ece331b1

[54] https://www.indiamart.com/proddetail/rewalk-robotic-exoskeletons-for-paraplegic-patient-22360274491.html

[55] https://www.rfhospital.org/care-centres/our- technology/lokomat-hocoma-knowledge-platform

[56] https://www.sciencedirect.com/science/article/abs/pii/S0921 889011002181?via%3Dihub#preview-section-abstract

[57] https://www.walkbot.co.kr/en/sub/product- introduction.php

[58] https://i-walk.co.uk/product/i-walk-pro-robot/

[59] “Designing a Multiagent System for Elderly Care”, [Online]. Available: https://ebooks.iospress.nl/pdf/doi/10.3233/AISE200018.

[60] L. Asprino, P. Ciancarini, A. G. Nuzzolese, V. Presutti, and A. Russo, “A reference architecture for social robots,” Journal of Web Semantics, vol. 72, p. 100683, 2022, doi: 10.1016/j.websem.2021.100683.

[61] Savage, N. Robots rise to meet the challenge of caring for old people. Nature 2022, 601, S8–S10.

[62] Sawik, B.; Faulin, J.; Serrano-Hernandez, A.; Ballano, A. A Simulation-Optimization Model for Automated Parcel Lockers Network Design in Urban Scenarios in Pamplona (Spain), Zakopane, and Krakow (Poland). In Proceedings of the 2022 Winter Simulation Conference (WSC), Singapore, 11–14 December 2022; pp. 1648–1659.

[63] Sawik, B.; Serrano-Hernandez, A.; Muro, A.; Faulin, J. Multi-Criteria Simulation-Optimization Analysis of Usage of Automated Parcel Lockers: A Practical Approach. Mathematics 2022, 10, 4423.

[64] Sawik, T.; Sawik, B. A rough cut cybersecurity investment using portfolio of security controls with maximum cybersecurity value. Int. J. Prod. Res. 2022, 60, 6556–6572.

[65] Carolyn Johnston. “Ethical Design and Use of Robotic Care of the Elderly.” Journal of Bioethical Inquiry, vol. 19, no. 1, Springer Science+Business Media, Mar. 2022, pp. 11– 14, doi:10.1007/s11673-022-10181-z.

[66] N. Sun, E. Yang, J. Corney, Y. Chen and Z. Ma, "A review of high-level robot functionality for elderly care," 2018 24th International Conference on Automation and Computing (ICAC), Newcastle Upon

ISSN 2394 - 7780

Tyne, UK, 2018, pp. 1- 6, doi: 10.23919/IConAC.2018.8749031.

[67] Tuuli Turja. “Uncertainties about accepting care robots.” frontiers in digital health, vol. 5, Frontiers Media, May 2023, doi:10.3389/fdgth.2023.1092974.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024

ISSN 2394 - 7780

OPTIMIZING FINANCIAL WELLNESS: A THOROUGH EXAMINATION OF MODERN MONEY MANAGEMENT SYSTEMS

Neelam Naik[1] and Prachi Mistry[2]
[1]SVKM's Usha Pravin Gandhi College of Art's Science and Commerce, Vile Parle, Mumbai 400056

ABSTRACT
This research paper will provide a thorough analysis of every technical solution that is now available online anywhere in the world for finance management at an individual level. It will also outline the benefits and drawbacks of the available solutions. This paper studies five different applications (walnut, mint, YNAB, Moneyfy and Goodbudget) in detail and a comparative study between sixteen other application tools available in similar line. This study highlights the comparative study on the parameters like Investment suggestions, Loan offers, Expenses tracker and insurance suggestion. Concluding that there are many tools available but either they ask for subscription or are not available in India. Moreover, majority of tools available gives suggestion on different savings techniques, but there is a need for some tool which helps in predicting near future savings for individual.

INTRODUCTION
Money often costs too much. Money frequently comes with excessive expenditures. The future is uncertain; crises might strike at any time. A secure future is created by money saved. A more tranquil existence is left behind the more they save. Investing is a smart method to use money you've saved and might even help you become wealthy. As technology advances, there are a growing number of websites and mobile applications offering various investing options. Finding every technology on the internet that can be used to increase wealth is the goal of this investigation. The characteristics, benefits, and drawbacks of the various tools are the primary objective of the study.

LITERATURE REVIEW
Considering other studies on the similar ground the literature review says that [1] The dimensions of PFM are determined by studying the literature, and the impact of each part of it on the overall digital financial management (DFMB) is a proven experiment. Additionally, the study confirmed the psychometric value of the tool for measuring personal financial management behaviour (PFMB) using digital platforms. [2] Researchers have explored the use of mobile services in technology and business information, but few researchers have paid attention to the applications and benefits of these mobile services from the customer perspective. [3] Aims to design a mobile application which will help in managing personal finance. Researchers have divided the paper into two phases where one highlights the past present and future transactions and the other phase shows application design in form of class and case diagram.[4] The main purpose of building personal finance is to manage personal money, track expenses and plan resources, as recoding with pen and paper is not easy to organize, delete and search. [5] The bachelor's thesis discusses the analysis, design and implementation of a mobile application for financial management and budgeting on the iOS platform. [6] The purpose of this study is to examine working age and evaluate whether smartphone applications can be used to improve work behaviour. People who take these apps are more likely to track their income and expenses and show greater resilience when faced with financial crisis. [7] This study aims to evaluate the impact of mobile application use on household savings and consumption behaviour from three different perspectives. By explaining the student management and spending tracking solution, it has been determined that various decisions and the use of mobile applications have an impact on saving and spending behaviour [8] The development of this application includes financial management, application development, overhead management, gaming and user interface development.

Problem Definition:
The study involves analysing every tool that may be available, such as a website or mobile application that provides financial options or makes specific savings predictions at an individual level.

Research Methodology:
Saving a penny is earning a penny. Since money is the most essential component for survival, it is critical to preserve it in order to meet all of one's needs in our cutthroat society. This study focuses on any smartphone application, website, or web application that assists an individual in managing their money wisely and keeping track of all daily transactions.

I. WALNUT

 ISSN 2394 - 7780

Axio Digital Pvt. Ltd is the company that developed of this application, which is freely accessible on a website and as a mobile application. This program is easy to use and monitors all bank SMSs in addition to attentively tracking every transaction. All of the transactions are cleverly divided into three categories by this application: food, travel, and bills. It also provides a summary on all the costs incurred throughout a specific time frame. In addition to recommending cabs, movies, activities, etc., it monitors credit card balances.

II. YNAB (You need a budget)

On October 20, 2015, the ynab.com created and released this application. The user interface is really appealing. The program begins by requesting general information from the user, including who, how, and what questions. This information is used by the application's algorithm to create budget plans. Due to its monthly or early payments, the application is not available for free.

III. Good Budget

The greatest budget software for budgeting with envelopes is also this one made by Dayspring Partners. Both the website and mobile apps for this application are widely accessible. The user is prompted to input estimated savings, monthly income, and costs (food, travel, groceries). The expenditures are separated into discrete amounts known as envelopes, from which the completed transactions are subtracted.

IV. Mint

Another well-liked program created by Excel Net Solution Pvt Ltd provides financial tools, market updates, investment routes, and a website. It is accessible as a mobile application as well. Investment pathways provides consumers with the newest fund offerings, investment plans, and top SIP programs. The application's market update area displays a report with the most recent NAV and market indexes. Financial instruments such as the Lumpsum Calculator, Calculators for SIP, Cost of Delay SIP, Education, Marriage, Retirement, SIP Tenure, EMI, SIP step-up, SIP Planner, STP Planner, and SWP Planner are available.

V. Moneyfy

TATA Capital built this application in a unique way and made it accessible online and on mobile devices. It provides a broad range of recommendations for any kind of loan or credit card, as well as well-liked stock, mutual fund, SIP, and savings plans. offers a variety of programs for other insurance kinds as well. This application's special feature is its abundance of video lectures that offer advice on wise investments. Additionally, it enables users to construct their investment portfolio

Results:

There are many alternative options accessible globally that give a wise approach to managing finances, so tighten your belt. The comparative study of several applications' characteristics, such as investments, expense tracker, loan, and insurance, is shown in the table below.

App Name	Registration	Subscription	Investments options				Investment Report
			FD	SIP	Stock	Mutual Funds	
Mint				✓		✓	
GoodBudget	✓						
YNAB	✓	✓					
MoneyFy	✓			✓	✓	✓	✓
Walnut	✓						
MoneyView	✓						
RealByte	✓						
Bishinews							
ET Markets			✓	✓	✓	✓	✓
Wallet							
Money Manager							
Expense Manager	✓	✓					
CRED	✓						
Grow	✓			✓	✓		✓
Finserv	✓		✓	✓		✓	✓
Dhani	✓				✓		✓

Table 1.1: Investments Suggestions

App Name	Monthly Expense Tracker				Expense Report	Saving Suggestions
	Grocery	Bills	Medical	Travelling		
Mint						
GoodBudget	✓	✓	✓	✓	✓	✓
YNAB	✓	✓		✓	✓	
MoneyFy						
Walnut	✓	✓	✓	✓	✓	
MoneyView	✓	✓	✓	✓	✓	✓
RealByte	✓	✓	✓	✓	✓	
Bishinews		✓		✓	✓	
ET Markets						
Wallet	✓	✓	✓	✓	✓	
Money Manager		✓		✓	✓	
Expense Manager	✓	✓	✓	✓	✓	✓
CRED	✓	✓	✓	✓	✓	✓
Grow						
Finserv						
Dhani						

Table 1.2: Expenses Tacker

App Name	Loan offers					Loan Tracker Report
	Personal	Vehicle	Home	Gold	Education	
Mint						
GoodBudget						
YNAB						
MoneyFy	✓	✓	✓	✓	✓	✓
Walnut						
MoneyView						
RealByte						
Bishinews						
ET Markets						
Wallet						
Money Manager						
Expense Manager						
CRED	✓					✓
Grow						
Finserv	✓	✓	✓	✓	✓	✓
Dhani	✓	✓	✓	✓	✓	✓

Table 1.3: Loan Schemes

App Name	Insurance Options			Insurance Report	Management Tutorial	Money Calculator	Market Update
	Life	Vehicle	Medical				
Mint						✓	✓
GoodBudget							
YNAB							
MoneyFy	✓	✓	✓	✓	✓	✓	
Walnut						✓	
MoneyView						✓	
RealByte							
Bishinews						✓	
ET Markets					✓	✓	✓
Wallet						✓	
Money Manager						✓	

Expense Manager						✓	
CRED						✓	✓
Grow						✓	✓
Finserv	✓	✓	✓	✓			
Dhani						✓	

Table 1.4: Insurance Suggestions

DISCUSSION

Considering the choices that are accessible Numerous programs exist that give banking, investing, and other suggestions; however, access to these resources requires a monthly or annual subscription fee. Additionally, there are a lot of options that are unavailable in India. Then, there is a significant subset of these money management tools that are only offered to businesses.

CONCLUSION

Money has never, and will never, make a man happy. A man's desire increases with his possessions. It creates a vacuum rather than trying to fill one. Following a comparison of several global solutions, a tool that enables people to forecast their savings in the coming years is required so that people may budget their extra costs and satisfy their appetites for luxuries.

REFERENCES

[1]: Neetu Chhilar, Swaranjeet Arora, "Personal Financial Management Behavior Using Digital Platforms and its Domains", 2022, journal of financial management, markets and institutions vol. 10, no. 2 (2022) 2250009, doi: 10.1142/s2282717x22500098

[2]: Jeong Hee Yeo, Patti J. Fisher, “Mobile Financial Technology and Consumers’ Financial Capability in the United States”, 2017, Journal of Education & Social Policy

[3]: Brilly Andro Makalew, “Android Based Personal Finance Management Application: Design and Development”, 2022, JURNAL EMACS (Engineering, MAthematics and Computer Science) Vol.4 No.1 January 2022: 5-9, DOI: 10.21512/emacsjournal.v4i1.8085

[4]: Oshin Raina, Sakshi Mishra, Prof. Santoshi Pote, “Personal Finance Application- GROW MORE”, 2022, International Journal for Research in Applied Science & Engineering Technology (IJRASET), DOI: https://doi.org/10.22214/ijraset.2022.42166

[5]: Hoang Anh Ngo, “Personal Finance Management Mobile App for iOS”, 2021

[6]: French, D., McKillop, D., & Stewart, E. “The effectiveness of smart phone apps in improving financial capability. European Journal of Finance”,2020, https://doi.org/10.1080/1351847X.2019.1639526

[7]: Rajat Deb, “Influence of Mobile Apps on Household Saving-Spending Behaviour”,2020, NMIMS Management Review

[8]: Nur Irdina Azhar, “Development of Smart Mobile Money Management Application for Students”, 2020, https://www.researchgate.net/publication/338342868

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

A REVIEW ON ADVANCED TECHNIQUES IN THREE-DIMENSIONAL IMAGE RECONSTRUCTION FROM TWO-DIMENSIONAL IMAGES

Mustafa Riyaz Maruf and Dr. Rajesh Maurya
Usha Pravin Gandhi College of Arts, Science and Commerce, Vile Parle, Mumbai, India

ABSTRACT

Recent advancements in Three-Dimensional model visualization techniques have seen significant growth, impacting both technical and hardware aspects. Unlike the past, expensive machinery is no longer a prerequisite for experiencing Three-Dimensional environments; a simple computer now suffices. Traditionally, research efforts focused on developing Three-Dimensional information and acquisition technique for objects and scenes, requiring expertise and complex calibration procedures. In response to that need for flexibility in acquisition methods, various techniques have emerged, with some only requiring computer and camera to generate Three-Dimensional representation of scenes.

Keywords: Three-Dimensional reconstruction, Approach, Two-Dimensional images, Views.

INTRODUCTION

Constructing a Three-Dimensional model from Two-Dimensional images, aiming for maximum realism, represents a key challenge in image-based modeling and computer vision. Optimal solutions involve automated scene reconstruction with minimal user involvement. Presently, various methods exist for transforming Two-Dimensional images into Three-Dimensional reconstructions, each algorithm characterized by specific execution conditions, strengths, and weaknesses.

This paper delineates the defines and application domains of Three-Dimensional reconstruction from Two-Dimensional images. We introduce a set of algorithms for this reconstruction process and provide a comparative analysis. Finally, we conclude by summarizing the findings relevant on this review.

Summary of Reconstructing Three-Dimensional Structures from Two-Dimensional Images

What Does Reconstructing Three-Dimensional Structures from Two-Dimensional Images Mean?

Three-dimensional reconstruction is the process of reconstructing Three-dimensional models from a set of two-dimensional images. This contrasts with the process of creating two-dimensional images from three-dimensional scenes. Because a Three-dimensional image is generated by projecting a three-dimensional scene onto a two-dimensional surface during image generation, one image doesn't contain the information necessary to reconstruct the three-dimensional scene. As a result, the points visible in the images are projected onto the actual points of the scene, resulting in a loss in depth.

Areas where Three-Dimensional Reconstruction from Images is Applied

In addition to medicine, three-dimensional reconstructions are used in free-view point video reconstructions, in robotic mapping, in city planning, in gaming, in virtual environments, in virtual tourism, in landslide inventory mapping, in robot navigation, in archaeology, in augmented reality, in reverse engineering, in motion capture, in gesture recognition, and in hand tracking. Within the medical realm, Three-Dimensional reconstruction from Two-Dimensional images serves as a valuable tool for both therapeutic and diagnostic purposes. By employing a camera to capture multiple images from various angles, this technique offers an alternative to expensive and potentially risky medical imaging methods such as MRI and CT scanning. These conventional methods may not be suitable for patients with ferromagnetic metallic implants and often necessitate patients to lie down, altering the natural structure of bones. On the other hand, techniques such as the Stereo Coordinate Point Based Technique (SCBBT) or Non Stereo Coordinate Profile (NCSP) allow for Three-Dimensional reconstruction while keeping patients upright, using X-ray imaging with low radiation exposure.

In the field of robotic navigation, autonomous robots leverage Three-Dimensional maps created from images taken by their cameras for real-time processing. This capability aids in navigation, helping robots find their way and avoid obstacles in their path, providing valuable spatial measurements.

Prerequisites for Three-Dimensional Reconstruction from Images

Achieving the desired coordinates for scene points involves addressing several key challenges:

- ***Calibration Problem:***

ISSN 2394 - 7780

Addressing the calibration issue entails projecting scene points onto the image utilizing the pinhole model. In this context, grasping the intrinsic camera parameters, such as focal length and image center, holds paramount importance. In addition, understanding the camera positions is important if you want to find the coordinates of the points in a frame that isn't dependent on the camera. These extrinsic parameters encompass the camera's spatial orientation and position.

- ***Matching Problem:***

The matching problem revolves around the capability to recognize and associate points that appear across multiple images.

- ***Reconstruction Problem:***

Solving the reconstruction issue involves establishing the Three-Dimensional coordinates of points through the identified associations and calibration parameters.

- ***Reconstruction Density:***

After obtaining the coordinates for a specified group of points in space, the next challenge is identifying the surface associated with these points, allowing for the creation of a mesh or a detailed model. This phase is crucial since, without it, even though a substantial number of points may be acquired, the resultant point cloud might delineate the object's form visually, yet the reconstruction remains sparse.

LITERATURE SURVEY

Three-dimensional reconstruction is the process of reconstructing Three-dimensional models from a set of two-dimensional images. Considerable research has been done on this subject. Some studies that concentrate on Three-dimensional reconstruction are listed below.

In [1] Wikipedia discusses the evolution of Three-Dimensional model visualization, emphasizing advancements in both technical and hardware aspects. Expensive machinery is no longer necessary; a basic computer suffices. Previously, research focused on developing Three-Dimensional information sources and extraction techniques, requiring expertise and complex calibration. Flexibility in acquisition methods is crucial, leading to the development of numerous techniques, many of which only necessitate a camera and computer for generating Three-Dimensional models.

In [2] Marshall J. A., Burbeck C. A., Ariely D., Rolland J. P., Martin K. E. explored if blurry boundaries between focused and blurred areas indicate relative depth. Participants judged depth in image pairs with varying boundary clarity. Both experiments showed participants consistently used boundary blur to perceive depth, but its effectiveness varied. This blur cue aids in resolving depth ambiguity in focus-based depth calculations.

In [3] Michael Bach highlights a significant paradox in human perception: despite our ability to see the world filled with objects, we tend to perceive everything as "real" and act accordingly. However, upon reflection, we realize that our perception is merely a limited representation of reality, as we are unaware of much that surrounds us. Our senses are confined to what we can perceive, leaving us oblivious to phenomena such as radio waves, x-rays, and other sensory inputs beyond our range. Additionally, some changes in the world occur too rapidly or slowly for us to detect, such as the flickering of a fluorescent light or the movement of stars. Moreover, the microscopic realm, despite its significance, remains invisible to us due to its scale.

In [4] Gupta, Sharad & Shukla, Dericks propose using drones to accurately map landslide dimensions, reducing costs compared to high-resolution satellite data. Their study near IIT Mandi, Himachal Pradesh, utilized a DJI Phantom 3 Advanced drone to capture high-resolution images. These images underwent processing with the Scale Invariant Feature Transform (SIFT) technique for feature detection and matching. Bundle block adjustment estimated Three-Dimensional positions and orientations, resulting in a sparse Three-Dimensional point cloud densified with the Clustering View for Multi-View Stereo (CMVS) algorithm. Surface reconstruction via the Poisson Surface Reconstruction method validated against field measurements and total station data showed the Three-Dimensional model's accuracy, with differences below 5%. This drone-based approach provides precise measurements at the centimeter level, aiding in landslide mapping and monitoring with sub-meter resolution digital elevation models (DEMs).

In [5] Wikipedia elucidated parallax scrolling, a technique in computer graphics where background images move slower than foreground ones, giving a sense of depth in a Two-Dimensional scene. Originating from traditional animation's multiplane camera technique in the 1930s, parallax scrolling gained prominence in Two-Dimensional computer graphics with its incorporation into video games during the early 1980s. Examples include its use in arcade games like Jump Bug (1981) and Moon Patrol (1982), which popularized the technique by employing varying background speeds to create depth.

 ISSN 2394 - 7780

In [6] Joseph S Lappin clarified the geometric primitives of binocular disparity. Stereoscopic depth perception arises from disparities in higher-order image structures like intensity, texture, and motion, which are correlated with observed surfaces. Binocular disparity reflects surface spatial structure, not requiring separate spatial coordinates for stereoscopic vision. Stereopsis is particularly sensitive to structural disparities related to local surface shape, with disparate positions on retinal anatomy not essential for this perception.

In [7] George Mather explained how images of Three-Dimensional scenes naturally contain areas with varying degrees of blur due to depth-of-focus constraints in imaging devices. Recent studies show that this blur difference serves as a depth cue: regions with sharp focus versus blurred texture can be perceived at different depths, even without other depth cues. Optical calculations demonstrate that blur variation mirrors binocular disparity in depth perception. Computational models reveal similarities between blur effects on single-step edges and random fractal patterns, suggesting comparable discrimination thresholds. Comparing blur discrimination with binocular stereopsis suggests they cover different distance ranges, with stereopsis more effective for closer distances and blur information for larger distances.

In [8] Cozman, F. & Krotkov, E. examined how light changes in the atmosphere affect image brightness, known as atmospheric scattering. They explored techniques to extract depth cues from these effects in images, useful for indoor and outdoor environments. Real image experiments show promise in accurately recovering depth cues, beneficial for autonomous vehicles.

In [9] Herbort and Wöhler introduced photometric methods for Three-Dimensional shape reconstruction and surveyed photometric stereo techniques, covering active and passive acquisition methods. They discussed the methodical background, including the canonical photometric stereo setup, local gradient-based reconstruction, and various reflectance models. The survey extends to non-standard settings like non-distant light sources and non-Lambertian surfaces, with a focus on specular reflections and estimation of surface reflectance properties. They also explored combining photometric techniques with triangulation-based approaches.

In [10] this paper "Three-Dimensional Reconstructing an Autonomous Robot's Journey," led by TAMAS FAZAKAS and Róbert TAMAS Fekete, the team presented a detailed Three-Dimensional reconstructive process to guide an autonomous robot's journey. The system uses pre-existing multichannel stereo algorithms that automatically capture video or images of the robot's surroundings as input and generate a Three-Dimensional model of the environment being explored, including the path of the robot. The effectiveness of the system was tested in a variety of environments, showing the potential of this cutting-edge approach.

Methods for Reconstruction: Active and Passive Approaches

Achieving the recovery of depths for visible points in an image is feasible via active or passive approaches.

Active Approach

In the active reconstruction process, external sources of energy or illumination are utilized to assist in the reconstruction. This method typically entails projecting patterns of structured light, laser beams, or other types of electromagnetic radiation onto the scene or object. Sensors like cameras or laser range finders capture the reflected or scattered energy to derive depth and surface details. The effectiveness of active reconstruction techniques is often characterized by their precision in providing depth measurements and intricate surface information. Structured light scanning, time-of-flight (ToF) cameras, and laser scanning are examples of methods used in active reconstruction.

These methods are typically more accurate and faster but can be more intrusive and expensive. The structured light scanning based method [11] projects a pattern of light onto the subject and observes the deformation of this pattern from a different angle. By knowing the pattern and how it deforms, it's possible to calculate the shape of the subject. Laser scanning based method involves shooting laser [12] beams at the object and measuring the time it takes for the light to return. The time delay gives information about the distance of different parts of the object, thus creating a Three-Dimensional model. Time-of-Flight Cameras [13] are similar to laser scanning, but these cameras emit a light signal and then measure how long it takes for the light to return to the sensor, allowing for the capture of Three-Dimensional scenes in real-time.

Passive Approach

Conversely, passive reconstruction relies exclusively on ambient light or existing illumination sources available in the surroundings. This approach involves capturing images or video frames of the scene or object using cameras or other imaging devices. Depth information and the geometry of the scene are deduced from the captured images through computational analysis and stereo vision techniques. Passive reconstruction methods are generally less obtrusive and do not necessitate additional light sources, making them well-suited for diverse

 ISSN 2394 - 7780

applications. Examples of passive reconstruction techniques encompass stereo vision, photogrammetry, and structure-from-motion (SfM) algorithms.

Passive methods do not emit any kind of energy towards the subject but instead rely on analyzing the natural light reflected from the subject. These methods are generally less intrusive and can be cheaper but might require more complex processing and are often less accurate than active methods. Stereoscopy uses two or more images from different viewpoints. By finding correspondences between these images (i.e., identifying the same point in multiple images), it's possible to triangulate the position of points in Three-Dimensional space. Structure from Motion (SfM) [14] is an extension of stereoscopy that uses many images, possibly from a moving camera. By tracking the apparent motion of objects across a sequence of images, it infers both the Three-Dimensional structure of the scene and the motion of the camera. Photogrammetry [15] involves taking measurements from photographs to create Three-Dimensional renderings of a subject. This can be considered a broader category that includes techniques like SfM but is also applicable to static images from multiple angles. Other useful methods include Multi-view Stereo (MVS) [16] and use of Monocular Depth Cues [17]. MVS An advanced form of stereoscopy that uses many images from different viewpoints. Unlike basic stereoscopy, MVS can produce high-resolution Three-Dimensional models by employing sophisticated algorithms to find correspondences across many images. Monocular Depth Cue techniques infer depth from a single image using cues such as perspective, texture gradients, and shadows. These methods are very challenging due to the inherent ambiguity in interpreting Two-Dimensional images as Three-Dimensional scenes but are an active area of research, especially with the aid of machine learning models.

Each method has its specific use cases and requirements for success. Active methods are often preferred for industrial applications where precision is crucial and the environment can be controlled. Passive methods, on the other hand, are widely used in applications where active illumination is impractical, such as in outdoor environments or cultural heritage documentation, where the object cannot be interacted with directly.

Useful Insight for Converting Two-Dimensional Images to Three-Dimensional

There are two main categories of conversion algorithms, distinguished by the number of input images they utilize. The first category involves algorithms dependent on 2 or more images, which can be obtained from multiple stationary cameras with diverse viewing angles or from a single camera capturing scenes with moving elements. This category employs multidimensional depth cues. On the other hand, the second category relies on algorithms using only one static image, where the depth cues are termed monocular dimensional depth cues.

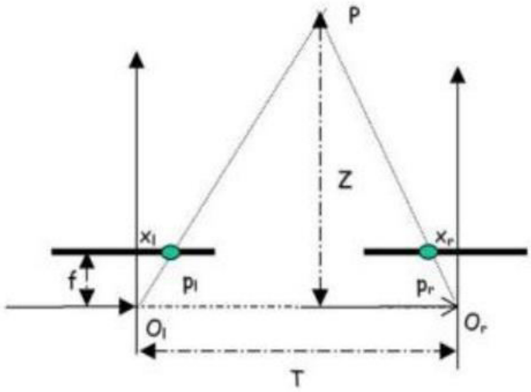
Table I. Depth cues utilized in algorithms for converting Two-Dimensional images to Three-Dimensional.

Number of Input Images	Depth Cues
Two or More Image	Motion parallax Binocular disparity Image blur
One Single Image	Liner Perspective Shape from Shading Atmosphere Scattering

Binocular Disparity

To find the depth of a particular point, we can use the triangulation method. The first step is to find a subset of points in each of the two images, taken slightly apart from each other. The second step is to find the depth of that particular point within each of those two images.

Figure I: Binocular disparity.



Let's consider Pl and Pr to be point P's projections onto two images and O1's and O2's to be the origin of coordinate systems for 2 cameras.Let's see how depth Z can be determined for point P:-D = xr – xl

$Z=f(T/D)$

Motion Parallax
Depth perception is affected by camera and scene motion. Objects near the camera appear to move more quickly than objects farther away.

Motion parallax is a critical contributor to depth perception, aiding the brain in discerning the depth and relative distances between objects. This phenomenon is a regular occurrence in everyday scenarios, such as when navigating through traffic or strolling down a busy street. When the observer is in motion, objects closer to them seem to traverse the visual field more rapidly than those at a greater distance, generating a perception of depth. Essentially, motion parallax is the visual illusion resulting from the relative movement between an observer and objects in their environment, manifesting when the observer moves and objects at varying distances exhibit different speeds across their field of vision. Consequently, objects in proximity to the observer give the impression of faster movement than those situated farther away.

- This principle has been used in a variety of contexts, including:
- Wiggle stereoscopy: motion parallax reproduces stereoscopic images
- This is a much more powerful signal than other monocular signals, even more so than binocular disparity.
- Parallax scrolling: in games, the foreground and background are moved at different rates.

Figure II: Motion Parallax Mechanics.

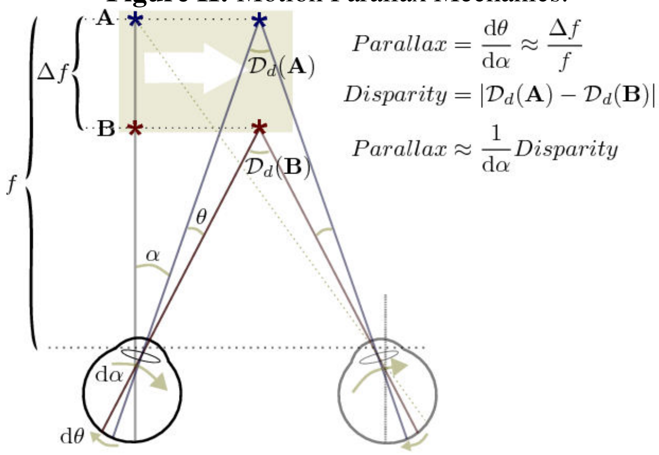


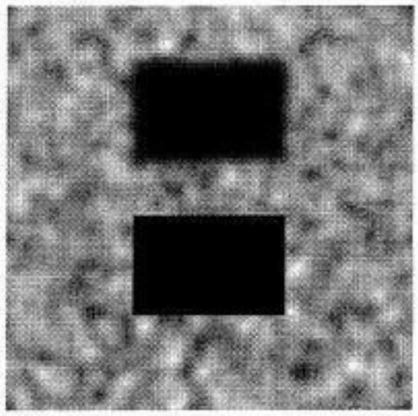
Image Blur
Many researchers, including Mather and Marshall (2006), have shown that image blur is relevant to depth perception. Mather and Marshall's work focused on ambiguous figures—ground stimuli that included two areas of texture separated by wavelike boundaries. Mather and Marshall found that objects in focus appear clearly defined while objects at various distances appear blurring.

The next general equation, first proposed by Pentland (1987), relates the distance from a point (d) to a lens (r) and the range (s) of the blurred image of that point.

d = Frv/(rv- F(r + s))

In this scenario, F stands for the focal length, r denotes the lens aperture radius, and v signifies the distance from the lens to the image plane. With knowledge of the values for F, r, and v, along with a measurement of image blur (s), the absolute distance can be computed. Equation (1) is applicable for predicting retinal blur based on distance.

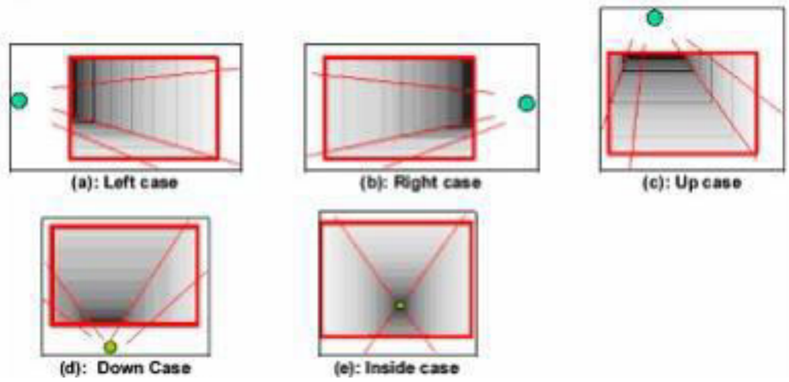
Figure III: Blur as a depth indicator in irregular designs.



Linear Perspective

Linear perspective involves the phenomenon where parallel lines within a Three-Dimensional environment seem to meet at a vanishing point when projected onto a Two-Dimensional image surface. This convergence effect aids in perceiving depth and distance in the depicted scene. Through the analysis of line convergence and their interrelationships in Two-Dimensional images, algorithms can deduce the relative positions of objects within the Three-Dimensional space. In the realm of Three-Dimensional reconstruction, linear perspective plays a crucial role in ascertaining the relative depth of objects, estimating their spatial configurations, and reconstructing the geometry of the scene. Techniques like camera calibration, feature matching, and triangulation utilize the principles of linear perspective to extract the Three-Dimensional structure from Two-Dimensional images.

Figure IV: Blur as a depth indicator in unpredictable arrangements.



Shape From Shading

Shape from shading is a technique used to determine the normal shape of an object by looking at how light reflects off an object. The reflection of light on an object's surface changes depending on its orientation. This technique was first introduced by B.K. Horne P. Woodham in 1980. When there is only one image available, it is called shape from shading. This technique was further developed by B. K., Horne P.

Figure V. Illustration depicting the concept of shape from shading.

Atmosphere Scattering

The method of atmospheric scattering relies on the way light's energy and path changes as it passes through the atmosphere, which is affected by tiny particles. Objects closer to the camera appear brighter, while objects farther away appear bluer. In 1997, the Krotkov-Cozman model of physical scattering, based on Lord Rayleigh's 1871 model of atmospheric scattering, was published. Their method is especially useful for determining the resolution of outdoor images that include sky elements.

Figure VI: Depth map derived from atmospheric scattering.

Comparison

Conducting a thorough assessment of the effectiveness of various Two-Dimensional to Three-Dimensional conversion algorithms necessitates the meticulous formulation of criteria and datasets. Many articles lack a clear quantitative analysis of performance, making the evaluation process challenging. Therefore, it would be unjust to assert that one method exhibits a reduced error rate or a longer execution time in comparison to others. Complicating matters further, each algorithm possesses distinct characteristics and performances. Therefore, when addressing aspects like accuracy or speed for each depth cue algorithm, we reference, where applicable, the experimental findings outlined in the representative algorithms' respective articles.

Depth Scope

This facet outlines the range of depth perception humans can effectively achieve, considering the various depth cues available. For instance, linear perspective operates effectively across all depth ranges, whereas atmospheric scattering primarily influences distant objects.

Absolute or Relative Depth

In the realm of Three-Dimensional reconstruction techniques from Two-Dimensional images, both absolute and relative depth hold significant importance.

Absolute Depth pertains to the precise distance of a point within the reconstructed Three-Dimensional environment from a designated reference point or plane in the real world. It offers a direct measurement of the actual physical distance between objects and the camera or a specified reference point. Absolute depth estimation commonly involves methodologies such as triangulation, stereo vision, or structure-from-motion algorithms, which aim to accurately ascertain the spatial coordinates of objects in the scene.

On the other hand, Relative Depth focuses on the depth relationships among various points within the same scene. Rather than providing absolute distance measurements, it delineates the spatial arrangement of objects in relation to one another. Relative depth estimation finds application in tasks like scene comprehension, object detection, and segmentation. Techniques such as depth maps, depth from focus, and depth from defocus are frequently employed for relative depth estimation.

Image Characteristics

This refers to the attributes that images must possess for algorithms to process them effectively and function properly.

Motion Detection

This facet establishes whether elements within the image exhibit motion across various frames, a consideration specific to multilocular depth cues, as monocular depth cues depend solely on a single image.

Image Acquisition

This facet distinguishes between active and passive methods, referring to the characteristics of the image acquisition system. Most multilocular depth cues necessitate particular camera setups, while the majority of monocular depth cues do not require such specific configurations.

Sparse Depth Map or Dense Depth Map

This aspect concerns the depth map density. A depth map can be dense or sparse. Certain depth cues can also be used to generate dense or sparse depth maps depending on how much the algorithm prefers local feature points instead of global structures. In dense depth maps, the features of the image are stacked on top of one another. Each layer corresponds to a pixel of depth in the entire image. In sparse depth maps, the only thing that contributes to the depth is the feature points. This type is more suitable for extracting Three-Dimensional shapes.

Table II suggests that Binocular disparity is used within 30 meters to determine absolute depth, suitable for active methods, producing both dense and sparse depth maps. Motion parallax applies to distances less than 30 meters, accommodating all images through both active and passive means, with variable map density. Image blur targets objects with complex surfaces for absolute depth, exclusively through active acquisition, resulting in dense maps. Linear perspective operates over any range, providing relative depth from images with geometric appearances via passive methods, yielding dense maps. Shape from shading is effective across all distances, necessitating moderately lit images for relative depth assessment, with passive acquisition leading to dense surface mapping.

Atmospheric scattering is optimal between 900 and 8000 meters, utilizing haze to infer relative depth, employing passive techniques to achieve dense maps.

Table III suggests that Binocular Disparity is ideal for high-quality Three-Dimensional reconstruction within 30m, using binocular differences. Adapts to active/passive techniques for flexible map density. Motion Parallax enhances Three-Dimensional reconstruction quality for objects under 30m, leveraging relative motion. Compatible with both active and passive methods for versatile depth mapping. Image Blur specializes in detailed Three-Dimensional reconstruction without depth limit, utilizing differential focus. Active acquisition targets complex surfaces for precise dense maps. Linear Perspective elevates Three-Dimensional model accuracy over any distance, through geometric interpretation. Passive capture of linear convergence ensures detailed dense maps. Shape from Shading improves surface detail in Three-Dimensional models for all ranges, via shading analysis. Passive technique generates intricate dense maps on surfaces. Atmospheric Scattering is suitable for expansive outdoor Three-Dimensional reconstructions (900-8000m), using haze for depth. Passive acquisition provides extensive dense mapping for relative depth.

Table II: Comparison of depth Cues

Depth Cues	Depth Scope	Relative /Absolute Depth	Image Characteristics	Motion Detection	Image Acquisition	Dense or Sparse Depth Map
Binocular disparity	< 30 m	Absolute	All	Yes	Active	Dense/Sparse
Motion parallax	< 30 m	Absolute	All	Yes	Active/Passive	Dense/Sparse
Image blur	N/A	Absolute	Objects with complex surface characteristic	No	Active	Dense
Linear perspective	All ranges	Relative	Image contains geo-metric appearance	No	Passive	Dense
Shape from shading	All ranges	Relative	Image must not be too dark.	No	Passive	Dense on surface
Atmosphere scattering	900-8000 m	Relative	Scene contains haze	No	Passive	Dense

Table III: Performance Comparison

Method	**Accuracy**	**Speed**	**Cost**	**Intrusiveness**	**Complexity**	**Best Use Cases**
Active Methods						
Structured Light	High	Fast	Moderate-High	Moderate	Moderate	Precision engineering, quality control
Laser Scanning	Very High	Moderate-Fast	High	Moderate-High	High	Cultural heritage, topography, industrial design
Time-of-Flight Cameras	Moderate-High	Very Fast	Moderate	Low	Low	Gaming, interaction systems, rapid environment capture
Passive Methods						
Stereoscopy	Moderate	Moderate	Low-Moderate	Low	Moderate	Film industry, virtual reality
Structure from Motion (SfM)	High	Variable	Low	Low	High	Archaeology, urban modeling, environmental

ISSN 2394 - 7780

						studies
Photogrammetry	High	Slow-Variable	Low	Low	High	Cultural heritage, geology, architecture
Multi-view Stereo (MVS)	Very High	Slow	Moderate	Low	Very High	Detailed Three-Dimensional model creation, research
Monocular Depth Cues	Low-Moderate	Fast	Very Low	Very Low	Very High	Consumer applications, preliminary Three-Dimensional sketching

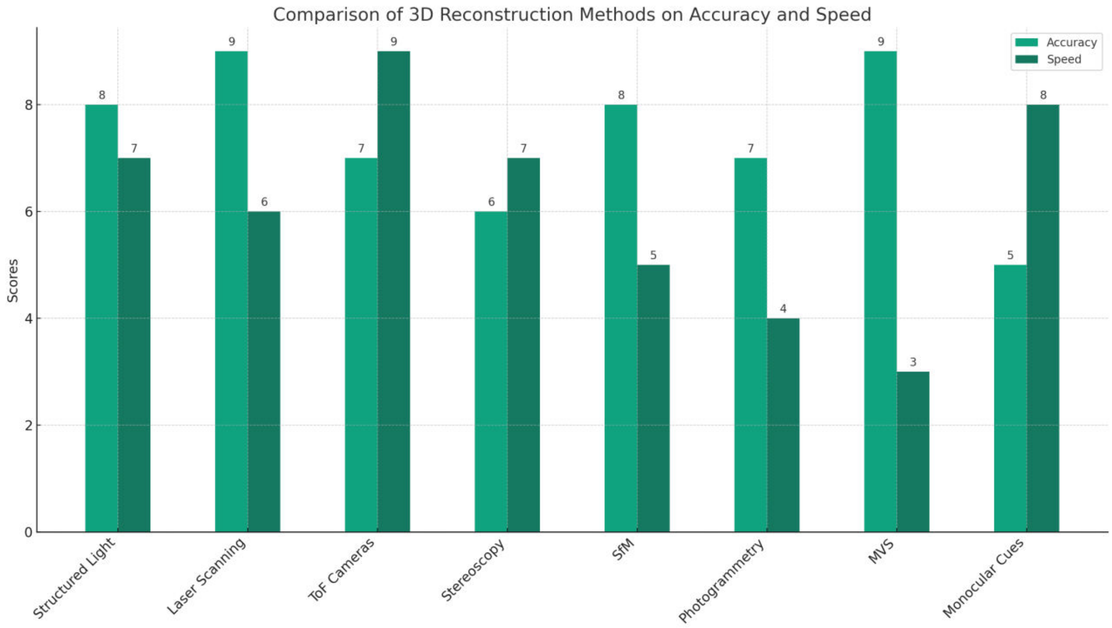


Figure VII: Comparing Three-Dimensional Reconstruction Methods [18]

Figure VII[18] suggests that Laser Scanning and Multi-view Stereo (MVS) methods demonstrate the highest accuracy levels among the techniques evaluated. This underscores their suitability for applications requiring detailed and precise Three-Dimensional models, such as cultural heritage preservation and detailed architectural modeling. On the lower end of the accuracy spectrum, Monocular Depth Cues exhibit the least accuracy. This limitation highlights the inherent challenge in deducing Three-Dimensional information from single images without the context provided by additional viewpoints or depth information.

Time-of-Flight (ToF) Cameras emerge as the leaders in speed, indicating their efficiency in real-time Three-Dimensional scene capture. This makes them particularly advantageous for interactive applications, such as augmented reality (AR) and human-computer interaction (HCI) where rapid feedback is essential. Multi-view Stereo (MVS) ranks as the slowest among the evaluated methods. The extensive computational requirements to process multiple images into a coherent Three-Dimensional model account for this slower speed, suggesting that MVS is better suited for non-real-time applications where model accuracy is prioritized over immediate processing.

CONCLUSION

This paper has explored into various depth cues for Three-Dimensional reconstruction, it's evident that each cue holds specific merits for improving the fidelity and realism of Three-Dimensional models across varied applications. Binocular disparity is pivotal for precise depth measurement within 30 meters, adaptable through both active and passive methods, making it ideal for environments where control and detail are paramount. Motion parallax, sharing this range, adds versatility by capturing the dynamics of both observer and object movement, enhancing the depth perception in active scenes. The utility of image blur, focusing on differential focus to discern distance, is unmatched for objects with intricate surface details, facilitated by active acquisition for producing detailed dense maps. Linear perspective's strength lies in its ability to convey relative depth over any distance, making it indispensable for reconstructions that require geometric precision, such as urban landscapes. Similarly, shape from shading, effective in all lighting conditions, excels in revealing surface

ISSN 2394 - 7780

nuances, enriching the texture and detail of the models. Atmospheric scattering, valuable for expansive outdoor scenes, leverages environmental haze to estimate depth, ideal for landscape reconstructions. The choice between dense and sparse depth maps offered by these cues underscores their adaptability to the specific needs of a project, from detailed modeling to broad spatial analysis.

This work highlights on the criticality of selecting suitable depth cues tailored to the project's specifics—considering depth range, subject nature, and desired model accuracy. Such strategic selection can significantly elevate Three-Dimensional reconstruction quality, propelling advancements in virtual reality, urban planning, and conservation, thereby enriching the practical and academic landscapes in India and beyond.

REFERENCES

[1] Three-Dimensional reconstruction from multiple images,Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Three-Dimensional_reconstruction_from_multiple_images. (Accessed 6 August 2019)

[2] Marshall J. A., Burbeck C. A., Ariely D., Rolland J. P., Martin K. E. “Occlu-sion edge blur: A cue to relative visual depth” , Journal of the Optical Socie-ty of America A, (1996). 13, 681–688.

[3] StereoKinetic phenomenon from Michael Bach’s "Optical Illusions & Visual Phenomena" (January 2013)

[4] Gupta, Sharad & Shukla, Dericks. “Application of drone for landslide map-ping, dimension estimation and its Three-Dimensional reconstruction.” Journal of the Indian Society of Remote Sensing. . (January 2018).

[5] Parallax scrolling, Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Parallax scrolling. (Accessed 8 may 2019)

[6] Joseph S Lappin, “What is Binocular Disparity. (August 2014) 1-4.

[7] George Mather, The use of image blur as a depth cue: (February 1997)

[8] Cozman, F.; Krotkov, E. “Depth from scattering”, IEEE Computer society, conference on Computer Vision and Pattern Recognition, Proceedings. (1997) 801–806

[9] Steffen Herbort and Christian Wöhler “An introduction to image-based Three-Dimensional surface reconstruction and a survey of photometric stereo methods”. (Sep-tember 2011) 23.

[10] Tamas Fazakas, Róbert Tamás Fekete, “Three-Dimensional reconstruction system for auton-omous robot navigation”, 2010 11th International Symposium on Computa-tional Intelligence and Informatics, Budapest (November 2010)

[11] Stjepan Jecić and Nenad Drvar "The assessment of structured light and laser scanning methods in Three-Dimensionalshape measurements".(January 2003)

[12] ASC Technology Solutions LLC "Complete Guide on Three-DimensionalLaser Scanning for Construction | Benefits of Laser Scanning | Process of Scan to BIM" on Linkedin.(August 2017)

[13] Time-of-flight camera,Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Time-of-flight_camera. (Accessed 6 February 2024)

[14] Structure from motion,Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Structure_from_motion. (Accessed 4 January 2024)

[15] Photogrammetry,Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Photogrammetry. (Accessed 9 February 2024)

[16] Multi-View Stereo phenomenon from Yasutaka Furukawa and Carlos Hernández "Multi-View Stereo: A Tutorial" (2015)

[17] Michael Kalloniatis and Charles Luu "The Perception of Depth".(June 2007)

[18] Wenyao Zhu and Shuyue Zhou "Three-DimensionalReconstruction Method of Virtual and Real Fusion Based on Machine Learning".(May 2022)

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

CRICKET MATCH RESULT PREDICTION USING MACHINE LEARNING

Dr. Neelam Naik[1] and Ayush Patel[2]
[1]Department of Information Technology and [2]Master of Information Technology, SVKM's Usha Pravin Gandhi College of Arts, Science and Commerce

ABSTRACT
Cricket, as a sport characterized by its intricacies, dynamic nature, and global popularity, has become a focal point for predictive analytics. This research introduces an advanced machine learning model tailored specifically for forecasting cricket match results. The model incorporates a comprehensive array of factors, include player statistics, team performance metrics, past match data, and outside factors like weather. The significance of accurate match predictions extends beyond the realm of sports enthusiasts to impact sports betting, fantasy sports, and strategic decision-making for teams. The findings not only promise to offer a valuable tool for cricket enthusiasts but also help to the evolving spirit of sports analytics and prediction, shedding light on the intricate dynamics that shape cricket match outcomes. Metrics which are used are recall, precision, F1 score and accuracy. Additionally, feature importance analysis is performed in order to determine the critical elements influencing match outcomes. By offering an advanced data- driven method for cricket match prediction.

Keywords: Cricket match, Winning, Data Science, Prediction, Sport analytics, Naïve Bayes, , Random Forest Classifier, Support Vector, Gradient Boost Algorithm.

1 - INTRODUCTION

- Cricket a popular game, a sport celebrated for its rich history, strategic intricacies, and global fan fervour, stands as a cultural phenomenon with unparalleled appeal. In the fervent world of cricket, where every delivery, shot, and wicket unfolds in a symphony of unpredictability, the ability to predict match outcomes becomes a captivating endeavour. The exhilarating nature of the sport often propels enthusiasts into a realm of speculation and anticipation, prompting a keen interest in unravelling the complex factors that determine the fate of a match.
- Cricket betting involves placing wagers on the outcomes of cricket matches or specific events within a match. It is significant aspect of the sports in betting industry, and the amount of money involved can be substantial –

Popularity and Global Reach: Cricket betting is immensely popular, especially in cricket-loving nations such as India, Pakistan, England and many other countries. The global nature of cricket, with international matches, domestic leagues, and tournaments which are worldly famous like the Indian Premier League (IPL).

Types of Bets: Cricket betting offers a variety of wagering options. Common types of bets include match outcome (win, lose, or draw), series winner, top run-scorer, top wicket-taker, total runs in an innings, and more.

Online and In-play Betting Platforms are also available in today's time. This dynamic form of betting adds to the excitement and can lead to a surge in betting activity during key moments of a game.

- There is more to the importance of cricket match prediction than meets the eye. As cricket enthusiasts and sports analysts keenly assess team dynamics, player performances, and contextual factors, the demand for more accurate and informed predictions has risen. Machine learning, a subclass of artificial intelligence, has changed sports analytics by giving sophisticated tools to get useful insights from huge and complex datasets. The fusion of cricket and machine learning has the potential to improve the fan experience and change how cricketing ecosystem makes strategic decisions

2 – OBJECTIVE

Objective and goal of the research paper is to prepare well-engineered machine learning model which is suitable for calculating cricket match results. The goal is to deeply investigate the complex elements that impact match results by using advanced computational techniques to find patterns and connections in the data. An accomplished model like this could add to the ever-growing field of sports analytics, provide cricket fans with insightful information, and help teams make strategic choices

Significance of the Study:
This study's importance is originated from its wider consequences for sectors associated to cricket as well as its ability to improve match forecasts. Reliable guessing have the potential to drive new earning streams and channels for participation for fantasy sports leagues, advertising, and betting markets. In order to improve player

choices, improved strategy, and obtain a competitive edge in the ever-changing cricket competition scene, teams and coaches can also make use of predictive information.

3 – LITERATURE REVIEW

NB – Naïve Bayes
RFC – Random Forest Classifier KNN – K-Nearest Neighbour DTR – Decision Tree Regression LR – Logistic Regression

TITLE OF THE PAPER	DATASET USED	PARAMETERS USED FOR PREDICTION	MACHINE LEARNING USED	BEST ALGORITHM
1. Sport analysis for cricket game results using machine learning[1]	https://www.kaggle.com/	Precision and Recall	NB, RFC, KNN	KNN
2. Cricket match outcome prediction using Machine Learning[2]	https://www.espncricinfo.com/	Accuracy	DTR, RFC, NB, LR	DTR
3. Winner prediction in one-day International cricket match using ML Framework[3]	https://www.espncricinfo.com/	Precision, Recall, F1 score, Mean Square value	LR, NB, KNN, XgBoost	LR
4. Prediction of IPL match outcome using ML Technique[4]	https://www.kaggle.com/	Accuracy	RFC, LR, KNN	RFC
5. Cricket team prediction using ML Technique[5]	https://www.espncricinfo.com/	Precision	DTR, RFC	RFC
6. The Cricket winner prediction with application of ML and Data Analysis[6]		Regularization Parameter	NB, DTR, XgBoost	DTR
7. Analysis and winning prediction in T20 Cricket using Machine Learning[7]	https://www.kaggle.com/	Accuracy, Confusion Matrix	RFC, KNN, DTR, NB, LR	RFC
8. Predicting match winner using machine learning[8]	https://www.espncricinfo.com/	Accuracy	SGD Regression, KNN, LR, DTR, NB	NB
9. Predicting results of IPL T20 matches using Machine Learning[9]	https://www.espncricinfo.com/	Precision, Recall, F1 score,	NB, LR, GBC, RFC, DCT	NB
10. Cricket match outcome prediction using machine learning[10]	https://www.kaggle.com/ https://www.espncricinfo.com/	Accuracy	DTR, LR, Support Vector	DTR

4 – RESEARCH METHODOLOGY

I. METHODOLOGY USED:

To do this, a comprehensive method has been created that entails gathering data, preparing it, and using a machine learning algorithm. Numerous factors are considered in this study, including individual statistics, team performance metrics, data from prior games, and environmental factors like the weather. Because it was trained on a carefully selected dataset, the selected machine learning technique, [insert algorithm name], is well suited to handle the complexity of cricket data.

II. DATASET:

A cricket match dataset is a systematic collection of data that records various game-related features and statistics | Research, analysis, and statistical model building are all areas where these datasets are used. A cricket match dataset has the following common parts:

- **Match Information:** Include information about the participating teams, as well as the location, date, and time of the match
- **Player Information:** Details about the players who play in the game are included, including their names, positions (for example, bowler, batsman, etc.), and teams they belong to.

- **Innings Data:** Describes every inning of the game, including how many runs scored, how many wickets taken, how many overs bowled, and other relevant information for every team
- **Batsman Statistics:** Provides individual statistics for each batsman, including runs scored, balls faced, number of boundaries, strike rate, and duration of their innings.
- **Bowler Statistics:** Includes information about each bowler's performance, like how many overs they bowled, how many wickets they took, how many runs they conceded, etc.
- **Fall of Wickets:** Specifies when each wicket fell, the runs scored at the time, and the batsman dismissed.
- **Match Outcome**: Indicates the result of the match, whether it's a win, loss, or draw.

The Dataset is been used from the website which is known as KAGGLE [11][12]which includes a set of Rows & Columns:

For Eg: The TestDeliveries contains 31795 rows by 21 columns & 118667 rows by 21 columns. The Trainmatches contains 501 rows by 14 Columns.

The Dataset has the data for 500 matches including 11 Teams From the year 2008-2014 and also year 2017.

III. MACHINE LAERNING ALGORITHMS:

1 - GAUSSIAN NAIVE BAYES

This variant is particularly useful when working with continuous data or features that can be reasonably modelled by a normal distribution. Gaussian Naive Bayes is a upper version of the Naive Bayes algorithm tailored for datasets with continuous features assumed to follow a Gaussian distribution. While it makes simplifying assumptions, it can be effective in certain scenarios, especially when the data conforms reasonably well to the Gaussian model.

Gaussian Naive Bayes assumes that the continuous characteristics inside each class have a normal distribution which indicates that a bell-shaped curve, or Gaussian distribution, can be used to characterise the probability distribution of each attribute for a particular class.

2 - DECISION TREE REGRESSION

DTC predicts continuous values which is useful for regression applications. Unlike Decision Tree Classification, which is meant for categorical outcomes, Decision Tree Regression predicts a continuous target variable Decision Tree forms a tree-like structure with each leaf node delivering the outcome and each inner node indicating which is based on a feature

Tree Organisation:
Root Nodes: Depicts both the feature that leads to the optimal split and the complete dataset.

Internal Nodes: Respond to choices made in light of particular characteristics.

Leaf Nodes: Show the expected result (regression coefficient).

3 - SUPPORT VECTOR CLASSIFIER

Used for classification problems. Finding the boundary that splits the data into as many classes as possible while optimizing the classes spacing is an SVC's main goal. Support vectors are data points near the decision boundary. The margin is the area that divides the decision boundary from these support vectors

Backing when working with high-dimensional feature spaces or in situations where the data cannot be separated properly line wise, the Vector Classifier technique proves to be highly effective.

4 - RANDOM FOREST CLASSIFIER

It is a tree-based model family member and an ensemble learning algorithm. It builds several decision trees during training and creates a class. Random Forests are well-liked, flexible, and well-known for their exceptional accuracy and durability. They are widely used in practice and are particularly well- suited for complex classification jobs and workloads involving high-dimensional data.

5 - GRADIENT BOOST ALGORITHM

Gradient Boosting is a group learning approach that combines weak learners' predictions. Applications combining both regression and classification benefit greatly from it. The Gradient Boosting Machine (GBM) and its variants, LightGBM, CatBoost, and XGBoost, are the most popular gradient boosting implementations.

Gradient boosting is a powerful and popular technique in machine learning. Variations of gradient boosting, including as XGBoost, LightGBM, and CatBoost, have further improved gradient boosting's is very useful in the real world application.

6 – LOGISTIC REGRESSION ALGORITHM

Logistic regression uses statistical technique which is used for binary classification tasks, such as those containing categorical output variables with two classes (0 or 1, True / False, Yes / No). Rather than being used for regression, logistic regression is utilised for classification.

5 – RESULT AND DISCUSSION

A - Metrics Used for Model Performance: To begin, list the performance metrics that were employed to assess your machine learning model. Accuracy, precision, recall, F1-score are measures for classification jobs.

B: Comparing with Baseline - Showcase the performance metrics of your ML model next to those of any baseline models or straightforward heuristics you may have.

C – Predictive Insights - Provide a few examples of predictions made by your model, especially cases where the model performed exceptionally well or poorly.

D – Discussion of Challenges - Discuss any challenges encountered during data preprocessing, feature engineering, or dealing with missing data.

The Toss winning prediction was also found as 56.3% as YES and 43.7% as NO, which means the toss winning is more than losing the toss.

This are the results for the Dataset with have been run into the following algorithms, to find the most accurate percentage for the cricket match winning prediction,

ALGORITHM USED	ACCURACY
Support Vector Classifier	60.0%
Decision Tree Regression	81.0%
Gaussian Naïve Bayes	91.0%
Random Forest Classifier	88.0%
Gradient Boost Algorithm	91.0%
Logistic Regression	84.0%

The results suggest that Gaussian Naïve Bayes and the Gradient Boost Algorithm performed well with accuracies of 91.0%. These models might be suitable for the given task, depending on other considerations such as interpretability, computational efficiency, and the nature of the data. Random Forest Classifier also demonstrated strong performance with an accuracy of 88.0%, highlighting its capability to handle complex relationships and reduce overfitting. Decision Tree Regression and Logistic Regression achieved moderate accuracies (81.0% and 84.0%, respectively) and could potentially be improved with further optimization or the use of more advanced techniques. The Support Vector Classifier had the lowest accuracy at 60.0%, indicating that its linear separation might not be well-suited for the data. Adjusting hyperparameters or studying non-linear kernels may improve its performance

6 – CONCLUSION

We have explored and evaluated a number of algorithms in order to identify their efficacy in this difficult task. Our goal is to use machine learning to predict cricket match winners. These models' diverse results have revealed their strengths and shortcomings

To analyse and predict the MATCH winner, various branches of data science have been combined. To predict the winner, a number of machine learning models have been used on certain features, and the results were outstanding

Gaussian Naïve Bayes and the Gradient Boost Algorithm emerged as top performers, achieving an impressive accuracy of 91.0%. These algorithms demonstrated a robust ability to make the patterns easy to calculate the predictions. The Support Vector Classifier faced challenges, yielding the lowest accuracy at 60.0%, suggesting that linear separation may not be optimal for the given data. The implications of successful machine learning

ISSN 2394 - 7780

models in this domain extend to sports analysts, teams, and enthusiasts, providing valuable insights for strategic decision-making. As the field evolves, these predictive models can contribute to a deeper understanding of team dynamics, player performance, and the cricket matches' ever-changing scene. Finally, the journey of predicting cricket match winners using machine learning is an ongoing study that may have useful applications in sports analytics in the real world.

7 - REFERENCES

1. Kumash Kapadia, Hussein Abdel-Jaber, Fadi Thabtah, Wael Hadi, “Sport analytics for cricket game results using machine learning: An experimental study”, 2019, Applied Computing and Informatics Vol. 18 No. 3/4, 2022 pp. 256-266 Emerald Publishing Limited e-ISSN: 2210-8327 p-ISSN: 2634- 1964 DOI 10.1016/j.aci.2019.11.006.

2. Pallavi Tekade , Kunal Markad, Aniket Amage, Bhagwat Natekar, “CRICKET MATCH OUTCOME PREDICTION USING MACHINE LEARNING”, 2020, INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS.

3. Manoj Ishi, Dr. Jayantrao Patil, Dr. Nitin Patil, Dr. Vaishali Patil, “WINNER PREDICTION IN ONE DAY INTERNATIONAL CRICKET MATCHES USING MACHINE LEARNING FRAMEWORK: AN ENSEMBLE APPROACH”, 2022, Indian Journal of Computer Science and Engineering (IJCSE).

4. Srikantaiah K C1,* , Aryan Khetan1 , Baibhav Kumar1 , Divy Tolani1 , Harshal Patel, “Prediction of IPL Match Outcome Using Machine Learning Techniques”, 2021, Proceedings of the 3rd International Conference on Integrated Intelligent Computing Communication & Security (ICIIC 2021).

5. Nilesh M. Patil, Bevan H. Sequeira, Neil N. Gonsalves, Abhishek A. Singh, “CRICKET TEAM PREDICTION USING MACHINE LEARNING TECHNIQUES”, Fr. Conceicao Rodrigues College of Engineering, Mumbai, Maharashtra, India.

6. Daniel Mago Vistro, Faizan Rasheed, Leo Gertrude David, “The Cricket Winner Prediction With Application Of Machine Learning And Data Analytics”, 2019, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 8, ISSUE 09, SEPTEMBER 2019 ISSN 2277-8616.

7. Shristi Priya, Ankit Kumar Gupta, Atman Dwivedi, Aryan Prabhakar, “Analysis and Winning Prediction in T20 Cricket using Machine Learning”, 2022, 022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) | 978- 1-6654-1120-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICAECT54875.2022.9807929.

8. Rushikesh Bhor, Ajay Jagdal , Shubham Pisal, Rohit Korke, “Predicting Match Winner Using Machine Learning”, January 2022| IJIRT | Volume 8 Issue 8 | ISSN: 2349-6002.

9. Shilpi Agrawal, Suraj Pal Singh, Jayash Kumar Sharma, “Predicting Results of Indian Premier League T-20 Matches using Machine Learning”, 2018, 8th International Conference on Communications Systems and Network Technologies-978-1-5386-5956-4/181$31.00 2018I EEE DOI: 10.1109/CSNT.2018.15.

10. P. Manikiran, N. Sri Ram, K.V.V. Abhilash, A. Vamsi Krishna, Prof. Mohammed Zabeeulla A N, “Cricket Match outcome prediction using Machine learning techniques”, 2022, ISO 3297:2007 Certified□□Impact Factor 7.39□□Vol. 11, Issue 6, June 2022 DOI: 10.17148/IJARCCE.2022.11619.

11. **https://www.kaggle.com/code/robinreni/cricket-winner-prediction**

12. **https://www.kaggle.com/code/robinreni/cricket-winner-prediction/input**

ISSN 2394 - 7780

OPTIMIZING TRAVEL ITINERARY PLANNING USING A* ALGORITHM

Manisha Divate and Krupa Panchal
Department of Information Technology, SVKM's Usha Pravin Gandhi College of Arts, Science and Commerce, Maharashtra, Mumbai-400056

ABSTRACT
*Travel itinerary planning has been a crucial aspect of the modern world of travel, combined with an efficient algorithm that proves to be essential for providing users with optimal routes and detailed itineraries. Better algorithms are vital for creating travel itinerary plans in the modern era. Maximum routes and schedules are needed for the fastest routes and schedules to be provided to the users. Users demand creative route plans to be devised using their budget, time limits, and interrogations. This paper presents a complete system for creative travel itinerary plans. This system makes use of a travel dataset of a variety of node locations with viable modes of commutation and costs. The A * Pathfinding Algorithm and constraint satisfaction under the user's jurisdiction are used by the system. User-supplied details such as starting and ending locations, durations, budgets, and interrogation results are generated using a console interface. The system uses these inputs to generate unique travel plans based on user requirements in terms of budget, time and other constraints. The effectiveness of this model can be gauged through the use of such metrics as adherence to itinerary costs, user satisfaction feedback and efficiency of travel time. Comparing our travel planner with the existing ones and with diverse real-world user studies our system can be enhanced and evaluated. This will make sure to provide users with a solution that is adaptable and flexible, allowing them to create their personalized travel itinerary that best fits into their financial capabilities, free time availability and personal interests. Literature survey in this research suggests that A* algorithm outstands the travel optimized performance making it suitable for problem solving in travel industry. This research presents key findings, potential research direction and the overall impact of the algorithm leading to enhancement in the overall trip design process.*

INTRODUCTION
Travel Itinerary planners has become a crucial component for this modern travel era, where user looks for easy and efficient ways to get around with diverse destinations. With the ever increasing demand in technological advancements and availability of travel options there is significant rise for an optimized, effective and efficient travel itinerary planner. Planning a system that involves intricacies such as selecting optimal routes, minimizing travel time and considering various factors that lead to users travel satisfaction. The complexity of travel itinerary route is a challenging problem for creating an itinerary generator system. Using traditional methods it is complex to play with large datasets to find optimized travel route. Advance algorithms can be used to solve this problem and to improve efficiency and efficacy of travel itinerary planning system. Existing systems studies gap in finding such type of systems. A detailed approach is required to cope up with this problem and meet up users travel expectations.

The purpose of this study is to overcome the limitations of state-of-the-art travel itinerary planners. Hence, the purpose of this study is to find a smart and optimized solution that helps users with their unique travel itineraries based on their budgets, time available and their preferred attractions, experience, and travel style. An efficient travel planning tool is the fundamental need of anyone who plans on traveling. There are several tools online that can help you book your flight tickets, hotel booking and rental cars but none of these tools seem to have the answer to major headache-breeding problem of online travel planners and while it might not seem like a huge problem, not getting the information that is best suited to your travel itinerary can ultimately decide your entire experience. The goal of this study is to develop a travel itinerary planner using A* algorithm. This algorithm is a graph based search algorithm that aims to find a path between a specified start state to a destination target state. Secondly, it reduces gaps and may choose a slightly more optimized path. Lastly it will choose the least expensive path by finding the edges with the edge weights that minimizes the accumulated costs. The research aims to design a new system for optimising travel itineraries that could overcome known limitations and provide bespoke travel experiences. Such research takes into account the complexity of user constraints and preferences resulting in a multifaceted approach that leverages data, efficient algorithms and intelligent user interaction. The ultimate goal here is to contribute to the advancement of travel planning algorithms, enhancing the overall travel experience for users.

LITERATURE SURVEY
This systematic literature review comprehensively surveys the A* search algorithm's present role in pathfinding, offering insights into its strengths, limitations, and evolving applications. It addresses challenges

ISSN 2394 - 7780

faced by the traditional A* algorithm in meeting the demands of contemporary pathfinding problems, particularly as grid sizes increase. Despite the aging nature of the classic A* algorithm, improved derivatives like HPA* prove capable of keeping up with modern demands. The review suggests that HPA*, with its remarkable speed and relatively low overhead cost, could emerge as a new default option for certain pathfinding challenges. The improved variants of A*, incorporating modifications like hash tables and refined heuristics, are highlighted as crucial for the algorithm's future development in addressing complex problems and sustaining efficiency [1]. The paper discusses the development of an Intelligent Travel Planning System using the A-star algorithm, aiming to overcome limitations in current trip planning systems. The proposed system aims to overcome these challenges by considering both urban and inter-city traffic and providing detailed and user-friendly travel plans. The model generates three complete route planning schemes that are “most time-saving” and “most Save money and "most comfortable", catering to different travel requirements. Data construction and storage in the system, outlining the system's execution flow is discussed. The paper introduces design ideas of the heuristic function and the cost function in the A-star algorithm and its influence on the system planning process. In conclusion, the intelligent travel planning system leverages the A-star algorithm to connect city and intercity transportation networks efficiently. [2] This paper investigates the application and comparison of Dijkstra's and A-star algorithms for finding the shortest path, focusing on route selection among 24 gas stations (SPBU) in Medan City. Dijkstra's, a greedy algorithm, ensures an optimal path but at the cost of longer search times, contrasting with A-star, a best-first search algorithm that offers faster results but may not always yield an optimal solution. The study assesses the advantages and disadvantages of both algorithms, particularly in the context of route optimization, using a directed graph representation of SPBU locations. The practical implications of these findings in solving the shortest path problem, demonstrate that both algorithms successfully address the task but may produce different routes and total distances in specific cases. The paper concludes by highlighting the faster running time of A-star, aligning with its heuristic-driven approach, and the comparable algorithmic complexity of Dijkstra's and A-star.[3] The paper introduces an Enhanced Hybrid path-planning algorithm, combining the Artificial Potential Field (APF) algorithm with the A-star path-planning technique to overcome the local minimum challenge in traditional APF. Overall, the hybrid algorithm presents a promising solution for efficient mobile robot path planning in dynamic environments. Two cases are presented:

Table 2.1: Comparison of Algorithm [4]

	Algorithm	Time	distance
Case I	A-Star	1.163 s	929 unit
	the Traditional APF	0.032 s	669.7 unit
	the Modified APF	0.046 s	669.7 unit
Case II	A-Star	2.084 s	951 unit
	the Traditional APF	-	-
	the Modified APF	1.621 S	748.4 unit

The experiments reveal that the proposed Enhanced APF outperforms A-star in terms of time and distance, reaching an optimized path to the goal 50% faster compared to A-star[4]. Additionally, it avoids the local minimum issue faced by traditional APF, demonstrating its effectiveness in overcoming the limitations of both traditional APF and A-star.[4] Path Planning problem using an Improved A-star Algorithm paper states that the evaluation criterion is the ability to generate shorter paths, especially in situations where the traditional A-star falls short. Simulation and Validation give details of the proposed algorithm's validity and feasibility are assessed through simulations. Improved A-star algorithm successfully mitigates the identified issue in certain path planning scenarios, providing more efficient and shorter paths compared to both the traditional A-star and its competitors. Overall, the research contributes to the field of robotics path planning by offering an innovative algorithm that addresses shortcomings in the traditional A-star approach, particularly when it comes to ensuring the shortest paths under specific conditions. [5]

An innovative approach is introduced by Interactive itinerary Planning to personalize travel planning by incorporating user feedback in an iterative process. Addressing the challenges of selecting Points-of-Interest (POIs) and constructing itineraries, the Optimal Itinerary Construction and POI Batch Selection Problems, proving NP-completeness. Real-time heuristic algorithms efficiently compute itineraries, validated through extensive experiments on real datasets. By utilizing Hamiltonian paths within hypercubes and utilizing a streamlined heap-based data structure for point of interest (POI) pruning, improving the computational speed and scalability of the heuristic algorithms in real-time. In addition to proving NP-completeness for key problems, a probabilistic model for computing expected scores is presented, particularly in the context of set semantics. [6] Trip planning route optimization with the operating hour and duration of stay constraints, suggests a solution that goes beyond the standard Traveling Salesman Problem (TSP) algorithm by taking into consideration practical limitations such as location hours and length of stay at each station[7]. To account for real-world travel, it leverages the Google Maps Directions API. The simulation's findings in this paper demonstrate that the recommended system's overall travel time closely matches the information gleaned from the Google Maps Directions API, resulting in an itinerary that is both optimal and compliant with the parameters of operating hours and stay length. By overcoming limitations like operation hours and length of stay, by offering an offline sequencing solution without keeping maps or routes in the system, the suggested approach distinguishes out. [7] Optimization Route to various Tourism Places in West Java Using A-STAR Algorithm focuses on addressing the complexities of tourism destinations. In response, this study employs the A-STAR algorithm, that is a heuristic search algorithm, to find optimal routes influenced by factors like distance and traffic density. The research involves transforming the intricate road network into a graph and processing relevant data from government agencies to make the A-STAR Algorithm's application easier. The paper provides insights into the potential of the A-STAR algorithm in optimizing travel routes for tourists exploring West Java's diverse tourism places. [8]

Trajectory Planning of a Mobile Robot using Enhanced A-Star Algorithm[9], addresses the optimization of robot navigation through the introduction of an enhanced algorithm. The key innovation lies in the addition of a new parameter that is p(n), which is the number of turns, that contributes to the algorithm's ability to generate optimal paths. Simulation experiments conducted to evaluate the proposed Enhanced A-Star Algorithm showcase its superior performance compared to the original A-star algorithm, particularly in reducing the elapsed time of travel. Moreover, they suggest future enhancements to adapt the algorithm for dynamic obstacle scenarios in unknown environments and real-time implementation using autonomous mobile robots. This study adds to the ongoing efforts to improve trajectory planning for mobile robots in a variety of circumstances in terms of efficiency and effectiveness. [9] A Tourist Itinerary Planning Approach which is based on Ant Colony Algorithm proposes an innovative approach to figure out the fastest route between cities or inside a single city for tourism resources considering comprehensive factors such as transportation, lodging, and Points of Interest (POIs) between and inside each destination. Recognizing the NP-complete nature of itinerary planning, the authors leverage the ACO algorithm to address the complexity and efficiently solve the tourist planning problem. The system aims to generate high-utility itineraries by providing multi-city plans with detailed visiting schedules and considering user-specified constraints such as starting and ending locations/times, budgets, and selected attractions. The authors emphasize the versatility of their approach in providing a generic method for creating itinerary designs both inside and between locations, offering a novel contribution to the field of automatic tourist itinerary planning. [10] ATIPS: Automatic Travel Itinerary Planning System for Domestic Areas addresses the challenges faced by Taiwanese residents in planning travel itineraries for leisure trips.[11] The system operates by allowing users to input their travel time, departure point, and destination, after which it autonomously generates a travel itinerary. The proposed algorithm integrates various factors influencing travel preferences and employs a greedy algorithm to select tourist spots based on a defined radius from the current position, ultimately creating a personalized travel itinerary. The authors conducted experiments and surveys to evaluate the effectiveness of ATIPS model. The system impressed users, with their higher satisfaction rates of 70% for outputs and 82% for preference learning. The paper positions ATIPS as a valuable tool for users who prefer self-planned trips, offering an efficient method for generating personalized travel routes. [11]

The paper "Automatic Itinerary Planning for Traveling Services" acknowledge the NP-completeness of the team orienteering TOP and propose an approximate algorithm to handle the complexity of searching for optimal itineraries. Their proposed approach overcomes new emerging points-of-interest limitations by considering multiday itineraries, allowing explicit user preferences, and efficiently handling a large number of candidate itineraries through MapReduce. This proposed approach is evaluated using real data collected from Yahoo Travel, demonstrating its ability to generate high-quality customized itineraries efficiently. A comprehensive solution to the challenging problem of automatic itinerary planning is presented, introducing a novel approach that combines graph-based modeling, MapReduce preprocessing, and an approximate algorithm for generating multiday itineraries tailored to individual user preferences. [12] The paper "Improving Mobility in Smart Cities with Intelligent Tourist Trip Planning" introduces a heuristic algorithm based on the Variable Neighbourhood Search (VNS) framework to efficiently address the combinatorial optimization challenges inherent in TTDP (Tourist Trip Design Problem).[13] The results showcase the algorithm's superiority over baseline algorithms, achieving an average error of only 0.47% within a short computational time of 30 seconds. Moreover, the algorithm demonstrates its suitability for mobile devices by efficiently producing high-quality solutions (approximately 97% accuracy) in a few milliseconds. By creating a useful mobility management platform for Barcelona, the authors evaluate the usability of the suggested model and solution algorithm that presents a novel

ISSN 2394 - 7780

mathematical model for TTDP, and provide a real-world dataset designed for MOP with a variety of graph topologies. [13] Robot Path Planning based on improved A* Algorithm addresses the computational challenges in the traditional A* algorithm when traversing OPEN and CLOSED tables. By accessing array elements through a single operation, which locates the number ranks each time a specified element is visited, the improved A* algorithm significantly reduces operating time compared to the original algorithm. The survey highlights the maturity of the A* algorithm and the common strategies employed to enhance its efficiency, including reducing algorithm running time and optimizing storage space. The experimental results are demonstrating an over 40% increase in operating efficiency for the improved A* algorithm while noting that the impact on shortest path optimization is not explicitly evident. [14] A* algorithm used for finding the shortest path addresses the study of places that particularly focus on heuristic search, categorizing it into A* algorithm, Dijkstra algorithm, ant colony algorithm and genetic algorithm. The author argues that Dijkstra's algorithm, while a typical method for searching the shortest path, is less efficient due to the need to traverse many nodes. In contrast, the A* algorithm, characterized by its heuristic nature, reduces the number of nodes searched through heuristic functions, thereby increasing search efficiency. Renhao et al. (2015) support the assertion that heuristic search, by simulating the human brain's cognitive model, significantly improves search efficiency compared to traditional methods. The A* path planning algorithm incorporates the raster method to model environments. The results confirm that the A* algorithm performs exceptionally well in enabling faster robot obstacle avoidance path planning. [15]

Tourist itinerary planning is a complex problem known in the literature as the Tourist Trip Design Problem provides a systematic review in the field of Operations Research[16]. The predominant focus here is on single-objective problems (67.64%), with time windows and simultaneous planning for multiple routes being recurrent variants. The study here found that Iterated Local Search (ILS) and Greedy Randomized Adaptive Search Procedure (GRASP) are the go-to methods among heuristic and metaheuristic techniques.[16] The authors emphasize the efficiency of memetic and hybrid algorithms, demonstrating superior solutions and computational times compared to traditional algorithms like Tabu Search, Variable Neighborhood Search, Great Deluge, Ant Colony Optimization, and ILS. Notably, they acknowledge the role of optimal solutions obtained with CPLEX for certain instances, serving as benchmarks for algorithmic comparisons. [16]. A Survey on Tourist Trip Planning Systems presents the features and functionalities considered by authors that include personal interest estimation, POI selection, path routing, required POIs, dynamic trip plan recalculation, multiple-day trip planning, POI opening hours, budget constraints, and weather dependency. Some features, such as Max n Type and Mandatory Types in POI selection planning services, as well as weather and current time in context dependency planning features, are not considered by any of the systems. To set themselves apart, travel planners should concentrate on adding these absent qualities. The authors propose considering trip cost as an upper limit or as a soft constraint, allowing for an optimal cost trip within a budget. [17] Design of a Travel Itinerary Planning System Based on Artificial Intelligence addresses that existing systems predominantly rely on travel agencies for planning results, excluding users from the decision-making process. The survey delves into the existing landscape of intelligent travel itinerary planning systems, analyzing their main relevant statuses. It also explores the market development trends and identifies the shortcomings that the proposed AI-based system aims to address. This comprehensive review informs the establishment of system requirements for the AI-based travel itinerary planning system, laying the foundation for the overall design and detailed implementation. The paper then proceeds to present the prototype of the system and validate its feasibility through performance tests.[18] A Genetic Algorithm for Generating Travel Itinerary Recommendation with Restaurant Selection addresses the proposed solution that employs a Genetic Algorithm (GA) to effectively address this challenge[19]. Utilizing Google Maps for visualization, the authors demonstrate the algorithm's success in perfectly planning each tourism place during its opening hours and scheduling each restaurant within appropriate meal times. The generated itinerary also recommends a set of locations with a high total utility value. The authors states that their developed algorithm satisfactorily solves the travel itinerary planning problem, meeting the specified constraints and producing high-quality travel plans.[19] The development of Travel Itinerary Planning Application using the Travel Salesman Problem and K-Means Clustering Approach addresses the approach that involves two key steps: macro grouping using k-means clustering to organize tourist destinations for each day and micro tour arrangement using the TSP to minimize the total travel distance. The results indicate successful clustering and optimization, with destinations grouped closely together and an optimal order of visitation. The authors acknowledge the need for further improvements to enhance application speed and handle additional constraints. The paper contributes to the field of travel enhancement, showcasing the potential of AI-based algorithms in optimizing travel plans.[20] Comparative Analysis of Pathfinding Algorithms namely A*, Dijkstra, and BFS on Maze Runner Game provides a thorough exploration of the Maze Runner game that involves players creating mazes and obstructing NPC paths using Tetris-like blocks, necessitating efficient pathfinding algorithms.[21] The research methodology adopts a comparative test across three different levels, measuring process time, path length, and the number of blocks that are involved in the computation process for each algorithm. The paper underscores the critical impact of algorithm selection on various aspects of the game, including computing processes, memory usage, and computing time. The comparison of A*, Dijkstra, and BFS, coupled with the applied methodology, enhances our understanding of algorithmic efficiency in gaming applications[21]. Table 2.1 below shows the listings of online application that produces the itineraries of the trip and display budget traveling, suggest places names, gives hotel recommendations but there are still gaps in the existing works, that is the shortest route to travel is not known. If the shortest path is known it will be beneficial to take a tour with additional user preferences which will help user find perfect personalized travel planner Itinerary. Aim here is to find optimized route for Travel Itinerary.

Table 2.1: Comparision of Existing travelling models

APP NAME	INPUT	OUTPUT	DESCRIPTION	Trip Itinerary
MakeMyTrip [22]	Destination, travel dates, preferences (flight class, hotel type).	Flight options, hotel suggestions, holiday packages.	Flight and hotel search algorithms, dynamic packaging for holiday deals.	YES
TripAdvisor [23]	City or attraction name	Reviews, ratings, photos, and information about hotels, restaurants, attractions, and activities	crowdsourced reviews and ratings from travelers to provide recommendations and insights into local experiences.	YES
Kesari [24]	Destination, Travel dates	Itinerary, Meal, Budget, Travel Plces, Ways to travel	Kesari is a travel app engaging millions of users with advanced-level functionalities across the user community. It is loaded with features that empower the application interface and the online market image.	YES
GetYourGuide [25]	Destination, interests	Tours, activities, and experiences in various cities, allows booking and managing tickets	Connects travelers with local tour operators and activity providers.	YES
Goibibo [26]	Destination, travel dates, preferences.	Flight and hotel options, bus, and train tickets.	Incorporates various search algorithms, real-time booking updates.	YES
Yatra [27]	Travel details, preferences, package inclusions.	Customized travel packages, booking options.	Integrates advanced algorithms for package customization.	YES
Google Maps [28]	Location, destination, mode of transportation (optional)	Directions, estimated travel time, traffic updates, points of interest (POIs), reviews, photos. [28]	Uses GPS and map data to provide turn-by-turn navigation, real-time traffic conditions, and information about local businesses and attractions. [28]	YES
Kayak [29]	Locations, travel	Tour Packages, Hotel	Find top deals &	YES

	dates	accomodations, Flight or Travel bookings,	manage trips seamlessly - flights, hotels, cars, security times & maps, all in one app. One-stop shop for trips	
Sygic Travel [30]	Dates, No.of hours or days	Location, Images, Budget, Ways to travel, Guide	Collaborative city guides offer a user-friendly and concise overview of popular destinations around the world, compiled through collective contributions.	YES
Cleartrip [31]	Travel details (flights, hotels, trains), preferences.	Booking options, itinerary details.	Uses algorithms for real-time availability checks, fare predictions.	YES
IRCTC Tourism [32]	Travel Destination, Domestic	Travel Itinerary, Package, Travel ways, Budget	To promote domestic tourism, IRCTC Tourism is launching affordable online package booking options, making travel within India more accessible.	YES
Tourism of India [33]	Destination, No.of people, departure from, travel dates,additional information	Trip Itinerary, Packages details	A comprehensive India travel planner encompassing must-see attractions, diverse destinations, detailed transportation information, and optimal travel timing recommendations.	YES
Booking.com [34]	Destination, travel dates, number of guests	Accommodation options (hotels, apartments, hostels, etc.), prices, availability, reviews, photos	Aggregates listings from various accommodation providers and allows users to compare prices and book directly through the app.	YES
Airbnb [35]	Destination, travel dates, number of guests	Unique accommodation options (apartments, houses, rooms, etc.), prices, availability, reviews, photos	Matching algorithms pair users' preferences with relevant listings based on various criteria.	YES

METHADOLOGY

Comprehensive datasets here include various elements such as location details, time estimates, travel options, accommodation details and distance matrix that maps distances between locations enabling efficient route mapping. To curate this rich dataset, we relied on trustworthy sources like Google Maps, travel applications and tourism websites available, travel blogs, user reviews on the web and other online travel agencies. After collecting Data it needs to be structured, and then this data undergoes rigorous cleaning to address inconsistencies, missing values and outliers. Data is pre-processed and formatted to meet compatibility with the

A* algorithm, which ensures it encapsulates the parameters that are crucial for crafting travel itinerary problems. Using inputs such as start and end destinations, travel time taken, estimated budget, preferred travel dates and additional personal preferences proposed system will generate an itinerary that seamlessly integrates user-specified constraints and preferences. Measuring success in our proposed system is not only including all the above constraints but to continuously refine our system to ensure that it delivers optimal results each time.

The heart of our proposed system lies in complex algorithmic architecture, which should be designed to navigate complicated user constraints and specified preferences. After specifying user constraints the A* algorithm steps in. For this system, we use the A* algorithm to tackle path-finding problems in travel planning. This algorithm is a graph search algorithm that aims to find a path between a specified start state to a destination target state. This algorithm simultaneously explores multiple nodes in the tree, always choosing the path to the goal that has the lowest accumulated cost. Once the travel itinerary and its associated costs graph has been created from the dynamic hierarchy, one can then use this network graph for planning a personalized travel itinerary in various ways. The first type of planner simply includes those edges with the least cost and returns a complete path from start to finish. The second type reduces gaps and may choose a slightly more optimized path. The final type will be chosen as the least expensive by finding the edges with the edge weights that minimize the accumulated costs. Using the pre-processed distance matrix as a guide, these pathfinding algorithms determine the best order of places to cut down on travel time while still honoring user preferences for the route that is chosen. Algorithm working takes place in a sequential and well-coordinated manner ensuring that the itinerary generated not only meets user constraints but aslo reflects personalized travel aspirations.

The effectiveness and reliability of our proposed itinerary system undergo validation and evaluation process to assess the models performance and identify potential areas for enhancement. Validation takes place within the varied key parameters that are budget, time, distance and other preferences within a reasonable range and observes their impact on the generated itineraries. This analysis that takes place helps to understand the models responsiveness to the user input and identify the key potential vulnerabilities. Travel experts can be consulted to compare systems-generated itineraries against the manually crafted plans for specific scenarios by the domain. Qualitative assessments can offer critical insight into the models capability to generate travel plans that are both realistic and feasible. User studies need to be conducted with real travelers, inviting them to provide feedback for the generated itinerary based on their overall experience and preferences. This type of user-centric evaluation can help us gauge the system effectiveness and also help in identifying areas for improvement in terms of usability and user satisfaction.

Travel itinerary system can be evaluated based on qualitative metrics that is itinerary adherence, travel efficiency, user satisfaction and quantitative metrics include expert feedback and user comments. The itinerary generated can be evaluated by measuring the degree to which it meets specified user constraints such as travel duration, money, number of locations of the trip. Further measuring the time taken and the distance between destinations can determine the effectiveness of the route displayed. User feedback can be generated through surveys and questionnaires, quantifying their satisfaction with the generated itinerary preferences and overall experiences. This qualitative feedback can be analyzed by travel experts to identify recurring patterns and areas where our model performance can be further enhanced. User feedback for our model can be analyzed to learn specific issues that user faces, recommendations and overall enhancements that can be taken into consideration with an emphasis of usability, intuitiveness and the ability to store various travel preferences should be highly prioritized.

EXPECTED RESULTS

An optimized Itinerary system proposed aims to generate day-wise itineraries that depend upon factors like Time taken to travel between two destinations, ensuring our system gives an optimized route that is also efficient in utilizing travel time. Users will here be provided with options for customized inputs which include preferences and constraints that enable the system to generate personalized itineraries specifically for their needs. The aim here is to generate a realistic and well-structured itinerary that should reflect the diversity of user preferences and their personal interests. Improvements in personalization, Interface Design and ensuring a user-centric approach are the ways which will be tackled by collecting valuable feedback from users. The itinerary generator will be manually tested and evaluated by travel experts to assess the system's performance and effectiveness in meeting the demands of users.

CONCLUSION

This research aims to propose an optimized itinerary generator that effectively addresses user constraints and incorporates their preferences. By incorporating a comprehensive dataset, an efficient path-finding algorithm, and a user-friendly interface we achieve a model which prioritizes users budget, traveling time, and personal interests to make it a valuable tool for planning a trip. This system offers the potential to fundamentally transform the travel experience which contributes to technological advancement. Travel will be seen in a whole new light for users who will be equipped with customized itineraries based on their own requirements and preferences.

REFERENCES

[1] Foead, Daniel, et al. "A Systematic Literature Review of A* Pathfinding." Procedia Computer Science, vol. 179, 2021, pp. 507-514. ISSN 1877-0509

[2] Zhou, Yicheng, and Xiaoyu Cheng. "Intelligent Travel Planning System based on A-star Algorithm." IEEE Xplore, 2020, doi: 10.1109/ICISCE50825.2020.00057.

[3] Candra, Ade and Budiman, Mohammad Andri. "Dijkstra's and A-Star in Finding the Shortest Path: a Tutorial." Proceedings of the 2020 International Conference on Data Science, Artificial Intelligence, and Business Analytics (DATABIA), 2020.

[4] Abdel-Rahman, Ahmed S., and Sherief Nafea. "Enhanced Hybrid Path Planning Algorithm Based on APF and A-Star." The International Archives of the Photogrammetry Remote Sensing and Spatial Information Sciences, December 2023.

[5] Ju, Chunyu, et al. "Path Planning Using an Improved A-star Algorithm." Proceedings of the 11th International Conference on Prognostics and System Health Management (PHM-2020 Jinan), 2020.

[6] S. B. Roy, G. Das, S. Amer-Yahia, and C. Yu, "Interactive Itinerary Planning," Univ. of Texas Arlington, Yahoo! Labs, Google Research, 2015. [Online]. Available: https://arxiv.org/abs/1502.00336

[7] W. C. Chia, L. S. Yeong, F. J. X. Lee, and S. I. Ch'ng, "Trip planning route optimization with operating hour and duration of stay constraints," in 2016 11th International Conference on Computer Science & Education (ICCSE), Nagoya, Japan, 2016, pp. 7581613. doi: 10.1109/ICCSE.2016.7581613.

[8] M. H. P. Yudha, S. Supian, and H. Napitupulu, "Optimization Route to Tourism Places in West Java Using A-STAR Algorithm," CAUCHY –Jurnal Matematika Murni dan Aplikasi, vol. 7, no. 3, pp. 464-473, 2022, doi: 10.18860/ca.v7i3.17032.

[9] P. Sudhakara and V. Ganapathy, "Trajectory Planning of a Mobile Robot using Enhanced A-Star Algorithm," Indian Journal of Science and Technology, vol. 9, no. 41, pp. 1-6, Nov. 2016, doi: 10.17485/ijst/2016/v9i41/93816.

[10] L. Yang, R. Zhang, H. Sun, X. Guo, and J. Huai, "A Tourist Itinerary Planning Approach Based on Ant Colony Algorithm," in Proceedings of the IEEE Conference on Computer Science and Engineering (CSE), 201X, pp. 400.

[11] H.-T. Chang, Y.-M. Chang, and M.-T. Tsai, "ATIPS: Automatic Travel Itinerary Planning System for Domestic Areas," in Proceedings of the IEEE International Conference on Data Engineering (ICDE), 2016, Article ID 1281379. DOI: 10.1155/2016/1281379.

[12] G. Chen, S. Wu, J. Zhou, and A. K. H. Tung, "Automatic Itinerary Planning for Traveling Services," IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 3, March 2014.

[13] P. Mrazovic, J. L. Larriba-Pey and M. Matskin, "Improving Mobility in Smart Cities with Intelligent Tourist Trip Planning," 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC), Turin, Italy, 2017, pp. 897-907, doi: 10.1109/COMPSAC.2017.144.

[14] J. Peng, Y. Huang, and G. Luo, "Robot Path Planning Based on Improved A* Algorithm," Cybernetics and Information Technologies, vol. 15, no. 2, pp. 173-186, 2015. DOI: 10.1515/cait-2015-0036.

[15] Y. Yan, "Research on the A Star Algorithm for Finding Shortest Path," Highlights in Science, Engineering and Technology, vol. 46, pp. 154-161, Apr. 25, 2023. DOI: 10.54097/hset.v46i.7697.

[16] J. Ruiz-Meza and J. R. Montoya-Torres, "A systematic literature review for the tourist trip design problem: Extensions, solution techniques and future research lines," Operations Research Perspectives, vol. 9, p. 100228, 2022. DOI: 10.1016/j.orp.2022.100228.

[17] K. Sylejmani and A. Dika, "A Survey on Tourist Trip Planning Systems," International Journal of Arts & Sciences, vol. 4, no. 09, pp. 13–26, 2011.

[18] Peilin Chen, "Design of Travel Itinerary Planning System Based on Artificial Intelligence," Journal of Physics: Conference Series 1533, 032078 (2020). doi:10.1088/1742-6596/1533/3/032078. Published under license by IOP Publishing Ltd.

[19] B. S. Wibowo and M. K. Handayani, "A Genetic Algorithm for Generating Travel Itinerary Recommendation with Restaurant Selection," in 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), December 2018, doi: 10.1109/IEEM.2018.8607677.

[20] K. N. Kholidah, S. Rani, and S. N. Huda, "A Development of Travel Itinerary Planning Application using Traveling Salesman Problem and K-Means Clustering Approach," in 7th International Conference, Feb. 2018, doi: 10.1145/3185089.3185142.

[21] S. D. H. Permana, K. B. Y. Bintoro, B. Arifitama, and A. Syahputra, "Comparative Analysis of Pathfinding Algorithms A*, Dijkstra, and BFS on Maze Runner Game," International Journal of Information System & Technology, vol. 1, no. 2, pp. 1, May 2018. DOI: 10.30645/ijistech.v1i2.7

[22] MakeMyTrip Holidays India. (2000). Retrieved from https://www.makemytrip.com/holidays-india/

[23] TripAdvisor. (2023). TripAdvisor: Read Reviews, Compare Prices & Book. Retrieved from https://www.tripadvisor.com/

[24] Kesari. (1984). Kesari. Retrieved from https://www.kesari.in/

[25] GetYourGuide. (2008). GetYourGuide. Retrieved from https://www.getyourguide.com/?cmp=brand&ad_id=77790582689305&adgroup_id=1244647642226370&bid_match_type=be&campaign_id=377198634&device=c&feed_item_id=&keyword=getyourguide&loc_interest_ms=&loc_physical_ms=116073&match_type=e&msclkid=f2794d3f31ac11fc551f28801073a43b&network=o&partner_id=CD951&target_id=kwd-77790717506301:aud-806416224&utm_adgroup=ct%3Dbrand%7Cfn%3Df1&utm_campaign=ct%3Dbrand%7Cln%3D29%3Aen%7Ctc%3Dall&utm_keyword=getyourguide&utm_medium=paid_search_brand&utm_query=getyourguide&utm_source=bing&utm_term=getyourguide&utm_content=ct%3Dbrand%7Cfn%3Df1

[26] MakeMyTrip Holidays India. (2022). Retrieved from https://giholidays.makemytrip.com/holidays-india/

[27] Yatra. (2006). Yatra Holidays. Retrieved from https://www.yatra.com/holidays

[28] Google Maps. (2005). Retrieved from https://www.google.co.in/maps/@32.2394704,77.1665202,14z?entry=ttu

[29] Kayak. (2004). Packages. Retrieved from https://www.kayak.com/packages

[30] Sygic Maps. (n.d.). Retrieved from https://maps.sygic.com/?utm_source=content

[31] Cleartrip. (2006). Flights. Retrieved from https://www.cleartrip.com/flights?utm_source=bing&utm_medium=cpa&utm_campaign=BR_Cleartrip%7CMain_E&msclkid=9f0b360aa2cb16973b9653b5b9e3b5d8

[32] IRCTC Tourism. (1999). Tour Packages. Retrieved from https://www.irctctourism.com/tourpacakage_search?searchKey=&tagType=&travelType=Domestic&sector=All

[33] Tourism of India. (n.d.). Retrieved from https://www.tourism-of-india.com

[34] Booking.com. (2000). Retrieved from https://www.booking.com/

[35] Airbnb. (2008). Retrieved from https://www.airbnb.co.in/a/discover/?account_id=31003615&campaign_id=303117718&ad_id=80951624440025&ad_group_id=1295224714906336&keyword_id=kwd-80951555865320:loc-90&device=c&c=.pi2.pk303117718_1295224714906336&ghost=true&msclkid=5107bce9b24a1f79dbf7d956794dceab&utm_source=bing&utm_medium=cpc&utm_campaign=IND%3ADTM%3ASRC%3ABRD%2BAirbnb%5BEXACT%5D&utm_term=airbnb&utm_content=Airbnb%3A%2BExact

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

UNVEILING THE SECRETS OF KEYSTROKES USING UNDER-COVER TYPING

Smruti Nanavaty and Tushar Varma
Department of Information Technology, SVKM's Usha Pravin Gandhi College of Arts, Science and Commerce
Ville Parle(west), Mumbai, India

ABSTRACT

In the modern world, information technology is developing quickly. For cyber professionals, maintaining security and privacy is a big concern. Studies indicate that the amount of newly discovered malware is rising quickly. A very sophisticated spyware known as a keylogger captures every keystroke made on the computer, giving the attacker the ability to steal vast quantities of extremely sensitive data covertly and without the owner of the message's consent. To prevent sensitive information from leaking and data loss, it's critical to identify the keylogger. Heuristics and behavior analysis are used by antivirus software to identify keyloggers; however, if the keylogger is not a known danger, antivirus or anti-malware software will not identify it as a virus. Malware may be identified with accuracy using machine learning. This study aims to identify each application's collection of of rights and storage levels and differentiate between keylogger apps that can abuse permissions and programs with appropriate access. This method of detecting keyloggers is completely opaque; it relies on common behavioral characteristics shared by all keyloggers rather than the underlying workings of the keylogger. In this study, a machine learning-based keylogger detection model has been developed to identify spyware and keyloggers. In order to detect host activity when a keylogger is operating on the system, the model has been trained using a dataset of spyware and keyloggers. In order to determine if the system was successful in detecting keylogger spyware, the findings will be assessed using a number of metrics and reported based on the classification report and confusion matrix.

Keywords: Keylogger, Malware Detection, Artificial Intelligence.

I. INTRODUCTION

Experts in data security handle dangers and challenges related to security on a daily basis. These professionals work hard to remain on top of fresh security risks as cybercriminals strive to create fresh infiltration plans and improve their methods of assault to undermine personal computers. There are an increasing number of these attackers in the world of PCs nowadays. The keylogger identifies and records what intruders do while making advancements . Keylogging programs, sometimes known as keyloggers, are malware that tracks user input from the keyboard to steal personal and confidential information [2].

Keylogging attacks, session hijacking, phishing, pharming, and visual fraudulence cannot be combated simply by en- abling encryption [3]. Keyloggers track client information from the comfort of their homes to recover personal and confidential information [4]. These days, a lot of electronic and financial

The two categories of services threats are channel-breaking attacks and credential theft. An Malevolent Assault on Keylogging

Credentials such as login, password, and PIN are all susceptible to theft by an attacker. Listening in on the conversation.The main focus of channel-breaking attacks is the communication between users and a financial institution [3]. Software keyloggers can be installed at the kernel or user level [5]. User-level keyloggers frequently employ high-level API to record keystrokes. For instance, Windows' GetAsyncKeyState function may determine whether a key is pressed during process invocation and whether it was pressed following the original call. User-space Keyloggers are easy to create, but they're also easy to find with hook-based methods [6].

Upon Kernel-level keyloggers, on the other hand, operate inside the OS kernel and record every character typed on the keyboard. Frequently, a kernel-level keylogger records certain driver activities or system calls. All user keystrokes that are routed through the hooked function call are captured by the malicious code that has been inserted.

Although more advanced and discrete than user-level keyloggers, kernel-level keyloggers are detected by kernel integrity and code attestation tools since they primarily rely on changes to the kernel code [7].

Users need to be aware of this kind of malware in order to combat such threats. It is still necessary for software professionals and students to have knowledge about creating, putting into practice, and keeping an eye on efficient keylogger assault defenses. Keyloggers that are built into devices may be used on their own to obtain passwords and other data. In addition, for the programmers In addition, it may be used for additional security purposes, such identifying suspicious activity, establishing frameworks for department heads, and looking into the objectives of different regions, such as monitoring minors under supervision, identifying unethical behavior, and identifying criminals. Keyloggers may also be a useful tool for identifying attackers and their tools. [8]

One definition of a keylogger is a piece of software that records keystrokes made on a computer. Authors referred to touchloggers—virtual keys that are pressed—as key loggers for mobile devices. Keyloggers are mostly used to obtain sensitive data, such as passwords and financial information, that is transferred to third parties for criminal purposes [9]. They are however occasionally used as lawful personal tools or as professional IT monitoring. A few keyloggers With the best antivirus software (like Norton, BitDefender, Intego, or Panda), you can easily find and remove certain keyloggers from your computer, but others may be more challenging.anti-malware instruments. Even worse, certain keyloggers function with more privilege than standard cybersecurity software, which makes it almost impossible to identify and eliminate them [10]. Since spyware exposes systems to potential security breaches and sensitive personal information, it has become a serious risk for the majority of Internet users. Without the user's knowledge or consent, spyware programs have the ability to collect and share personal data, including passwords, credit card numbers, and browsing habits, to a third party. [11].

Machine learning and data mining have shown encouraging outcomes. in locating further risky programs like worms and viruses, however they haven't been used for spyware detection yet. The goal of this research is to identify unique, unidentified binaries by applying principles from machine learning and data mining [12]. In this study, we proposed a novel machine learning-based ani-keylogger and keylogger detection technique that can differentiate between malicious and legitimate files. Furthermore, we will contrast our anti-spyware system's overall accuracy and false-positive rate (FPR) with those of competing anti-spyware systems. The experiment findings show that our strategy outperforms the current approaches.

II. STUDY AIM AND OBJECTIVES

The research goal is to identify a model that can recognize and stop keylogger-spyware damage on the system after training the model on the primary characteristics and behavior of the keylogger. This will ensure the CIA triad on the system and improve the security of our information and digital systems. The significance of the study may stem from the speed at whichspyware and keylogger features, methods, and delivery systemsare evolving. Additionally, a security solution should be integrated into the security system and cooperate with it. Systems are becoming increasingly sophisticated and capable of identifying and reducing the risk of keylogger spyware through the use of machine learning and classification techniques. The goal of this project is to create, implement, and assess a keylogger program that ethical hackers utilize. The The goal of the study is to develop a model that, once trained on the primary characteristics and behaviors of keyloggers, can identify and stop keylogger-spyware damage to the system.The following goals bolster this objective:

1) Examine the kinds, features, operation, and methods of keyloggers.

2) Apply many machine learning techniques to categorize the dataset.

3) Reduce the risk of Keylogger software on your devices.

In this research, the boundaries will be more concerned with identifying the keylogger using the system's database and the kinds of cases when the keylogger has not used API to retrieve data from the computer. This method may be used to boost keylogger stealth and evade network detection, but it requires more system study.

III.BACKGROUND

Based on where they are placed on the computer, keyloggers can be categorized as either hardware- or software-based. In both of these categories, the five most common types of keyloggers are as follows [13]:

A. Hardware Keyloggers

There are several shapes and sizes of hardware keyloggers available. There may be an external attachment positioned between the keyboard and the port. These are tiny cylinders on a cable segment that coordinates with the keyboard cable's color scheme. It takes less than a minute to install them. Because they are on the back of the machine, they are hard to see. It is also possible to put hardware keyloggers within the keyboard or next to the keyboard connector. The computer user is unable to notice these devices because they are not visible.

B. Keyloggers for Software

You may locate a variety of keyloggers by searching for "keylogger" on a search engine. You may also get free software keyloggers from any keylogger forum. It is possible to install a software keylogger on a computer with administrator rights.

They are available in an array of sizes and forms. A Visual Basic application can be utilized as a keylogger. It might be a device driver that takes the place of the current I/O driver and has keylogging built in. Windows hooks are used in the majority of C/C++ keylogger development projects. It is almost hard to combat the effects of hardware keyloggers from a software perspective. exclusively for regular users. Avoid using shared systems to access their bank accounts as a line of defense. Keyloggers for software, on the nonetheless, is can to be prevented. Even if it is a problem, via some methods.

Software keyloggers come in a variety of forms:

1) Hypervisor-based A hypervisor that is infected is executing within the operating system. Theoretical malware, such as Blue Pill, is intended to evade detection even when. The algorithm used by the virus is well known.
2) Kernel-based: The malware process has to operate in kernel space or user space. The use of a kernel-based keylogger requires advanced knowledge. Userspace is where 95 percent of keyloggers run. They are really difficult to write about and identify. Rootkits masquerade as keyboard drivers and are used to get access to system resources.

In order to prevent regular processes with lower access levels from doing this, the malicious process would need to elevate to the status of superuser.

3) Application Programming Interface- based: There are several vulnerabilities in the Windows API thatmake it simple for attackers to exploit to entice harmful software. At the heart of a keylogger is a Windows hook. The system message- handling mechanism has a place called a hook where an application may include a program to access messages coming into and going out of the Windows process.
4) Analyzing packets: These malicious programs intercept network information. HTTPS was specificallydesigned to fend off these kinds of assaults.
5) Acoustic Keyloggers: Due to their great complexity, acoustic keyloggers are hardly often used. They employ hardware-level keyboard recording techniques based on ideas from acoustic cryptanalysis. Every key on the keyboard has a unique sound to it. irrespective of who utilizes it. A sample may be examined using a few, but somewhat different, statistical techniques to identify individual signatures. It will take a while, though, and the results might not be as precise as those of other keyloggers.

IV. CLASSIFICATION

Random Forest, SVM, and Decision Tree classifiers will all be used in this paper's classification process to segment the data that is evaluated. Create an ideal hyperplane using SVM, Decision Tree, and Random Forest using the training set that was utilized. The function converts inputs into desired outputs using this set of variables. By employing this method, the computer may also make judgments that are distinct from one another. The computer is designed to continuously teach itself through trial and error.

A. ***SVM, or Support Vector Machine***

Regression classification falls into two categories where this kind can be applied. A dividing hyperplane that is used to distinguish between the plots or classes is part of it. This method works well in high dimensional spaces and selects the hyperplane based on the optimal separation area.

Let us assume that the input data is xj = (xj1...xjn). On the other hand, · is a map that mathematically labels (x1, y1),... (xm, ym) by mapping function space to the space of a mark y with multiple vectors.

B. ***Tree of Decisions***

A decision tree is a hypothetical outcomes tree that is formed by organizing the relevant decisions and then clearly and outwardly speaking coming to a conclusion. It makes use of a decision-making paradigm often used in information and machine learning mining. It has blocked several areas of machine learning, including as classification and regression. An unsociable node at the top of the decision tree branches into several outcomes and income levels. The decision nodes are the X-variables. Variables a and b are attributes' bounds that split decisions into three tree routes based on names or numbers. Each node has an attribute. The examined object has to be classified since the variables in a class are like the leaves of a tree.

C. ***The Forest at Random***

Leo Biermann's random forestry method, which produced excellent classification job results in 2001, was a potent technique. Using a sample of bootstrap data, RF An ensemble of classification trees is utilized in tree building to accomplish random variable selection and bagging. Every split is chosen at random. from any possible combination of variables. The process of creating each tree and partially randomly selecting dividers

ISSN 2394 - 7780

introduces randomness into a variety of random subsamples. The goal of cultivating every tree is to yield a low lip. Bagging and random variable collection keep the correlation for individual trees low. By averaging across a large set of low-life, high variance, but low correlation trees, the method creates a forest of the ensemble.

V. RELATED WORK

Keyloggers have existed since the Soviet Union created the "Selectric bug" in the middle of the 1970s to target typewriters. Since then, keyloggers have advanced significantly. Efficiency and usefulness have increased within the last 10 years.

Keyloggers, as its name suggests, can only provide output in the event that the keys are logged [14]. One major problem was that Microsoft Windows 8 came with a touchscreen personal keyboard when it was first introduced in 2012 [15]. In "Touch Interface and Keylogging Malware," S. Moses examines the capacity of keyloggers to record inputs from a virtual keyboard. It also displays the responses from other keyloggers. According to A. Bhardwaj's argument in [16], keyloggers ought to be categorized according to their execution location and available functionality.

Furthermore, the keylogger may be software- or hardware- based. New keyloggers have been released, and keylogger

Detection technology is also developing. In 2013, E. Ladakis

[5] presented a novel approach to creating a covert keylogger: instead of providing a host environment for the keylogger to operate in, he investigated the world of graphics cards. Since mobile devices have become a necessary part of our lives, banking services are now accessible through mobile applications. The program is increasingly gaining traction among users since it streamlines the banking process. Keyloggers are used by these mobile applications, which raises security concerns, as noted by A. Kuncoro [13]. In [17], security software is reviewed. Graphics Processing Units are another tool mentioned by Y. Albatain in [18] for identifying keyloggers. To determine whether keyloggers can be located, Keyloggers are evaluated against the most widely used and efficient programs. In [19], Danial Javaheri offers a brand-new technique for identifying and eliminating malware, including keyloggers, with 93 percent accuracy.

Numerous surveys are conducted annually to have a better understanding of the data monitoring process. It's unclear how much any large firm routinely documents employee and client data. System Monitoring and Security Using Keylogger describes the keylogger's scope, core concepts, and adoption dynamics. HawkEye [20] version 9 According to IBM, keylogger usage has surged recently. The aforementioned research indicates that keyloggers continue to be an intriguing area of investigation [6]. This paper describes a new, advanced version of keylogger using a Python method.

Most often, malware detection is evaluated as static or Dynamic versus static requires mark discovery, which calls for a harmful mark is included in the archive. The technique's. The fact that it is unrelated to the new keyloggers is its major fault. It is best to employ the dynamic location; behavior-based

There has been usage of identification. Given that Keyloggers routinely employ Windows snares, A subterranean insect snare shield that employs a hailing program to capture insects was studied by Aslam et al. . Framework schedulesare frequently the target of keyloggers; yet, Keylogger authorscan easily circumvent this tactic by employing methods other than Set Windows Hooked to record client activity.

The authors of provided a technique for identifying keyloggers in the system and eliminating any that are currently in place. from the laptop. They are the ones that do all of the espionage and steal all of the important, private, and delicate data. The writers have made an effort to resolve this grave problem. Nevertheless, the researchers unveiled a brand-new detection technique that finds every keylogger on our computer by utilizing a machine-learning algorithm. The different keyloggers that are installed or accessible are recognized using the Support Vector Machine learning technique. After several studies, the result was acquired, and it was cross-checked with a few of the anti-keylogger tools that are now on the market.

Ninety percent of today's keyloggers are found to execute in user space in [10], meaning they don't need any permission to carry out. The authors want to find user-space keyloggers so they can stop them from collecting information and personal data by using a strategy based on techniques for detecting userspace keyloggers, a prevalent kind of malware.

The model claims detection if there is a substantial correlation between any process and a simulated user behavior. The reasoning for this is because the keylogger will need to do more I/O operations in order to record keystrokes into the file, the stronger the keystroke stream.

describes Software Keyloggers as a prevalent harmful program that surreptitiously logs every action made by users in order to delicate data. The authors With the use of state-of- the-art artificial immune system (AIS) technology, the suggested. The goal of the project is to create a secure environment by continuously checking virtual machines for keyloggers. The algorithms utilized in the domain of The immune system is used by AIS using learning and memory capabilities to tackle a range of issues by implementing an architecture where the host operating system and

To guarantee kernel integrity, a virtual machine (VM) layer actively interacts. We may study VM using this cooperative method by watching occurrences and use a negative selection algorithm (NSA) to identify anomalies.As stated in , The authors employed three key features to create a malware classifier.

Using text mining techniques, printable strings are examined word by word to create a string feature matrix with a very large dimension. Then, we minimize the size of string characteristics using the singular value decomposition method. Second, Shannon entropy is approximated over printed texts and PSI characteristics to account for their unpredictable nature. API queries. Ultimately, all of the attributes come together to form the training feature set, which is then utilized to build malware classifiers via machine learning techniques. The proposed technique has been evaluated on 8422 benign and 16489 malicious files. Based on the experimental results, it is possible to identify viruses with 99.54% accuracy by using ensemble machine learning algorithms.

The developers of provide a method for identifying, tracking, and eliminating ransomware and malware, including stealthy and disguised keyloggers, screen recorders, and blocks.

The proposed method is based on a dynamic behavioral analysis that uses JRIP, J48 decision tree, and linear regression classifiers to detect three different forms of malware through transparent and deep hooking of kernel-level functions.

The whole design blueprint for an anti-spyware application to Malware traces are also displayed. The suggested methodology

Spyware was identified with a 93 percent accuracy rate and a 7 percent error rate. Additionally, an operating system may be disinfected against spyware infestation with an 82 percent strike probability using the recommended remedy.from the laptop. They are the ones that do all of the espionage and steal all of the critical, sensitive, and private information.

details. The writers have made an effort to resolve this grave problem. Nevertheless, the researchers unveiled a brand-new detection technique that finds every keylogger on our computer by utilizing a machine-learning algorithm. The different keyloggers that are installed or accessible are recognized using the Support Vector Machine learning technique. After several studies, the result was achieved, and it was cross-checked with some of the anti-keylogger programs that are now on the market. Ninety percent of today's keyloggers are found to execute in user space in [10], meaning they don't need any

Permission to carry out. By using a strategy based on detection techniques for userspace keyloggers, a prevalent kind of malware, the authors hope to detect userspace keyloggers and stop them from obtaining confidential information.

The model claims detection if there is a substantial correlation between any process and a simulated user behavior. The reasoning for this is because the keylogger will need to do more I/O operations in order to record keystrokes into the file, the stronger the keystroke stream.

Describes software Keyloggers are a type of malicious software that is frequently used to covertly record user activity in order to delicate data. The authors With the use of state-of- the-art artificial immune system (AIS) technology, the suggested. The goal of the project is to create a secure environment by continuously checking virtual machines for keyloggers. the field of AIS, algorithms utilise the immune system's using learning and memory capabilities to tackle a range of issues by implementing an architecture where the host operating system and an electronic device To guarantee kernel integrity, the VM layer actively communicates. We may study VM using this cooperative method by watching occurrences and use a negative selection algorithm (NSA) to identify anomalies.As stated in, The authors employed three key features to create a malware classifier.

Text mining techniques are used to examine printable strings word by word, producing a string feature matrix with a very large dimension. Then, we minimize the size of string characteristics using the singular value decomposition method. Second, Shannon entropy is approximated over printed texts and API requests to take into account the unpredictable nature of PSI and API features. Ultimately, all of the attributes come together to form the training feature set, which is then utilized to build malware classifiers via machine learning techniques.

The proposed technique has been evaluated on 8422 benign and 16489 malicious files. Based on the experimental results, it is possible to identify viruses with 99.54% accuracy by using ensemble machine learning algorithms. The developers of provide a method for identifying, tracking, and eliminating ransomware and malware, including stealthy and disguised keyloggers, screen recorders, and blocks. The recommended method is predicated on a dynamic behavioral analysis by deeply and transparently hooking kernel-level functions and using the classifiers of JRIP, J48, and linear regression as a means of detecting three different kinds of malware.

An anti-spyware program's whole architectural blueprint for tracking malware traces is also displayed. The suggested methodology

Spyware was identified with a 93 percent accuracy rate and a 7 percent error rate. Additionally, an operating system may be disinfected against spyware infestation with an 82 percent strike probability using the recommended remedy.

VI. RESEARCH METHODOLOGY

Keyloggers that are built into devices may be used on their own to obtain passwords and other data. In addition, programmers may use it to safeguard other areas, such identifying suspicious activity in department leaders' frameworks, examining the function of other areas like monitoring guardianship children and identifying improper behavior, and identifying criminals. Keyloggers can also be a useful tool for differentiating between attacks and their tools.

Though they haven't been used for spyware detection yet, data mining and machine learning have demonstrated encouraging results in finding other harmful applications like viruses and worms. The goal of this research is to discover new, unidentified binaries by applying machine learning and data mining approaches. We proposed a novel approach for keylogger detection and keylogger generation. Using machine learning, which is able to differentiate between legitimate and spyware files. Furthermore, we will contrast ouranti-spyware system's overall accuracy (ACC) and false- positive rate (FPR) with those of another anti-spyware system. The experiment findings show that our strategy outperforms the current approaches.

VII. DATASET ANALYSIS AND DESCRIPTION

The current data, which came from the CIC website, includes benign and 523616 Keylogger samples.

1) Benign Information Including 309315 Observations

2) Keylogger Information with 214209 Notes

VIII. IMPLEMENTATION

Utilizing machine learning, one may identify the incursion in the recommended course of action. Several deep and machine learning techniques will be used to implement the recommended solution. Depending on the appropriate parameters, each machine learning algorithm will be subjected to HyperParameter and CV-FOLD. A general flowchart for the recommended method, as seen in figure 1, is provided below. Each stage in the suggested strategy is broken down into the following details:

A. *Splitting and Loading the Raw Dataset*

The model will only work with one kind of dataset each run due to the variety of dataset types. The dataset, which includes traffic, hazardous material, and attacks of all kinds, will be split into two groups: training and testing. 70% of the A third of the data will be utilized for testing, and the remaining 40% for training.

Numerous operations were carried out on the training dataset, including as cleaning, normalization, encoding of the data and labels, and Hayperparameters. The machine learning model will be predominantly trained on the dataset using a variety of assault kinds and detrimental substance. After learning from the dataset, machine learning will be able to identify malicious content, which will decrease FP and TN and increase malevolent understanding.

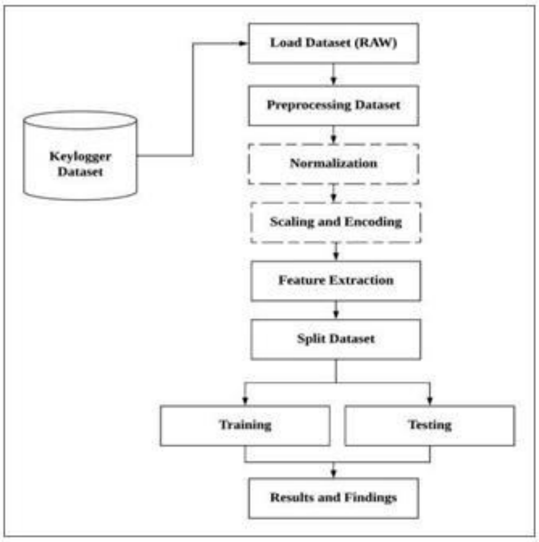


Fig. 1: General Approach for the Proposed Method

Testing will be used by the network's created devices, which will communicate with one another via the testing data. This will include a healthy proportion of both harmful and benign traffic. The traffic will be used by the classifiers as a testing dataset, and following the interaction, the results of the classification and confusion matrix will be shown.

B. *Possessing Data*

For all datasets employed in the suggested strategy, unified X (training) and Y (testing) data will serve as the foundation for data preparation. After the data is entered into the model, the following will happen:

1) Swap out the technique will begin to substitute identical data and numbers into unified forms. For instance, the words (IP, Ip, iP, and ip) all have the same meaning, but in a model, each term has a specific meaning .
2) The data will be cleaned and normalized to remove any extraneous information, such as dots, blanks, etc.
3) Assign numerical weights to the labels and listed terms, such as "risk." [‘high’, ‘medium, ‘low’] to Risk[2, 1, 0].
4) Segments the words so they may be computed and turned into vectors. Only numerical data is accepted by machine learning.
5) Tokens will be applied to the vectors in order to encode and compute them.Feature Extraction and Selection

The dataset is compressed using linear algebra in Principal Component Analysis, or PCA. Generally, this is considered a data reduction strategy. The ability to choose the number of dimensions or major variables in the transformed outcome is one of PCA's features. A p-dimensional ellipsoid with features, where each ellipsoid axis represents a main portion, may be thought of as being suitable for PCA. The divergence is minor along the ellipsoid axis if it is small [28].

The data around the origin should be orientated and the mean of each vector should be deducted from the data collection in order to determine the location of the ellipsoid axis. Next, we compute the covariance matrix of the data and determine the values of the associated vectors and the covariance matrix. To become unit vectors, any of the orthogonal vectors must first be normalized. Following that, an ellipsoid axis may be used to represent each unit individually It has a reciprocal orthogonal unit fitted to the details.

C. *Training and Testing*

During the training phase of supervised learning, we use the training information to find the optimal model that, given the feature set X, will create the accurate label Y for objects that have not yet been observed. File statistics and a list of frequently used API calls are two examples of characteristics of file content or behavior that may be X in the context of malware detection. Labels Y could be classified as malware, benign, or even more specifically as a virus, Trojan-Downloader, or adware. We must choose a family of models, such as decision trees or neural networks, for the training phase. Typically, a family of models is defined by its parameters. Training entails looking for a model within the chosen family that has a In supervised learning, the training data is used to determine a specific set of parameters that, when applied to the collection of reference objects, provide the trained model with the best accurate results in terms of a given metric. Stated otherwise, we will

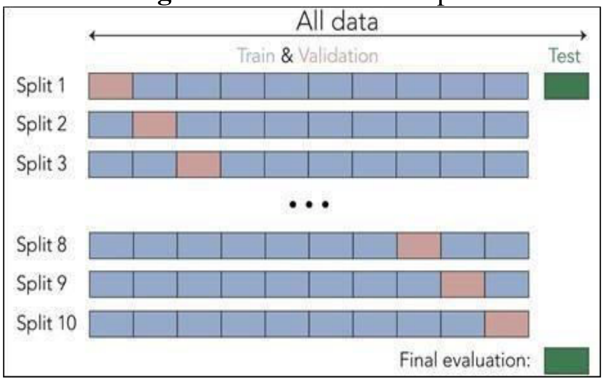
ISSN 2394 - 7780

discover the ideal parameters that establish a legitimate mapping from X to Y. The following step involves applying the trained model to new objects once its quality has been confirmed. The model's type and parameters remain unchanged during this phase. All that the model does is forecast. This is the protective stage when it comes to malware detection. Vendors frequently provide consumers with a trained model, allowing the product to make decisions on its own by using the model's predictions. Errors can have disastrous effects on a user; taking out an OS driver is one example. The dealer needs to make a careful choice of model family. To identify the model with the highest detection rate and lowest false-positive rate, the vendor has to employ an effective training process.

D. *Cross-Validation*

Machine learning models are tested on tiny datasets using a resampling method known as CV-FOLD. The method's sole parameter, k, determines the number of groups into which a given data sample should be split. Consequently, a common nomenclature for the procedure is K-fold cross-validation. You can substitute a particular integer for (k) in the model's reference, e.g., k=10 for 10-fold cross-validation. A machine learning model's performance on anonymous data is evaluated using a small sample and a cross-validation approach to see how well the model predicts data that was not included in training. As seen in figure 2.

Fig. 2: Dataset CV-Fold split



E. *Tuning Parameters for Machine Learning*

The learning process is controlled by hyperparameters, which specify the model parameters that an algorithm learns. The learning procedure and the final model parameters are both governed by "top-level" parameters. As machine learning engineers, we select and define the Hyperparameter values that our learning algorithm will use prior to the model being trained. Since the values of hyperparameters cannot be changed during training or learning, they are external to the model. Even though they are not included in the final model, hyperparameters are employed while the learning algorithm is learning. This model does not contain the Hayperparameters that were utilized during training. When examining a model, we are unable to determine which Hyperparameter values; the only things we know about the model are its parameters.as seen in figure 3.

IX. RESULTS

We employed many assessment methods, including confusion matrix, accuracy, precision, and recall, in the suggested approach to assess the outcomes and derive the conclusions. The variance between the results in the main five runs, the standard deviation, and the mean of the main five runs have all been used to analyze and assess the findings.

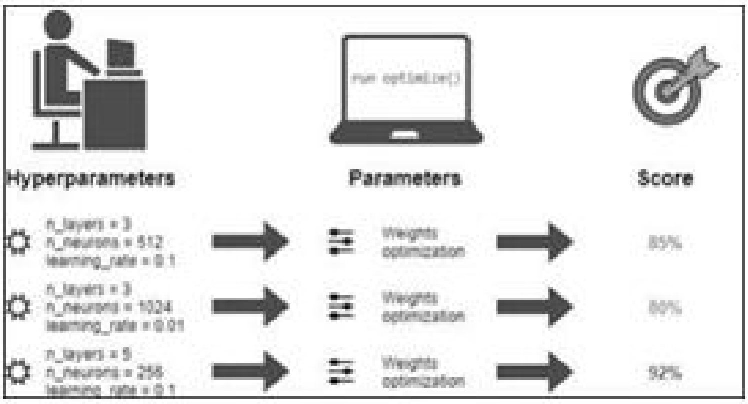


Fig. 3: Machine learning Hyperparameter

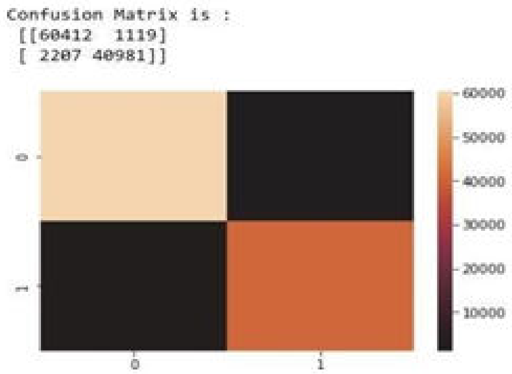


Fig. 4: Result confusion matrix

A. *Confusion Matrix*

A performance measure for machine learning classification jobs that provide output in two or more classes is the confusion matrix. It's a table with a combination of the actual and anticipated outcomes. When describing a classification model's performance on a set of test data whose true values are known, a confusion matrix is a table that is commonly employed. As seen in figure 4, TP, FP, FN, and TN may all be used to quantify the AUC ROC curves, recall, precision, and accuracy.

B. *Random Forest*

The outcomes and effectiveness of the suggested model's performance using the Adaboost Classifier are shown in Table In terms of accuracy scale, the model performed best across all runs. It made x happen. It is considered that 02:44.64 seconds is a reasonable length of time for all classifiers to conduct the classification operation. Upon interpreting by taking into consideration all potential labels and judgments, the random forest produced the optimum tree for the end findings, producing high accuracy outcomes. These accuracy values were achieved via the training and testing procedure. Random Forests are ideal for improving decision tree performance on binary classification issues. The game was originally released under the name Random Forests. Random Forests may be used to improve any machine learning technique. It is excellent for students who are not as smart as the rest of the class. These models outperform random chance in terms of accuracy on a classification task. When working with Random Forests, one- level decision trees are the most practical and often used method. Because they are so brief and only offer one classification option, these trees are referred to as choice stumps.

Table I: Results of Random Forest Algorithm

Run	Accuracy %	Precision %	Recall %	F-score %
1	0.97	0.95	0.95	0.97
2	0.97	0.95	0.95	0.97
3	0.97	0.95	0.95	0.97
4	0.97	0.95	0.95	0.97
5	0.97	0.95	0.95	0.97

C. *Decision Tree*

Table II displays the results and efficacy of the proposed model's operation using the Decision Tree classifier. With respect to the accuracy scale, our proposed method yielded the best results and performed at a level of 70%; it took x seconds to finish the classification process and achieved x. Unlike the other classifiers, the decision tree shows different results for each run with an average accuracy rate (x). The decision tree began deaccessioning the findings based on distinct and extremely restricted classing for each run, which resulted in various labels being assigned to nodes. In our suggested model, the decision tree with the various outputs produced a satisfactory outcome. One advantage of a decision tree is that it forces you to consider every possible course of action. and following each route to its end. It produces a thorough analysis of the consequences along each branch and identifies the decision nodes that need additional research. Decision trees designate values for each problem, decision path, and specific outcome. The costs and benefits are made clear by the use of monetary values. This approach reduces uncertainty, makes clear the relevant decision paths, and elucidates the financial effects of various solutions. Decision trees don't require complex formulas, making them easy to use and understand. They provide quick explanations and a clear, graphical representation of each option for quick comparisons.

 ISSN 2394 - 7780

Table II: Results Decision Trees

Run	Accuracy %	Precision %	Recall %	F-score %
1	0.97	0.97	0.96	0.97
2	0.97	0.97	0.96	0.97
3	0.97	0.97	0.96	0.97
4	0.97	0.97	0.96	0.97
5	0.97	0.97	0.96	0.97

D. *Support Vector Machine*

Table III The results and efficacy of the proposed model's operation using the second classifier utilized in Because we'll be working with integers and matrices, math libraries like Numpy, pandas, and matplot-library will be used to display the graphs in this research, which employs support vector machines (SVM). In addition to existing libraries, Sklearn's machine learning will include confusion matrices, accuracy ratings, and SVM classifiers. Reading the dataset from the file and dividing it into data is how the function begins. Includes labels for the sections used for testing and training. in an understandable manner with succinct explanations. This variation of Regression classification is applicable to both of the collectives. It has a dividing hyperplane for classifying and splitting the graphs. The aircraft that is hyperplane selected in light of the optimal separation zone; high-dimensional spaces are a good fit for this method.

Table III Results Svm Algorithm

Run	Accuracy %	Precision %	Recall %	F-score %
1	0.95	0.95	0.95	0.95
2	0.94	0.95	0.95	0.95
3	0.95	0.95	0.95	0.95
4	0.95	0.95	0.95	0.95
5	0.94	0.95	0.95	0.95

X. CLASSIFIER COMPARISON

The accuracy rate for each training split as well as the overall accuracy rate will be used for comparison. In order to identify the best and most effective classifiers used in this study, performance and time will also be taken into account. A comparison of the classifiers used in the suggested strategy is displayed in Figure 5. RF had a higher accuracy rate in each split data quantity for the classifier shown in Figure 5 rate of accuracy for every data split. The RF classifier is the most efficient classifier for classifying the images and data on it using the recommended method because of the parameters. A neural network's parameter count grows quickly as the number of layers rises.

Due to this, training models may become computationally demanding (and occasionally not possible). It can take a lot of work to adjust so many parameters.

XI. CONCLUSION

By applying this machine learning technique, we are able to identify the different dangerous actions that keyloggers within the system carry out. Many keystrokes and patterns are produced by the keylogger. These patterns and the keys being pressed served as the foundation for our system. This work proposed a machine learning-based keylogger detection model to identify host behavior when keyloggers were running on the system. The model was trained using datasets containing keyloggers and spyware. The results will be derived from a variety of metrics and presented in the form of a confusion matrix and classification report to assess the effectiveness of the system in detecting keylogger malware. The keylogger dataset was classified using a variety of machine learning techniques in the suggested approach. The classifiers included SVM, Decision trees and random forests. The decision tree received the lowest accuracy score of 94% and the longest run time, while the RF obtained the maximum accuracy of 99.6% and the longest run time. Subsequent research endeavors will persist in examining the issue through the utilization of sophisticated deep learning technologies for categorization, as well as network monitoring to augment problem comprehension and fortify host and network security.

REFERENCES

[1] S. Yadav, A. Mahajan, M. Prasad, and A. Kumar, "Advanced keylogger for ethical hacking."

[2] D. Nyang, A. Mohaisen, and J. Kang, "Keylogging-resistant visual authentication protocols," *IEEE Transactions on Mobile Computing*, vol. 13, no. 11, pp. 2566–2579, 2014.

[3] P. K. Veni and B. Naresh, "A novel visual authentication protocols implementation based on keylogging-

resistant," *International Journal of Scientific Engineering and Technology Research*, vol. 4, no. 28, pp. 5470–5477, 2015.

[4] Y. A. Ahmed, M. A. Maarof, F. M. Hassan, and M. M. Abshir, "Survey of keylogger technologies," *International journal of computer science and telecommunications*, vol. 5, no. 2, 2014.

[5] H. Al-Masalha, A. A. Hnaif, and T. Kanan, "Cyber-crime effect on jordanian society," *Int. J. Advance Soft Compu. Appl*, vol. 12, no. 3, 2020.

[6] A. P. Kuncoro and B. A. Kusuma, "Keylogger is a hacking technique that allows threatening information on mobile banking user," in *2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)*. IEEE, 2018, pp. 141– 145.

[7] A. Dwivedi, K. C. Tripathi, and M. Sharma, "Advanced keylogger-a stealthy malware for computer monitoring," *Asian Journal For Conver- gence In Technology (AJCT) ISSN-2350-1146*, vol. 7, no. 1, pp. 137–140, 2021.

[8] S. Moses, J. Mercado, A. Larson, and D. Rowe, "Touch interface and keylogging malware," in *2015 11th international conference on innovations in information technology (IIT)*. IEEE, 2015, pp. 86–91.

[9] M. Davarpanah Jazi, A.-M. Ciobotaru, E. Barati *et al.*, "An introduction to undetectable keyloggers with experimental testing," *International Journal of Computer Communications and Networks (IJCCN)*, vol. 4, no. 3, pp. 1–5, 2014.

[10] Y. Albabtain and B. Yang, "The process of reverse engineering gpu malware and provide protection to gpus," in *2018 17th IEEE Inter- national Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 2018, pp. 1669–1673.

[11] I. Arghire, "Business users targeted by hawkeye keylogger malware," *Security Week*, vol. 28, 2019.

[12] A. Bhardwaj and S. Goundar, "Keyloggers: silent cyber security weapons," *Network Security*, vol. 2020, no. 2, pp. 14–19, 2020.

[13] M. Aslam, R. N. Idrees, M. M. Baig, and M. A. Arshad, "Anti-hook shield against the software key loggers," in *Proceedings of the 2004 national conference on emerging technologies. Citeseer, 2004, p. 189.*

[14] *J. Singh and J. Singh, "Detection of malicious software by analyzing the behavioral artifacts using machine learning algorithms," Information and Software Technology, vol. 121, p. 106273, 2020.*

[15] *H. Huseynov, K. Kourai, T. Saadawi, and O. Igbe, "Virtual machine introspection for anomaly-based keylogger detection," in 2020 IEEE 21st International Conference on High Performance Switching and Routing (HPSR). IEEE, 2020, pp. 1–6.*

[16] *R. S. Sreenivas and R. Anitha, "Detecting keyloggers based on traffic analysis with periodic behaviour," Network Security, vol. 2011, no. 7, pp. 14–19, 2011.*

[17] *A. Wajahat, A. Imran, J. Latif, A. Nazir, and A. Bilal, "A novel approach of unprivileged keylogger detection," in 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET). IEEE, 2019, pp. 1–6.*

[18] *Z. M. Darvas, M. Dom´ınguez-Jime´nez, and G. B. Wolff, "From climate change to cyber-attacks: incipient financial-stability risks for the euro area," Bruegel Policy Contribution, Tech. Rep., 2020.*

[19] *A. Jegede, G. Odii, M. Magaji, G. Aimufua et al., "Assessment of security awareness level of mobile device users in tertiary institutions in plateau state of nigeria," Journal of Advanced Computing Technology and Application (JACTA), pp. 1–8, 2021.*

[20] *D. Granato, J. S. Santos, G. B. Escher, B. L. Ferreira, and R. M. Maggio, "Use of principal component analysis (pca) and hierarchical cluster analysis (hca) for multivariate association between bioactive compounds and functional properties in foods: A critical perspective," Trends in Food Science & Technology, vol. 72, pp. 83–90, 2018.*

 ISSN 2394 - 7780

SYNTHETIC SPEECH DETECTION USING DEEP

Saurabh Gupta and Rajesh Maurya
Usha Pravin Gandhi College of Arts, Science & Commerce Vileparle, Mumbai, India

ABSTRACT
The evolution from harmless text-to-speech (TTS) systems to deceptive audio deepfakes, the AI generated audio became a threat capable of impersonation and spreading misinformation. Deep learning (DL) techniques has exacerbated this danger, crafting ever-more convincing fabrications necessitating robust detection methods. While existing research has achieved impressive results, their real-world generalizability remains limited due to single-dataset training and assessment, impractical for representing the diverse landscape of modern audio deepfakes. This paper tackles the same problem by strategically combining diverse audio data and contructing a dynamic training superset. This incorporates enriching the widely used Fake or Real (FoR) dataset with diverse audio data, ensuring the model adaptability across genders, languages and accents along with several TTS systems. This departure from prior research highlights our focus on real-world generalizability. We experiment with DL methods like artifical neural networks (ANNs) and long short term memory (LSTMs). Our model, leveraging MFCC (Mel Frequency Cepstrum Coefficient) features and LSTM networks, achieves benchmark accuracy of 85.5% and exhibits promising real-world generalizability, demonstrating its potential to address this critical challenge.

Keywords: Audio deepfakes, synthetic speech, deepfake detection models, deep learning, MFCC, AI.

1. INTRODUCTION

Albert Einstein's famous equation, $E=MC^2$ was initially conceived as a theoretical framework for understanding the universe, its evolution, and exploring energy generation, while its transformative power was tragically wielded in the development of the atomic bomb. Throughout the history of mankind, such transformative discoveries have often been accompanied by their paradoxical potential for destructive applications. Artificial Intelligence is exactly that double-edged sword that embodies a similar duality, offering both societal progress and the specter of annihilation. Another consequence of such an evolution of artificial intelligence (AI) are the deepfakes.

Deepfakes are AI - synthesized or manipulated media in which a person's face or voice is swapped with that of another person, to make it appear as if a person is saying or doing something that they never actually said or did. Deepfakes can be used to damage someone's reputation, to spread misinformation, or to create a false impression of reality. They are created using a variety of techniques that involves deep learning methods such as generative adversarial networks (GANs).

This study specifically targets the audio deepfakes (ADs). Audio Deepfakes are audio clips that are synthetically generated or manipulated by AI to sound like a certain person. With the advent of deep learning methods such as GANs, AI-synthesized speech (AI-SS) becomes completely indistinguishable from real speech. GANs are like two AI models playing a game to deceive each other. One, the generator, tries to create realistic audio samples indistinguishable from real ones. The other, the discriminator, acts as a critic, trying to identify fake audio. Through this adversarial back-and-forth, the generator gets better at mimicking real audio, while the discriminator hones its detection skills.

This pervasive influence of AI, now extends to the auditory realm, blurring the lines between reality and fabrication. The ability of this level to fabricate convincing depictions of reality poses significant threats to reputation, information integrity, and the perception of truth. Therefore, this research work aims to experiment with certain deep-learning techniques like artificial neural networks (ANNs) & long short-term memory (LSTM) for the development of such an AI model that can determine whether an audio clip is real or was synthetically generated by AI with high confidence. Identifying a synthesized speech, from a real one could be an arduous task especially when they are generated by stupendous deep learning models with high accuracies that make it indistinguishable.

Therefore, as a prerequisite, a study was performed to get a brief understanding of the fundamentals of audio signal processing & overall sound energy that encompasses all features of sounds ranging from basic wavelength, amplitude, and frequency to some advanced terminologies such as sampling rate, spectral characteristics, time domain features, etc along with some natural vocoder artifacts. By understanding audio signals, this foundational research served as the beginning of the construction of the AI-SS detection model.

Earlier research in AI-SS detection often relied on the ASVSpoof dataset[1], considered the first automatic speaker verification spoofing and countermeasures dataset. However, its limitations became apparent when it lacked audio data generated by the latest text-to-speech (TTS) models [2]. Therefore, we used the Fake or Real (FoR) dataset [3], because it contains both real utterances as well as fake audio clips from recent TTS models providing a more robust platform for training and evaluating an AI-SS detection model. The study then proceeds with developing an architecture for a detection model followed by training, testing, and evaluation part where we provide a detailed comparative insight into the model performances.

2. LITERATURE REVIEW

In 1961, at Bell Labs John Larry Kelly Jr. and Louis Gerstman laid the foundation for modern text-to-speech technology with their invention "vocoder" [4]. The "vocoder" was a TTS system, despite not yet achieving realistic speech quality, marked a significant breakthrough in the technology's development. However, its high cost and complexity limited its widespread adoption. Since then, there have been a lot of advancements in this technology. Since then, TTS technology evolved so rapidly that by the early 2000s, they were integrated into widespread applications from audiobooks, voicemails, and navigation systems to chatbots. This proliferation further intensified with the emergence of intelligent assistants like Apple's Siri, Google Assistant, and Alexa, solidifying TTS as a keystone of human-computer interaction.

Now, at this point the TTS systems were at their peak since they had reached a remarkable level of naturalness with their near-human quality captivating audience expressiveness that resonated with users, fostering emotional connections and diverse applications. However, the arrival of deep learning and neural networks propelled this technology beyond mere "text-to-speech", empowering it with the unprecedented ability to flawlessly replicate individual voices. This leap in capability redefined the usual "TTS systems" and turned into "speech synthesis" in no time which later gave rise to the brutal reality of what we today know as the "deepfakes". With DeepFakes now anyone had the power to impersonate, pretend to be somebody else, and spread hate, wrong information, or harm someone's reputation which could lead to serious negative consequences. DeepFakes thus were a potential danger that should be regulated thoroughly. This realization ignited a critical need for countermeasures and sparked the development of audio deepfake detection technologies.

The existing method for detection of audio deepfakes primarily falls into two main categories: Machine Learning (ML)-based and Deep Learning (DL)-based approaches. ML-based methods exhibit higher accuracy irrespective of the features used, but their reliance on manual feature extraction impedes scalability and generalization. Conversely, DL methods, while more scalable, often demand specific audio data transformations and are susceptible to overfitting [5]. Classical ML models, particularly Support Vector Machines (SVMs), have been prominent in the detection of AI-SS. In a study by Arun Kumar and Priyanka Singh, a Quadratic SVM achieved an impressive 96.3% accuracy, outperforming traditional methods and other ML models [6]. Similarly, Ameer Hamza et al. employed SVM for classifying fake speech, achieving 97.57% accuracy on the For-2sec dataset and a remarkable 98.83% on the For-rerec dataset [7]. These results underscore the efficacy of classical ML models in accurately identifying AI-synthesized speech. The further exploration and development incorporates deep learning techniques.

Deep learning models have introduced more sophisticated approaches to tackle the challenges posed by the increasing quality and accessibility of AI-SS. Nisha Subramani and Delip Rao proposed CNN-based architectures, including Efficient-CNN and RES-EfficientCNN, achieving F1 scores of 94.14 and 97.61, respectively [8]. M. Ballesteros et al. introduced a 2D CNN model, Deep4SNet, visualizing the audio dataset as histograms and achieving a high accuracy of 98.5% in detecting AI-SS [9]. C. Sun, S. Jia, et al. proposed a multi-task learning-based RawNet2 model, focusing on vocoder artifacts.

This model achieved the lowest Equal Error Rate (EER) of 1.41% on the LibriVoc dataset and 0.19% on the WaveFake dataset, surpassing other baselines [10]. Most evaluations were conducted on the Automatic Speaker Verification (ASV) spoof challenge 2019 dataset, a large-scale public database created to assess and enhance the performance of spoofing countermeasures in ASV systems. In summary, ML-based methods offer high accuracy but with limitations in scalability and generalization due to manual feature extraction. DL models, while more scalable, face challenges related to overfitting and specific data transformations. Advances in both ML and DL approaches signify significant progress in detecting audio deepfakes.

3. RESEARCH METHODS

A. DATASET DESCRIPTION

Developing a robust AI-SS detection model hinges on one crucial element: training data. While the internet provides vast oceans of datasets, finding one that accurately represents both real and synthetic speech proves to be an arduous task. For effectively training the model, the primary difficulty lies in ensuring the absence of biases. The datasets we encountered online exhibited diverse characteristics with some leaning heavily towards real speech audio data, while others favored synthetic speech. Linguistic differences and gender-based imbalances further complicated the dataset selection process. For instance, some seemingly ideal datasets contained a disproportionate number of male voices compared to female voices, or vice versa. In conclusion, the pursuit of a dataset that adequately represents both real and synthetic speech for AI-SS detection remains a complex and multifaceted endeavor. To achieve high accuracy, it is imperative to proactively mitigate any potential biases that could arise during the training phase.

The dataset finally used was for-norm from the Fake-or-Real (FoR) dataset. So, to tackle the problem of biases, inconsistencies in audio formats, linguistic discrepancies, and gender imbalances, we enriched this dataset blended some other ideal datasets, and developed a superset, one that encompasses no potential biases or skewness. This approach ensures the model's ability to generalize better on diverse audio clips in real-world scenarios transcending linguistic, or gender-based indifferences. Additionally, this consolidation aimed to mitigate overfitting issues that persisted despite optimizing and fine-tuning algorithms during training on one specific dataset. All the datasets used are mentioned in Figure 1.

DATASET	TYPE	LANGUAGE	FORMAT	NOISE	SAMPLING_RATE	AVG_DURATION
Common Voice	Real	Hindi + English	.mp3	Yes	32KHz	6 seconds
LibriTTS	Real	English	.mp3	No	24KHz	7 seconds
CMU Arctic	Real	English	.wav	No	16KHz	3 seconds
FoR	Fake/Real	English	.wav	No	16KHz	2 seconds
SP22	Fake	English	.wav	No	16KHz	4 seconds

Figure 1: Audio Datasets

B. DATA PREPROCESSING

Dataset inconsistencies in sampling rates, file formats (WAV, FLAC, MP3, etc.), and sampling rates precluded direct model training. Another challenge stemmed from inconsistencies in audio clip durations. For example, a selected real speech dataset might exhibit an average audio clip duration of 9 seconds, while the finalized synthetic dataset possessed an average duration of 3 seconds. To address this, all audio clips were pre-processed with unified sampling rates, format conversion to .wav, and duration truncation before training, ensuring standardized inputs for robust model development.

C. FEATURE EXTRACTION

Previous studies on audio fundamentals provided valuable insights into the distinctive features of audio clips. The primary objective was to identify the most reliable and crucial features capable of distinguishing between real and fake speech, since they both exhibit similar features. Therefore, we came up with the idea of extracting mel-frequency cepstral coefficients (MFCCs). It's a widely used feature for speech recognition purposes. We opted for this approach because, among various features, MFCCs were identified as particularly effective [11] for the purpose of AI-SS detection & speech recognition as a whole.

D. DETECTION MODELS

a) Fully Connected ANN Model

Our pursuit of an effective model to differentiate between real and synthetically generated audio clips led us to explore fundamental approaches, including simple fully connected feed-forward artificial neural networks (ANNs) or recurrent neural networks (RNNs). Choosing an ANN as the foundational strategy, we initiated training on our dataset. The model architecture depicted in Figure 2, adopted a sequential design, with an input layer flattening 2D Mel-Frequency Cepstral Coefficients (MFCCs) into a 1D vector, followed by two hidden layers.

 ISSN 2394 - 7780

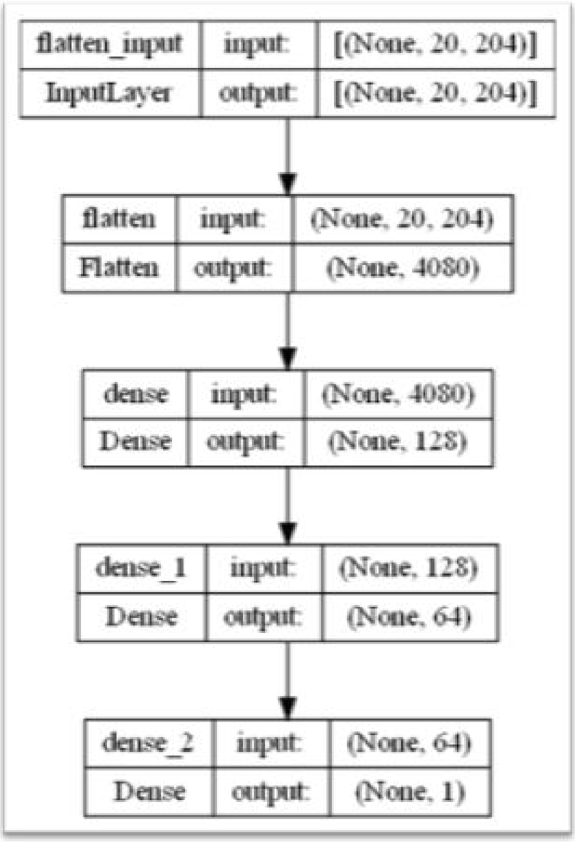


Figure 2: ANN Architecture

The first dense layer comprised 128 neurons with ReLU activation, introducing non-linearity, while the second dense layer featured 64 neurons with ReLU activation for further refinement of features. The output layer employed a dense layer with one neuron and sigmoid activation for binary classification (real or fake).

Throughout the training process, real and fake audio files were loaded, and MFCC features were extracted. Features were standardized for consistent shape, and the model, compiled with an Adam optimizer, binary cross-entropy loss function, and accuracy metric, underwent 100 epochs of training. Although the model demonstrated a satisfactory accuracy of 75% on the validation dataset, its performance on the testing dataset and real-world data revealed limitations, emphasizing the necessity for meticulous data normalization and hyperparameter tuning to enhance its efficacy.

b) Optimized ANN Model

Despite promising results on the validation set, the initial ANN model struggled with generalization to unseen data. In an effort to enhance robustness for real-world scenarios, a new architecture was devised with key changes, incorporating flattening and batch normalization layers.

These additions aimed at regularizing training, preventing overfitting, and improving adaptability to diverse synthetic audio. The revamped model depicted in Figure 3, retains a sequential structure with notable alterations: a larger input layer flattening 25 MFCCs, batch normalization for stability, and learning rate scheduling to avoid overfitting. The training process involves separate directories for validation data, error-checking during feature extraction, StandardScaler for normalization, and a more aggressive training approach with 60 epochs and a smaller batch size. Overall improvements include an increased number of MFCCs, batch normalization, learning rate scheduling, separate validation and testing data, and saving both model and scaler for future deployment or experimentation.

This optimized model, integrating strategies like feature normalization and learning rate scheduling, demonstrates enhanced efficiency compared to its predecessor with an accuracy of 83.7%. While performing well on both validation and testing datasets, its real-world applicability is limited, hinting at potential overfitting. Recognizing the constraints of the ANN architecture, a paradigm shift led to the exploration of a different deep learning approach: the Recurrent Neural Network (RNN) architecture, specifically the Long Short-Term Memory (LSTM) model. However, hardware limitations constrained exploration of more

 ISSN 2394 - 7780

sophisticated models, such as deep, multi-layered RNNs, which could have further improved accuracy and generalizability.

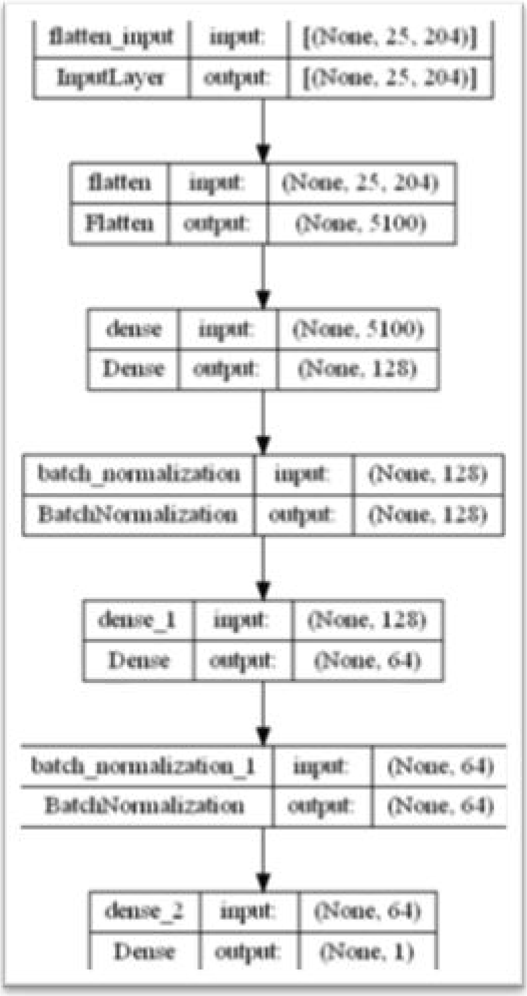


Figure 3: Optimized ANN Architecture

c) LSTM Model

In response to the underwhelming real-world performance of prior ANN models, a shift toward Recurrent Neural Networks (RNNs), specifically Long Short-Term Memory (LSTM) models, was undertaken. While maintaining the general architecture of its predecessors, this model incorporated LSTM layers to capture temporal dependencies within audio data. However, this computational prowess came at a cost, demanding significant resources and hours for training.

The model's architecture as depicted in Figure 4, follows a sequential structure with key components:

- The first LSTM layer comprises 128 units, processing the entire sequence with return_sequences=True.
- The second LSTM layer consists of 64 units to capture deeper temporal features.
- Batch normalization is implemented after each LSTM for stability.
- The dense output layer features 1 neuron with sigmoid activation for binary classification.

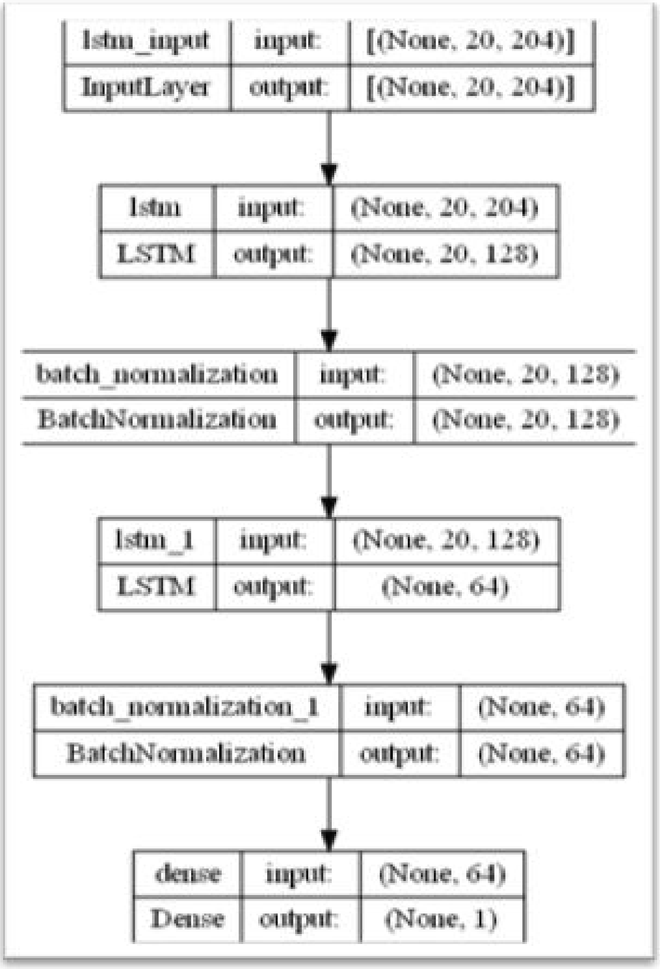


Figure 4: LSTM Architecture

In the training process, features are reshaped back to a 3D format (20 MFCCs x max_length) before feeding to the LSTM. Early stopping is introduced to prevent overfitting, halting training after 5 epochs with no validation loss improvement. A slightly larger batch size (32) is utilized due to the potentially higher computational cost of LSTMs. Key improvements and potential benefits include the LSTM's ability to capture long-term dependencies within audio sequences, potentially capturing subtle nuances missed by feedforward models. Early stopping prevents overfitting, enhancing generalizability, and LSTMs show promise for achieving higher accuracy in audio classification tasks, including fake audio detection.

This model signifies a significant advancement, utilizing LSTMs and early stopping to enhance performance and generalizability. Compared to previous feed-forward ANN models, it demonstrated superior performance across all metrics, achieving an accuracy of 85.5%. However, despite setting a new benchmark, its reliability in real-world applications remains uncertain. Moreover, the model's computational demands stretched available resources to their limits, underscoring the complexity and resource intensity of this approach.

4. RESULTS & DISCUSSIONS

Our initial experiment employed a simple fully connected ANN model that performed reasonably well and showed promising results with an accuracy of 75%. Despite performing well, analysis revealed that it is still far from being applicable on real-world data. The confusion matrix depicted in Figure 5 reveals an unacceptably high false positive rate of approx. 40% for this model.

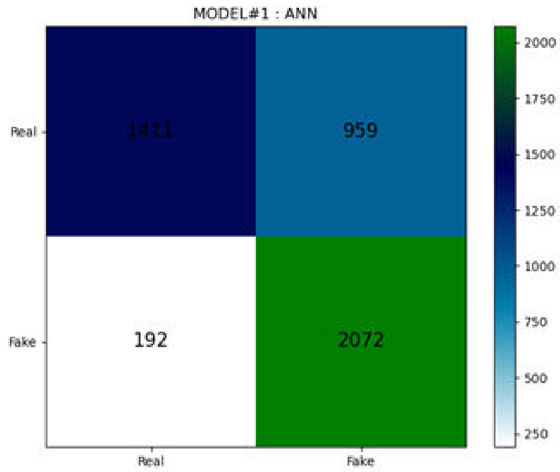


Figure 5: Confusion Matrix of ANN Model

The second model integrated an improved algorithm with optimization strategies, achieving an 83.7% accuracy on testing sets. Nevertheless, it faced challenges in generalizing to real-world data. Notably, this model exhibited a worrisome high false positive rate of 23.42%, while the false negative rate remained lower at 8.65%. Refer to Figure 6 for the confusion matrix of this optimized ANN model.

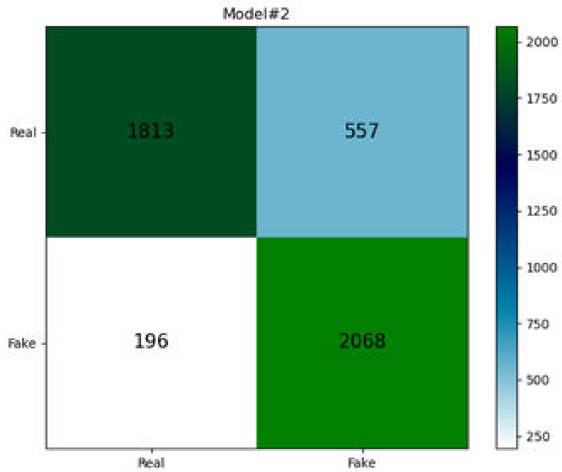


Figure 6: Confusion Matrix of optimised ANN Model

Despite commendable performance, both of our initial models fell short of our objectives, prompting a transition to a different neural network framework. Introducing LSTM layers, the new model utilized LSTMs and early stopping, achieving an accuracy of 85.5%. While maintaining elevated false positive rates at 18%, it marked an improvement over previous models, resulting in an overall error rate of 14.31%, the lowest observed so far. Refer to Figure 7 for the confusion matrix.

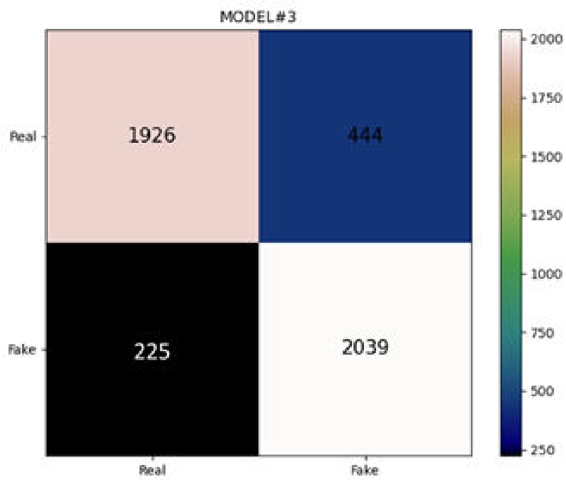


Figure 7: Confusion Matrix of LSTM Model

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

The model was subjected to testing using randomly generated AI and real audio clips from various sources, yielding the anticipated results. It demonstrated quite accurate and reliable predictions, showcasing superior generalization with real-world data compared to all previously trained models. However, further enhancements are still required to augment its accuracy even more. While this model surpassed its predecessors, it still lacked the required accuracy for real-world applications. Despite its performance, the high error rates deem it unreliable in practical scenarios. Nonetheless, being an ongoing research, we anticipate further studies to unveil more reliable technology and a more suitable framework with enhanced and accurate predictions.

During the evaluation of all these models, we observed a vulnerability—they were more prone to making inaccurate predictions when tested on audio clips containing noise. Moreover, different languages have unique phonetic characteristics and speech patterns. This made models prone to prediction errors, though the impact is minor yet significant. Model performance was observed to be improved when trained on a specific language, presenting challenges in cross-language predictions for the models we developed.

Figure 8 briefly showcases the metric of all the models. It's important to note that we trained numerous models beyond the three mentioned, but the majority proved ineffective, yielding inaccurate predictions. Consequently, we opted to discuss only those models whose performance showed some improvement and demonstrated a degree of effectiveness in detecting AI-SS. Moreover, since all these models were trained on NVIDIA GTX 1050 3GB DDR5, hardware limitations also restrained us from further exploration.

Figure 8: Model Metrics

MODEL NAME	PRECISION	RECALL	ACCURACY	F1 SCORE
ANN	0.68360277	0.91519434	0.7516184	0.7826251
OPTIMIZED ANN	0.78780952	0.91342756	0.8375053	0.8459807
LSTM	0.82118405	0.90061837	0.8556322	0.8590688

The comparative ROC curve analysis in Figure 9 illustrates the superiority of the LSTM model over both the ANN and optimized_ANN models in AI-SS detection. The LSTM model attains the highest AUC score (0.8566), signifying its superior capability to distinguish between true positives and false positives. The curve's shape suggests better performance in predicting positive cases (true positives) than negative cases (true negatives).

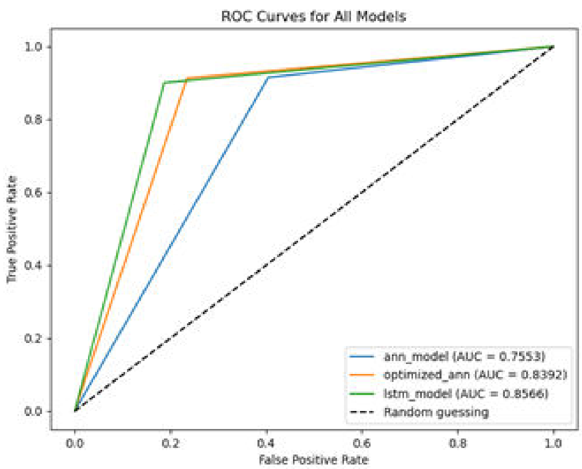


Figure 9: Comparative ROC Analysis

These results imply that LSTM-based approaches hold promise for further research aimed at enhancing the accuracy and robustness of AI-SS detection systems. Further analysis of curve shapes reveals the LSTM and optimized ANN's well-calibrated decision-making process, while the standard ANN may benefit from additional calibration fine-tuning.

5. CONCLUSION

Initial exploration of AI-SS detection using various DL models yielded promising results, with benchmark accuracy reaching 85.5%. However, hardware constraints further hindered the investigation of deeper, potentially more powerful architectures. The consolidation of diverse audio datasets into a comprehensive superseding set for training the model more dynamically proved instrumental. Evaluation results demonstrated our models' impressive accuracy in real-world scenarios, showcasing resilience across gender and linguistic variances to a notable extent.

Nonetheless, the feasibility of extrapolating these results to real-world applications remains uncertain, hinting at limitations in model generalizability and potential overfitting. This distinctive approach of dynamic training using combined dataset to enhance generalizability distinguishes our study from prior research in the field, marking a significant stride towards robust and inclusive audio deepfake detection.

6. REFERENCES

[1] Z. Wu et al., "ASVspoof 2015: the first automatic speaker verification spoofing and countermeasures challenge," in Interspeech 2015, ISCA: ISCA, Sep. 2015, pp. 2037–2041. doi: 10.21437/Interspeech.2015-462.

[2] J. Khochare, C. Joshi, B. Yenarkar, S. Suratkar, and F. Kazi, "A Deep Learning Framework for Audio Deepfake Detection," Arab J Sci Eng, vol. 47, no. 3, pp. 3447–3458, Mar. 2022, doi: 10.1007/s13369-021-06297-w.

[3] R. Reimao and V. Tzerpos, "FoR: A Dataset for Synthetic Speech Detection." [Online]. Available: https://www.kaggle.com/percevalw/englishfrench-translations/kernels

[4] B. Lambert, "Louis Gerstman, 61, a Specialist In Speech Disorders and Processes," The New York Times, Mar. 1992, Accessed: Jan. 28, 2024. [Online]. Available: https://www.nytimes.com/1992/03/21/nyregion/louis-gerstman-61-a-specialist-in-speech-disorders-and-processes.html

[5] Z. Almutairi and H. Elgibreen, "A Review of Modern Audio Deepfake Detection Methods: Challenges and Future Directions," Algorithms, vol. 15, no. 5. MDPI, May 01, 2022. doi: 10.3390/a15050155.

[6] A. K. Singh and P. Singh, "Detection of AI-Synthesized Speech Using Cepstral & Bispectral Statistics," Sep. 2020, [Online]. Available: http://arxiv.org/abs/2009.01934

[7] A. Hamza et al., "Deepfake Audio Detection via MFCC features using Machine Learning," IEEE Access, 2022, doi: 10.1109/ACCESS.2022.3231480.

[8] N. Subramani and D. Rao, "Learning Efficient Representations for Fake Speech Detection." [Online]. Available: https://www.wsj.com/articles/fraudsters-use-

[9] D. M. Ballesteros, Y. Rodriguez-Ortega, D. Renza, and G. Arce, "Deep4SNet: deep learning for fake speech classification," Expert Syst Appl, vol. 184, p. 115465, Dec. 2021, doi: 10.1016/J.ESWA.2021.115465.

[10] C. Sun, S. Jia, S. Hou, E. AlBadawy, and S. Lyu, "Exposing AI-Synthesized Human Voices Using Neural Vocoder Artifacts," Feb. 2023, [Online]. Available: http://arxiv.org/abs/2302.09198

[11] R. Reimao and V. Tzerpos, "Synthetic Speech Detection Using Neural Networks," in 2021 International Conference on Speech Technology and Human-Computer Dialogue (SpeD), IEEE, Oct. 2021, pp. 97–102. doi: 10.1109/SpeD53181.2021.9587406.

REVOLUTIONIZING RETAIL: A SMART SHOPPING CART APPROACH WITH RFID INTEGRATION

Dr. Neelam Naik Ashish Mondal and Mihir Jalgaonkar
Department of Information Technology SVKM's Usha Pravin Gandhi College of Arts, Science and Commerce
Maharashtra, Mumbai, 400056

ABSTRACT

The retail landscape is undergoing a transformative shift driven by technological advancements, with IoT and RFID technology at the forefront. This article introduces an innovative IoT-based Smart Shopping Cart, leveraging RFID to disrupt traditional retail dynamics. Seamlessly integrating the physical and digital realms enhances shopping efficiency and provides data-driven insights for a customized customer experience.

Revised Content: Technology has reshaped conventional shopping, introducing solutions for efficiency and convenience. This article details an IoT-based Smart Shopping Cart system using RFID to revolutionize the shopping experience. Blending physical and digital realms streamlines shopping, optimizes inventory management, and offers crucial data for merchants and consumers.

The RFID Smart Trolley System represents a paradigm shift in retail, incorporating RFID tags and readers into shopping carts for an intelligent retail environment. Real-time product registration eliminates manual scanning and reduces checkout times. The system enables real-time inventory tracking, allowing proactive restocking and minimizing stockouts. Integration of customer profiles with RFID provides a personalized shopping experience, offering tailored recommendations and promotions. RFID tags also deter theft, triggering alarms for unregistered items.

The system generates valuable data analytics on customer behavior, popular products, and peak shopping times, empowering retailers for strategic decision-making. The RFID Smart Trolley System, with contactless payment alternatives, meets the demand for safe and convenient payments. This system remains a pioneering force in retail innovation, laying the groundwork for a more efficient, data-driven, and customer-centric future.

Keywords: RFID, Smart Shopping Cart, IoT, Retail Innovation, Inventory Tracking, Personalized Shopping, Theft Deterrence, Data Analytics, Contactless Payment, Customer-Centric Commerce.

I. INTRODUCTION

Within the ever-changing landscape of retail, continuous technological advancements are reshaping our approach to the shopping experience. The RFID Smart Trolley System represents a revolutionary device seamlessly integrating Radio-Frequency Identification (RFID) technology into the traditional shopping cart. This groundbreaking technology not only transforms the checkout process but revolutionizes the entire shopping journey.

Through automated product identification, real- time inventory management, and personalized shopping experiences, the RFID Smart Trolley ushers in a new era in retail, where efficiency, convenience, and customer satisfaction converge to define the future of shopping. This introduction establishes the groundwork for a comprehensive exploration of the myriad benefits and implications of the RFID Smart Trolley System in the dynamic and competitive realm of modern retail.

In recent years, the retail sector has experienced a profound technological shift, especially within the Internet of Things (IoT) domain. A notable application of IoT technology in retail is the emergence of smart shopping carts, leveraging Radio-Frequency Identification (RFID) for enhanced functionalities. This innovative development underscores the industry's commitment to embracing technology to redefine the customer shopping experience.

ISSN 2394 - 7780

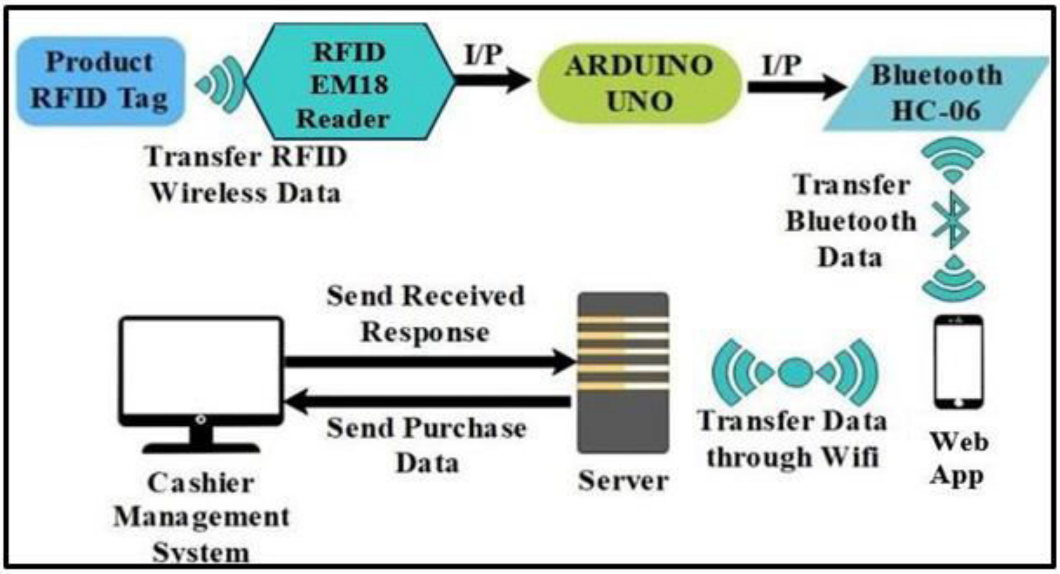


Fig 1.1 Data Flow Diagram

The above diagram data flow diagram delineates a holistic system designed for efficient product tracking, inventory management, smart billing, and an enhanced shopping experience. The process initiates with Passive RFID tags affixed to products, serving as data sources with unique identifiers and product information. As these tagged products traverse the retail space, the RFID Reader (EM18) captures and interprets the data.

The processed information undergoes seamless transmission to an Arduino Uno, functioning as a central processing unit. Integrated with a Bluetooth module (HC-06), the Arduino Uno enables wireless communication, establishing a connection with the Cart website. This connectivity ensures real-time updates not only for inventory management but also for smart billing purposes.

The inclusion of smart billing features allows the system to automate transaction processes, providing customers with an efficient and hassle-free checkout experience. Additionally, the system contributes to a smart shopping experience by offering personalized recommendations and promotions based on the RFID-tagged products in the customer's cart. This intelligent integration of technology not only streamlines inventory processes but also elevates the overall retail environment by enhancing customer satisfaction and optimizing operational efficiency.

II. METHODOLOGY

In the contemporary day, when a consumer wants to buy an item, he or she must place it in the shopping cart, where the RFID reader reads the RFID passive tag that is connected to each object. Product data will be shown on the Cart Website tied to the customer's shopping cart.

A. Procedure

This entire procedure is based on case study and survey.

B. Components

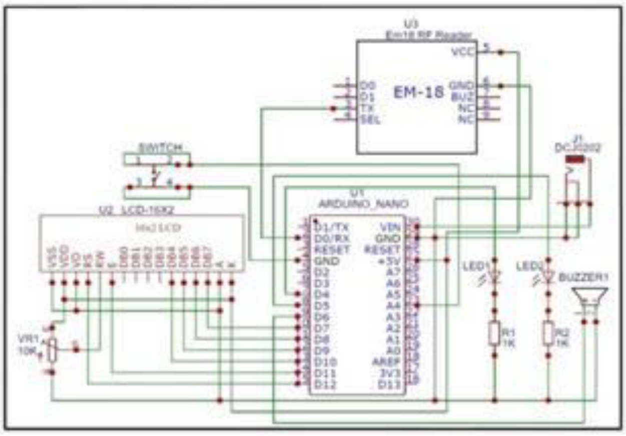


Fig 2.1 Schematic Diagram

 ISSN 2394 - 7780

Fig. 2.2 RFID EM18 module

1. EM18 RFID Reader:

EM18 is a RFID reader which is used to read RFID tags of frequency 125 kHz.

After reading tags, it transmits unique ID serially to the PC or microcontroller using UART communication or Wiegand format on respective pins.

EM18 RFID reader reads the data from RFID tags which contains stored ID which is of 12 bytes. EM18 RFID reader doesn't require line- of-sight. Also, it has identification range which is short i.e. in few centimeters.

RFID Reader EM-18 Features:
1. Serial RS232/TTL output
2. Operating Frequency is 125 KHz.
3. Range is 5-8 cm.

Specification of RFID EM18
- Operating frequency: 125kHz
- Operating voltage: DC 5V
- Supply current: <50mA
- Read distance: up to 100mm (depending on the tag used)
- Interface: UART (TTL level)
- Dimensions: 40mm x 40mm x 16mm
- Communication protocol: UART
- Baud rate: 9600, 8, N, 1

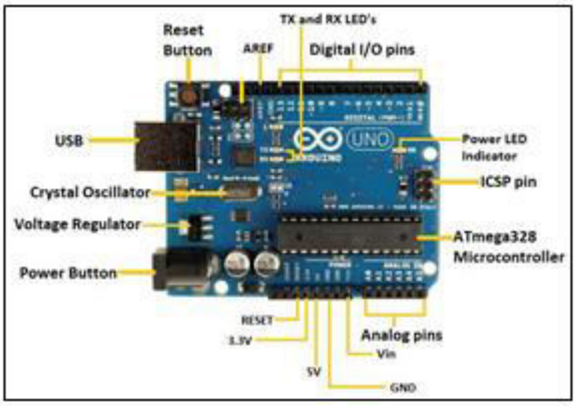


Fig 2.3 Arduino UNO

2. **Arduino UNO**

Arduino UNO is a microcontroller board built on the ATmega328P. It contains 14 digital input/output pins (6 of which may be used as PWM outputs), 6 analog inputs, a 16 MHz ceramic resonator, a USB port, a power connector, an ICSP header, and a reset button. It includes everything necessary to support the microcontroller; simply connect it to a computer via USB connection or power it with an AC-to-DC converter or battery to get

ISSN 2394 - 7780

started. You can tamper with your UNO without worrying about making a mistake; worst case scenario, you can replace the chip for a few bucks and start over.

Arduino board designs incorporate a range of microprocessors and controllers. The boards provide sets of digital and analog input/output (I/O) pins that may be connected to various expansion boards ('shields'), breadboards (for prototyping), and other circuits. The boards provide serial connection ports, including Universal Serial Bus (USB) on some variants, which may also be used to load applications. The microcontrollers may be programmed using the C and C++ programming languages (Embedded C), as well as a standard API known as the Arduino Programming Language, which is inspired by the Processing language and runs on a modified version of the Processing IDE.

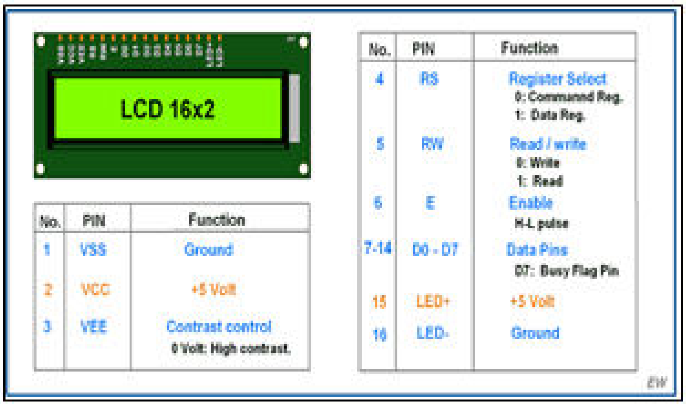


Fig 2.4 LCD Module 16x2

3. **LCD**

Liquid Crystal Display (LCD) is widely used in various electronics applications. It is commonly used in various systems to show different status and parameters. LCD16x2 has 2 lines with 16 characters in each line. Each character is made up of a 5x8 (column x row) pixel matrix.

First two pins of LCD16x2 are used for ground and supply (+5 V).

Pin 3 - VEE pin

This pin is used for adjusting the contrast of the display. Voltage on this pin defines contrast on display, lower the voltage, higher the contrast. We can connect 4.7 k pot for contrast adjustment or simply connect this pin to ground to get maximum contrast.

Pin 4 –RS: Register Select pin

RS = 0: Data on the D0 to D7 pins is considered as a command.

RS = 1: Data on the D0 to D7 pins is considered as data to display

Pin 5 – RW: Read / Write pin RW = 0: Write data to the LCD RW = 1: Read data from the LCD Pin 6 –E: Enable

This pin is used to latch the data present on the data pins D0 to D7. High to low pulse with a minimum width of 450 ns is required to latch the data to the display.

Pins 7:14 - DATA pins D0 to D7

Data pins are used to send data/command to the LCD16x2 as parallel 8 data bits.

Pin 15:16 - LED + and LED -

Liquid Crystal Displays don't have their own light like seven segment displays. Therefore, the module has a backlight LED. Supply to this LED is provided through these pins.

Specification of LCD16x2

Display Type: Alphanumeric character display. Character Format: 5x8 dots matrix format.

Display Size: 16 characters x 2 lines. Display Color: Blue or Green.

Backlight: LED backlight. Voltage Supply: 5V DC.

 ISSN 2394 - 7780

Operating Temperature: -20°C to +70°C. Interface: 4-bit or 8-bit mode.

Dimension: 84.0 x 44.0 x 13.0 mm.

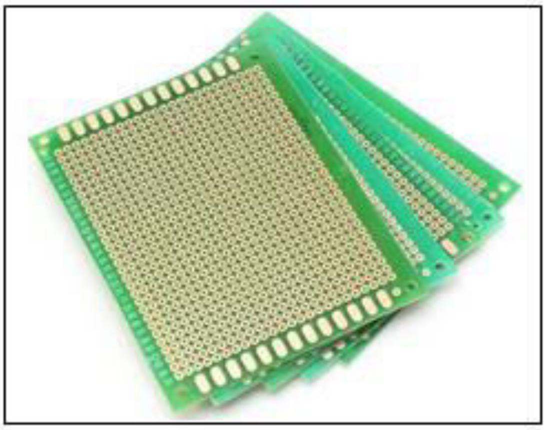


Fig 2.5 PCB Solder Board

4. **Green PCB Solder Board**

PCBs are primarily utilized to link and support a circuit's electrical components. They are common in electrical gadgets and may be easily identified as the green board in most circumstances. PCBs have a wide range of applications, making it difficult to choose a single one. In reality, practically every gadget or thing that use a PCB requires its own distinct version. Now, the general aim of a PCB is to connect all of the components that a device requires. The PCB helps the gadget work by employing a variety of materials and can even allow for sophisticated procedures.

6. Jumper Wires

Jumpers are small metal connectors used to seal or open circuit components. They have two or more connecting points that control an electrical circuit board.

Fig 2.6 Buzzer

5. **Buzzer**

The piezo, often known as the buzzer, is a component used to produce sound. It is a digital component that connects to digital outputs and generates a tone when the output is HIGH. It may also be coupled to an analog pulse-width modulation output to produce different tones and effects. The Grove Buzzer has a sound output of 85 decibels and may run at 3.3V or 5V. This module may be used to offer auditory feedback to your application, similar to the click of a button on a digital watch.

Inside the buzzer, a membrane, similar to a drumhead, vibrates in response to electric current. When tone(BUZZER, 85) is executed, current flows across the membrane and deforms it. For noTone(BUZZER), the current ceases and the membrane returns to its previous form. When the current is swiftly switched on and off, the membrane vibrates back and forth, producing audible sound waves. The speed of the vibration may be controlled by adjusting the rate at which the current is switched on and off. Faster vibrations produce higher pitches, and slower vibrations produce lower pitches.

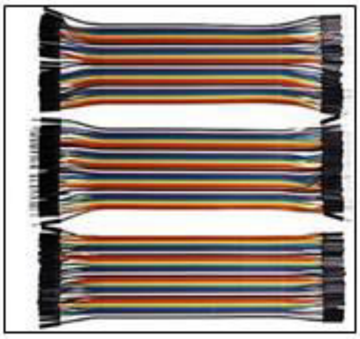


Fig 2.7 Jumper Wires

Their job is to configure the settings for computer devices such as the motherboard. Assume your motherboard supports intrusion detection. A jumper can be used to activate or deactivate it.

Jumper wires are electrical lines having connection pins on both ends. They are used to link two locations in a circuit without using solder.

Jumper wires can be used to alter or troubleshoot circuits. Furthermore, they are best employed to bypass a section of the circuit that lacks a resistor and is thought to be defective.

Types of Jumper Wires

Jumper wires come in three versions:

- Male-to-male jumper
- Male-to-female jumper
- Female-to-female jumper

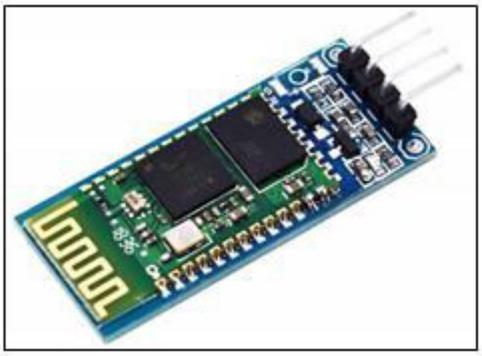


Fig 2.8 Bluetooth Module HC-06

7. **HC -06 Bluetooth Module**

The HC-06 is a Bluetooth module used to facilitate short-range wireless data transmission between two microcontrollers or systems. The module operates on the Bluetooth 2.0 communication protocol and can only function as a slave device. This is the cheapest and most versatile means of wireless data transfer, and it can send files at speeds of up to 2.1Mb/s.

The HC-06 employs the frequency hopping spread spectrum method (FHSS) to prevent interference with other devices and to provide full duplex communication. The gadget operates on frequencies ranging from 2.402 GHz to 2.480 GHz.

Pin configuration

The HC-06 module has six pins, as illustrated in the pinout. We just need four in order to effectively interface the module. Due to this, some breakout boards will only have four output pins.

The module is linked to a +5V standard regulated power source, and the UART interface is configured as indicated in the picture. All you need to do is link the Arduino's RXD to the module's TXD, which is connected to the module's RXD via a resistor voltage divider. This voltage divider is designed to convert 5V logic signals

ISSN 2394 - 7780

delivered by the Arduino to +3.3V logic signals suited for the module. If different power sources are utilized, the arduino and module's ground must be linked to provide voltage reference.

Fig 2.9 3.7 V battery

8. **Power Supply or Battery**

All Arduino boards require electrical electricity to work. A power supply provides electric power to the boards and might be a battery, USB cable, AC adapter, or a regulated power source device.

There are several ways to power an Arduino board. The most frequent method is to use the USB connector found on every board, but there are a few additional ways to power your board.

Arduino boards can function successfully with power from the USB port. It delivers 5V DC electricity and may be powered by a PC, wall socket converter, or portable power bank.

Some boards have a Li-Po (Lithium-ion Polymer) battery socket that accepts this type of battery. This capability is available on MKR boards (with the exception of the MKR FOX and WAN 1300). These batteries produce 3.7V, are rechargeable, and can deliver more energy than ordinary lithium batteries.

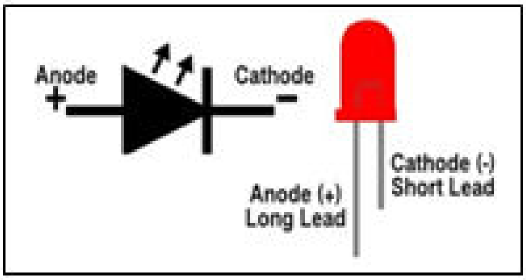


Fig 2.10 LED bulb

9. **LED Lights**

LEDs (light-emitting diodes) are tiny, brilliant, energy-efficient lights that are widely utilized in electrical equipment.

An LED light is a polarized component, which means it must be connected to a circuit in a specific way to function properly. Each LED has two legs: one positive and one negative. These may be detected visually by their length: the negative leg has been shortened.

To make it easier to plug the LED into a breadboard, carefully bend the positive leg as illustrated until all legs are the same length. You can still see them visually: the straight leg is negative, while the bent leg is positive. The negative leg of the LED must be connected to GND (-). The positive leg is attached to any I/O pin that will act as a power source (+).

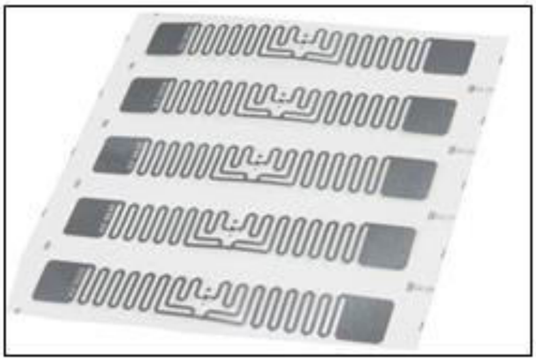


Fig 2.11 Passive RFID Tags

10. **RFID Tags**

RFID (Radio Frequency Identification) tags are quickly becoming a part of our everyday life, although many people are still unfamiliar with the technology. RFID tags are tiny electronic devices that store data and connect with other devices via radio waves. They are used for a number of purposes, including tracking inventory in warehouses and monitoring animal movements. These radio waves carry data from the tag to a reader, which sends it to an RFID computer software. RFID tags are commonly used for commerce, but they may also be used to track automobiles, pets, and even Alzheimer's patients.

There are two types of RFID tags: battery- operated and passive.

Battery-operated RFID tags use an inbuilt battery as a power source. Battery-powered RFID tags may also be referred to as active RFID tags.

Passive RFID tags are not battery-powered and instead rely on electromagnetic energy delivered from an RFID reader.

Passive RFID tags employ three major frequencies to send information:

There are three frequencies: 125-134 KHz (Low Frequency), 13.56 MHz (High Frequency), 865- 960 MHz (UHF), and Near-Field Communication.

III. Case Study

Numerous studies have looked extensively into understanding the IOT-Based smart shopping cart using RFID. The researcher [1] presents a shopping system that streamlines processes, reduces queues, and improves customer satisfaction. It uses RFID technology, IR sensors, and a Django Web Application to track transactions. The system is connected to a Raspberry Pi for inventory management and an Amazon RDS MySQL for customer history. Future designs may incorporate RFID reader and weight mats. The author [2] proposes a system in shopping centers to improve the process of billing. All merchandise in the mall should be equipped with RFID tags and each trolley should have an RFID reader and digital display screen. The

RFID tag will automatically identify the item's code, name, and cost, adding it to the total bill. If the item is removed, the cost is deducted from the total, and the data is sent to a central billing unit via ZigBee module. The research

[12] Decathlon, a leading sports retailer, has strategically implemented RFID tags and mobile payments to revolutionize the shopping experience at its newest store in Mumbai, Maharashtra, India. This case study explores the seamless integration of RFID technology and mobile payments, enabling customers to use self-checkout kiosks without the need to scan barcodes, exemplifying Decathlon's commitment to disruptive and innovative retail solutions.

RFID Technology Implementation:

Decathlon's Mumbai store, utilizes RFID tags strategically placed on items across the premises. These tags enable automatic recognition of products when customers use self-checkout.

User Experience:

Customers simply place items in a designated area on the self-checkout kiosk, allowing the RFID tag to be read and the product's details captured. The innovative system streamlines the checkout process, providing a hassle-free experience. In cases where an item is not automatically recognized, customers are prompted to scan the barcode.

Mobile Payment Integration:

Decathlon's self-checkout system incorporates mobile payments using India's electronic payments systems. After reviewing and verifying their order, customers use the kiosk's touchscreen to complete the payment process, ensuring a convenient and efficient transaction.

Innovative Store Features:

The Decathlon Mumbai Lab serves as a test bed for disruptive and innovative solutions. Beyond RFID technology, the store features interactive zones for customers to test products, such as basketball-playing areas and surfaces for trying running shoes. The implementation of cutting-edge technologies aligns with Decathlon's commitment to providing a unique and engaging shopping environment.

Fulfillment and Delivery:

Decathlon's use of RFID tags extends beyond in-store transactions to efficient order fulfillment. The technology enables the retailer to pick and fulfill online orders promptly. Customers can opt for two hour delivery or choose to collect their orders directly from the store, showcasing the versatility and effectiveness of the RFID system.

 ISSN 2394 - 7780

Fig 3.1 Decathlons smart checkout counters

[13] France sporting goods retailer Decathlon said, last year their sales increased by 11% and thanks to the RFID technology deployed by 951 stores and 43 warehouses (Logistics Center). Decathlon RFID project leader Jean-Marc Lieby said the company also reduced the rate of 9% loss of goods. At present, most of the stores using RFID technology at the checkout counter and security, used for inventory check purposes. India and Brazil stores use RFID only for inventory tracking. In addition, the company's new opened stores will use RFID technology in the future.

The retailers attributed 5% sales growth to the use of RFID inventory tracking system. The company added that new stores and rising of commodity prices are also part of reason for sales rising.

Decathlon is the world's largest retailer of sports goods and sportswear, stores in Europe, China, Morocco, India, and Brazil. The retailer uses 50,000 containers shipped 6.5 billion items each year. Lieby said about 85% products using RFID tags.

[3] proposed to eliminate the time-consuming shopping process and improve service quality. It consists of RFID sensors, Arduino microcontroller, Bluetooth module, and a mobile application. RFID tags and readers efficiently read product information, which is displayed in the mobile application. The system can be easily implemented and tested on a commercial scale, making it more competitive than other models. The research states [4] IOT is revolutionizing the way we interact with everyday objects, transforming the way we shop. A smart shopping system, equipped with an RFID reader, allows for the automatic reading of RFID tags on products placed in a smart cart. This system streamlines inventory management and reduces customer wait times at checkout. The system also includes smart shelving for stock monitoring and updates to a central server. This innovative approach to smart shopping is a game-changer in IOT technology. The research purpose [5] RFID technology is revolutionizing the way people shop and pay at retail stores. It reduces the time spent on the tedious process of preparing bills using bar code readers. This innovative concept of Intelligent Smart Shopping and Billing aims to provide a technology- oriented, economical, and scalable system for efficient, convenient, and efficient shopping in person. [6] RFID technology is being increasingly used in online shopping and shopping centers. A smart shopping cart is being proposed that uses RFID and ZIGBEE technology to identify product details and send data wirelessly to receivers. The cart can display available products on-screen and interact with the Main Server to generate bills for added products. This system aims to avoid queues in shopping malls and make shopping more enjoyable. Key terms include IR Sensor, ZIGBEE, RFID Reader, RFID Tags, and smart cart. [7] E-commerce has led to increased shopping in supermarkets and malls, but customers still face difficulties in the billing process. Waiting in queues consumes time and inconvenience, especially in overcrowded supermarkets. Shopkeepers are considering smart machines to automate the billing process,

reducing manpower and time spent. The main aim is to satisfy customers and reduce time spent on the billing process. Customers can add products, pay by ATM cards or pre-recharged cards, and ensure security for theft prevention. The ultimate goal is to reduce time consumption, customer comfort, and biller waging. [8] The paper presents a cost-effective Smart Shopping Cart using IOT innovations for Walmart and supermarkets. This system streamlines the shopping process, reducing work and providing superior customer experience. It offers predefined and random shopping, allows for parallel shopping using multiple carts, and detects shoplifter theft. The system also allows for Cart-to- Cart communication, allowing customers to share their shopping list with co-shoppers. It also allows for valuable business insights by analyzing customer behavior and predicting sales rates. This system ensures customers have a seamless shopping experience, leading to increased visits to Walmart. [9] The paper proposes a Smart Cart that uses IOT and a mobile app to generate bills for traditional shopping. The cart uses RFID tags, receivers, load cells, LCD displays, and Raspberry Pi to scan products, prevent theft, and display product amounts. Customers can easily pay bills through the mobile app. [10] The project aims to improve comfort, accommodation, and efficiency in daily life by utilizing the Internet of Things (IOT) in smart shopping carts. The prototype consists of RFID tags for product identification and RFID readers for scanning. The data collected from the tags is stored in a NodeMCU, allowing customers to pay at the billing counter. This innovative approach reduces human effort, queue time, and time spent on billing, making it more convenient for customers. [11] This research explores the use of radio frequency identification (RFID) technology in the Internet of Things (IOT), focusing on its potential applications in healthcare, construction, smart shopping, hospitality, and transportation. The system aims to generate digital bills for shopping carts, saving customers time and ensuring secure transactions. The study highlights the potential of RFID technology in improving future shopping experiences.

IV. CONCLUSION

Finally, the introduction of smart trolleys with passive RFID tags represents a paradigm change in the retail and logistics industries. The seamless integration of this cutting-edge technology not only improves the overall efficiency of shopping experiences, but it also transforms inventory management systems. Passive RFID tags, with their minimal cost and power needs, provide a long-term and scalable option for organizations looking to optimize their processes. As we enter an era dominated by the Internet of Things (IoT), these smart trolleys demonstrate the potential of networked technologies to redefine traditional operations.

These RFID-enabled trolleys give businesses priceless insights about consumer behavior and product preferences, opening the path for individualized marketing campaigns. Furthermore, the strengthened security measures instill trust in consumers, reducing concerns about theft and product misplacement. As we enter the era of smart retail, the smart trolley with passive RFID technology emerges as a driver of enhanced consumer happiness, operational efficiency, and sustainable business practices. It not only exemplifies the convergence of innovation and pragmatism, but it also acts as a lighthouse, directing the future landscape of the retail business to unparalleled levels of technological improvement and consumer-centricity.

V. REFERENCE

[1] Sinha, Dipayan, et al. "Automated billing system using rfid and cloud." 2019 Innovations in Power and Advanced Computing Technologies (i- PACT). Vol. 1. IEEE, 2019.

[2] Prof. Roopa C1, N. C. Reddy Smart Shopping Cart. July-August-2020

[3] M. shahroz, M. faheem m, M. ahmad, S. ullah, A. mehmood, AND G. sang choi IOT-Based Smart Shopping Cart Using Radio Frequency Identification. 2020

[4] R. Li, T. Song, N. Capurso, J. Yu, J. Couture, and X. Cheng IOT Applications on Secure Smart Shopping System IEEE 2017

[5] Z. Ali, R. Sonkusare RFID based Smart Shopping 2014

[6] Komal Machhirke, Priyanka Goche, Rupali Rathod, Rinku Petkar, Manohar Golait A New Technology of Smart Shopping Cart using RFID and ZIGBEE. 2017

[7] Manikandan T*, Mohammed Aejaz M.A, Nithin Krishna N.M, Mohan Kumar A.P, Manigandan R RFID based Advanced Shopping Trolley for Super Market 2017

[8] An IOT Based Smart Shopping Cart for Smart Shopping Srinidhi Karjol, Anusha K. Holla, C. B. Abhilash, P. V. Amrutha & Y. V. Manohar 2018

[9] S Kowshika; S.S Madhu mitha; G Madhu Varshini; V Megha; K Lakshmi IOT based Smart Shopping Trolley with Mobile Cart Application 2021

ISSN 2394 - 7780

[10] IOT Based Smart Cart Using RFID and NodeMCU Sumanth Kasula 2021

[11] Rajeev Ratna Vallabhuni; S. Lakshmanachari; G. Avanthi; Vallabhuni Vijay Smart Cart Shopping System with an RFID Interface for Human Assistance 2020

[12] https://twitter.com/ishanagarwal24/status/16 38454301956911105

[13] https://www.linkedin.com/pulse/decathlons- rfid-project-achieved-remarkable-results- you-rfid-cathy-wu/

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

GROCERY CART BILLING SYSTEM USING OBJECT DETECTION ALGORITHM

Dr. Manisha Divate and Krishnakumar Singh
SVKM'S Usha Pravin Gandhi College of Arts, Science and Commerce, Vile Parle, Mumbai, India

ABSTRACT
This research work presents a technique to provide a cost-effective solution to minimize the labor cost, keep track of inventory of stock and stay competitive in market. Growing technologies have made the world move fast. Automations have made life easy and fast-moving. Cashier less Toll paying (Fast Tag) saves much of the time by not standing in long queues. Amazon Go, a convenience store chain is operated cashier less in the United States and the United Kingdom. This not only makes shopping easy but helps in automating the inventory system.

Keywords: Grocery, Retail, Product Recognition, Item Identification, Inventory monitoring, Object-detection, Billing System, Supermarket.

1. INTRODUCTION

Growing technologies have made the world move fast. Automations have made life easy and fast-moving. Cashierless Toll paying (FastTag) saves much of the time by not standing in long queues. Amazon Go, a convenience store chain is operated cashierless in the United States and the United Kingdom. This not only makes shopping easy but helps in automating the inventory system. In India, "WATASALE" is a shopping mart located in Karela have an auto-billing system whose idea proposed through Amazon Go. On a similar ground, we proposed the Auto-Grocery Billing system, which will help the buyer to buy the product hassle- free.

This research work provides a cashier less store, it allows consumer to pick any product and put into the basket and leave the store without waiting in a huge line for checkout. This research work proposes Smart shopping Cart. This is achieved by machine vision so cart will contain camera that will keep track of identify item placed into cart. The Raspberry Pi will be used to process the data and display to the customer. At the end system team will generate bill on customer mobile phone.

The four phases which cashier less store focuses are: the before purchase phase, the check-in phase, the product selection phase and the check-out phase. The technologies used by cashier less stores are sensor fusion and deep learning phase which help in track of products.

This research had noticed that traditional retailors need to pay cost to labors for monitor shelf-inventory. Currently in India, all shopping marts require cashier for checkout and billing purpose. This in retailer point of view is extra waste of money. This system [1][3] is very useful in minimizing human involvement in marts or superstores and save labor charges.

2. LITERATURE SURVEY

This section is going to introduce about retail product recognition system and defining about automation retail product recognition system. Then it will define about the proposed system how it benefits from other existing system.

In India, "WATASALE" is a shopping mart located in Karela

[1] have an auto-billing system whose idea proposed through Amazon Go. It works on a combination of computer vision, AI, and sensor fusion. The pre-requisites are Watasale app that needed to scan while entering into store that keep sum up of digital bill amount that will get deducted through app.

IKEA has a self-scanning and checkout system [2]. The user needs to pick the product needed then at checkout machine they must enter cell phone and start scanning product, it will generate bill that need to pay using Google Pay, QR Code, Card, etc. and walk out.

In Automatic Retail Product Identification System for Cashier less Stores [3], the computer vision plays main role for recognition product picked by customer from shelf or put back onto the shelf. It was lacking between similar product having same color, shape, and appearance. With Image recognition and text classification is used for resolving issue of retail product Identification by its label. Word2Vec and Mittens are used to get all text data from product.

In AIM3S (Autonomous Inventory Monitoring through Multi- Modal Sensing for Cashier-Less Convenience Stores), it has focused mainly on weight based and vision-based Image detection system. Weight keeps help of

ISSN 2394 - 7780

track of good lifted by consumer from the shelf or dropped back on shelf and Image try to capture human posture and actions, it will keep track of good for Inventory management system. Shelf having sensors and camera placed around it, sensor keep track of weight of product lifted and based on lifted product camera will recognize the product and text and charge accordingly.

3. EXISTING SYSTEM

In the existing system, the idea of a smart trolley has to be started implementing in the supermarkets. It is daily routine to shop and purchase the product from supermarket or malls. Currently, in malls people use to select their product and they will move to the billing counter to pay the bills, and cashier uses barcode scanner to scan the product to generate the bills. This takes long time to customer to stand in the queue waiting for their turn. To overcome the above-mentioned problem, machine vision along with machine learning is adopted on the cart to proposed smart shopping system.

4. PROPOSED SYSTEM

The proposed system will overcome with existing problem of standing in long queue for paying bill in checkout counter. The advanced shopping cart will be having Camera, Raspberry pi 4, Loadcell and LCD screen. To add the item into list, customer have to add item to the cart and camera will scan the product or QR code. The data of added item are stored into the cloud database.

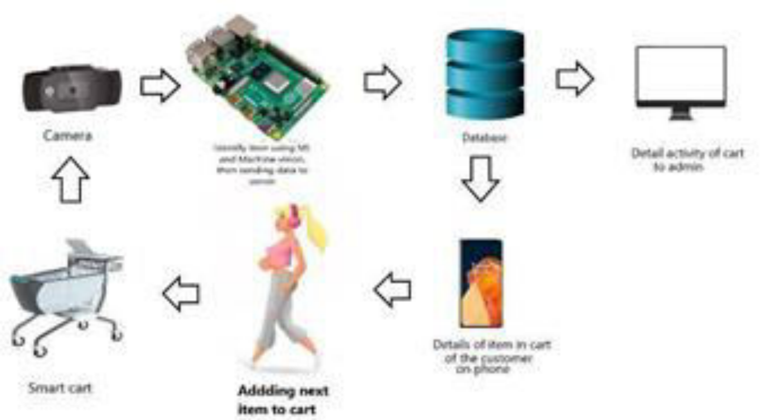


Fig. 1 Process Diagram

Once the shopping will be completed, LCD display list of item added into cart then user select the option of Checkout to pay the bills.

The Raspberry Pi does the barcode reading and object detection. In Proposed system we are using NoSQL database server. The data of scan product from Raspberry Pi will be stored in database in secure manner.

The steps of proposed smart shopping cart are as follows:

Step 1: First customer will scan QR code of shopping cart in their phone to make link between mobile device and shopping cart, which will help in bill generation and invoicing system.

Step 2: Customer have to grab product from the shopping mart and place into shopping cart.

Step 3: The camera will use object recognition feature and while placed product in cart and Loadcell will detect weight of an object which will help to recognize the product. This will help to update the user cart database and display product in shopping cart display.

Step 4: If product is not recognized properly through camera then Loadcell will help to detect product with its weight.

Step 5: If customer does not wish to buy item placed in the cart, they simply need to grab the product from the cart. This will be detecting an object using camera and update the database of user.

Step 6: If customer completes its shopping, they simply need to click on Checkout button to proceed for payment of the product.

Step 7: This will redirect customer to payment processing page for complete the payment.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

5. HARDWARE DESCRIPTION

5.1 Raspberry Pi 4 Model B

Fig. 2: Raspberry Pi 4

The Raspberry Pi 4 as presented in Fig. 2, used in this project which comes with all required hardware specification. It has 1.5 GHz quad core processor, Wi-Fi, Bluetooth, ethernet, micro-HDMI port, USB C port for power Raspberry Pi 4, it has 2GB RAM which is sufficient for this project, it has 2 USB 3.0 port and 2 USB 2.0 port which will connect all the required hardware.

5.2 Loadcell:

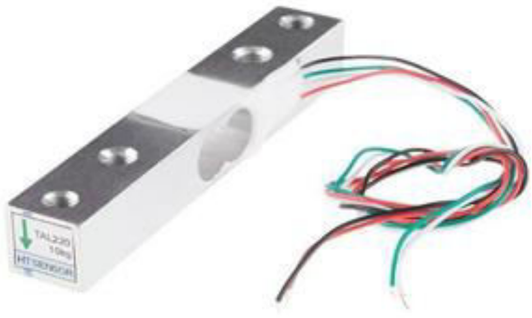


Fig. 3: Loadcell

Load cells in Fig. 3 is the sensor that detect force. The applied force in the load cell gets converted to electrical signal. This straight bar load cell can translate up to 20kg of pressure (force) into an electrical signal. The roll if load cell in this project is to help in verify that the item is scanned before it is placed in the cart and help in the process of detection when a customer removes an item from the cart.

Load cells are also known as "load transducers," because they convert a load (force) into electrical signals.

5.3 Display:

Fig. 4: Display

Display in Fig.4 is a mid-sized 7-inch touch screen display. This is used to display all different kind of information such as a text, image, shapes, and videos. It has resolution of 720p which is perfect fit for this project. In this project it will show the product name, price and quantity of the product while placed product in the cart.

5.3 Camera:

Fig. 5: Camera

Camera Fig. 5 Raspberry Pi Camera is used for project implementation. It has 5mp camera having high resolution of HD 1080p video. This mini camera is very powerful to detect small details of object placed in cart.

6. CONCLUSION AND FUTURE WORK

The proposed system will overcome with existing problem of standing in long queues. This will help consumer to easily checkout and process payment without standing in long queue. The proposed system will let valuable customer to get product information before purchase. The proposed shopping cart will play a vital role for shopping marts by helping to be competitive in market.

7. REFERENCES

[1] Vinci Mathews, Co-Founder & CFO, WATASALE, Automated billing system, 2018.

[2] "IKEA reopens in Ottawa during COVID-19 pandemic". 26 May 2020. Archived from the original on 6 April 2023. Retrieved 18 June 2022.

[3] Shiting Zhong, Automatic Retail Product Identification System for Cashierless Stores, February 2021

[4] Schogel, Marcus (2020). "Cashierless Stores – the New Way to the Customer?" (PDF).

[5] "What is Computer Vision? | IBM". www.ibm.com. Retrieved 2023-04-08.[6] "What is Deep Learning? - Deep Learning Explained - AWS". Amazon Web Services, Inc. Retrieved 2023-04-06.

[7] "What is sensor fusion?: AI terms explained - AI For Anyone". www.aiforanyone.org. Retrieved 2023- 04-06.

[8] “How Automated Billing Can Improve Productivity”. (https://gocardless.com/guides/posts/how-automated- billing-can-improve-productivity-for-startups.) Written by GoCardless

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024

ISSN 2394 - 7780

SEGMENTATION AND ANALYSIS OF GEOSPATIAL FEATURES FROM HIGH DIMENSIONAL DATA

Maurya Rajesh Kumar and Kaprawan Sandhya
Department of Information Technology, Usha Pravin Gandhi College of Arts, Science and Commerce Vile Parle(w), Mumbai, 40056

ABSTRACT

This document discusses the segmentation and analysis of geospatial features from high-dimensional data using machine learning techniques. It addresses the challenges in applying machine learning to geospatial data, such as handling high dimensionality, spatial dependencies, and model interpretability. It highlights the challenges of analysing such data and the effectiveness of methods like Kd-tree and deep learning. The paper emphasizes role of machine learning in land use classification and potential of novel algorithms for handling complex geospatial data. Analysis section details methodologies like decision trees and support vector machines, and experiments on hyperspectral unmixing and segmentation using models like Segment Anything Model (SAM) with high accuracy metrics. The paper concludes with the importance of machine learning in land use classification and potential improvements in performance through advanced technologies like drones and satellite imagery

Keywords: Kd-tree, SAM, CART, CNN-MTR, RF

I. INTRODUCTION

Geospatial feature segmentation and analysis from high- dimensional data using machine learning techniques is a rapidly evolving field that holds significant potential for a wide range of applications. This field involves the extraction of meaningful information from geospatial data, which is often high-dimensional, meaning it has many features or variables from which information can be extracted. Machine learning techniques, including both supervised and unsupervised learning algorithms and are increasingly being used to analyse this high-dimensional data. These techniques can identify patterns and structures within the data that may not be apparent through traditional analysis methods.

The segmentation of geospatial features involves dividing the data into distinct segments based on certain characteristics. This can help in understanding the spatial distribution of various features and in identifying areas of interest.

The analysis of these segmented features can provide valuable insights, such as identifying trends, predicting future scenarios, and informing decision-making processes. This can be particularly useful in fields such as disaster management, urban planning, environmental monitoring, etc.

However, the application domain of machine learning techniques to geospatial feature segmentation and analysis is not without its challenges. These include dealing with the high dimensionality of the data, handling spatial dependencies, and ensuring the robustness and interpretability of the models.

A portion of location-enhanced data known as geospatial data is formed by consumer electronics like mobile phones, RFID-tagged products, position and orientation sensors, and remote sensing equipment. These kinds of geographic data are typically employed in military settings. These geographical data have been the basis for numerous beneficial civilian applications that have been developed and implemented recently. For instance, a recommendation system that helps travellers in a certain area choose restaurants or tourist attractions. Civic organizations are now using geographical data from remote sensing devices to give residents enhanced services like weather reporting, pothole detection, and traffic monitoring.

Geospatial feature segmentation and analysis from high- dimensional data using machine learning techniques is a field that aims to extract meaningful information from geospatial data. This field is concerned with developing algorithms that can automatically segment and classify geospatial features such as buildings, roads, and vegetation from high- dimensional geospatial data. The high-dimensional nature of geospatial data makes it challenging to analyse using traditional machine learning techniques. Therefore, researchers have developed novel machine learning techniques that can handle high-dimensional geospatial data. These techniques include deep learning, support vector machines, and decision trees.

In this paper, we will explore the various machine learning methods that have been developed for geospatial feature segmentation and analysis from high-dimensional data. We will discuss the advantages and disadvantages of each technique and provide a comparative analysis of their performance. We will also discuss the challenges associated with geospatial feature segmentation and analysis from high- dimensional data.

ISSN 2394 - 7780

II. LITERATURE SURVEY

A. Literature review

Geospatial data analysis requires the spatial grouping and display of 3D topographic relief data. It is crucial to develop the methods and frameworks for effectively analysing topographical reliefs and terrain areas. It was noticed that iintroduction of techniques such as the Kd-tree and nearest neighbour estimates has showcased their effectiveness in segmentation and picturing of topographical terrain, thus facilitating a transformative approach to data interpretation

[1]. Additionally, there is a clear focus on clarifying morphological relationship between points in clusters and the associated surface, which is a fundamental step in improving our comprehension of the importance and behaviour of geographic characteristics in high dimensional data [1].

Image segmentation in large remotely sensed imagery data poses significant challenges due to the immense volume and complexity of the data. Developing proper segmentation techniques and algorithms for large-scale imagery data is essential. As discussed by Zhang et al., deep learning-based semantic segmentation has emerged as a powerful tool for effectively segmenting and labelling vast point cloud data sets with high dimensional features [2]. It is observed by researchers that by applying deep learning algorithms, the image segmentation process becomes more efficient and overcomes a multitude of challenges encountered in processing high-dimensional remotely sensed imagery data for segmentation and analysis. These advancements in deep learning methods play a significant role in revolutionizing the segmentation and analysis of geospatial features by enhancing the accuracy and speed of processing.

In another paper, In order to assist researchers and farmers in selecting the appropriate algorithms for their researched crops and the hardware they are using, researchers examined the most current CNN-based techniques used to UAV-based remote sensing picture processing for crop/plant categorization. This research addressed potential obstacles and their remedies for crop identification using UAV data [3]. A deep learning model called "Convolutional neural network (CNN) based multiple training round (CNNMTR) deep learning model" has been suggested and utilized to classify and evaluate the city's vegetation cover in order to create a map of land use and land cover classes (LULC). In the current work, the CNN-MTR model, which is based on deep learning, is built to classify the 2009 and 2019 LISS-III photos in order to examine the dynamic change in the vegetation cover of Mysuru City. According to the data released by researchers, it was noted that the city's vegetation cover area was 39.09 sq. km (30.43%) in 2019 and 43.32 sq. km (33.86%) in 2009.

According to these findings, the city's vegetation cover shrank by 3.43% in a ten-year period. According to a model accuracy evaluation, the 2019 picture has an accuracy of 94.17%, while the 2009 image has an accuracy of 95.20%. It is also noted throughout an experiment that a model's accuracy varies according to the total number of layers and training rounds that are taken into consideration [4]. After taking into account various factors, researchers concluded that for performance analysis of models, researchers mostly used confusion matrix, F1 score, stratified Random Method and Non-Parametric Kappa coefficient, ROC curve, user, producer and overall accuracy, etc [5] [6].

Table 1: Literature Survey

Author /Year	Paper Title	Algorithm Used	Key points	Conclusion
Mansour ifaf et al. (2021) [7]	GAN-Based Satellite Imaging: A Survey on Techniques and Application [7]	Generative Adversarial Networks (GANs)	This research covers various Generative Adversarial Networks GAN-based models used for image enhancement, super-resolution and classification, challenges and future research trends, and the substantial effect of the GANs on improving performance	The authors conclude that GAN- based models have shown promising results in satellite imaging. Still some challenges are there, to be addressed in further research such as the lack of labelled data, complexity of the models, and

			compared to old methods.	interpretability of complex results.
Isola et al. (2017) [8]	Image-to-Image Translation with Conditional Adversarial Networks [8]	Conditional Adversarial Networks (CAN)	This research demonstrates the effectiveness of this approach on various domain as style transfer, semantic segmentation, object transfiguration and also provide a comparative analysis of researchers approach with SOA (state-of-the- art) methods and its effectiveness at synthesizing photos from label maps, reconstructing objects from edge maps, and colorizing images.	The authors of this paper states that their approach using CANs is effective in I-to-I (image-to-image) translation. They also highlight the potential of their approach in various other domain such as robotics, image editing, virtual reality, etc.
Xing et al. (2020) [9]	The challenges of image segmentation in big remotely sensed imagery data [9]	Traditional and deep learning based algorithms	This research discusses the exact challenges brought by big remotely sensed imagery datasets. It proposes a 4-layered image segmentation GCI and tests this GCI. The researchers discuss the various techniques and algorithms used for image segmentation and highlight the challenges and limitations of these methods.	Researchers conclude that the existing methods for image segmentation in large remotely sensed imagery data have limitations in terms of accuracy, efficiency, and scalability.
Zhang et al. (2021) [10]	A Review of Deep Learning-Based Semantic Segmentation for Point Cloud [10]	Deep learning-based algorithms	This research offers the complete review of the recent advancements in deep learning based semantic-segmentation for the point-cloud dataset.	The authors conclude that deep learning based approaches have shown significant improvements in the point-cloud segmentation. Yet, there are still some difficulties that need to be taken care of in further research, as lack of labelled data,

				complexity of the models and the interpretability of the results.
Arpita et al. (2023) [11]	Land use and land cover classification using machine learning algorithms in google earth engine [11]	RF, SVM, CART	In this research, authors examined the LULC classified by the training sets using supervised classification models. NDVI (Normalized difference vegetation index) was evaluated and was fine-tuned to increase classification accuracy.	Researchers offers a reliable and fully automated approach for LULC classification, they also declare results for LULC classification in Indian State (Karnataka).
Swapan etal., (2020) [12]	Land-Use Land-Cover Classification by Machine Learning Classifiers for Satellite Observations- A Review [12]	RF, SVM, ANN, Fuzzy ARTMAP, SAM and Mahalanobis Distance (MD)	This paper inspected six ML algorithms for LULC mapping. Accuracy assessment was performed using methods such as Kappa coefficient, RoC (Receiver operational curve), index-based validation and RMSE (Root mean square error).	Researchers conclude that "ANN and RF algorithms are the best LULC classifiers and RF algorithm has the maximum accuracy level in comparison to the others."

In summary, the segmentation and analysis of geospatial features play a crucial role in the processing of high-dimensional data in remote sensing. These spatial analyses allow for a comprehensive understanding of geographic phenomena within a data-rich era. Moreover, the potential impact of machine learning algorithms in this context cannot be understated, particularly in addressing the challenges associated with big spatiotemporal data. The utilization of machine learning algorithms for land-use and land-cover classification has shown promise in providing solutions to longstanding challenges in the field. As such, there is a clear call to action for further research and development in order to harness the full potential of segmentation and analysis of geospatial features. This will enable geographic knowledge production that can have a meaningful impact on steering advancements in this domain.

III. EXPERIMENT AND ANALYSIS

Machine learning algorithms have appeared as an essential tools for land use and land cover classification, providing an overview of the diverse methods employed for this purpose. Such methodologies include "Decision trees, random forests, and support vector machines among many others", each equipped with unique attributes and applications.

For First Experiment, we used Google earth engine platform and analysis of hyperspectral unmixing of features. We used Kmeans algorithm for segmentation on Landsat 8, Top of Atmosphere reflectance for nearby areas to ROI points [78.0219,30.184].

ISSN 2394 - 7780

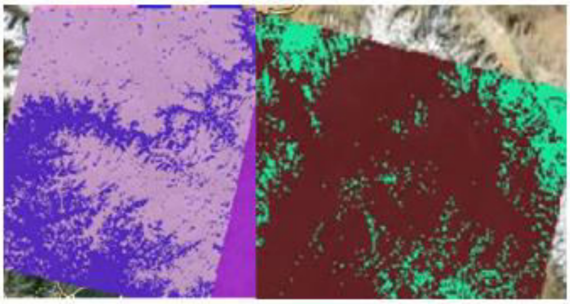


Figure 1: Segmentation for part I of ROI

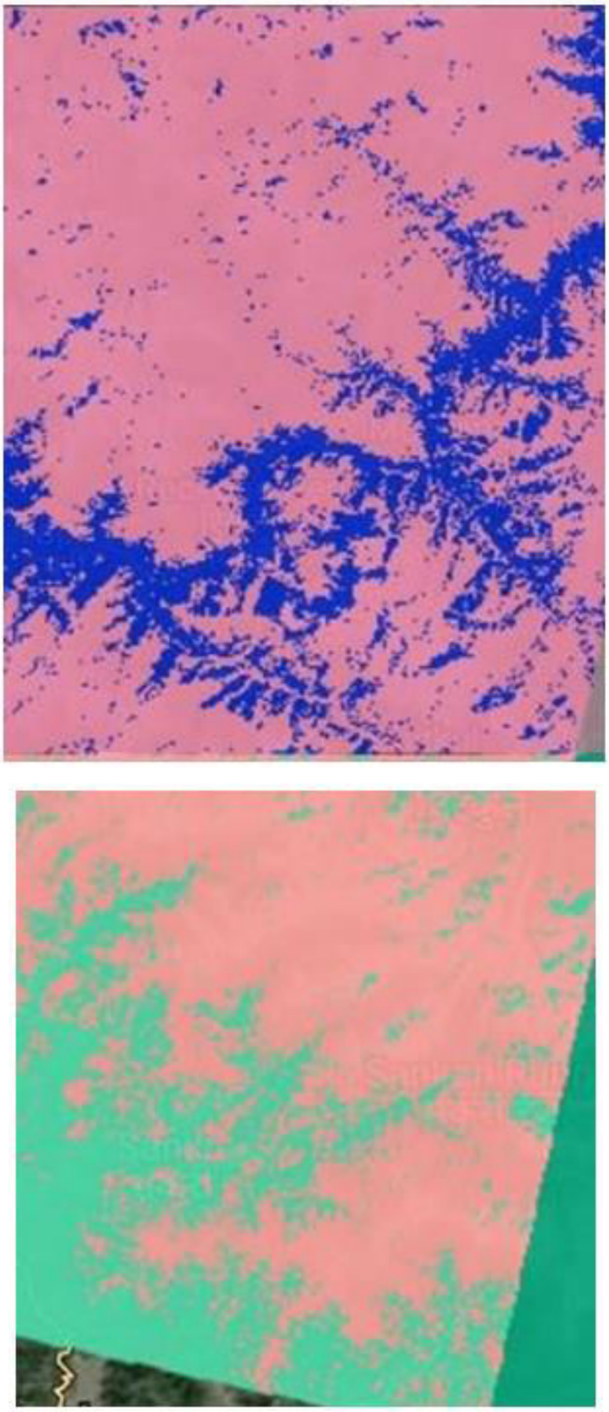


Figure 2: Segmentation of small region.

In Second Experiment, we used segmentation approach, Segment anything model [13] was used on google earth image for ROI of [73.0052, 19.0739, 73.0094, 19.0782] on Google Colab platform. In this, the Houses, land, roads, distinct vehicles, etc were segmented using SAM model with leafmap for base map requirement.

ISSN 2394 - 7780

Figure 3: ROI area capturing for SAM

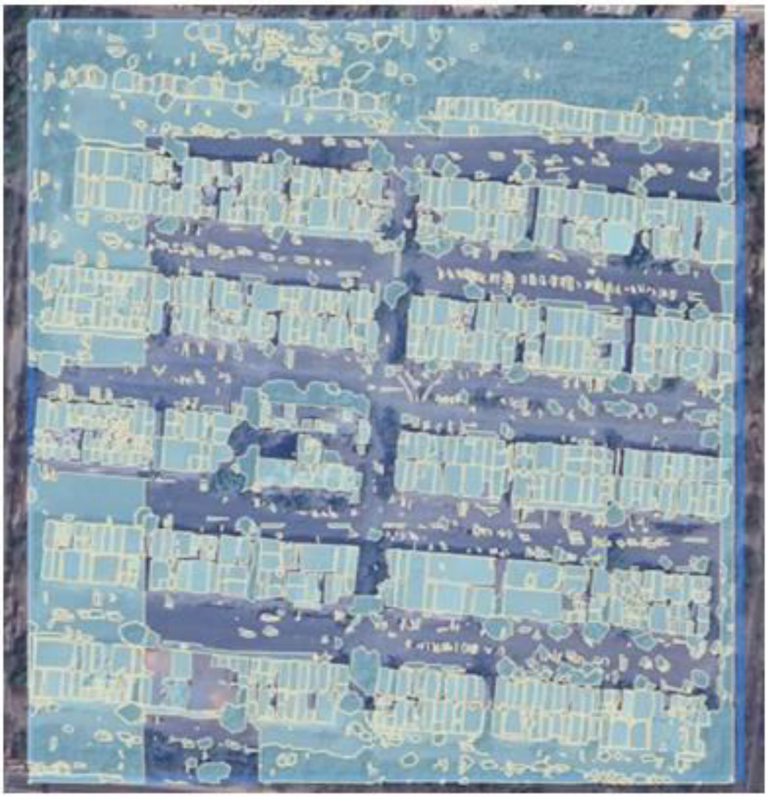


Figure 4: Segment anything model applied to ROI: [73.0052, 19.0739, 73.0094, 19.0782]

In last experiment, USGS Landsat 8 Level 2, Collection 2, Tier 1 Surface reflectance dataset from google Data catalog were used on geometry of points [78.982052, 30.283245] over Dehradun District of Uttarakhand. Different classifier was used to identify Water, Forest, Herbaceous species and development regions. K-mean, RF classifier and CART result are as aaccuracy Metrics for CART algorithm: Test Confusion matrix: [[8,0,0,0][0,11,0,0][0,0,6,0][0,3,0,3]].

It has Test Overall Accuracy of 0.903225, Producers Accuracy as [[1], [1],[1],[0.5]], Consumers Accuracy as [[1,0.7857142857142857,1,1]] and Kappa as 0.8655.

ISSN 2394 - 7780

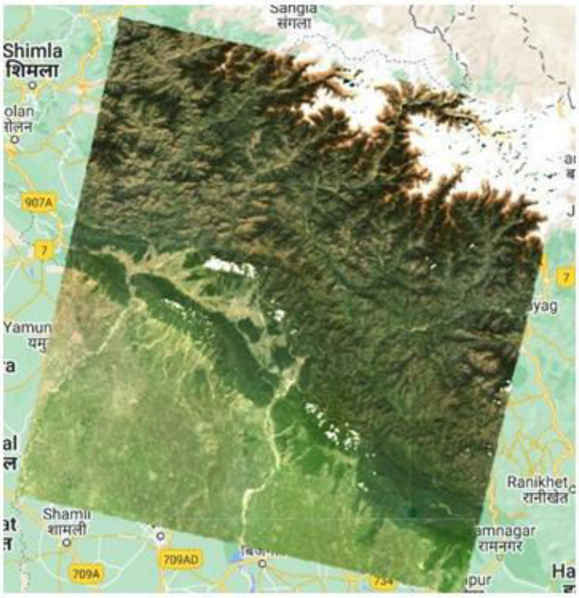


Figure 5: Landsat 8 Image applied over part of Uttarakhand

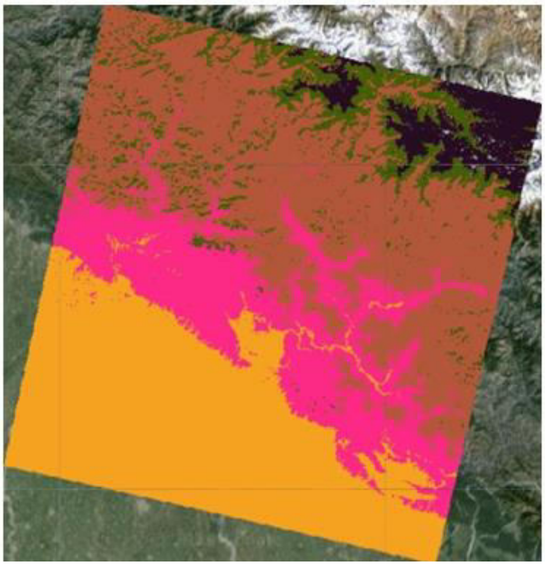


Figure 6: K-means classifier for 5 clusters (with random colors) applied over part of Uttarakhand.

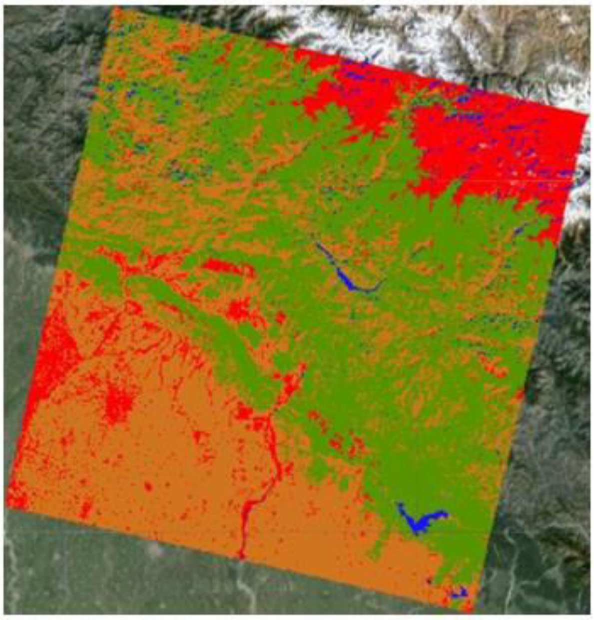


Figure 7: Random Forest Classifier applied over part of Uttarakhand.

 ISSN 2394 - 7780

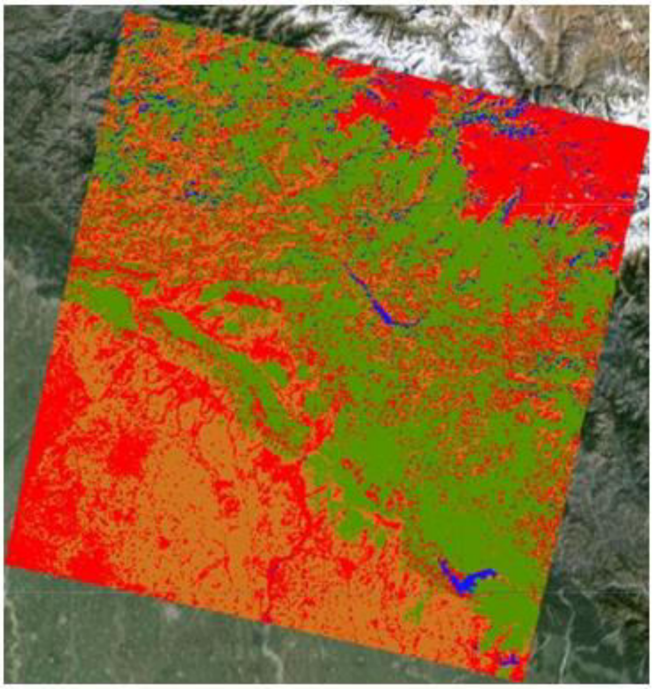


Figure 8: CART Algorithm applied over part of Uttarakhand.

IV. CONCLUSION

The paper discusses the use of machine learning techniques for segmenting and analyzing high-dimensional geospatial data, highlighting its applications in urban planning, environmental monitoring, and disaster management.

In summary, the segmentation and analysis of geospatial features play a crucial role in the processing of high-dimensional data in remote sensing. These spatial analyses allow for a comprehensive understanding of geographic phenomena. Machine learning is important aspect in land-use classification and it has potential improvements in performance through advanced technologies like drones and satellite imagery. We can further apply Deep Learning approaches to get better understanding of our data.

In conclusion, machine learning algorithms play a crucial role in “Land-use and Land-cover classification”, with various methods like “Decision Tree, Random Forest, and Support Vector Machine” being utilized. This Paper also highlights the application of hyperspectral unmixing for feature analysis, segmentation using the Segment Anything Model, and the use of different classifiers like “K-mean, Random Forest classifier, and CART” for identifying different land cover types some part of Uttarakhand, with a high overall accuracy of 0.903225 and a Kappa value of 0.8655.

V. REFERENCES

[1] S. T. K. R. K. Maurya, "Multidimensional spatial clustering and visualization of 3D topographic relief data," International Journal of Information Technology, vol. 13, no. 2, pp. 581-592, 2021.

[2] S. B. M. H. B. R. O. V. Chiyuan Zhang, "Understanding deep learning requires rethinking generalization," arxiv.org, 2016.

[3] .. S. H. A. M. Y. a. A. A. V. Eisavi, "Land cover mapping based on random forest classification of multitemporal spectral and thermal images," Environmental Monitoring and Assessment,, vol. 187, no. 5, p. 291, 2015.

[4] S. M. a. S. R. S. H. N. Mahendra, "An assessment of vegetation cover of Mysuru City, Karnataka State, India, using deep convolutional neural networks," Environmental Monitoring and Assessment, vol. 195, no. 4, p. 526, 2023.

[5] R. S. S. S. A. A. H. M. A. B. a. S. E. Z. Hassan, "Dynamics of land use and land cover change (LULCC) using geospatial techniques: a case study of Islamabad Pakistan," SpringerPlus, vol. 5, no. 1, p. 812, 2016.

[6] S. L. H. a. S. G. V. Bhanage, "Prediction of land use and land cover changes in Mumbai City, India, using remote sensing data and a multilayer Perceptron Neural Network Based Markov Chain model," Sustainability, vol. 13, no. 2, p. 471, 2021.

[7] A.H. M. B. K. D. M. S. S. H. Mansourifar, "GAN-Based Satellite Imaging: A survey on Techniques and applications," IEEE Access, vol. 10, p. 118123– 118140, 2022.

[8] J.-Y. Z. T. Z. A. A. E. Phillip Isola, "Image-to-Image Translation with Conditional Adversarial Networks,"In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 1125-1134, 2017.

[9] R. S. M. K. Jin Xing, "The challenges of image segmentation in big remotely sensed imagery data," Annals of GIS, vol. 20, no. 4, pp. 233-244, 2014.

[10] X. Z. Z. C. Z. L. JIAYING ZHANG, "A Review of Deep Learning-Based Semantic Segmentation for Point Cloud," IEEE Access, vol. 7, pp. 179118-179133, 2019.

[11] S. A. A. N. H. M. Arpitha, "Land use and land cover classification using machine learning algorithms in google earth engine," Earth Science Informatics, vol. 16, no. 4, p. 3057–3073, 2023.

[12] P. S. S. M. S. Y. A. L. A. R. S. Talukdar, "Land-Use Land-Cover Classification by Machine Learning Classifiers for Satellite Observations—A review," Remote Sensing, vol. 12, no. 7, p. 1135, 2020.

[13] E. M. N. R. H. M. C. R. L. G. T. X. S. W. A. C. B. W.-Y. L. P. D. R. G. Alexander Kirillov, "Segment Anything," ARXIV, 2023.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

INFLUENCE OF SOCIAL MEDIA ADVERTISEMENTS ON CONSUMERS CLOTH PURCHASING PATTERN

Dr. Neelam Naik and Shweta Nanji Kariya
Department of Information Technology (University of Mumbai) Usha Pravin Gandhi College (University of Mumbai) Mumbai, India

ABSTRACT
To find out does social media have any influence in consumers purchasing pattern is the main study of this research. It was observed that there is a huge influence of social ads on consumer's selection making. Various factors were considered to conclude variety of result such as which gender is more influenced by the social advertisements, which age group is more likely to make an impulse decision, how often people use social media in their day to day, does it help fashion firm to grow its business and so on. It was later concluded that both fashion firms and consumers are benefited by social media advertisement.

Keywords: social media advertisements, fashion firm, impulse purchasing, fast fashion.

INTRODUCTION
Impact of social media site on our lives in this online era is huge and one area where this impact is most seen is in consumer's cloth purchasing behavior. Social media advertisements significantly influence customer apparel purchasing habits. Brands are now using social media sites like Instagram, Facebook, Pinterest as effective tools to display their products and interact with customers. The image posting on these platforms allows producers to display their recent collections, trends, and styles. Because of this customer follow current fashion trends, which helps them to make their choices and preferences.

The most important feature of social media marketing is their capacity to generate trends and define fashion standards. Influencers and celebrities who frequently collaborate with brands use their huge fan followings to popularize new designs. This trendsetting feature helps customers to copy the looks and designs which they see on their screens. Social site highly relies on advertisements as a key source of income. These ads generate remarkable revenue for the sites. Different social websites publish ads differently; some suggest ads depending on consumer's recent activity. For Example, Facebook. While registering for the first time on Facebook user is asked to provide some information such as their gender, date of birth, fashion interests, and favorite celebrities etc. Upon this data, user will be recommended ads which are relevant to their fashion interest.

The interactive nature of social media platforms allows customers to provide feedbacks which later on help brands with valuable insights. Social media advertising is almost

as common as television or radio advertising for brand awareness. Consumers are look upon social media sites to find brands and even buy from these brands. when shopping consumers keep Social media trends in mind. It has been observed that while purchasing a product more than half a percentage of consumers read feedbacks on social media. Even a single negative reviews on a post can stop the consumer from buying that product. The intent of the study is to figure out whether social advertisements have any effect on customer's apparel purchasing pattern. Do people consider social media advertisement while making any purchase? Is female group more influenced by social advertisement over male group? A survey was conducted on different age group of people. Depending on the responses several hypothesis was generated.

H_{11}: Social media advertisements have changed consumer's cloth purchasing pattern

H_{21}: There is relation between gender and buying clothing product post viewing them displayed on social media.

H_{31}: People regret a clothing purchase made post viewing an ad on social sites.

H_{41}: There is a remarkable linkage between age group and the likelihood of making impulse cloth buying depending on social advertisements.

LITERATURE REVIEW
1. In recent day's large number of people are using social media due to which these social websites are growing rapidly. Brands use social media advertisements to boost their products. Social media feeds are filled with advertisements. The principal reason of this research is to get insight of the elements which influences consumer's behavior towards display of advertisements on social sites. 613 social media users participated in an online survey that produced data that was later used to construct and evaluate a research

model. Our research provides strong evidence that the advertising content influence the performance of display ads on social media. [5].

2. Every new second, social media sites such as Pinterest, Instagram, Facebook, and others generate enormous amounts of data. On average, 400 million active users share about 5 billion recommendations on Facebook each month. Due to its numerous uses and ability to examine how members of a network interact, express opinions, and recognize relationships, social network analysis has become more popular. Now it is possible to extract useful information such as user's interests. This article presents an approach to analyze user's interests and present advertisements that are relevant to them based on theanalysis of those interests. [7].

3. Social media has grown to be an essential tool for marketing. This platform is mostly used as marketing tools and medium for introducing new products. Famous social connecting sites such as Twitter, LinkedIn, Facebook, and YouTube bring in millions of users from different part of the world who put in a decent amount of time on these websites every day. The goal of this article is to offer a platform which allows users to control all of their different social media accounts in one location. [10].

4. Earlier Newspaper articles and television commercials used to play a big role in product promotion. But in the current digital world, where billions of people rely on technology for everyday needs social media serve as one of the method to market a product. Social media and recent marketing trends have dramatically influenced consumer's behavior and purchase decisions. The goal of this research is to get further insight into how consumer decisions made on the Internet or through social media are influenced by behavioral targeting. Moreover, to discover which social media site influence customer choice [1].

5. The advertising firm is growing rapidly on social media. There might be up to one billion active users on Facebook at any given period of time for an advertisement. A company's advertisement can reach to a huge number of accounts on Facebook. With these kinds of numbers, it is very easy to go mad and spend a lot of cash for advertising. However, this points towards the crucial question: Can small companies benefit from social media advertising? In order to give a solution to the query, a case study has been done on Facebook advertisement and kept a track on their website traffic. Additionally, it has found that a lot of people interact with Facebook ads. Findings show that even with a low click-on rate social media advertising may be successful for small businesses. [3].

6. To market their products, firms stated to use social media website. Among all Facebook emerged out as the most widely used communication tool. The Intent of this research was to analyze how marketing strategy of Facebook affect costumer's behavior to purchase cloth. It was observed that Facebook marketing had both good and bad effects on the consumers and businesses. A survey was conducted in order to meet its goals and the data was collected. After analysis it was found that the objective of the researcher was fulfilled. [4].

7. For marketing of the product businesses are spending large amount of money in social media sites. Research has been done to observe if there exists any connection between social sites and costumer-brand interactions. Poll was conducted where responses were taken from consumers from the United Kingdom, France, and the United States. Later it was observed that social media sites and consumers brand relationship had a correlation. Survey was conducted and data was collected from adults and consumer populations. After analyzing the survey, it was found that the observation was in the favor of the research main goal. [9].

8. Marketing relies on segmentation. One of the segment is birth age which helps to divide populations in groups. A study is conducted on two different age group i.e. Baby Boomers and Generation Y in order to analyze their buying pattern and in-store service. It was observed that Baby Boomers prioritize in-store service while Generation Y is less likely to go with in-store service. For Baby Boomers, purchasing begins with a vendor who helps in suggesting the best product. While Generation Y select their own product. The study shows the influence of retail strategies on different generations and how retailers should learn from the outcomes and build consumer relationships. [2].

9. The Intent of this research is to observe the impact of various factors on costumer's product purchasing behavior. Later on study how this factors influence sales in fashion industry in order to achieve business objectives. This study mainly focuses on different marketing practices and techniques which are used to manipulate consumer's buying pattern. This study collects data using questionnaires-based approach. The study is conducted only on the fashion industry of Pakistan. Research was conducted on the promotional

strategies which were then used by Pakistan's fashion firms during their ‘Eid festival and how it influenced customer purchasing behavior. From the data it was observed that the strategies used benefited fashion firms a lot and their sale increased. [6].

10. This study provides an analysis on the elements that influence consumer’s purchasing decisions. Different research papers were examined that addressed factors influencing the marketing of clothes and fashion items. Various cultural, social, psychological, personal, and environmental elements were also considered. Market-related factors, such as product attributes, the channel of purchase, pricing, and advertising, were also taken into

RESEARCH METHODOLOGY

About Dataset:
A google form with various types of Questions was created. This form was then circulated among different age group of people and their feedback was taken. Varieties of questions such as Multiple Choice Question (Select one out of multiple choices), Multiple Select Question (Select Multiple option out of multiple question), Open-Ended Questions. Questions included in the survey form were Age, Gender,

How frequently they use social media sites? , Which social media sites do they regularly use for individual use?, How often do you come across clothing advertisements on social sites?, Have you ever purchased clothing product post seeing them advertised on social sites?, Do you follow fashion influencers or brands on social sites?, Have you ever modified your clothing purchase after viewing an user-generated content?, Do you think that social advertisements have changed your clothing purchasing patterns compared to traditional advertising methods (e.g., TV, magazines)?, How likely are you to make impulse clothing purchases depending on social media advertisements?, Do you think social media advertisements accurately represent the actual quality and appearance of clothing items?, Have you ever regretted a clothing purchase made after viewing an advertisement on social site?, What improvements, if any, would you suggest for social media advertisements to better influence your clothing purchasing decisions? 78 people participated in the survey by sharing their valuable feedback. These responses were then analyzed and Hypothesis were proven.

Methods Applied
Once the responses where collected from the users they were then stored in google sheet for further study. This excel sheet has about 15 columns. Each and every column was taken into consideration while performing testing method. After observing the columns Chi-Square Test came out to be more suitable test for analysis. Chi-Square X^2 Test is the fundamental test for testing hypotheses arranged in a frequency table. Univariate test involving nominal or ordinal variables that are calculated with a Chi-Square Test. Generally, Chi-Square test is associated with goodness-of-fit. Goodness-of-fit determines the numbers matches in two different matrix of the same size. Test is between observed frequency value and expected values. Calculated Chi- Square Formula: (Observed Value - Expected Value) ^2 / Expected Value. This calculated value is then compared with Chi-Square Distribution (Critical Value). If Calculated Chi value is greater than Critical Chi value, then Null Hypothesis was rejected.

RESULT AND DISCUSSION
Chi-Square test was applied on the responses to find out is there any association between two independent variables. Accordingly, null hypothesis and alternate hypothesis were accepted.

EV- EXPECTED VALUE

OV- OBSERVED VALUE

SV- SIGNIFICANCE VALUE

DOF- DEGREE OF FREEDOM

NH-NULL HYPOTHESIS

AH-ALTERNATE HYPOTHESIS

CV- CRITICAL VALUE.

TableA1:

To figure out the influence of social media advertisement on consumer’s cloth purchasing pattern.

Question: Do you think that social media advertisements have changed your cloth purchasing patterns? was asked to the users. Based on their responses chi-square test was applied.

Q- QUESTION ASKED

Q	EV	OV	OV - EV	(OV-EV)^2	(OV-EV)^2 / EV
yes	26	46	-20	400	15.3846
no	26	19	7	49	1.8846
not sure	26	13	13	169	6.5
Total	78	78	0	618	**Calculated Value:** 23.7692

Fig. 14. Calculation table for TableA1

SV	DOF	NH	AH	CV
0.05	3-1 = 2	Social media advertisements do not have any impact consumers cloth purchasing pattern	Social media advertisements have changed consumers cloth purchasing pattern	**5.991**

Fig. 15. Calculation table for TableA1

In Fig 2, **Null Hypothesis:** say that Social media advertisements do not have any influence on consumer's cloth purchasing pattern. **Alternate Hypothesis:** Social media advertisements have changed consumer's cloth purchasing pattern. **Degree of freedom** was calculated as (N-1) which is (3-1= 2). **Significance Value** was considered as 5% (0.05). Now looking into Chi-Square Distribution Table with the help of Degree of freedom and Significance Value Critical value came out to be 5.991. Here Calculated Chi-Square value is **greater** than the critical value which means that the alternate hypothesis is supported. **Result:** Social media advertisements have changed consumer's cloth purchasing pattern.

Table A2:

To find out if there is any connection between gender and buying cloth items after viewing their advertisement on social media.

Y: YES;

N: NO;

S: SOMETIMES;

T: TOTAL

MY: MALEYES;

MN: MALE NO;

MS: MALESOMETIMES;

FY: FEMALE YES;

FN: FEMALE NO;

FS: FEMALE SOMETIMES

Question: Have you ever purchased clothing product after seeing them displayed on social media? was asked by the male group and female group. Based on their responses chi-square test was applied.

Q	Y	N	S	T
Male	13	12	5	30
Female	23	7	18	48
Total	36	19	23	78

Fig. 16. Observation Tanle for Table A2

Q	EV	OV	OV-EV	(OV-EV)^2	(OV-EV)^2 / EV
MY	13.85	13	-0.85	0.7225	0.0521
MN	7.31	12	4.69	21.9961	3.009
MS	8.85	5	-3.85	14.8225	1.6748

FY	22.15	23	0.85	0.7225	0.0326
FN	11.69	7	-4.69	21.9961	1.8816
FS	14.15	18	3.85	14.8225	1.0475
T	78	78	0	75.0822	**Calculated Value: 7.6976**

Fig. 17. Calculation Tanle for Table A2

SV	DOF	NH	AH	CV
0.05	(2-1)(3-1)=2	There is no remarkable connection between gender and purchasing clothing product after viewing their advertisement on social sites.	There is remarkable connection between gender and purchasing clothing product after viewing their advertisement on social sites.	**5.991**

Fig. 18. Calculation Tanle for Table A2

In Fig 5, **Null Hypothesis:** states that there is no remarkable connection between gender and purchasing clothing product after viewing their advertisement on social sites.. **Alternate Hypothesis:** There is remarkable connection between gender and purchasing clothing product after viewing their advertisement on social sites.. **Degree of freedom** was calculated as (No. of rows-1) *(No. of column-1) which is ((2-1) *(3-1) = 2). **Significance Value** was considered as 5% (0.05). Now looking into Chi-Square Distribution Table with the help of Degree of freedom and Significance Value Critical value came out to be 5.991. Here Calculated Chi-Square value is **greater** than the critical value which means the alternate hypothesis is supported. **Result:** There is an connection between gender and their probability of buying clothing product after seeing them advertised on social media.

Table A3:

Later out to figure out if people ever regretted their purchase after viewing a social advertisement. **Question**: Have you ever regretted a clothing purchase made after viewing an advertisement on social sites? was asked to the users. Based on their responses chi-square test was applied.

Q	EV	OV	OV-EV	(OV-EV)^2	(OV-EV)^2 / EV
Yes	26	43	-17	289	11.1153
No	26	18	8	64	2.4615
Not Sure	26	17	9	81	3.1153
Total	78	78	0	434	**Calculated Value: 16.6921**

Fig. 19. Calculation Tanle for Table A3

SV	DOF	NH:	AH:	CV
0.05	3 -1=2	People do not regret a clothing purchase made after viewing an advertisement on social media.	People regret a clothing purchase made after viewing an advertisement on social media.	**5.991**

Fig. 20. Calculation Tanle for Table A3

In Fig 7, **Null Hypothesis:** states that People do not regret a clothing purchase made after viewing an advertisement on social media. **Alternate Hypothesis:** People regret a clothing purchase made after viewing an advertisement on social media. **Degree of freedom** was calculated as (No. of rows-1) which is (3-1=2). **Significance Value** was considered as 5% (0.05). Now looking into Chi-Square Distribution Table with the help of Degree of freedom and Significance Value Critical value came out to be 5.991. Here Calculated Chi-Square value is **greater** than the critical value which means the alternate hypothesis is supported. **Result:** People regret a clothing purchase made after viewing an advertisement on social media.

Table A4:

To checkout there is a significant association between age group and the likelihood of making impulse clothing purchases based on social media advertisements.

L: LIKELY

N: NEUTRAL

U: UNLIKELY

T: TOTAL

Question: How likely are you to make impulse clothing purchases based on social advertisements? was asked to different age group of people. Based on their responses chi-square test was applied.

Q	L	N	U	T
Under 18	1	1	1	3
18-24	14	19	8	41
25-34	8	3	4	15
35-44	8	6	3	17
45-55	1	1	0	2
Total	32	30	16	78

Fig. 21. Observation Tanle for Table A4

Q	EV	OV	OV-EV	(OV-EV)^2	(OV-EV)^2 / EV
Under 18 Likely	1.23	1	-0.23	0.0529	0.043
18-24 Likely	16.82	14	-2.82	7.9524	0.4728
25-34 Likely	6.15	8	1.85	3.33	0.5415
35-44 Likely	6.97	8	1.03	1.0609	0.1522
45-55 Likely	0.82	1	0.18	0.0324	0.0395
Under 18 Neutral	1.15	1	-0.15	0.0225	0.0196
18-24 Neutral	15.77	19	3.23	10.4329	0.6616
25-34 Neutral	5.77	3	-2.77	7.6729	1.3298
35-44 Neutral	6.54	6	-0.54	0.2916	0.04459
45-55 Neutral	0.77	1	0.23	0.0529	0.8229
Under 18 Unlikely	0.62	1	0.38	0.1444	0.2329
18-24 Unlikely	8.41	8	-0.41	0.1681	0.0199
25-34 Unlikely	3.08	4	0.92	0.8464	0.2748
35-44 Unlikely	3.49	3	-0.48	0.2304	0.066
45-55 Unlikely	0.41	0	-0.41	0.1681	0.41
Total	78	78	0	32.4588	**Calculated Value: 5.13109**

Fig. 22. Calculation Tanle for Table A4

SV	DOF	NH	AH	CV
0.05	((5-1) *(3-1) = 8)	There is no significant connection between age group and the probability of making impulse clothing purchases based on social media advertisements	There is a significant connection between age group and the probability of making impulse clothing purchases based on social media advertisements	**15.507**

Fig. 23. Calculation Tanle for Table A4

In Fig 10, **Null Hypothesis:** states that There is no significant connection between age group and the probability of making impulse clothing purchases based on social media advertisements. **Alternate Hypothesis:** There is significant connection between age group and the probability of making impulse clothing purchases based on social media advertisements. **Degree of freedom** was calculated as (No. of rows-1) *(No. of column-1) which is ((5-1) *(3-1) = 8). **Significance Value** was considered as 5% (0.05). Now looking into Chi-Square Distribution Table with the help of Degree of freedom and Significance Value Critical value came out to be **15.507**. Here Calculated Chi-Square value is **greater** than the critical value which means the alternate hypothesis is supported.

RESULT

There is significant connection between age group and the probability of making impulse clothing purchases based on social media advertisements.

CONCLUSION

There is significant impact of social media advertisement on consumer's cloth purchasing pattern. Through analysis of consumer's behavior different conclusions can be drawn. From Table A1 it is observed that user's decisions have changed post viewing social advertisement. Depending on current ongoing trends and how influencing the advertisement is user takes their decision. It has also found that females are more influenced by

ISSN 2394 - 7780

social ads than males. Female make more cloth purchased after seeing social ads. Fashion firms uses different trick to influence people so that they make more purchase. They use techniques such as recommending ads which are relevant to their interest, collaborating with the social influencers to promote their brands product and many more. It was also observed that young age group of people use social media very frequently in their day to day life. Due to frequent usage of social media applications they regularly come across social advertisements. Because of which they are more likely to make an impulse purchase after viewing advertisements. Due to this impulse purchasing fashion firms are benefitted the most as it helps them grow their sales. Even consumers are benefitted with social advertisement as they get to view variety of products and designs. Due to social media advertisements both consumers and producers are benefitted the most.

REFERENCES

[1] Abhilash Gogulamudi, Sandeep Prabhu. “Consumer decisions under the influence of social media & behavioral targeting”, 2022, International Conference on Decision Aid Sciences and Applications (DASA), IEEE.

[2] Anders Parment,” Generation Y vs. Baby Boomers: Shopping behavior, buyer involvement and implications for retailing”, 2013, Journal of Retailing and Consumer Services.

[3] Dawn Carmichael, David Cleave.” How effective is social media advertising? A study of Facebook Social Advertisements”, 2012, The 7th International Conference for Internet Technology and Secured Transactions, IEEE.

[4] T. Kingsley Bernard, A. A. S. N. Munasinghe, I. K. R. J. Premarathne, S. Wijayarathne, “The Influence of Facebook Marketing On Consumer Buying Intention Of Clothing: Evidence From Young Adults “, 2020, Archives of Business Review – Vol. 8, No.9.

[5] En Mao, Jing Zhang. “What Drives Consumers to Click on Social Media Ads? The Roles of Content, Media, and Individual Factors”,2015, 48th Hawaii International Conference on System Sciences, IEEE, DOI 10.1109/HICSS.2015.410.

[6] Fazal ur Rehman, Rosman Bin Md Yusoff, Shafie Bin Mohamed Zabri and Fadillah Binti Ismail,” Determinants of personal factors in influencing the buying behavior of consumers in sales promotion: a case of fashion industry”, 2017, Young Consumers Insight and Ideas for Responsible Marketers.

[7] Jagadish P, Anjan K Koundinya.“ Social Media Ads Analysis”, 2021,International Confernece on Forensics, Analytics, Big Data and Security, IEEE.

[8] Reham Abdelbaset Sanad,” Consumer Attitude and Purchase Decision towards Textiles and Apparel Products”,2016, World Journal of Textile Engineering and Technology.

[9] Simon Hudson, Li Huang, Martin S. Roth, Thomas J. Madden, “The influence of social media interactions on consumer-brand relationships: A three-country study of brand perceptions and marketing behaviors”, 2015, International Journal of Research in Marketing.

[10] Umi Najiah Ahmad, Razimi Muhammad Zulhaziq Tazul Ayrizan, Zurida Ishak. “Online Social Media Platform for Marketing Generator”, 2021, IEEE.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

ARTIFICIAL INTELLIGENCE AND ITS ROLE IN GENETIC ENGINEERING AND MODERN MEDICINE

Dr. Manisha Divate[1] and Anjali Singh[2]
[1]Bachelor of Science in InformationTechnlogy SVKM'S Usha Pravin Gandhi College
Mumbai, India
[2]line; Bachelor of Science in InformationTechnlogy SVKM'S Usha Pravin Gandhi College
Mumbai, India

ABSTRACT
This Paper gives an overall insight about how Artificial Intelligence has proved to be a prominent tool for the health sector and its contribution in curing diseases like cancer Artificial intelligence(AI) is the mantra for future. Last many decades have observed a tremendous change in the field of Artificial Intelligence. This exploration paper explores the profound impact of Artificial Intelligence(AI) on the fields of Genetic Engineering and Modern Medicine. As AI technologies continues to advance, they play a vital part in revolutionizing inheritable exploration, diagnostics and medical treatments. The paper delves into the operations of AI in decoding complex inheritable data, enhancing individual delicacy, contributing to the development of individualized drug and furnishing an overview about the places performed by AI in colorful inheritable conditions like cancer and diabetes etc. also, it investigates the part of AI in inheritable engineering processes, where machine literacy algorithms aid in optimizing gene editing ways and prognosticating the functional issues of inheritable variations. The study underscores the transformative eventuality of AI in reshaping the geography of inheritable exploration and medical practices for bettered healthcare issues.

Keywords: Artificial Intelligence, Modern Medicine-Genetic engineering-data decoding-algorithm's.-role played by AI in curing genetic diseases.

I. INTRODUCTION (HEADING 1)
Artificial Intelligence(AI) has come a ubiquitous term in our contemporary terrain, resonating across different disciplines.1st paper on the subject in 1971, AI in medicine is 25 times old this time(Nordyke etal.). In reviewing the field in 1984, Clancey and Shortliffe handed us with the following description " Medical artificial intelligence is primarily concerned with the construction of AI programs that perform opinion and make remedy recommendations. Unlike medical operations predicated on other programming styles, analogous as purely statistical and probabilistic styles, medical AI programs are predicated on representational models of complaint realities and their relationship to patient factors and clinical manifestations. " important has changed since also, and moment we would consider this description to be excessively narrow in compass and vision. For its day, still, it was revolutionary. AI in medicine(AIM), at that time a largely a US disquisition community, had a bold vision of the way it would revolutionize medicine, and push forward the borders of technology. It attracted the swish computer scientists and, by any measure, their affair in the first decade of the field remains a remarkable achievement. Throughout the eighties, the affair from a now global disquisition community was steady and substantial. Europe in particular, had developed a significant disquisition community that amped and broadened the compass of earlier disquisition. AIM was not still successful if we judge success as making an impact on the practice of medicine. A period of soul searching and redefinition of pretensions has followed. Its authors rightly characterize AIM as an adolescent field(Shortliffe, 93), nearly as if to excuse the bold and immature idealism of the early days, and the apparent failure to deliver on it. Further while the AIM community has remained fairly small and nearly connected, the broader field of medical informatics has grown much larger. It's also extensively more successful in landing the interest and involvement of the clinical community. People have thus begun to question whether the points of AIM, as captured in the description over, are still valid. Artificial Intelligence in medicine is a cold- thoroughbred field. It's formed out of the union of two distinct enterprises. Artificial Intelligence, no longer just concentrated on recreating sentience, is a broad church of technologies and pretensions. slightly aged than AIM, it has its own struggles with identity and purpose. Medicine, on the other hand, is aged and clearer about its pretensions. These two fields, united through AIM, can interact in three fairly distinct ways. firstly, the relationship can be technology driven. Medicine can give AI researchers with a complex set of real- world problems on which to exercise their ways. The outgrowth of good technology- driven disquisition is the development of general purpose technologies that can be applied in multitudinous different disciplines. An AIM researcher working in this way would judge their disquisition to have been a success if it was published in an AI journal. For illustration, much of the early work in computer-predicated opinion concentrated on medicine because it was such a good testing ground. moment, the same

 ISSN 2394 - 7780

researchers in opinion are more likely to be working on fault position for digital circuits or photocopiers, which give them with a set of problems applicable to their current conditions.Artificial Intelligence(AI) is decreasingly chancing operations in inheritable laboratories, revolutionizing the geography of inheritable exploration and healthcare. using Machine Learning ways. AI is poised to play a vital part in relating and amending inheritable conditions in the future. The practice of drug generates large volumes of complex data taking the need for advanced and logical tools. The use of tools can be understood as an " extension " to mortal smarts functionality. Intelligence has historically been humanity's most precious asset for thriving on Earth, and the development of Al technology suggests the eventuality for a new period in mortal productivity. Al is a conception encompassing colorful delineations from different perspectives. Generally accepted delineations include Al as a branch of computer wisdom enabling computers to execute tasks typically taking mortal intelligence. Another perspective defines Al as a system perceiving the terrain and taking conduct with a minimal liability of task completion. To achieve" intelligent" functions, a myriad of algorithms, styles, or strategies has been developed. crucial approaches in Al technology involve problem- working through searching, knowledge- grounded logic and planning, uncertain knowledge- grounded logic, and learning from exemplifications. The styles strategies for problem- working encompass oblivious or heuristic quests, original quests, optimizations, evolutionary calculations, and inimical quests. Knowledge- grounded logic and planning involve sense programming, automated logic, and ontological engineering. Uncertain knowledge- grounded logic incorporates Bayesian networks, hidden Markov models, Kalman pollutants, mileage proposition, and decision networks. Learning from exemplifications is predicated in fine/ statistical bracket and machine literacy, with machine literacy standing out as the most extensively used Al fashion in academia and assiduity. AI in healthcare simulates the neural network of the mortal brain and leverages multidimensional information to learn how to interpret data, making informed opinions. Machine literacy(ML), a pivotal branch of AI, encompasses two extensively used algorithms Supervised literacy and Unsupervised literacy. In Supervised literacy, labelled input data is used for training until the error chance reaches the asked range, after which the model is stationed. Unsupervised literacy utilizes unlabelled datasets to reveal retired connections and identify differences an parallels between objects without mortal intervention. Deep literacy(DL), falling under Machine Learning marquee, includes input subcaste, multiple retired layers and affair layers. For complex problems, multiple layers are necessary to construct an accurate model. Unlike traditional ML's supervised literacy, where point birth depends on mortal moxie, DL's model construction is entirely performed by machines. This makes DL system more cost-effective, effective and improves individual delicacy. still, DL algorithms demand further time and advanced computing power, may demand further time and advanced computing power, may introduce bias, and warrant high interpretability. Convolutional Neural Networks(CNN's), is a typical DL algorithm correspond of layers that transfigure and calculate input samples into a series of class chances. CNN are important in achieving high delicacy with a minimum error rate, particularly in image- related tasks similar as image bracket, selection, interpretation and object identification in images. thus, this composition has conducted a comprehensive review of the exploration in this field and provides a perspective on the direction of unborn developments

II. ARTIFICIAL INTELLIGENCE IN DETECTION,PREDICTION OF CANCEROUS DISEASES GENOMIC ANALYSIS OF CANCER:

Cancer stands as one of the foremost causes of death globally ,with projections indicating that the number of affected individuals in developing countries will reach 20 million annually by 2025.This has intensified the focus on effective and precise cancer prognosis ,along with the stratification of patients into subgroups with distinct predicted outcomes .

A plethora of biomarkers ,including histopathological images , genetic mutations ,genetic expression signatures ,and protein markers ,have been developed and applied for cancer prognosis .Histopathology images are particularly deemed the gold standard due to their Ability to provide morphological attributes closely tied to cancer aggressiveness. With the expanding computing resources ,computational histopathologic systems have emerged to extract morphological biomarkers, aiding in the prognosis of various cancer like lung, Breast ,and kidney cancers.

In addition to histopathological images ,genomic mutations are recognized as key contributors to cancer development .Researches leverage patients' molecular profiles, encompassing genetic alterations and gene expression signatures ,to inform diagnostic ,prognostic , and therapeutic practices .In numerous studies acquiring multiple biomarkers is common for a more accurate assessment of disease status and progression stages .Recent research endeavor's explore the synergies between imaging and genomic markers for cancer.

III. BREAST CANCER

Breast Cancer is a type of cancer that begins in the cells of breast.It can occur in both men and women .The exact cause of breast cancer is not known, but it occurs when abnormal cells in the breast begin to grow and divide uncontrollably ,forming a mass or lump. Early Diagnosis helps in major role in treatment of such diseases. An alternative ML-based algorithm-based BCD diagnosis system has been proposed by Sharmin et al. Using the feature selection method, 12 significant characteristics were chosen from 30 input features. SVM and Random Forest (RF) have demonstrated the highest classification accuracy among all deployed models [5]. Naji et al. have developed a categorization technique for the identification of breast cancer. RF, Decision Tree, and SVM are the various classifiers that are employed. A quarter and a half of the data are used for the classifiers' testing and training, respectively. The SVM has the highest reported accuracy among all the classifiers utilized in this study [6]. Dhanya et al. used a variety of supervised machine learning methods to create a prediction system. Among all the algorithms put into practice, RF has demonstrated the best classification accuracy.

Compared to women in the West, current statistics indicate that a greater percentage of the disease is striking Indian women at a younger age. In order to track changes in the incidence of cancer, the National Cancer Registry Program analyzed data from cancer registries for the years 1988 to 2013. Every population-based cancer registry indicates that the trend for BC has significantly increased[6]. In India in 1990, the cervix was the most common location of cancer, followed by BC in the registries of Delhi (21.6% vs. 20.3%), Bangalore (23.0% vs. 15.9%), Bhopal (23.2% vs. 21.4%), Chennai (28.9% vs. 17.7%), and Mumbai (24.1% vs. 16.0%). By the years 2000–2003, things had shifted, with breasts surpassing.

IV.PROGRESS OBSERVED DUE TO AI(ARTIFICIAL INTELLIGENCE)IN BREAST CANCER:

The most common malignancy among women to be diagnosed is still breast cancer. The early diagnosis of breast cancer and the reduction in patient mortality rates have been made possible by significant advancements in medical imaging modalities and technology. However, because breast cancers and fibro-glandular tissue are highly heterogeneous, reading and interpreting breast pictures remains challenging. This leads to reduced cancer detection sensitivity and specificity as well as significant inter-reader variability. Researchers have worked hard to create computer-aided detection and/or diagnosis (CAD) schemes of breast images to give radiologists decision-making assistance tools to help them overcome these clinical obstacles. The development of high throughput data analysis techniques and artificial intelligence (AI) technologies, especially radiomics and deep learning approaches, has accelerated recently.

V. LUNG CANCER:

One of the main causes of death worldwide is lung cancer. In India, it is also a significant healthcare issue.[1] On February 20, 2016, a web search with the terms "lung cancer India" produced the following results. Google returned 43,80,000 hits; 1,77,000 results were for scholarly papers; and 2592 manuscripts could be found on the nlm.nih.gov website within the PubMed Medline database. The Indian articles on lung cancer that are cited in PubMed are displayed in Figure 1. The fact that oncologists in particular and the medical profession as a whole are continually adding to our understanding of lung cancer is encouraging. It increased from 42 articles in 2004 to a whopping 407 publications at its peak in 2006—nearly a ten-fold increase. In lung cancer research, methods like feature engineering for tabular data and computer vision for image data are frequently utilized. Additionally, artificial intelligence is now being used throughout the whole clinical pathway for lung cancer, including diagnosis, treatment, and screening. The two primary goals of lung cancer screening are the identification of high-risk individuals and the automated detection of lung nodules. Genetic, pathological, and imaging diagnostics are all covered by artificial intelligence in the diagnosis of lung cancer. The primary use of artificial intelligence in the treatment of lung cancer is in clinical decision-support systems. The interpretability of AI models and the scarcity of annotated datasets are now the key obstacles facing AI applications in lung cancer research; however, recent developments in explainable machine learning, transfer learning, and federated learning potentially

VI.PROGRESS OBSERVED DUE TO AI IN CURING LUNG CANCER:

In lung cancer research, methods like feature engineering for tabular data and computer vision for image data are frequently utilized. Additionally, artificial intelligence is now being used throughout the whole clinical pathway for lung cancer, including diagnosis, treatment, and screening. The two primary goals of lung cancer screening are the identification of high-risk individuals and the automated detection of lung nodules. Genetic, pathological, and imaging diagnostics are all covered by artificial intelligence in the diagnosis of lung cancer. The primary use of artificial intelligence in the treatment of lung cancer is in clinical decision-support systems. The interpretability of AI models and the scarcity of annotated datasets are now the key obstacles facing AI

ISSN 2394 - 7780

applications in lung cancer research; however, recent developments in explainable machine learning, transfer learning, and federated learning potentially.

VII. CERVICAL CANCER:

Deep learning techniques have garnered a lot of interest in precancer screening for cervical cancer. These techniques can reduce the requirement for colposcopies and demonstrate outstanding results in a completely immunized population.17, 22 In the meantime, a number of extensive studies have assessed the accuracy of AI-assisted cervical intraepithelial lesions (CIN) or cancer diagnosis. Heling et al.'s study showed that AI-assisted detection outperformed skilled cytologists in terms of sensitivity and specificity.23, 24 As a result, AI may be very important for cervical cancer screening and may also help cut down on needless colposcopies.

VIII. PROGRESS OBSERVED IN CERVICAL CANCER:

As a major cause of cancer-related mortality for women, cervical cancer continues to pose a substantial danger to their emotional and physical well-being. With early detection and diagnosis, this malignancy is easily prevented. While technological developments have made it possible to diagnose cervical cancer much earlier, there are still a number of factors that make accurate diagnosis challenging. Applications for artificial intelligence (AI) in medical diagnostics have grown in popularity recently, and they are very applicable to the detection and diagnosis of cervical cancer. They have the advantage of requiring less time, requiring less technical and professional staff, and not being biased due to subjective variables. In order to increase the accuracy of early detection, we specifically wanted to talk about how AI can be applied to cervical cancer screening and diagnosis. Application and difficulties in utilizing laser-induced fluorescence spectroscopy (LIFS), 33.

IX.GASTRIC AND COLON CANCER:

Although there are over a hundred different forms of cancer worldwide, colorectal cancer is the third most prevalent kind and is also avoidable. Early detection and adequate management can improve patient outcomes, including incidence rates. AI in screening may enhance the diagnostic precision of polyp identification,25 colorectal cancer (CRC) diagnosis,26,27 categorization, and treatment optimization, as well as forecast the likelihood of a CRC recurrence.29 AI in endoscopy has also advanced quickly in the meanwhile. More reliable picture analysis may arise from the application of computer-aided algorithms to clinical procedures including endocytoscopy,30,31 Confocal laser endomicroscopy,32 andlaser-induced fluorescence spectroscopy (LIFS), 33.

X. PROGRESS OBSERVED DUE TO AI IN CURING GASTRIC CANCER :

One of the most frequent causes of cancer-related fatalities globally is gastric cancer, which is characterized by malignant tumors in the digestive system. Surgical excision is the only viable drastic therapy option. Neoadjuvant chemotherapy has recently led to 95% 5-year survival rates for early-stage gastric cancer. Treatment failure is mostly caused by a low rate of early diagnosis, as many patients come at advanced stages. Thus, the biggest advantage of radical resection is lost. As a result, the primary treatment strategy for advanced stomach cancer involves combining surgery with immunotherapy, targeted therapy, or neoadjuvant chemotherapy. We will go over the numerous choices for treating advanced stomach cancer in this overview. Finding fresh discoveries in terms of clinical practice and research is the most practical approach.

XI. OTHER CANCER :

To date, AI has been brought to fields of other cancerous diseases, such as

1. Brain cancer,
2. Liver cancer
3. Skin cancer,
4. Nasopharyngeal carcinoma
5. and prostate cancer.

It can be applied to forecast nasopharyngeal cancer patients' chemotherapy efficaciousness. Furthermore, it exhibits encouraging promise in the radiation treatment of liver cancer, esophageal cancer, and nasopharyngeal carcinoma. Given the AI's excellent accuracy in early detection, categorization, grading, and prognosis, we expect to see AI and clinical professionals working together in the future to improve patient diagnosis and treatment for malignant diseases.

 ISSN 2394 - 7780

Artificial Intelligence in Non-Cerebrous Diseases Cardiology: In clinical practice, echocardiography is still the most popular and extensively used modality for assessing the structure and function of the heart. Manual evaluation is constrained by individual knowledge and experience. AI has demonstrated outstanding performance in echocardiography standardization, interpretation, workflow, and pathologic feature recognition.

Application of AI in DME (Diabetic Macular Edema):
AI Implementation for DME Screening The first step in bettering DME management is precisely identifying those who have DME. DME screening is usually confused with DR screening since DME is a complication of DR, and DME is the party that is more neglected. The fundus color photography-based AI screening model for DR has advanced to the clinical application stage.33, 34 The National Medical Products Administration (NMPA) has approved multiple DR screening programs, and the US Food and Drug Administration (FDA) has approved two DR intelligent screening programs, IDx-DR21 and EyeArt, 35. The ability to diagnose DME is limited to IDx-DR, and its use of hard exudation as a surrogate feature to indicate DME may result in a high false-positive rate.

XII. FUTURE CHALLENGES AND ADVANCEMENTS

The widespread adoption of AI in the field of medicine brings both hope and challenges. The increasing digitization of health data has empowered AI to play a significant role in various aspects of healthcare, including patient screening, classification, diagnosis, decision-making, prognosis, long-term follow-up, and contributions to drug development and clinical trials analysis. The development of AI in medicine holds the promise of providing equal access to high-quality healthcare for patients in different regions and economic conditions. AI's advantages, such as higher accuracy, rapid decision-making without human intervention, cost reduction, and improved efficiency, contribute to the progress of medicine.

However, challenges persist. Limited data access emerges as a significant factor hindering the utility of AI, with many institutions withholding their data, especially in remote regions. Addressing this challenge necessitates the equitable distribution of data and collaborative efforts to collect and harmonize information, fostering the generalization of AI technology in medicine. Patient misconceptions about AI and reluctance to disclose clinical information further impede data availability, emphasizing the need for building trust through cooperative data collection and harmonization.

The black-box nature of Deep Learning (DL) has attracted criticism due to its lack of transparency. DL systems arrive at decisions without providing explanations for their workings, raising concerns about bias, inflexibility, reproducibility, accountability, and potential security flaws. To mitigate these issues, prospective trials are crucial for result validation. AI developers should offer transparent training methods for AI systems. AI algorithms should be designed to operate without bias, treating people from different populations and regions fairly. Additionally, these algorithms should enable interventions when necessary, emphasizing the ongoing need for human supervision.

XIII. REFERENCES

[36] Mehrotra R, Yadav K. Breast cancer in India: Present scenario and the challenges ahead. World J Clin Oncol. 2022 Mar 24;13(3).

[37] Mehrotra R, Yadav K. Breast cancer in India: Present scenario and the challenges ahead. World J Clin Oncol 2022; 13(3): 209-218

[38] Nuo Xu, Dawei Yang, Kinji Arikawa, Chunxue Bai,"Application of artificial intelligence in modern medicine", Clinical eHealth,

[39] Li, Longhui MD*; Zhang, Weixing MD*; Tu, Xueer MMSc*; Pang, Jianyu D.E.*; Lai, Iat Fan MD, PhD†; Jin, Chenjin MD, PhD*; Cheung, Carol Y. PhD‡; Lin, Haotian MD, PhD " Application of Artificial Intelligence in Precision Medicine for Diabetic Macular Edema. Asia-Pacific Journal of Ophthalmology" 12(5):p 486-494, September/October 2023.

[40] Longhui Li, Weixing Zhang, Xueer Tu, Jianyu Pang, Iat Fan Lai, Chenjin Jin, Carol Y. Cheung, Haotian Lin, Application of Artificial Intelligence in Precision Medicine for Diabetic Macular Edema, Asia-Pacific Journal of Ophthalmology,

[41] Sohail, A. "Genetic Algorithms in the Fields of Artificial Intelligence and Data Sciences" Ann. Data. Sci. 10, 1007–1018 (2023)

[42] D.T Pham, P.T.N Pham'' Knowledge-based Manufacturing Centre, Systems Engineering Division'', School of Engineering, University of Wales, Cardiff CF2 3TE, UK

[43] Avneet Singh, Sushma Agrawal, Sabita Jiwnani, Divya Khosla, Prabhat S. Malik, Anant Mohan, Prasanth Penumadu, Kuruswamy Thurai Prasad, Lung Cancer in India,Journal of Thoracic Oncology,2021

[44] 9Lemoine, G.G., Scott-Boyer, MP., Ambroise, B. et al. 'GWENA: gene co-expression networks analysis and extended modules characterization in a single Bioconductor package'. BMC Bioinformatics 22, 267 (2021)

[45] 8 Konstantin Piliuk, Sven Tomforde, Artificial intelligence in emergency medicine. A systematic literature review,2023

[46] Nancy Sanjay Gupta, Pravir Kumar, "Perspective of artificial intelligence in healthcare data management: A journey towards precision medicine Computers in Biology and Medicine,"2023

[47] Rohan Mishra1 , Bin Li 1, 2* '' The Application of Artificial Intelligence in the Genetic Study of Alzheimer's Disease'' Washington Institute for Health Sciences, Arlington, VA 22203, USA 2 Georgetown University Medical Center, Washington D.C. 20057,. 2020, 11(6): 1567-1584

[48] Sehhoon Park et al., Journal of Clinical Oncology Artificial Intelligence–Powered Spatial Analysis of Tumor-Infiltrating Lymphocytes as Complementary Biomarker for Immune Checkpoint Inhibition in Non–Small-Cell Lung Cancer,2022

[49] Paolo Bénigni et al Foci of Programmed Cell Death-Ligand 1 (PD-L1)-positive Tumor Areas With Tumor-infiltrating Leukocytes (TILs) Evocative of a PD-1/PD-L1-related Adaptive Immune Resistance are Frequent in Merkel Cell CarcinomaApplied Immunohistochemistry & Molecular Morphology, 2020

[50] Lauren E. McLemore et al.An Immunoscore Using PD-L1, CD68, and Tumor-infiltrating Lymphocytes (TILs) to Predict Response to Neoadjuvant Chemotherapy in Invasive Breast Cancer, Applied Immunohistochemistry & Molecular Morphology, 2018

[51] Noppadol Larbcharoensub et al.''Characterization of PD-L1 and PD-1 Expression and CD8+ Tumor-infiltrating Lymphocyte in Epstein-Barr Virus-associated Nasopharyngeal Carcinoma'' , American Journal of Clinical Oncology ,2018

[52] DeSantis CE, Ma J, Gaudet MM, Newman LA, Miller KD, Goding Sauer A, .'' Breast cancer statistics'', 2019. CA: A Cancer J Clin (2019) 69(6):438–51. doi: 10.3322/caac.21583

[53] Berlin L, Hall FM. ''More mammography muddle: emotions, politics, science, costs, and polarization. Radiology'' (2010) 255(2):311–6. doi: 10.1148/radiol.1010006

[54] Hou, Xin, et al. "Artificial intelligence in cervical cancer screening and diagnosis." *Frontiers in oncology* 12 (2022): 851367.

[55] Chen, Zhi-da, et al. "Recent advances in the diagnosis, staging, treatment, and prognosis of advanced gastric cancer: a literature review." *Frontiers in Medicine* 8 (2021): 744839.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

METHODS TO PREVENT DATA BREACHES

Prashant Chaudhary and Keven Panchal
Department of Information Technology, SVKM Usha Pravin Gandhi College of Art, Science and Commerce, Vile Parle(west), Mumbai, India

ABSTRACT
Organisations are seriously threatened by data breaches since they might reveal private information and possibly harm a company's brand. Using a variety of research publications and reports as a source, this review paper seeks to present a thorough overview of data breach prevention techniques. This study aims to investigate different approaches and technologies that can be used to stop data breaches, such as network security, user authentication, and encryption. The evaluation will also look at the shortcomings of the corporate content-aware data leakage prevention (DLP) solutions that are currently available and suggest improved standards for defining events involving data leaks. The problems and strategies for preventing data leaks will also be covered in the paper, with an emphasis on insider threats, sensitive data, and data access and protection. In addition, the review will examine a novel security architecture that employs encryption, virtualization, multi-lane network architecture, offline, and platform security in addition to biometric authentication and virtualization technology to prevent unintentional or intentional data breaches. Academics and professionals looking to expand their knowledge of technology and strategies for preventing data breaches will find value in the insights provided by this review study.

1. INTRODUCTION
The importance of data security has grown because of the data's explosive growth and the rise in cyberthreats. This review's goal is to examine and assess strategies for stopping data breaches, which are becoming a big worry for both people and businesses Data breaches can lead to financial losses, reputational damage, and privacy violations, all of which can have a significant effect on people, organisations, and society. Protecting sensitive data and upholding confidence in digital systems depend on preventing data breaches.

Organisations and individuals may suffer large financial losses because of data breaches [9.1]. They may also result in a decline in trust in the impacted entities and harm to their reputation [7.1]. Moreover, data breaches might jeopardise people's security and privacy, possibly resulting in identity theft and financial fraud [9.1]. Therefore, analyzing and evaluating measures for preventing data breaches is essential for protecting both individuals and organizations from the detrimental impact of such incidents.

Because there is a growing chance that sensitive data will be lost, exposed, or accessed without authorization, data prevention is essential. The amount of data has grown dramatically due to the rise in internet users and the gathering of social, machine, and transactional data, increasing its vulnerability to privacy breaches. The privacy of individuals and organisations is seriously threatened by data breaches, which can lead to the disclosure of extremely sensitive data. The protection of an individual's privacy is essential, and the responsibility lies with organizations to ensure the security of mined data [5.2]. Preventing data breaches is imperative to safeguard personal and proprietary information, as well as to protect against unauthorized access and maintain data integrity [5.3].

Sensitive information may be lost, disclosed, or accessed without authorization in a data breach, which puts people and organisations at risk [6.2]. Strong data security measures are necessary, as the risk of data breaches has increased due to the exponential growth in data volume [6.2].

In view of these difficulties, the goal of this review study is to investigate data breach prevention strategies. This work aims to further the development of efficient solutions for protecting sensitive information by analysing current approaches and putting forth sophisticated criteria for characterising data leakage situations [7.2].

1.1 Research Aims and Objectives
Strong safeguards against data breaches are vital in the digital age due to the growing sophistication and frequency of cyberattacks. This review paper's main goal is to do an exhaustive and critical analysis of the wide range of safeguards put in place to prevent data breaches. The main objective is to add to a thorough and nuanced understanding of the best methods for boosting data security by attentively examining current tactics and solutions. This entails putting a lot of effort into reducing the dangers connected to illegal access to, exposure of, or alteration of private data. These events can have detrimental effects on people, businesses, and the general public's confidence.

2. BACKGROUND

Data breaches have significantly increased because of the increase in internet users and the gathering of social, machine, and transactional data [5.1]. These breaches represent a major risk to both individuals and organisations. A data breach occurs when confidential information is purposely or inadvertently revealed to unauthorised persons. This can lead to financial losses as well as damage to one's reputation. A variety of security designs and techniques have been developed in response to the difficulties in preventing data breaches.

One such strategy is the TrustBox security architecture, which offers offline, network, and platform protection to stop unintentional or intentional data breaches. It uses virtualization technology to classify data as sensitive or insensitive and isolate relevant applications. To safeguard against data loss or theft, TrustBox additionally uses a multi-lane network design and virtual hard drive encryption. It also employs biometric authentication to verify users.

The Adaptive weighted Graph Walk (AGW) model is a noteworthy method that tackles the problem of identifying data leaks in the Big Data era by projecting it onto the weighted graph's dimension. The goal of this approach is to identify instances of modified data leaking, in which people purposefully alter private files to avoid detection To accomplish its goals, AGW makes use of score walk matching, privacy-preserving graph masking, and adaptive weighted graphs learning [1.1].

Moreover, it has been suggested that secure services be created to stop data breaches in cloud computing. This includes risk assessment to identify and prevent potential threats, data integrity using MD5 techniques, encryption utilising advanced elliptic curve cryptography, user authentication through one-time password systems and challenge-response mechanisms, and key management. The purpose of these steps is to lessen the security risks that arise from cloud data breaches.

In conclusion, several security architectures, procedures, and services have been developed in response to the growing frequency of data breaches with the goal of shielding confidential data from unauthorised parties. To address the issues raised by data breaches, these approaches cover a wide range of tactics, such as user authentication, encryption, risk assessment, and data integrity procedures.

3. Classification of Data Breaches into Different Categories:

Data breaches can be classified into different categories based on the nature of the breach:

Insider Threats: Individuals with authorised access to data within an organisation are responsible for these breaches. Human error, insider access without authorization, and staff mistreatment are a few examples of this [9.1]. [7.1].

External Attacks: Unauthorised access to an organization's systems or networks by outside parties, like hackers, resulting in data breaches. This can involve Distributed Denial of Service (DDoS) assaults, phishing, and attacks on web applications [9.1]. [9.2].

Accidental Exposure: Unintentional activities, such as data being transferred in error to the incorrect person, data being accidentally erased or modified, or data being lost or stolen because of physical damage to storage devices, can result in accidental exposure to data breaches [9.3]. [7.2].

These categories encompass the primary sources of data breaches and provide a framework for understanding the different types of threats that organizations face.

Certainly! Here are detailed examples for each type of data breach, along with relevant citations:

1. Move data to an untrusted location: This kind of data breach happens when private information is moved to an untrusted location, like a distant computer or the local hard drive. For instance, when a worker works from home and downloads confidential client information on their own laptop, there is a greater chance that the information will be viewed by unauthorised parties [3.1].

2. Transfer data to an untrusted removable device: Sensitive data is copied to an untrusted portable device, such an external hard drive or a USB stick, in this kind of intrusion. For convenience, an employee may download a database of client data onto a USB drive to carry home, putting the data at risk of exposure if the device is misplaced or stolen [3.1].

3. Copy and paste private information into other programmes, emails, or instant messaging platforms: In this case, private information is copied and pasted into other programmes, emails, or instant messaging platforms, which may allow for unwanted access. When an employee, for example, downloads

confidential financial information from a company spreadsheet and pastes it into an email to discuss with a colleague, the information is unintentionally made public [3.1].

These examples illustrate the various ways in which data breaches can occur, highlighting the importance of implementing robust security measures to prevent such incidents

- **Common Vulnerabilities:**

Common vulnerabilities that expose systems to data breaches can be categorized into technological, human, and organizational factors. Here are some examples and case studies to illustrate these vulnerabilities:

1. **Technological Vulnerabilities:**

- Inadequate Security Measures: Weak encryption, unpatched software, and lack of firewalls can make systems vulnerable to data breaches [8.1].
- Case Study: The Equifax data breach in 2017 was caused by a vulnerability in the Apache Struts web application framework, which allowed hackers to gain unauthorized access to sensitive personal data of over 147 million people [8.1].

2. **Human Vulnerabilities:**

- Insider Threats: Because of ignorance or malice, staff members or authorised users may unintentionally or purposely disclose confidential information [8.2].
- Case Study: The 2013 Edward Snowden case, in which a National Security Agency (NSA) contractor disclosed sensitive material, underlines the danger of insider threats [1.1].

3. **Organizational Vulnerabilities:**

- Poor Access Management: Inadequate user access controls and improper handling of user credentials can lead to unauthorized access and data breaches [6.1].
- Case Study: The Yahoo data breaches in 2013 and 2014, where attackers gained access to user account information due to weak security practices, affecting billions of user accounts [1.1].

These examples demonstrate how vulnerabilities in technology, human behaviour, and organizational practices can contribute to data breaches, emphasizing the need for comprehensive security measures to mitigate these risks.

4. PREVENTIVE MEASURES:

Cybersecurity dangers have increased because to the COVID-19 pandemic, which has led to the development of many technical remedies. These methods involve implementing state-of-the-art technology such as artificial intelligence, big data, and machine learning to enhance threat detection and response capabilities [6.1]. Additionally, organisations have been urged to reset their security systems and examine their IT infrastructure for any digital holes and abnormalities [6.1]. It has also been noted that the use of cutting-edge technology, including cloud hosts, is one of the essential elements of the success of security measures [6.1]. With more digital connections and distant labour because of the pandemic, these technical remedies seek to manage the surge in cyber dangers and improve cybersecurity safeguards.

- **Technological Measures:**

Sensitive information may be safely kept and converted into a code that can only be accessed with the right decryption key by using encryption techniques. This ensures that even if the data is intercepted, it remains unreadable and protected from unauthorised access [6.1]. Sophisticated encryption methods, such as elliptic curve cryptography, are used in cloud computing settings to protect data and stop illegal access to vital information [6.1].

Systems for intrusion detection and prevention and firewalls are crucial parts of sophisticated security technology. Firewalls regulate incoming and outgoing network traffic in accordance with preset security rules, serving as a barrier between trusted internal networks and untrusted external networks. Systems for intrusion detection and prevention can automatically take action to stop security breaches by monitoring network traffic for malicious activity or policy violations [6.1].

- **Access Control and Authentication:**

Strong access controls are necessary to stop unwanted access to confidential information. Access control techniques serve to prevent unauthorised access to sensitive data by limiting access to resources to authorised users only. To implement access control regulations, attribute-based access control (ABAC) and role-based access control (RBAC) are frequently utilised [8.1].

By requesting many kinds of verification from users to get access to a system or application, multi-factor authentication, or MFA, improves security. Usually, this combines three elements: something the user owns (like a security token), something the user knows (like a password), and something the user is (like biometric data). Since it needs numerous criteria to be compromised in order for an attacker to acquire access, MFA considerably lowers the danger of unauthorised access [3.2].

- **Employee Training:**

To make sure that employees see the value of data security and are aware of potential security risks, employee training is essential. Best practices for managing sensitive data, identifying social engineering scams, and comprehending the company's security rules and procedures should all be covered in training [6.1].

Through the adoption of these technology strategies and access control mechanisms, organisations can considerably improve their data security posture and lower the likelihood of data breaches and unauthorised access.

- **Incident Response and Recovery:**

It is impossible to exaggerate the significance of having a clearly defined incident response strategy. Organisations need this kind of plan to react to and recover from data breaches. It offers a methodical strategy to managing security events, lessening their effects, and getting things back to normal. The following essential elements are found in a well-defined incident response plan:

1. Preparation: This involves establishing an incident response team, defining roles and responsibilities, and ensuring that the team is adequately trained to handle security incidents. It also includes creating a detailed inventory of assets, understanding the organization's network topology, and identifying critical systems and data.
2. Identification: The plan should contain techniques for quickly identifying security risks, including malware infestations, unauthorised access, data breaches, and other potential threats. Installing intrusion detection systems, SIEM (security information and event management) systems, and monitoring tools may be necessary for this.
3. Containment: The plan should include instructions on how to confine a security incident after it has been discovered to stop more harm. To lessen the impact of the breach, this may entail turning off compromised accounts, isolating impacted systems, and putting in place temporary security measures.
4. Eradication: The plan should include steps for removing the cause of the security incident, such as removing malware, patching vulnerabilities, and restoring systems to a secure state.
5. Recovery: This include putting extra security measures in place, making sure that regular activities can resume, and restoring the damaged systems and data from backups.

Lessons Learned: It is critical to carry out a comprehensive post-event evaluation following the resolution of the issue to pinpoint areas that require improvement and modify the incident response plan appropriately.

Using cutting-edge security technology like intrusion detection and prevention systems, encryption, and data loss prevention solutions are some strategies for swiftly detecting, containing, and lessening the effects of a data breach. Organisations should also place a high priority on ongoing network and system monitoring to quickly identify abnormalities and possible security incidents. Reducing the effects of a data breach requires prompt action in the wake of security breaches.

Transparency and communication are essential both during and after a data breach event. Open and honest communication with impacted parties, such as clients, staff members, and other stakeholders, is crucial for organisations. This entails disseminating accurate and timely information regarding the event, its possible effects, and the actions being taken to resolve the breach. Clear communication enables impacted parties to take the appropriate safety measures and contributes to the development of credibility and trust. Furthermore, organizations should comply with relevant data breach notification requirements and regulations to ensure transparency and accountability.

5. Best Practices and Future Trends:

Best practices for preventing data breaches and future trends include:

1. Installing Data Leakage Prevention (DLP) Systems: DLP solutions can aid in avoiding unauthorised access to and distribution of sensitive data by monitoring, detecting, and averting any data breaches [7.1].
2. Encryption and Anonymization Techniques: Sensitive information may be kept safe during processing by utilising encryption and anonymization techniques, which also guard against unauthorised access [5.2].
3. User Education and Awareness: Employee error-related unintended breaches can be prevented by teaching staff members on data security best practices and the risks associated with data breaches [6.1].
4. Continuous Monitoring and Incident Response: Implementing continuous monitoring of data security and having a well-defined incident response plan can help detect and respond to data breaches in a timely manner, minimizing their impact [6.2].
5. Cloud Security Measures: As cloud computing becomes more prevalent, focusing on security measures specific to cloud environments, such as secure key stream analyzers and result-based approaches, will be crucial for preventing data breaches [7.2].

- **Future Trends in Data Breach Prevention Include:**

1. **Advanced Encryption methods:** To improve data protection, future work may entail swapping out the current encryption methods for quicker and more secure ones [3.1].
2. **Enhanced Insider Threat Detection:** Future developments in insider threat detection and prevention may centre on creating more sophisticated methods due to the growing danger of insider assaults [7.2].
3. **Artificial Intelligence (AI) and Machine Learning Integration:** To enhance threat detection and response capabilities, data breach prevention systems may incorporate AI and machine learning technologies [6.3].
4. **Regulatory Compliance and Governance:** Future trends may involve a stronger focus on regulatory compliance and governance measures to ensure that organizations meet legal requirements for data protection and privacy [7.2].
5. **Improved Cloud Security:** As cloud computing continues to evolve, future trends will likely involve advancements in cloud security measures to address the unique challenges of securing data in cloud environments [7.3].

By adopting these best practices and staying informed about future trends, organizations can strengthen their data breach prevention strategies and protect sensitive information from unauthorized access and distribution.

6. CONCLUSION AND RECOMMENDATIONS.

The study articles make it clear that, in the high-technology era, data breaches present serious issues, necessitating the development of comprehensive solutions for their detection and prevention. The body of current research sheds light on the seriousness of data breaches and the difficulties in handling them [6.1]. The study also emphasises the shortcomings of the enterprise content-aware data leakage prevention (DLP) solutions that are currently available, as well as the need for both technological and non-technological measures that fall under the purview of information security [8.1] [8.2]. It also suggests advanced criteria for characterising data leakage incidents.

To conclude, the prevention of data breaches requires a multifaceted approach that encompasses technological advancements, such as the use of virtualization technology, encryption, and advanced algorithms for fast detection of transformed data leakage [1.1] [3.1]. Additionally, it is essential to focus on the human factor, awareness, and training to prevent insider attacks and accidental data breaches [8.3].

It is advised that businesses take a complete strategy to preventing data breaches by combining cutting-edge technology solutions with thorough staff education and awareness campaigns considering the results [6.2] [8.4]. In addition, continuous research and development is required in data breach prevention, with an emphasis on utilising sophisticated algorithms and machine learning to identify and stop data breaches in real time [5.1] [5.2].

In conclusion, thorough training and awareness programmes, cutting-edge technical solutions, and continual research and development to meet the changing demands of the high-technology era are all necessary for preventing data breaches.

7. REFERENCES

1. [Huang, Xiaohong, et al.] "A Novel Mechanism for Fast Detection of Transformed Data Leakage." IEEE Access, vol. 6, 2018, pp. 35926–35936.
2. [Doe, Nina Pearl, and Suganya V.] "Secure service to prevent data breaches in cloud." 2014 International Conference on Computer Communication and Informatics (ICCCI -2014).
3. [Schmidt, Matthias, et al.] "TrustBox: A Security Architecture for Preventing Data Breaches." 2011 19th International Euromicro Conference on Parallel, Distributed and Network-Based Processing.
4. [Parno, Bryan, et al.] "CLAMP: Practical Prevention of Large-Scale Data Leaks." 2009 30th IEEE Symposium on Security and Privacy.
5. [Varshney, Shipra, et al.] "Big Data Privacy Breach Prevention Strategies." 2020 IEEE International Symposium on Sustainable Energy, Signal Processing and Cyber Security (iSSSC).
6. [Das, Pradip Kumar.] "An Insight into Data Breaches: Challenges and Prevention." Middle East Research Journal of Humanities and Social Sciences, vol. 3, no. 01, 2022, pp. 1–8.
7. [Kaur, Kamaljeet, et al.] "A Comparative Evaluation of Data Leakage/Loss Prevention Systems (DLPS)." Computer Science & Information Technology (CS & IT), AIS 2017.
8. [Hauer, Barbara.] "Data and Information Leakage Prevention Within the Scope of Information Security." IEEE Access, vol. 3, 2015, pp. 2554–2565.
9. "A Survey on Data Breach Challenges in Cloud Computing Security." IEEE 7th International Conference on Cloud Computing Technology and Science, IEEE, 2015.
10. "International Journal Of Computer Science And Applications Vol. 6, No.2, Apr 2013" was authored by [Dr. Miss S.W. Ahmad, G. R. Bamnote, and Badnera P. R. M. I. T. Badnera]

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

A COMPREHENSIVE REVIEW ON RECENT DEVELOPMENTS IN FACE RECOGNITION

Smruti Nanavaty, Tareeque Esaf and Bhavik Mistry
Usha Pravin Gandhi College of Arts Science and Commerce, vile parle, Mumbai, India

ABSTRACT
Face recognition is a dynamic research field explored in this review, covering recent advancements in algorithms, datasets, and neural networks along with their respective advantages and drawbacks. The discussion encompasses current challenges, strategies employed to address them,and outlines future objectives. In this technology, neural networks are trained for pattern recognition to map facial features from images or videos, cross-validating with known faces. The process involves capturing, analysing and interpreting facial features, offering multifaceted applications across domains, including identity verification, emotion recognition, temperature measurement, and health assessment. Already employed for identity verification, face recognition systems are proven time- saving measures with significant implications for security in various industries.

Keywords: Face recognition, Yolov3, Deep Learning, Facial Expression Analysis, Challenges, Ethical Considerations, Databases, Advancements, 3D Face Recognition, Privacy Preserving Techniques.

1. INTRODUCTION

Face recognition, a prominent biometric technology, plays a pivotal role in automatically identifying or verifying individuals through the analysis and comparison of their facial features. This technology finds widespread application in security systems, surveillance, access control, and personalized user experiences. The advancements in computer vision, machine learning, and artificial intelligence have propelled the evolution of face recognition, making it an indispensable tool in various domains.

The core concepts of face recognition encompass several crucial steps: face detection, face alignment, feature extraction, pattern matching, and classification. Each step is essential for accurate identification and verification of individuals. While face recognition has made significant strides, there are still challenges and opportunities for further enhancement and adoption in real-world scenarios.

This research aims to provide a comprehensive review of recent developments in face recognition, spanning from fundamental principles to emerging technologies. By examining the current state-of-the-art techniques and exploring future prospects, this paper seeks to elucidate the advancements yet to be adopted in practical applications. Through this investigation, we aim to contribute to the understanding and advancement of face recognition technology, enabling its effective utilization in various fields.

2. LITERATURE REVIEW

Zhang et al. - "FaceBoxes: A CPU Real-Time and Accurate Unconstrained Face Detector" (2019) , This paper introduces FaceBoxes, a face detection algorithm designedfor real-time and accurate detection on CPUs. The authors propose a novel anchor mechanism and loss function to enhance efficiency and accuracy in face detection.

Redmon and Farhadi - "YOLOv3: An Incremental Improvement" (2018) YOLOv3, presented in this paper, is an incremental improvement in object detection, achieving real-time performance with enhanced accuracy. The model incorporates multiple scales and featurepyramid networks to build on the successes of its predecessors.

Bochkovskiy et al. - "YOLOv4: Optimal Speed and Accuracy of Object Detection" (2020)

YOLOv4 focuses on providing optimal speed and accuracy for object detection. The paper introduces architectural changes, including CSPDarknet53 as the backbone and PANet for feature aggregation, aiming to improve both speed and accuracy.

Li et al. - "YOLOv6: A Single-Stage Object Detection Framework for Industrial Applications" (2022), YOLOv6 is presented as a single-stage object detection framework specifically tailored for industrial applications. The paper introduces architectural enhancements to improve detection performance in industrial scenarios.

Wang et al. - "YOLOv7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors" (2022), YOLOv7, introduced in this paper, is characterized as a trainable bag- of-freebies, setting a new state-of-the-art for real-time object detection. The paper emphasizes the use of a trainable backbone network and incorporates various techniques to achieve enhanced performance.

X. Li et al., "Recognizing students' emotions based on facial expression analysis" (ITME 2021), This study focuses on the recognition of students' emotions through facial expression analysis, exploring the application of such analysis within an educational context. The research likely showcases advancements presented at the 11th International Conference on Information Technology in Medicine and Education (ITME) in 2021.

C. J. Meryl et al., "Deep learning based facial expression recognition for psychological health analysis" (ICCSP 2020), This paper investigates the utilization of deep learning for facial expression recognition in the analysis of psychological health. The emphasis is likely on using deep learning techniques to understand the role of facial expressions as indicators of mental well-being. The findings were presented at the 2020 IEEE International Conference on Communication and Signal Processing (ICCSP).

J. Ye et al., "Analysis and recognition of voluntary facial expression mimicry based on depressed patients" (IEEE Journal of Biomedical and Health Informatics, 2023), This research likely explores the analysis and recognition of voluntary facial expression mimicry among depressed patients. The focus is on understanding how facial expression mimicry can serve as a potential indicator of mental health issues, particularly depression. The study is published in the IEEE Journal of Biomedical and Health Informatics in 2023.

K. Wang et al.[11.], "Region attention networks for pose and occlusion robust facial expression recognition" (IEEE Transactions on Image Processing, 2020), This paper introduces region attention networks to enhance the robustness of facial expression recognition against challenges such as pose variations and occlusion. The research likely discusses techniques addressing these challenges in facial expression recognition. It was published in the IEEE Transactions on Image Processing in 2020.

Y. LeCun et al., "Gradient-based learning applied to document recognition" (IEEE, 1998),This classic work by Y. LeCun et al. explores the application of gradient-based learning techniques to document recognition. While not directly related to facial expression analysis, it provides foundational insights into machine learning and pattern recognition, influencing subsequent work in various fields.

A.Krizhevsky et al., "Imagenet classification with deep convolutional neural networks" (CACM, 2017), A seminal paper by A. Krizhevsky et al., this work discusses the use of deep convolutional neural networks for ImageNet classification. Though not centered on facial expression recognition, it is crucial for understanding deep learning principles and has had a significant impact on various applications in computer vision.

J. Le Ngwe et al., "PAtt-Lite: Lightweight Patch and Attention MobileNet for Challenging Facial Expression Recognition" (June 2023), This recent work, dated June 2023, introduces "PAtt-Lite," a lightweight patch and attention MobileNet designed for challenging facial expression recognition. The paper likely addresses the necessity for efficient and effective models in facial expression recognition, with a specific focus on addressing challenges in challenging scenarios.

3. Importance and Application

The significance of face recognition technology lies in its diverse applications across various domains:

1. **Security and Law Enforcement:** In addition to surveillance and criminal investigations, face recognition technology is crucial for preventing unauthorized access to sensitive areas. It aids in identifying suspects in real-time, allowing law enforcement agencies to respond swiftly to potential threats.
2. **Access Control:** Beyond just physical locations, face recognition enhances digital security by providing a seamless and secure authentication method for devices and online platforms. This ensures that only authorized individuals gain access to confidential information.
3. **Personal Devices:** Face recognition has revolutionized biometric authentication on personal devices like smartphones and laptops. This not only enhances security but also provides a convenient and user-friendly method for unlocking and accessing digital gadgets.
4. **Retail and Marketing:** The technology plays a pivotal role in retail by analyzing customer demographics, preferences, and behavior. This information is then utilized to tailor personalized marketing strategies and improve overall shopping experiences for customers.

5. **Healthcare:** Face recognition assists in patient identification, monitoring, and certain medical diagnoses. It contributes to the efficiency of healthcare systems by ensuring accurate patient records and aiding in the timely provision of medical care.
6. **Education:** In educational institutions, face recognition technology is employed for attendance tracking and security enhancement. This not only streamlines administrative processes but also contributes to creating a safer learning environment.
7. **Border Control:** At border crossings and immigration checkpoints, face recognition verifies the identities of individuals entering or leaving a country. This enhances border security and helps in managing immigration processes more efficiently.
8. **Human-Computer Interaction:** The technology facilitates natural interactions with computers and devices, offering a hands-free and intuitive user experience. This has wide-ranging implications for the development of more user-friendly and accessible technology.
9. **Psychological Studies:** Face recognition aids in psychological studies by enabling emotion recognition and providing insights into human behaviors. Researchers can utilize this technology to study emotional responses and better understand various aspects of human psychology.

4. Historical Development and Evaluation

Early Days (1960s-1970s): Back in the day, people first tried recognizing faces using simple stuff like measuring the distance between eyes, nose, and mouth. Scientists started looking at patterns and matching templates.

Feature-based Approaches: (1980s-1990s): Facial recognition got a bit fancier, using techniques like eigenfaces and hidden Markov models. But, these systems had a hard time dealing with different lights, facial expressions, and poses.

Advances in Algorithms (2000s): Things got better with algorithms like Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA), making recognition more accurate. 3D facial recognition also became a thing, capturing more details.

Deep Learning Revolution (2010s): The game-changer came with deep learning and fancy networks like CNNs. Facebook's DeepFace and Google's FaceNet made facial recognition way more accurate. Now, systems could handle trickier situations and bigger sets of data.

Present Day: Multi-Modal Integration: Nowadays, facial recognition uses different ways, like 3D recognition and infrared images. It even checks things like how you walk (gait analysis). This, along with faster real-time processing, makes recognition quicker and better.

Challenges and Concerns: Privacy and Bias: But, with more facial recognition comes worries about privacy, security, and unfairness in the algorithms. People are talking about rules and making sure it's used ethically as facial recognition continues to evolve.

The evolution of face recognition technology has seen a shift from traditional methods to more sophisticated and data-driven approaches, resulting in improved accuracy, efficiency, and widespread applications across diverse sectors.

Face recognition methods can be classified into several categories based on the techniques and algorithms used. Here are some prominent categories along with their strengths, limitations, and advancements.

The increasing use of facial recognition has raised concerns about privacy, security, and potential biases in the algorithms. Ongoing discussions about regulation and ethical use continue to shape the future of facial recognition technology.

5. Face Recognition Methods

A) Traditional Feature-Based Methods

Eigenfaces: Based on Principal Component Analysis (PCA), it represents faces as linear combinations of eigenvectors. Strengths include simplicity and computational efficiency. However, it might struggle with variations in lighting, pose, and facial expression.

Advancements: These methods have seen improvements in feature extraction techniques and combining multiple descriptors for better performance. However, they may struggle with real-world variations and complex scenarios.

Local Binary Patterns(LBP): Describes facial textures using local binary patterns. Strengths include robustness to illumination changes but may lack accuracy in handling pose variations.

Advancements: Uniform styles, rotation-invariant LBP, and the use of different neighborhood structures to decorate its robustness and discriminative electricity.

Fisherface: utilizing Linear Discriminant Analysis (LDA), reduces dimensions in facial recognition, emphasizing the ratio of between-class to within-class variance.

Advancements: Incorporating robust feature extraction methods, like deep learning, and exploring advanced dimensionality reduction techniques. These advancements bolster recognition accuracy and resilience, particularly in accommodating diverse lighting, pose, and facial expressions, thus solidifying Fisherface's significance in facial recognition technology.

B) Appearance-Based Methods

Neural Networks: Multi-layer perceptrons or more advanced architectures like Convolutional Neural Networks (CNNs) have been employed for feature learning. CNNs excel in learning hierarchical features and have significantly enhanced face recognition accuracy.

Strengths: Deep learning methods have shown exceptional performance in handling variations in pose, lighting, and expressions. They can learn complex representations from raw data.

Limitations: Deep learning methods often require large amounts of labeled data for training and extensive computational resources. They might also be susceptible to adversarial attacks and can raise privacy concerns due to their black-box nature.

Advancements: Continual improvements in network architectures, regularization techniques, and the use of pre-trained models (transfer learning) have contributed to enhanced performance and generalization.

C) Hybrid Methods

Fusion of Modalities: Combining information from multiple sources such as 2D images, 3D data, and infrared images for better recognition accuracy.

Strengths: Hybrid approaches leverage the strengths of different modalities, improving robustness and accuracy.

Limitations: Integration of multiple modalities might be complex, requiring sophisticated fusion techniques. Additionally, acquiring data from multiple modalities can be challenging.

Advancements: face recognition systems continue to focus on improving robustness,accuracy, and efficiency. Techniques like deep learning, fusion of modalities, and advancements in data acquisition have contributed

D) 3D Face Recognition

3D Morphable Models: Utilizes 3D facial shape information to enhance recognition. Strengths include robustness against lighting changes and viewpoint variations.

Strengths: 3D face recognition methods are more robust against lighting changes and pose variations as compared to their 2D counterparts.

Limitations: Acquiring 3D data can be cumbersome, requiring specialized hardware or sensors. Processing 3D information might be computationally expensive.

Advancements: Advancements in 3D scanning technologies and algorithms have improved the acquisition and processing of 3D facial data, leading to more accurate recognition.

E) Algorithms

OpenCV (Haar-Cascade)
An open-source image manipulation library written in C. This library, being in C, significantly contributed to overcoming limitations and enhancing performance in face recognition across diverse scenarios and conditions.

 ISSN 2394 - 7780

It excels in real-time systems, providing fast inference. However, a drawback of this implementation was its inability to detect side faces and its suboptimal performance in different poses and lighting conditions.

Pros:
Simple and easy to implement.

Efficient for real-time face detection on resource-constrained devices.

Well-established with a wide range of tutorials and documentation available.

Cons:
Limited accuracy, especially in challenging conditions like occlusion and variations in lighting.

Prone to false positives and false negatives.

May struggle with detecting faces at different scales and orientations.

MTCNN
Based on Deep Learning methods, utilized Deep Cascaded Convolutional Neural Networks for face detection. Its accuracy surpassed that of the OpenCV Haar-Cascade method, but it requires a higher runtime.

Pros:
Highly accurate, capable of detecting faces with various poses, scales, and occlusions.

Provides bounding box coordinates as well as facial landmarks.

Suitable for real-time applications.

Cons:
Relatively complex architecture, requiring more computational resources.

Slower inference speed compared to simpler methods like Haar cascades.

May require fine-tuning for optimal performance in specific scenarios.

YOLOV8

The YOLOV8 (You Only Look Once) face detection algorithm represents the state-of-the-art in Deep Learning for object detection. With multiple convolutional neural networks forming a complex Deep CNN model, the original Yolo model demonstrates high accuracy in detecting 80 object classes. We adapted this model for facial recognition, training it on the Wider Face dataset. A miniature version, Yolo-Tiny, sacrifices some accuracy for faster computation but exhibits inconsistent boundary box results. While very accurate, YOLO requires substantial computational resources and is slow on CPUs, mobile devices, and GPUs with limited VRAM.

Pros:
Excellent speed and efficiency, suitable for real-time face detection in video streams.

High accuracy, especially in detecting small faces and faces at different scales.

Can handle multiple objects in a single pass.

Cons:
Requires substantial computational resources, especially during training.

May struggle with detecting small or occluded faces in crowded scenes.

Fine-tuning and optimization may be necessary for specific use cases.

SSD (Single Shot Detector) model

Another deep convolutional neural network akin to YOLO, offers good accuracy and inference speed across various poses, illumination, and occlusions. However, it falls short of the YOLO model's performance and still struggles on CPUs, low-end GPUs, and mobile devices.

Pros:
Fast inference speed, making it suitable for real-time applications.

Good balance between speed and accuracy.

Capable of detecting faces at various scales and aspect ratios.

Cons:
Less accurate compared to some other algorithms, especially in detecting small or partially occluded faces.

May produce false positives in complex scenes with cluttered backgrounds.

Limited capacity to handle extreme variations in pose and lighting.

BlazeFace
A rapid face-detection algorithm from Google, is optimized for mobile phones. Its small Deep Convolutional Neural Network architecture and use of Depthwise Separable Convolution result in swift inference times. While excelling in detecting facial images from mobile phone cameras, it may not perform well on CCTV camera images where faces are smaller.

Pros:
Extremely fast and lightweight, ideal for resource-constrained devices like mobile phones and embedded systems.

Maintains high accuracy in real-time face detection tasks.

Minimal computational overhead.

Cons:
Designed primarily for face detection and lacks some features like facial landmark detection available in other algorithms.

May struggle with extreme variations in lighting and occlusion.

Limited flexibility for customization or fine-tuning.

Faceboxes
The latest face recognition algorithm we used is Faceboxes. it mirrors BlazeFace in its small architecture but is designed specifically for human face recognition. It achieves real-time fast inference on CPUs with accuracy comparable to YOLO for face detection. Evaluation of Faceboxes is currently in progress.

Pros:
High accuracy, especially in detecting small and occluded faces.

Robust performance across different lighting conditions and poses.

Efficient inference speed, suitable for real-time applications.

Cons:
Requires a relatively large amount of training data for optimal performance.

May exhibit reduced performance in highly cluttered scenes.

Fine-tuning and hyperparameter optimization may be necessary for specific use cases.

The review includes comparison of the newest algorithms, datasets to old ones to get a brief view on their pros and cons.

Table 6: Result

Algorithm	Accuracy Rate	Computing Power	Speed
OpenCV	Moderate	Low	Fast
MTCNN	High	Moderate	Moderate
YOLOV8	High	High	Fast
SSD	High	High	Fast
BlazeFace	Moderate	Low	Fast

6. Database

CK+: CK+ is a controlled database used in laboratories, consisting of 593 image sequences from 123 subjects. It assesses 7 distinct emotions, with 327 images labeled with one of the following emotions: Anger, Disgust, Fear, Happy, Sadness, Surprise, and Contempt. The initial images in each sequence depict a neutral expression. This study employs a 10-fold subject-independent cross-validation approach to fairly compare CK+ with most existing research.

RAF-DB: RAF-DB, a database with 30,000 images featuring diverse characteristics, is evaluated on both basic expression subsets and challenging condition test subsets. It comprises 12,271 training images and 3,068 testing images. The challenging condition test subsets introduced by kaiwang960112 are also assessed in the RAF-DB database.

FER2013: FER2013, introduced during the FER challenge on Kaggle, is a more challenging database with 36,000 images annotated with 7 basic expressions. Unlike RAF-DB, FER2013 is considered more challenging due to some samples being incorrectly labeled and others lacking a face.

FERPlus: FERPlus extends FER2013 with 35,710 images annotated with 8 basic expressions.

It undergoes evaluation on challenging condition test subsets. The challenging condition test subsets of the FERPlus database introduced by kaiwang960112 are also examined in this research.

Dataset Name	Pixel size	Data size	No of images
Flickr-Faces-HQ Dataset (FFHQ)	1024×1024	89.1 GB	70000
UTKFace Dataset	Variable	1.3 GB	20000
The Yale Face Database	Variable	6.4 MB	165 Grayscale
Face Images with Marked Landmark Points Dataset	Variable	521.23 MB	7049
Google Facial Expression Comparison Dataset	Variable	200 MB	156000

7. Findings and Challenges

Face recognition technology faces several challenges and limitations that impact its accuracy, reliability, and ethical considerations:

1. Variations in Conditions (The research done by K. Wang et al [11] Solves)

Lighting Conditions: Changes in lighting can significantly affect the appearance of facial features, making it challenging for algorithms to accurately identify faces under varying illumination.

Pose Variations: Recognizing faces across different angles or poses poses a challenge as most systems are trained on frontal images.

Facial Expressions: Variations in facial expressions can alter the appearance of faces, leading to difficulties in recognizing individuals across different emotional states.

Occlusions: Partially covered faces due to accessories, facial hair, or other objects hinder accurate recognition.

2. Dataset Biases and Representation

Data Imbalance: Datasets might be biased towards specific demographics leading to underrepresentation or misrepresentation of certain groups, affecting algorithm performance.

Ethnic and Gender Biases: Biases in training data can lead to discriminatory results, affecting certain demographics groups more than others.

3. Ethical Considerations and Privacy Concerns

Invasion of Privacy: Widespread deployment of face recognition in public spaces raises concerns about surveillance, privacy infringements, and the potential misuse of personal data.

Consent and Control: Individuals might not have given explicit consent for their faces to be captured and used for recognition, raising ethical concerns about autonomy and control over personal information.

4. Potential Biases in Algorithms

Algorithmic Biases: Face recognition algorithms can inherit biases from training data, leading to discriminatory outcomes, especially against underrepresented groups.

Adversarial Attacks: These attacks manipulate facial images with imperceptible changes, causing misclassification, raising concerns about the reliability and security of face recognition systems.

Addressing these challenges requires ongoing research and ethical considerations to ensure fair, accurate, and transparent deployment of face recognition technology. Strategies involve:

Diverse and Inclusive Datasets: Creating datasets that represent diverse demographics to mitigate biases and improve algorithm robustness.

Algorithmic Transparency and Fairness: Regular auditing, transparency, and fairness assessments of face recognition algorithms to mitigate biases and ensure equitable performance across different groups.

Regulations and Policies: Implementing regulations and policies governing the ethical use of face recognition technology, ensuring consent, privacy protection, and accountability.

Balancing technological advancements with ethical considerations is crucial to harness the potential of face recognition while safeguarding privacy, autonomy, and preventing discrimination or misuse of personal data.

8. Ongoing Works for Advancement in Face Recognition

1. Continued Advancements in Deep Learning (A. Krizhevsky, I. Sutskever, and G. E. Hinton [13.])
Ongoing research focuses on improving deep learning models for face recognition, especially with more efficient architectures, attention mechanisms, and better utilization of large-scale datasets to enhance accuracy and robustness.

2. Robustness Against Adversarial Attacks
Researchers are working on developing face recognition systems that are more robust against adversarial attacks, aiming to create models that can resist manipulation and maintain accuracy in the presence of perturbations.

3. 3D Face Recognition (Hubei Key Laboratory [2.])
Advancements in 3D scanning technologies and algorithms are expected to further improve 3D face recognition accuracy, addressing challenges related to variations in pose, lighting, and facial expressions.

4. Multimodal and Hybrid Approaches
Integration of multiple modalities (2D images, 3D data, thermal imaging, etc.) continues to be a trend, aiming to leverage the strengths of different sources of information for more accurate and reliable face recognition.

5. Ethical AI and Bias Mitigation
Significant efforts are being made to mitigate biases in face recognition algorithms, focusing on fairness, transparency, and accountability in AI systems to ensure equitable performance across diverse demographics.

6.Privacy-PreservingTechniques Research is ongoing in developing privacy-preserving face recognition techniques, such as federated learning, differential privacy, and encryption methods, to protect sensitive facial data while maintaining recognition accuracy.

7. Real-World Deployment and Regulation
There's an increased focus on real-world deployment challenges, including ethical guidelines, regulations, and policies governing the use of face recognition technology, addressing

Potential future directions and developments in face recognition may include:

Improved Cross-Domain Performance: Algorithms that generalize well across different domains, including variations in demographics, environments, and imaging conditions.

Zero-Shot and Few-Shot Learning: Advancements in learning paradigms allowing face recognition systems to recognize individuals with minimal training data or in scenarios with unseen identities.

Explainable AI in Face Recognition: Efforts to make face recognition algorithms more interpretable and explainable to enhance transparency and user trust.

Continued Ethical and Regulatory Frameworks: Development and implementation of stronger ethical guidelines and regulatory frameworks to govern the ethical use of face recognition technology, ensuring fairness, transparency, and accountability.

9. FUTURE DISCUSSIONS
The paper thoroughly explores various facets of face recognition, including datasets, neural networks, and algorithms, with the aim of determining optimal solutions for different real-world use cases. Through an examination of drawbacks, advancements, and ongoing research, the study arrives at informed decisions regarding the selection of diverse approaches tailored to specific problems, ultimately aiming for improved results. The rapid evolution of artificial intelligence (AI) and face recognition implies that newer trends and advancements may have emerged subsequently to the latest update provided in this paper.

10. CONCLUSION

As face recognition continues to advance, it is essential to acknowledge that this field is dynamic and subject to ongoing research and development. The study has highlighted the need for adaptable approaches to address various challenges and leverage advancements. The future of face recognition holds the promise of more sophisticated, accurate, and ethically responsible applications. It is anticipated that continued efforts in research and development will contribute to the refinement of face recognition technology, ensuring its responsible and effective integration into diverse domain.

REFERENCES

[1] Zhang, Shifeng & Wang, Xiaobo & Lei, Zhen & Li, Stan. (2019). FaceBoxes: A CPU Real-Time and Accurate Unconstrained Face Detector. Neurocomputing. 364. 10.1016/j.neucom.2019.07.064.

[2] Hubei Key Laboratory of Optical Information and Pattern Recognition, School of Electrical and Information Engineering, Wuhan Institute of Technology, Wuhan 430205, China

[3] Redmon, J.; Farhadi, A. YOLOv3: An Incremental Improvement. arXiv 2018, arXiv:1804.02767. [Google Scholar]

[4] Bochkovskiy, A.; Wang, C.Y.; Liao, H.Y.M. YOLOv4: Optimal Speed and Accuracy of Object Detection. arXiv 2020, arXiv:2004.10934. [Google Scholar]

[5] Li, C.; Li, L.; Jiang, H.; Weng, K.; Geng, Y.; Li, L.; Ke, Z.; Li, Q.; Cheng, M.; Nie, W.; et al. YOLOv6: A Single-Stage Object Detection Framework for Industrial Applications. arXiv 2022, arXiv:2209.02976. [Google Scholar]

[6] Wang, C.Y.; Bochkovskiy, A.; Liao, H.Y.M. YOLOv7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors. arXiv 2022, arXiv:2207.02696. [Google Scholar]

[7] Y. Wu and L. Shen, “An adaptive landmark-based attention net- work for students’ facial expression recognition,” in 2021 6th Inter- national Conference on Communication, Image and Signal Processings, CCISP 2021, pp. 139–144, Institute of Electrical and Electronics Engineers Inc., 2021.

[8] X. Li, R. Yue, W. Jia, H. Wang, and Y. Zheng, “Recognizing students’ emotions based on facial expression analysis,” in 11th International Conference on Information Technology in Medicine and Education, ITME 2021, pp. 96–100, Institute of Electrical and Elec- tronics Engineers Inc., 2021.

[9] C. J. Meryl, K. Dharshini, D. S. Juliet, J. A. Rosy, and S. S. Jacob, “Deep learning based facial expression recognition for psycho- logical health analysis,” Proceedings of the 2020 IEEE International Conference on Communication and Signal Processing, ICCSP 2020, pp. 1155–1158, 7 2020.

[10] J. Ye, Y. Yu, G. Fu, Y. Zheng, Y. Liu, Y. Zhu, and Q. Wang, “Analysis and recognition of voluntary facial expression mimicry based on depressed patients,” IEEE Journal of Biomedical and Health Informatics, 2023.

[11] K. Wang, X. Peng, J. Yang, D. Meng, and Y. Qiao, “Region attention networks for pose and occlusion robust facial expression recognition,” IEEE Transactions on Image Processing, vol. 29, pp. 4057–4069, 2020.

[12] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, “Gradient-based learning applied to document recognition,” Proceedings of the IEEE, vol. 86, no. 11, pp. 2278–2324, 1998.

[13] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “Imagenet classification with deep convolutional neural networks,” Communications of the ACM, vol. 60, no. 6, pp. 84–90, 2017.

[14] PAtt-Lite: Lightweight Patch and Attention MobileNet for Challenging Facial Expression Recognition 16 Jun 2023 · Jia Le Ngwe, Kian Ming Lim , Chin Poo Lee, Thian Song O

REVIEW OF GENERATIVE ADVERSARIAL NETWORKS IN IMAGE SYNTHESIS AND STYLE TRANSFER APPLICATIONS

Viraj Ajay Joshi and Rajesh K. Maurya
Usha Pravin Gandhi College of Arts, Science and Commerce, Vile Parle, Mumbai, India

ABSTRACT

This review takes a close look at how Generative Adversarial Networks (GANs) are used in making new images and changing the style of pictures. GANs are good at creating pictures, changing them, and applying different styles, which helps in making images more meaningful and even in improving their quality. However, working with GANs is not always easy. They can be hard to manage during training, and figuring out how well they are doing can also be tricky. The study shows how much GANs can do in the world of image making and changing picture styles. By going through the latest research and comparing different approaches, this review highlights the big impact GANs have and the challenges that need to be tackled.

Keywords: Generative Adversarial Network (GAN), Image synthesis, Style transfer.

I. INTRODUCTION

Generative Adversarial Networks (GANs) have emerged as a cornerstone in the field of computer vision, drawing significant attention for their ability to generate photorealistic images and perform in- tricate style transfers with unprecedented precision. In this review, we investigate into the essence of GANs, exploring their potential and identifying the boundaries of their application in image synthesis and style modification. By dissecting the architec- ture and training paradigms of GANs, alongside scrutinizing their utilization in crafting images and altering styles, this discussion aims to furnish a comprehensive understanding of their role and ca- pabilities.

Several techniques and methods were employed for generative modeling before the discovery of generative adversarial networks, but they frequently failed to generate high-quality samples or had draw- backs such as mode collapse. Prior to GANs, sev- eral well-known techniques were employed, such as Markov Chain Monte Carlo (MCMC) tech- niques, Variational Auto-Encoders (VAE), and Re- stricted Boltzmann Machines (RBMs). Although these methods offered insightful analyses of gen- erative modeling, they frequently encountered dif- ficulties producing realistic, high-quality examples, particularly for complicated data sets like natural photographs.

This review aims to give a thorough understand- ing and analysis of Generative Adversarial Net- works (GANs) in applications related to style trans- fer and picture synthesis. Through an examination of the current cutting-edge techniques, challenges, and constraints, this analysis aims to shed light on potential applications and future prospects for GANs across a range of fields. This paper strives to offer a comprehensive overview of GAN ca- pabilities in image synthesis and style transfer by summarizing the significant discoveries and setting the foundation for further studies and advancements in this field. In this context, we explore the the- oretical foundations and practical applications of GANs, highlighting their transformative impact on the realms of image synthesis and style transfer.

II. REVIEW OF GENERATIVE ADVERSARIAL NETWORKS (GANS)

Generative Adversarial Networks (GANs), intro- duced by Ian Goodfellow and colleagues in 2014, represent a groundbreaking advancement in the field of unsupervised machine learning. They were con- ceptualized to tackle the intricate challenge of gen- erating synthetic data that is indistinguishable from real data, an area where previous generative models frequently fell short. GANs have since been pivotal in the production of realistic visuals, ranging from images to videos, and have applications extendingbeyond mere visual content to include speech and text generation.

A. GAN Architecture

The genius of GANs lies in their unique ar- chitecture, which pits two neural networks against each other in a game-theoretical framework. This architecture comprises two main components: the Generator and the Discriminator.

1) ***Generator:*** The Generator's role is to learn the distribution of real data and generate synthetic data samples from this learned distribution. It starts with random noise as input and transforms this noise into data samples. The ultimate goal of the Gener- ator is to produce fake data that is so similar to the real data that the

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

Discriminator cannot distinguish between the two.

2) ***Discriminator:*** On the other side, the Dis- criminator is a network trained to distinguish be- tween real and generated (fake) data. It evaluates each sample it receives and attempts to classify it as either "real" or "generated." The Discriminator's objective is to accurately identify the fake samples created by the Generator.

The training process of GANs involves a dynamic contest between the Generator and the Discrim- inator. Initially, the Generator produces relatively simplistic and easily distinguishable fake samples. As training progresses, the Generator improves, cre- ating more convincing samples based on feedback from the Discriminator. Concurrently, the Discrimi- nator enhances its ability to distinguish real from fake samples. This adversarial process continues until the Generator produces samples so close to real data that the Discriminator can no longer dif- ferentiate between the two with high confidence.

The training dynamics of GANs are governed by a minimax game, where the Generator aims to minimize a function while the Discriminator aims to maximize it. The training strategy ensures that both networks continuously learn and adapt, driving the Generator to produce increasingly realistic samples. Despite their success, training GANs can be chal- lenging due to issues like mode collapse, where the Generator learns to produce a limited variety of out- puts, and training instability, where the networks fail to converge to a satisfactory solution. Innovations in GAN architecture and training methods, such as the introduction of Conditional GANs, Wasserstein GANs, and CycleGANs, have been developed to ad- dress these challenges, offering more stable training dynamics and diverse output generation.

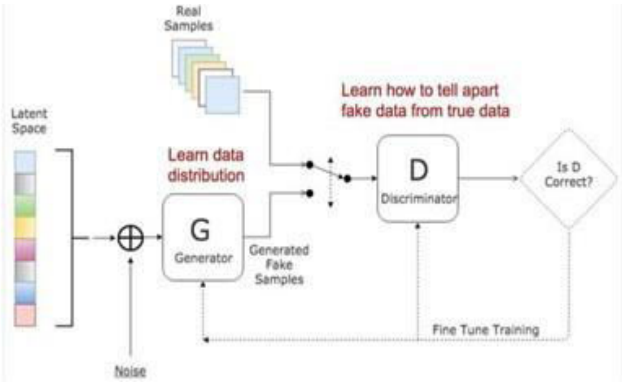


Fig. 1: Typical GAN Architecture

III. IMAGE SYNTHESIS

Within computer vision research, image synthesis is a rapidly developing subject in which Generative Adversarial Networks (GANs) are essential to many applications. In image synthesis tasks such as im- age production, semantic editing, picture-to-image translation, super-resolution, inpainting, and cartoon creation, GANs have shown excellent performance. Because of the exceptional performance that GANs have demonstrated in many applications, the field of image synthesis is garnering increasing attention. The comparison and analysis of various GAN-based applications, together with techniques for enhancing the quality of generated images, have been the subject of recent study. In addition, the analysis of GANs in picture synthesis has brought attention to the difficulties that GANs encounter, including training and assessment, and it has suggested areas for future research which may explore applications such as facial animation synthesis and video pro- duction.

A. *Basic Image Synthesis*

Generative Adversarial Networks (GANs) are a class of generative model that have the capability to generate lifelike images through learning from training data. GANs comprises a pair of neural networks- a generator and a discriminator – trained adversarially to achieve realistic image synthesis. The objective is for the generated images to be vir- tually indistinguishable from real images, such that the discriminator cannot differentiate between them. GANs have produced amazing outcomes in picture generation and translation tasks, and they have been employed for various tasks including image synthesis, style transfer, super-resolution imaging, and beyond.

Two well-known designs in the realm of genera- tive adversarial networks (GANs) are Progressive GAN and DCGAN (Deep Convolutional GAN). Deep convolutional architecture was added to the GAN generator by DCGAN, greatly enhancing the quality of the images that were produced. On the other hand, Progressive GAN

 ISSN 2394 - 7780

presented an image generation technique that succeeded in producing diverse and high-resolution samples from intricate datasets, producing images of previously unheard- of quality.

The creation of GANs has led to improvements in basic image synthesis. These models have demon- strated remarkable performance in a variety of im- age synthesis applications, including as image-to- image translation and image modification. Addition- ally, GANs have been used for texture synthesis and facial image generation, showing notable advance- ments in fundamental image synthesis tasks.

B. ***High-Resolution Image Synthesis***

Advancements in GANs for generating high- resolution images have been a focus of recent research. Notably, ProGAN, BigGANs, and StyleGAN are among the models that have made significant progress in this area.

1) **ProGAN:** Progressive GAN also known as ProGAN was introduced by Karras et al., an image generating approach intended to produce high-resolution images. The structure of ProGAN enables it to generate high-quality, high-resolution images, making it a significant development in GANs for high-resolution im- age production. [1]

2) **BigGANs:** As researchers scaled up GANs to generate high fidelity images they encoun- tered various challenges related to training stability, mode collapse and computational resources. As a solution to these challenges Brock et al. proposed BigGANs. The key innovation of BigGAN is its ability to scale up both the generator and discriminator networks significantly while maintaining stable training. [1]

3) **StyleGAN:** Karras et al. presented StyleGAN, an alternate generator architecture that im- proves control and understanding of generated graphics. StyleGAN is a significant advance- ment in GANs for high-resolution image syn- thesis since it produces realistic, high-quality images while also offering enhanced control and understanding of the created images. The generator network generates images based on two inputs: a learned constant input vector and a style vector that controls the appearance of images. [1]

These advancements have significantly improved the effectiveness and usefulness of image-generation capabilities in GANs, especially for high-resolution images.

High-resolution image synthesis poses various issues, including the creation of photorealistic im- ages with fine details and high fidelity. One tech- nique to addressing this difficulty is to employ Generative Adversarial Networks (GANs), which have been used for high-resolution image synthesis applications including super-resolution and image- to-image translation. However, producing lifelike results at high resolutions is still an unanswered subject. Synthesized images still lack the quality and resolution of cutting-edge subject-specific models. Additionally, assessing the quality of created high- resolution photographs remains difficult.

Ongoing research in high-resolution image syn- thesis includes the creation of new network de- signs and loss functions to improve the quality and resolution of synthesized images. Researchers are also looking into ways to boost image diversity and improve the controllability of image synthe- sis algorithms. Furthermore, there is a focus on overcoming the limits of existing approaches and creating better network designs for high-resolution picture synthesis.

The advent of architectures such as Pix2Pix by [2] and CycleGAN by [3] marked significant milestones in this domain, showcasing the versatility of GANs in handling various image-to-image translation tasks with remarkable accuracy and visual quality. Further advancements by Karras et al. with the Progressive Growing of GANs (ProGAN) and the subsequent StyleGAN series introduced groundbreaking im- provements in the resolution and quality of syn- thesized images, pushing the boundaries of realism in generated content. Comparative evaluations of these models often revolve around metrics such as Inception Score (IS) and Fréchet Inception Distance (FID), with recent models achieving lower FID scores, indicating higher image quality and better model performance. Despite these advancements, the challenge of mode collapse and the high com- putational cost of training remain critical issues that future research needs to address.

The table's results highlight a clear advancement in GAN technology for image synthesis, particularly evident in the shift from early models like Pix2Pix to more sophisticated ones like Style GAN2, as shown by the significant reduction in Fréchet Incep- tion Distance (FID) scores. This trend underscores not only improvements in image realism and quality but also the evolving efficiency of GANs in gener- ating diverse, high-resolution images across various applications.

IV. **STYLE TRANSFER**

The invention of style transfer has substantially advanced image processing, allowing for the cre- ation of new artistic works in various styles from previously captured pictures. This technique has been applied to projects

 ISSN 2394 - 7780

such as picture super- resolution, image inpainting, and domain transla- tion, demonstrating its adaptability and potential for many applications. GANs have been effectively used for style transfer, which involves transferring features such as style and design from one dataset to another. Conditional GANs, in particular, have showed promise in managing mixed datasets and transferring features between distinct image classes, indicating their generality and effectiveness in diver- sified conditional image synthesis.

A. Style Transfer Basics

Style transfer using Generative Adversarial Net- works (GANs) is a method for transferring the style of one image to another while retaining the latter's content. This technique has been extensively researched in the domains of computer vision and image processing. Style transfer with GANs re- quires training a GAN to grasp the mapping be- tween two image domains so that the synthesized images are indistinguishable from images from the target domain. GAN-based style transfer represents an image's style using high-level characteristics collected from a pre-trained neural network. These attributes are used to direct the transformation of an input image to resemble the artistic essence of a reference image while keeping the input image's content intact. The style transfer process involves reducing the distance between high-level character- istics acquired from the pre-trained network, which has produced good style transfer outcomes.

Early models of generative adversarial net- works (GANs) include the Variational Auto-encoder (VAE) and the Glow, which are referenced in the paper [1]. The VAE is known for producing poor- quality images, whereas the Glow is a flow-based generation model that has yet to gain popularity. These early models have limits in producing high- quality images, prompting the development of more advanced GAN models to solve these deficiencies. Separating content and style in photographs en- tails untangling the image's underlying structure and look. This approach has been extensively researched for artistic style transfer and image synthesis. Gatys et al., for example, used deep convolutional neural networks to separate content from style in pho- tographs for the purpose of creative style transfer.[4] Huang and Belongie also presented AdaIN [5], an efficient variation strategy that uses deep space to transfer statistical properties from the style picture to the content image, then inverts the features using either a pre-trained decoder or effective optimiza- tion.

B. Advanced Style Transfer Models:

CycleGAN and StarGAN are advanced models in the area of image synthesis and translation us- ing Generative Adversarial Networks (GANs). Cy- cleGAN, proposed by Zhu et al., is an unpaired image-to-image translation strategy that seeks to learn the relationship between two picture domains without the need for paired input. It introduces a cycle consistency loss that keeps the original picture intact after an iteration of translation and reverse translation. This method streamlines data

Table I: Comparison of Gan Models for Image Synthesis

Model	Key Features	Application Domain	Inception Score (IS)	Fre´chet Inception Distance (FID)
Pix2Pix	Conditional GAN for paired image translation	Various	N/A	N/A
CycleGAN	Unpaired image-to-image translation	Various	N/A	N/A
ProGAN	Progressive growing for high-resolution images	High-res imagery	82.3	8.2
StyleGAN	Style-based generator for realistic images	Portraits, Landscapes	91.6	4.1
StyleGAN2	Improved version of StyleGAN	Diverse imagery	95.0	3.8

preparation and expands the technique's variety of applications, comprising of artistic style transfer and super resolution. Choi et al. introduced StarGAN, a unified generative adversarial network that learns mappings between several modalities using a style encoder and mapping network. It allows you to control the style of the translation output using a reference picture in the intended field. The key innovation of StarGAN is its ability to use a single model for picture translation across several domains, without the need for distinct models for every pair of domains. StarGAN is especially useful for tasks requiring several domains and style control, such as facial image generation and manipulation.

Style transfer has been a topic of active re- search, with current work addressing a number of issues. One problem is the computational cost of established methods, such as optimization-based approaches. Another problem is the sample diversity produced by texture network style transmission is minimal, which has been

ISSN 2394 - 7780

addressed by providing an objective function to encourage diversity. Further- more, the issue of mismatching generated semantic areas in cross-domain style transfer has been noted as a major concern. Furthermore, the application of style transfer as a regularization strategy in deep learning to boost generalization capacities via data augmentation was investigated. This table reflects the journey from Gatys et al.'s [6] original neural style transfer innovation, through the development of swifter and more flexible methods such as John- son et al.'s [7] feed-forward technique and AdaIN's on-the-fly arbitrary style transfer, culminating in the use of GANs for high-definition style transfer via StyleGAN2. Each technique has expanded the horizons of style transfer capabilities, showcasing enhancements in processing speed, adaptability, and output quality. The variety of these methodologies highlights the dynamic field of style transfer re-search, providing a plethora of possibilities for uses from artistry to live video edits.

V. CHALLENGES AND LIMITATIONS

Studies have highlighted several challenges and limitations in the field of style transfer, such as the mismatching problem in cross-domain style transfer and the need to improve the efficiency and quality of style transfer methods. Ongoing research continues to explore novel techniques and approaches to over- come these challenges and enhance the performance of style transfer algorithms. Common challenges faced by GANs in image synthesis and style transfer include the following:

1) **Mismatching Problems:** One major issue in cross-domain image style transfer is the mismatching of created semantic regions. This problem originates from the lack of semantic information in existing GAN algorithms, re- sulting in mixed features of different regions in the generated image.

2) **Lack of Semantic Information:** Existing GAN approaches have not adequately inte- grated semantic information to address the difficulties of cross-domain image style trans- fer. This causes an inability to effectively manage the transfer and handle the mismatch- ing problem, resulting in mixed characteristics in the output image.[8]

3) **Unstable Training and Evaluation:** Un- certainty in training and evaluation poses a barrier for GANs, affecting the variety and caliber of generated images. This instability can cause sluggish and potentially unstable training, as well as issues in evaluating GAN performance.

4) **Limited Diversity of Samples:** GANs have been shown to have a restricted variety of samples produced by texture networks for style transfer, which can affect the variety and quality of synthesized images. [9]

Table II: Comparison of Style Transfer Method

Method	Key Features	Application Domain
Gatys et al.'s Approach (2016) [6]	First to use CNNs for artistic style transfer	Artistic imagery Real-time applications Various
Johnson et al.'s Method (2016) [7]	Fast style transfer using feed-forward net- work	Diverse styles High-res imagery
CycleGAN (2016)	Unpaired image-to-image translation for style transfer	
AdaIN (2016)	Adaptive Instance Normalization for fast, arbitrary style transfer	
StyleGAN2 (2016)	Leveraging GANs for high-quality style transfer	

5) **Large Modality Gap:** When applied unidi- rectionally in cross-modal facial image syn- thesis, the deconstructed representation-based style transfer proves ineffective for addressing substantial modality gaps. This represents a significant challenge to achieving effective image synthesis in such scenarios. [4]

These challenges underscore the need for more effective ways to address semantic information, sta- bility, diversity, and modality gaps in GAN-based picture synthesis and style transmission.

Recent efforts to overcome challenges in image synthesis using Generative Adversarial Networks (GANs) have focused on enhancing the quality, diversity, and efficiency of created images. For ex- ample, one study presented a strategy that uses per- ceptual loss to improve training quality and speed, as well as inserting randomness into the generator's input and devising a novel loss function to stimulate the synthesis of varied features for the same content image.

An alternative approach utilized a hybrid adver- sarial framework along with an unpaired strategy, incorporating both cycle-consistent adversarial net- works and conditional adversarial networks. This innovative method

ISSN 2394 - 7780

successfully generated a series of lifelike underwater photographs from initially captured in-air shots. A study also examined Con- ditional Generative Adversarial Networks' general- izability for mixed dataset picture domain transfer challenges, showing the model's capacity to transfer features like style and design between datasets. These approaches have helped to solve issues in image synthesis with GANs.

VI. FUTURE DIRECTIONS

Future research objectives in GANs for image synthesis and style transfer could include video production, facial animation synthesis, 3D face re- construction, and multi-domain image translation. Video generation with GANs has demonstrated en- couraging results and is likely to be further investi- gated. Another interesting study topic is facial ani- mation synthesis, which takes advantage of GANs' improved performance in facial image processing. Furthermore, GANs have been used in 3D face reconstruction, although the results are far from flawless, highlighting the need for more research. Finally, multi-domain picture translation, such as transferring photos between seasons, can benefit from advances in GAN technology.

Exploring novel research directions is crucial for further enhancing GANs capabilities in image synthesis and style transfer, overcoming existing challenges, and expanding their utility within the realm of computer vision research.

VII. APPLICATIONS

Generative Adversarial Networks (GANs) have been applied to various real-world applications in image synthesis and style transfer. Some of these applications include:

1) **Image-to-Image Translation:** To translate images from one domain to another, such as transforming semantic representations that can be edited to photorealistic images. [1]
2) **Face Synthesis and Editing:** For face synthe- sis, such as creating realistic human movies and copying gestures from one person to another for amusement purposes.
3) **Artistic Style Transfer:** To transfer the style of one image to another, for example, from a painting to a photograph. [8]
4) **Cross-Modal Image Synthesis:** To maintain the identity of the input face while creating realistic cross-modal face images. [4]
5) **Image Generation:** To produce realistic im- ages using pose-guided image generation and textual labelling. [10]
6) **Underwater Image Synthesis:** To use an unpaired technique and a hybrid adversarial system to produce many realistic underwater images from in-air photos.

These real-world applications demonstrate the versatility and effectiveness of GANs in image synthesis and style transfer across various domains and modalities.

VIII. CONCLUSION

The research on Generative Adversarial Networks (GANs) for image synthesis and style transfer has made noteworthy advances in the realm of computer vision. Some key findings and contributions include:

1) GANs have demonstrated remarkable perfor- mance in a range of image synthesis tasks, in- cluding style transfer, picture to image trans- lation, and image production.
2) New GAN-based models, including DRB- GAN and MSGAN, improve the artistic style transfer's effectiveness and visual quality.
3) GANs have been used to handle image syn- thesis difficulties, including realistic picture production, super-resolution, and image-to- image translation. They are a general-purpose method for transforming input images to out- put images.
4) Recent research has focused on develop- ing strategies to stabilize GAN training and increase image quality, resulting in break- throughs in image synthesis and style transfer. These studies and contributions demonstrate the adaptability and potential of GANs for picture syn- thesis and style transfer, paving the way for future advances in computer vision.

REFERENCES

[1] L. Wang, W. Chen, W. Yang, F. Bi, and F. R. Yu, "A state-of- the-art review on image synthesis with generative adversarial networks," *IEEE Access*, vol. 8, pp. 63 514–63 537, 2020.

[2] P. Isola, J.-Y. Zhu, T. Zhou, and A. A. Efros, “Image-to- image translation with conditional adversarial networks,” in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2017, pp. 1125–1134.

[3] J.-Y. Zhu, T. Park, P. Isola, and A. A. Efros, “Unpaired image-to-image translation using cycle-consistent adversarial networks,” in *Proceedings of the IEEE international conference on computer vision*, 2017, pp. 2223–2232.

[4] N. U. Din, S. Bae, K. Javed, H. Park, and J. Yi, “Cross modal facial image synthesis using a collaborative bidirectional style transfer network,” *IEEE Access*, vol. 10, pp. 99 077–99 087, 2022.

[5] X. Huang and S. Belongie, “Arbitrary style transfer in real- time with adaptive instance normalization,” in *Proceedings of the IEEE international conference on computer vision*, 2017, pp. 1501–1510.

[6] L. A. Gatys, A. S. Ecker, and M. Bethge, “Image style transfer using convolutional neural networks,” in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2016, pp. 2414–2423.

[7] J. Johnson, A. Alahi, and L. Fei-Fei, “Perceptual losses for real-time style transfer and super-resolution,” in *Computer Vision–ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11-14, 2016, Proceedings, Part II 14*. Springer, 2016, pp. 694–711.

[8] P. Li and M. Yang, “Semantic gan: Application for cross- domain image style transfer,” in *2019 IEEE International Conference on Multimedia and Expo (ICME)*. IEEE, 2019, pp. 910–915.

[9] H. Liu, P. N. Michelini, and D. Zhu, “Artsy-gan: A style transfer system with improved quality, diversity and performance,” in *2018 24th International Conference on Pattern Recognition (ICPR)*. IEEE, 2018, pp. 79–84.

[10] S. Murali, M. R. Rajati, and S. Suryadevara, “Image genera- tion and style transfer using conditional generative adversarial networks,” in *2019 18th IEEE International Conference On Machine Learning And Applications (ICMLA)*. IEEE, 2019, pp. 1415–1419.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

DETECTION OF KNEE OSTEOARTHRITIS STAGES USING CONVOLUTIONAL NEURAL NETWORK

Aditya pal
Usha Pravin Gandhi College of Arts, Science and Commerce

ABSTRACT
Nowadays, many people suffer from the problem of knee osteoarthritis (KOA). As the age is going to increases the chances of suffering from knee osteoarthritis increase simultaneously. Degeneration of the articular cartilage, the flexible, slick substance that typically shields bones from joint friction and impact, is what constitutes knee osteoarthritis. The disorder can also damage neighbouring soft tissues and result in alterations to the bone that lies beneath the cartilage. This study uses deep learning-based feature extraction and classification to demonstrate knee osteoarthritis detection at an early stage. At first, the x-ray images of different stages of knee osteoarthritis have taken for further processing. For classification, a mix of both healthy knee and defected has been taken. After that, the deep convolutional neural network (CNN) model for image classification has been used to detect whether the individual is suffering from knee osteoarthritis or not. The Kellgren–Lawrence (KL) system consists of Grade I, Grade II, Grade III, and Grade IV. This study offers 95% accuracy for identifying knee osteoarthritis. This research helps to detect knee osteoarthritis at early stages and classify knee osteoarthritis using the KL grading system.

Keywords: knee osteoarthritis, Convolutional Neural Networks (CNN), deep learning, Classification, KL grading

1 INTRODUCTION
Osteoarthritis (OA) is the most common chronic condition of the joints, causing pain and stiffness. It is characterized by cartilage degradation and bone changes [1]. The femur and the tibia are the two main bones that make up the knee joint. There is a substantial substance called cartilage in between these bones. The flexible and frictionless movement of the knee is aided by this cartilage. Aging or unintentional loss of cartilage might cause its volume to decrease [5]. Due to the loss of cartilage between the two bones the problem of knee osteoarthritis arises. The entire knee joint can be affected by KOA. There is no known cure for KOA. Since the initial OA alterations may appear in the subchondral bone before osteophytes and narrowing of the joint space, diagnosing OA in its early stages can be difficult. After detecting it is possible to reduce its progression into severe knee problems. At the advanced stage of KOA, the only way to cure is by doing total joint replacement surgery. To detect KOA at an early stage the only way present is to use magnetic resonance imaging (MRI) scanning which is only available at specialized centers which are very expensive [8]

A grading system known as Kellgren-Lawrence (KL) is used to define the various phases of OA. The KL grading system is based on the radiographic classification of Knee osteoarthritis. It has been determined to be the most authoritative categorization system. It is classified into Grade I, Grade II, Grade III, and Grade IV [5]. However, because bony changes only emerge in late OA situations, this technique creates a delay in diagnosis. The other method to detect KOA is by doing an MRI scan which is very costly and rarely used [4]. MRI technique gives proper information about cartilage thickness and roughness. Gait analysis also helps to detect KOA. Knee pain, swelling, surface roughness, morning pain, and more are the early symptoms of KOA. The average age of the patients is over forty-five years, even though KOA is identified in individuals under the age of forty [2]. The hip and knee OA is at the eleventh position in the highest global disability factor, inflicting a significant economic impact on society [8]. Proper exercise, heat and ice treatment, weight loss, and physiotherapy can also treat KOA alongside medication.

Various machine learning and deep learning algorithms have been employed to identify KOA in radiography pictures. Deep learning algorithms provide good results in the medical field [4]. With these techniques, diagnostic accuracy has already reached human standards and may potentially exceed human specialists in the future. In this research paper, a Convolutional neural network is used to detect KOA with KL grading. For this image processing of x-ray images must be performed. Convolutional neural networks (CNN) process pixel data which is used for image recognition or image processing. This study suggests detecting KOA using the KL grading system.

2 LITERATURE REVIEW
Abdelbasset Brahim et.al states the method for early detection of OA. He has used PSD combined with ICA to get relevant results. The proposed diagnosis approach yields classification results with up to 78.92% of accuracy

 ISSN 2394 - 7780

[1].Abdelbasset Brahim et.al provides us with the computer-aided diagnosis approach for the detection of OA using MLR and ICA. Further analysis of the proposed system also showed the difference between the Healthy Knee and an Osteoarthritic knee. He has used MLR and ICA approach and this system gives the result up to 82.98% for accuracy, 87.15% for sensitivity, and up to 80.65% for specificity [2]. Joseph Antony et.al have investigated different new methods for detection of Knee OA severity and they also investigated 3 pre-trained networks and found that the BVLC reference CaffeNet and VGG-M-128 network performs best and gives the best results [3]. Margarita Kotti et. al has proved the suitability of random forests for analyzing ground reaction forces to differentiate between healthy and OA knee the mean accuracy is 72.61% [4]. Rabbia Mahum et.al used CNN to detect KOA. She has also used Histogram of Oriented Gradient (HOG) and Local Binary Patterns (LBP) along with CNN. The multi-class classifiers such as Support Vector Machine (SVM), Random Forest (RF), K nearest neighbors (KNN) is also used by her. She performed Five-Fold validation and Cross-Validation on images and get an accuracy of 98% and 97.14% respectively using the algorithm [5]. Berk Norman et.al used a Densely connected Convolutional neural network (DenseNet) for staging osteoarthritis from plain radiographs. He tested sensitivity rates of no OA, mild, moderate, and severe OA and got 83.7%,70.2%,68.9%and 86.0% respectively and the corresponding specificity rates were 86.1%, 83.8%, 97.1%, and 99.1%. His study also stated that if the volume of radiographic images is increase then the diagnosis of OA will be precise [6]. Kim van Oudenaarde et.al proposed that referring to MR imaging was not cost-effective for patients having traumatic knee symptoms. He also proposed that MR imaging led to an increase in healthcare costs without an improvement in the KOA [7]. Aleksei Tiulpin et.al used plain radiograph to automatically diagnose and grade KOA. He has used the Deep Siamese Convolutional Neural Network to automatically score KOA according to the KL grading system. Instead of having a different testing set, he has achieved multi-class accuracy of 66.71%. He also got a radiographical OA diagnosis area Under the Curve (AUC) of 0.93, quadratic weighted Kappa of 0.83, and Mean Squared Error (MSE) of 0.48[8]. Marieke L. A. Landsmeer et.al explained KOA prediction in overweight women. He used Rotterdam Study (RS). He has included factors such as age, BMI, mild knee symptoms, knee problems climbing stairs, morning stiffness, postmenopausal status, and heavy work. He got an AUC of 0.71. After applying external validation, he got the same AUC [9]. Bochen Guan et.al used a deep learning model having a higher diagnostic performance for predicting pain progression rather than a traditional model which uses clinical and radiographic risk factors. He got an AUC of 0.807 which was higher than both the traditional model which has an AUC of 0.692 and the DL model which has an AUC of 0.770[10].

3 METHODOLOGY

3.1 Algorithm

This paper introduces and assesses a deep learning architecture for knee osteoarthritis detection. We have used Convolution Neural networks and this is the flow chart for CNN

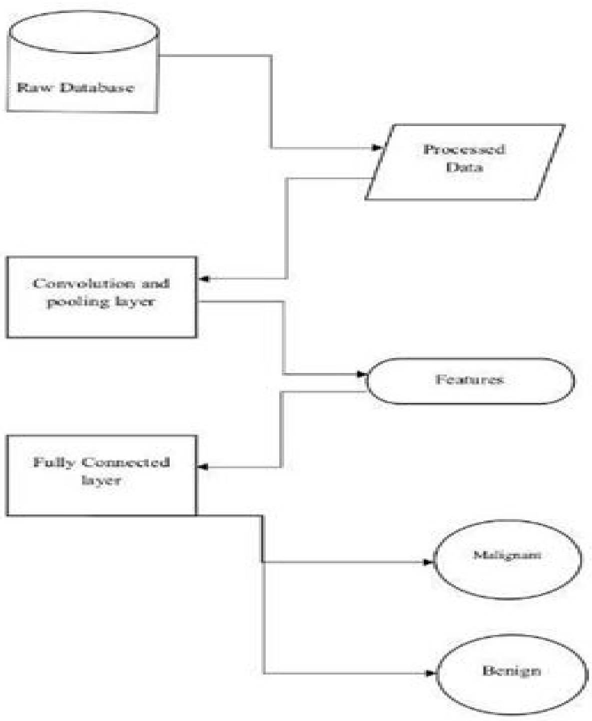


Figure 1: CNN Flow Chart

ISSN 2394 - 7780

3.2 Image Classification

We are using Convolutional Neural Networks the detecting knee osteoarthritis.

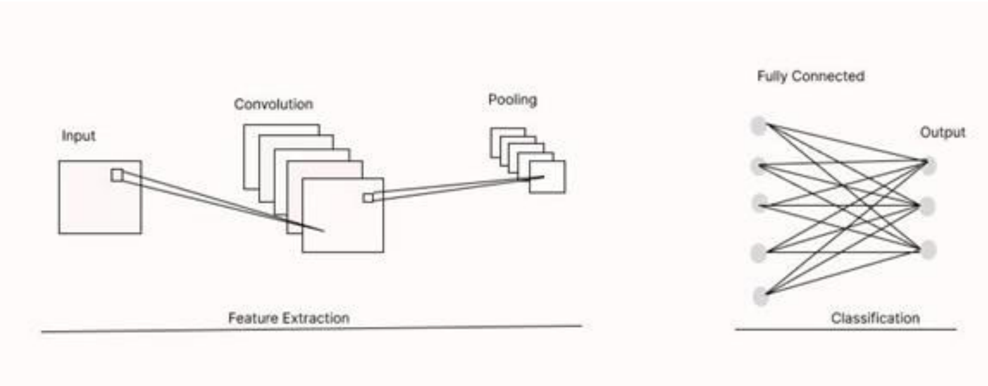


Figure 2: CNN Architecture for Input image

In CNN there are three different types of layers which are convolutional, pooling layers, and fully connected (FC) layers. When these layers are combined, a CNN architecture will be formed. In addition to these three layers, there are two more important parameters the dropout layer and the activation function.

3.3 Dataset

The images of X-rays that are used in this paper are taken from Kaggle having the KL grading system ranging from Grade 0 to Grade 4. The dataset contains a total of 5949 x-ray images, which were later divided into training and testing data for further processing using the CNN model.

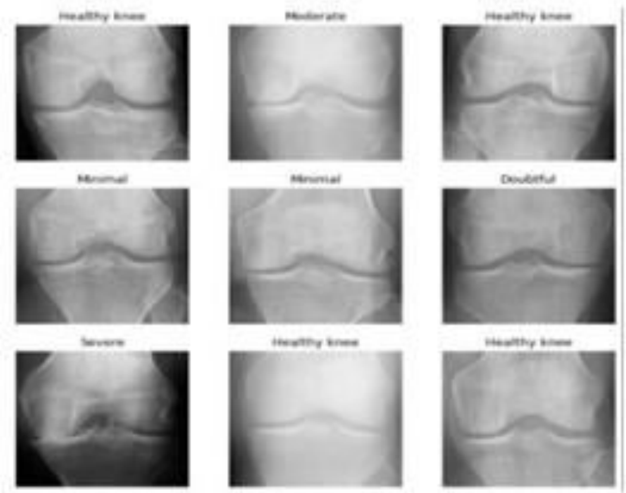


Figure 3: Different images taken from the Dataset: (a) Healthy Images; (b) Doubtful Images; (c) Minimal; (d) Moderate; (e) Severe

4 RESULT

A total of 5949 images of x-ray are taken to implement the concept of CNN in KOA. The x-ray images are further divided for training and testing purposes. Out of the total images, 80% of the images are taken for the training set and 20% for the testing set. Training set include4760 images and the testing set includes 1189 x-ray images. These images consist of five classes. These images were trained using the CNN model with image size 256. We have used the Softmax activation function, Adam optimizer, and categorical cross-entropy loss.100 epochs were performed to get better results for detecting KOA. We got a training accuracy of 95% and a loss of around 14% as shown in figure 4. Figure5 gives the accuracy and loss for testing data. After 100 epochs the accuracy and loss of testing data become constant. The confusion matrix shown in figure 6 gives the classification accuracy of images. It shows the testing accuracy of KOA stages using the CNN model.

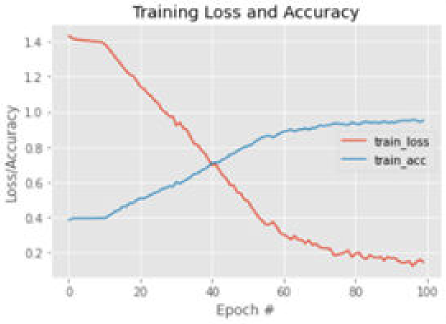


Figure 4: Training accuracy and loss

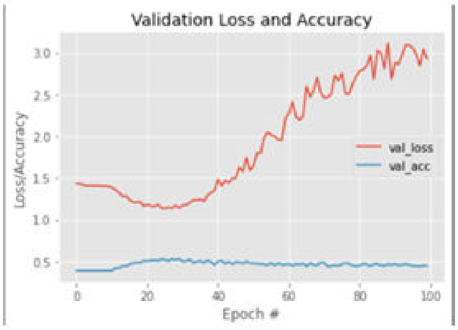


Figure 5: Testing accuracy and loss

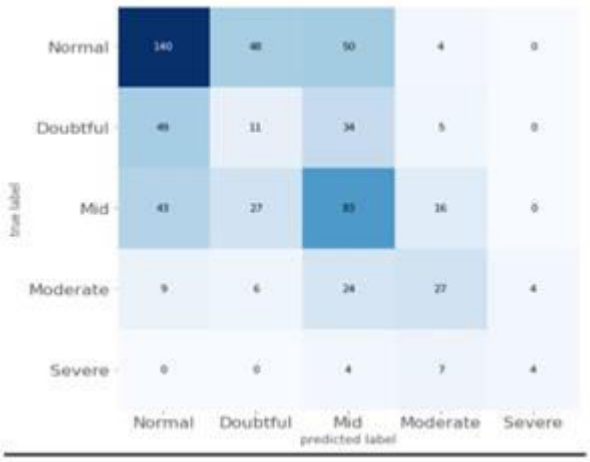


Figure 6: Confusion matrix of testing data

5 CONCLUSION

This study developed a classification for identifying the stages of KOA. The model takes x-ray images of different stages of KOA to classify it. The CNN model used in this work includes three hidden layers, three fully connected layers, and softmax activation. The hidden layer utilizes a 3x3 filter size. The number of output channels for each convolutional layer is taken as 128,64 and32. respectively. The algorithm gives an accuracy of 95% and a loss of 14%. The method looks promising to detect KOA stages making it easy for an individual to detect it at early stages.

6 REFERENCES

- Brahim A, Riad R, Jennane R. Knee osteoarthritis detection using power spectral density: Data from the osteoarthritis initiative. In International Conference on Computer Analysis of Images and Patterns 2019 Sep 3 (pp. 480-487). Springer, Cham
- Brahim A, Jennane R, Riad R, Janvier T, Khedher L, Toumi H, Lespessailles E. A decision support tool for early detection of knee OsteoArthritis using X-ray imaging and machine learning: Data from the Osteoarthritis Initiative. Computerized Medical Imaging and Graphics. 2019 Apr 1;73:11-8.
- Antony J, McGuinness K, O'Connor NE, Moran K. Quantifying radiographic knee osteoarthritis severity using deep convolutional neural networks. In2016 23rd International Conference on Pattern Recognition (ICPR) 2016 Dec 4 (pp. 1195-1200). IEEE.
- Kotti M, Duffell LD, Faisal AA, McGregor AH. Detecting knee osteoarthritis and its discriminating parameters using random forests. Medical engineering & physics. 2017 May 1;43:19-29.
- Mahum R, Rehman SU, Meraj T, Rauf HT, Irtaza A, El-Sherbeeny AM, El-Meligy MA. A novel hybrid approach based on deep CNN features to detect knee osteoarthritis. Sensors. 2021 Sep 15;21(18):6189.
- Norman B, Pedoia V, Noworolski A, Link TM, Majumdar S. Applying densely connected convolutional neural networks for staging osteoarthritis severity from plain radiographs. Journal of digital imaging. 2019 Jun;32(3):471-7..

- van Oudenaarde K, Swart NM, Bloem JL, Bierma-Zeinstra SM, Algra PR, Bindels PJ, Koes BW, Nelissen RG, Verhaar JA, Luijsterburg PA, Reijnierse M. General practitioners referring adults to MR imaging for knee pain: a randomized controlled trial to assess cost-effectiveness. Radiology. 2018 Jul;288(1):170-6.
- Tiulpin A, Thevenot J, Rahtu E, Lehenkari P, Saarakkala S. Automatic knee osteoarthritis diagnosis from plain radiographs: a deep learning-based approach. Scientific reports. 2018 Jan 29;8(1):1-0.
- Landsmeer ML, Runhaar J, van Middelkoop M, Oei EH, Schiphof D, Bindels PJ, Bierma-Zeinstra SM. Predicting knee pain and knee osteoarthritis among overweight women. The Journal of the American Board of Family Medicine. 2019 Jul 1;32(4):575-84.

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024

ISSN 2394 - 7780

ANT SPECIES RECOGNITION USING CONVOLUTIONAL NEURAL NETWORK

Swapnali Lotlikar, Prashant Chaudhary and Zaid Mansoori
Usha Pravin Gandhi College of arts Science and Commerce Mumbai, Maharashtra, India

ABSTRACT

Observation of biodiversity can take a lot of time; alternative approaches frequently produce indirect data and may be biased. Ants can be identified on the basis the key features like size, colour, other body characteristics, habits, or other information. Ecologists are beginning to depend more and more on photos as a source of information and on image data analysis to address these issues. Images may be a valuable tool in this regard. But the majority of what the current approaches do is picture categorization. In this study, we provide an effective approach for accessing more in-depth information about an image's content that is based on object detection. We developed a pipeline using high resolution pictures to slice the source images, carry out detections, and then fine-tune these findings. We illustrate the interest of this pipeline by using it on-field images taken into study ant species and the different characteristics of various species of ants. This paper documents the extensive dataset of ant species gathered from different sources for training, testing and validation procedure of the detector. The result of the process using convolutional neural network will easily identify the ant's species with significant accuracy.

Keywords: Ant species, Convolution Neural Network, Insect detection, Classification, Image processing.

I. INTRODUCTION

Considering knowledge of species names and ranges is crucial for scientific research and environmental monitoring programs, classifying species is a key component of biodiversity management [2]. The growth of works based on categorization knowledge is, however, currently hampered by several challenges in biodiversity research [2, 3]. There are many specimens that need to be identified, and there aren't enough individuals accessible to do it [3], which is one of these challenges. Deep learning approaches have been proposed as a solution to address these problems. Even while expert identification should be the preferable method of identifying specimens, computational intelligence systems may offer trustworthy alternatives to identification tools. Convolutional Neural Networks (CNNs), a machine learning technology widely used for image identification, are a viable method for tackling this challenge. We proposed a CNN automated ant species identification technique that uses the head, profile, and dorsum views of ant photos as input in order to efficiently identify many specimens. The dataset is moderate in size; though CNNs can detect discriminant attributes automatically, which is necessary for a high-performance ant genus identification in this case, they require a large dataset and over-fitting can be a problem. The three picture viewpoints (head, dorsum, and profile) were combined into ensembles to address the dataset's features, and several training methods were investigated.

II. MATERIALS AND METHODS

A. *Insect Dataset for Classification*

Aiming at the practical application of the ant species identification task, we introduce a large-scale dataset, which consists of species of ants. The dataset consists of three species of ants for identification purpose, head, profile, and dorsal views of ant images are the criteria for identifying ant species. In this research, we have considered three species of ants namely Little Black ant, Fire ant, Argentine ant, which are briefly explained below.

- Little black ants are among the most prevalent domestic intruders encountered in kitchens. Little black ants are omnivorous and will consume nearly everything they can find, which often includes sweets, fruits, vegetables, plant fluids, oil, and other insects. They are just as little as their name implies, measuring only 1.5 mm (.06 inches) in length, with a two-segmented waist and a black colour. Little black ants are endemic to the United States, and, like other ant species, they are social insects that dwell in colonies. Little black ants normally swarm from June to August. During this time, reproductive ants will couple off in mating flights, travel in different directions, and establish colonies of their own. The little black ants are not hazardous. Despite having stingers and biting mandibles, they are too little to have any discernible impact on people. Due of their propensity to break into houses and eat food, they are still seen as a nuisance.
- Fire Ants, the South American red imported fire ant was brought to Alabama. Because of the substantial dirt mounds connected to its nests and the unpleasant sting it administers, it is regarded as a pest. The invasive tawny crazy ant (also known as hairy crazy ant), a species found in South America that was first discovered

ISSN 2394 - 7780

in the United States (in Texas) in 2002, has replaced the red imported fire ant in some places. The hairy crazy ant is notoriously difficult to eradicate and is seen as a danger to local wildlife and ecosystems. The body and head of the Fire Ant are both reddish-brown in colour. The typical worker ant is 2–6 mm long and has sturdy mandibles with four to five distinct teeth. Its body is coated in a great deal of erect hairs, and it has a distinctive 2-part pedicel. The anatomy of fire ants is comparable to that of most ant species. Like other insects, fire ants have six legs, are red and black in appearance, and are covered in a strong exoskeleton for protection. An armoured thorax midsection, an abdomen made up of the pedicle and the gaster, and spherical heads with mandibles are all features of worker ants. Usually, the head is copper brown in hue. Workers of fire ant species have mandibles as well as an abdominal stinger.

- Argentine ant, which is endemic to Northern Argentina, is a pest that infests agricultural, urban, and natural areas all over the world. The Argentine ant may grow exceptionally large colonies because of extraordinarily low levels of intraspecific conflict. Its reputation as a troublesome insect in houses and its quick proliferation are both a result of this. Along with disrupting local ants, pollinators, and even vertebrates, this intruder also encourages plant-eating pest insects. The Argentine ant's body colour ranges from pale to dark brown. The queens of these ants are between 1/6 and 1/4 inches long, whereas the workers are around 1/8 inch long (monomorphic). Their bodies are proportionate to their legs. There are 12 segments on the antennas, however there is no clear club. The hue ranges from light brown to dark brown. Workers have a body length of 1/8 inch, whereas queens are between 1/6 and 1/4 inches long. Antennae feature 12 segments without a distinct club, and legs are proportionate to the body.

B. Image pre-processing

During image pre-processing, image enhancement techniques are used to sharpen and eliminate noise in the pictures for increased accuracy. It enhances picture quality for more accurate species identification and categorization. The datasets utilised in this analysis have previously undergone pre-processing and segmentation.

C. Image augmentation

Species identification involves various steps to be performed. The flow of steps for species classification is illustrated in Fig. 2. To increase the size of the training dataset, image augmentation is used on images from the insect dataset. Then, to categorise the ant species, shape characteristics taken from the insect images and a machine learning method termed convolutional neural network are applied. Ant species classification system based on convolutional neural network that has been adapted for maximum performance and accuracy. The flow of steps for insect classification is illustrated in Fig. 1.

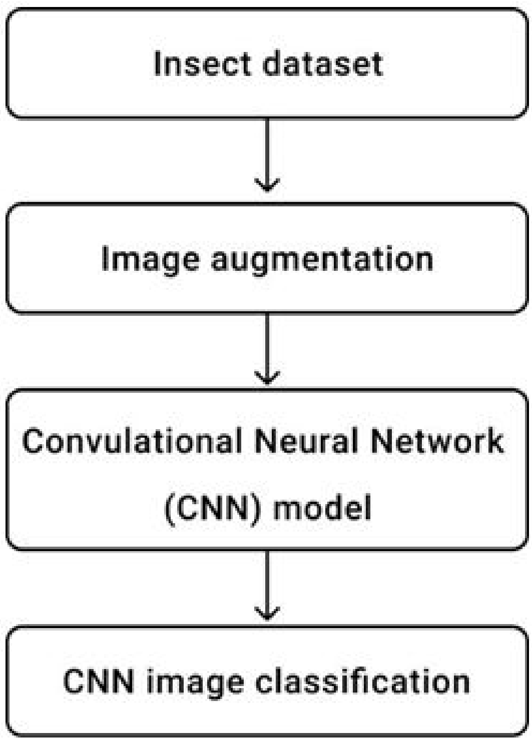


Fig. 1: Framework of ant species classification

III. LITERATURE REVIEW

Alan Caio R. Marques et.al in their paper of Ant genera identification using an ensemble of convolutional neural networks proposed a ensemble of neural networks in which the classifiers success in achieving an accuracy rate of over 80% on top-1 classification and an accuracy of over 90% on top-3 classification when integrated in an ensemble, helped to reduce the total classification error [4]. While, Paul Tresson et.al in their paper of Insect interaction analysis based on object detection and CNN suggested a approach on image classification to obtain more in-depth information about an image's content. The findings showed 87.8% accuracy and enabled the successful recognition and identification of 23 species and ant castes. In our paper we have proposed a model based on convolutional neural network, to train on a dataset consisting various species of ants and classify the species with an accuracy 93%, which is comparatively higher the previously proposed methods.

IV. CONVOLUTIONAL NEURAL NETWORK

A feed-forward neural network called a Convolutional Neural Network analyses visual pictures by processing data in a grid-like architecture. It is sometimes referred to as a ConvNet. To find and categorise items in a picture, a convolutional neural network is employed. The process of removing useful elements from an image begins with this. Multiple filters work together to execute the convolution action in a convolution layer. Each image may be thought of as a matrix of pixel values. A filter matrix with a 3x3 dimension is also included. To obtain the convolved feature matrix, move the filter matrix across the picture and compute the dot product. The rectified linear unit is referred to as ReLU. The next step is to transfer the feature maps to a ReLU layer after they have been retrieved. ReLU does an operation element-by-element, setting all the negative pixels to 0. The result is a corrected feature map, and it gives the network non-linearity. The down sampling process of pooling lowers the feature map's dimensionality. To create a pooled feature map, the corrected feature map is now passed through a layer of pooling. predict the classes with greater accuracy. At this step, the error is calculated and then backpropagated. The weights and feature detectors are adjusted to help optimize the performance of the model. Then the process happens again and again and again, in this way the network trains on the data. To distinguish distinct portions of the picture, such as edges, corners, bodies, feathers, eyes, and beak, the pooling layer employs a variety of filters. Flattening is the procedure's following phase. The generated 2-Dimensional arrays from pooled feature maps are all flattened into a single, lengthy continuous linear vector. To categorise the picture, the flattened matrix is provided as input to the fully linked layer

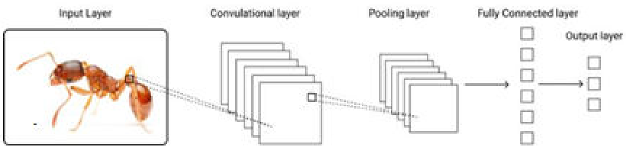


Fig. 2: Illustration of the proposed Convolutional Neural Network (CNN)

V. METHODOLOGY

Numerous photos in the dataset used for this study include properties that may be utilised to classify ant species. The distribution of training and validation data was 70% and 30%, respectively, with a total of 1000 photographs utilised for training and 300 images used for validation. In CNN, there are input and hidden layers as well as an output layer. The most frequent hidden layer types are convolutional, ReLU, pooling, and fully connected layers. RGB pictures of images are used as the model's initial input for images, and these colours combine to produce a three-dimensional matrix, which can be seen in Figure 3.

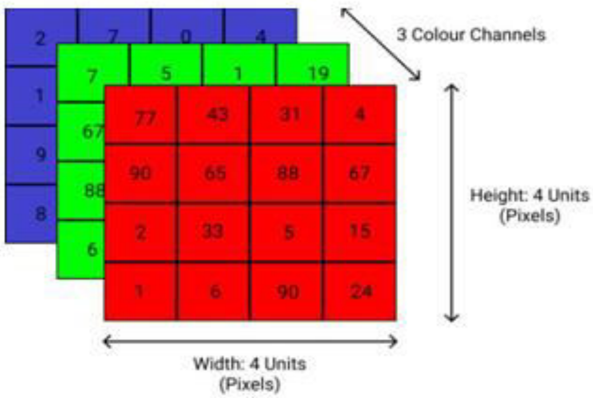


Fig. 3.1: Image as a pixel matrix

International Journal of Advance and Innovative Research
Volume 11, Issue 1 (XIV): January - March 2024
ISSN 2394 - 7780

The pictures are then resized for binary classification. They are scaled down to 200x200x3 pixels since the neural network cannot be given multiple-sized matrix pictures. Convolutional layers are then applied to the images with maximum pooling. To extract as many pixels as feasible, a 200x200x3 image with 16, 3x3 ReLu-activated filters and a 2x2 max pooling layer is applied at the first convolutional layer. Applying additional convolutional layers with 32 and 64 filters of size 3x3 with ReLu activation function over the image of size 200x200x3 and a max pooling layer of size 2x2 which increases the number of channels in the network, whichimproves model accuracy.

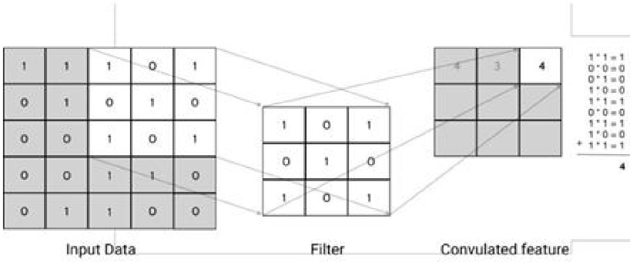


Fig. 3.2: Illustration of the convolution process

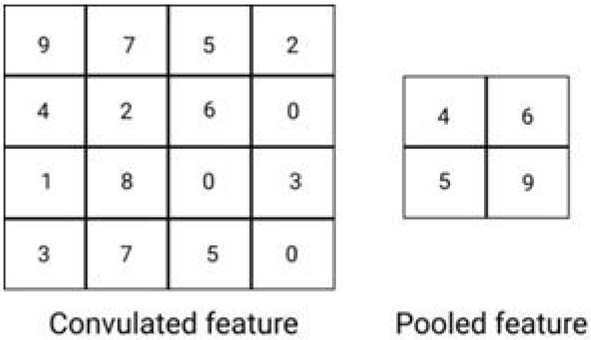


Fig. 3.3: Pooling process

Data is reduced using mean or max pooling in the pooling layer. The pooling process illustration is shown in Figure 3.3

The two-dimensional arrays of the pooled feature maps are then flattened, which yields a single, extensive continuous linear vector. Images are categorised using the output of convolutional layers after the application of two dense layers with SoftMax activation functions.

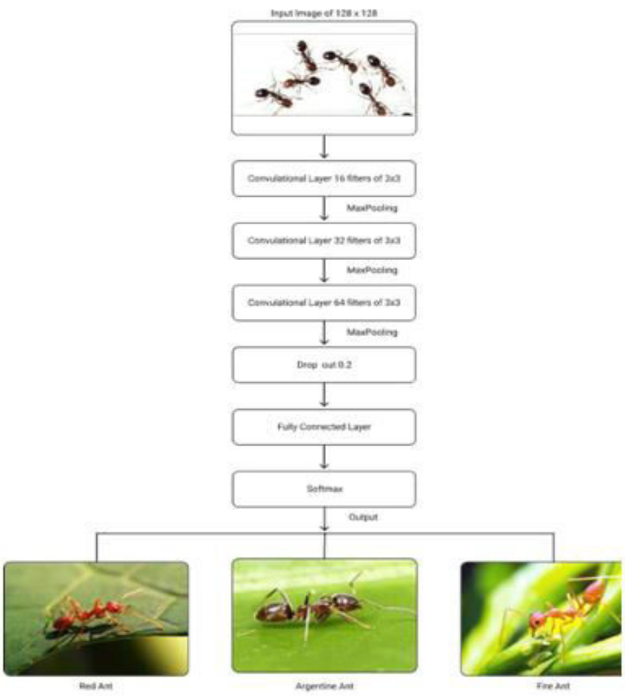


Fig. 3.4. Illustration of the proposed model

 ISSN 2394 - 7780

VI. RESULTS

Classification performed using shape features obtained from image processing technique with machine learning algorithms. For the categorization of ant species, CNN is utilised. To enhance the model for classifying ant species, the algorithm is applied to a collection of 1000 images of insects, some of which are modified test and train images. The CNN model was used to train this set of images, and a number of optimizer strategies were used, such as loss category cross-entropy, RMS, and an optimizer. The output layer uses SoftMax as the activation function, which is applied to the input and hidden layers. The CNN model was trained with a batch size of 4, 30 epochs, and a learning rate of 0.001. Table 1 compares the accuracy and loss performance of the proposed model for each optimizer used. RMS optimizer offers the most accurate and loss-effective performance. The supervised learning model is superior to the traditional, untrainable techniques.

Table 1 and Figure 4. shows the result from epochs.

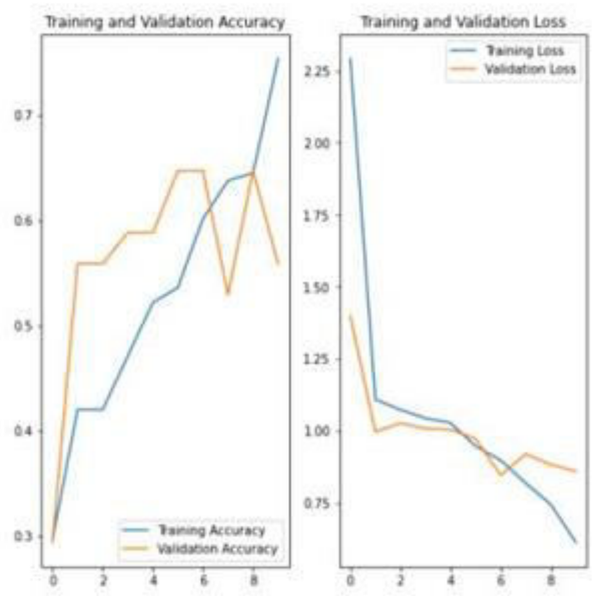


Fig. 4: Graph illustrating accuracy using RMS optimizer

The accuracy and loss graph shows a lot of spikes, which suggests as much. While the accuracy of the system model that applies Adam optimization. Training and validation data are less, and the system false also starts to decline at each iteration. The proposed CNN model can classify different ant species with good performance and gives low error.

Table I: Results Depicting Accuracy Gained By Cnn

Epochs	Accuracy	Validation Accuracy
Epoch 1/10	0.5556	0.4
Epoch 2/10	0.4286	0.538
Epoch 3/10	0.7778	0.461
Epoch 4/10	0.5714	0.538
Epoch 5/10	0.4444	0.538
Epoch 6/10	0.5714	0.769
Epoch 7/10	0.8571	0.9231
Epoch 8/10	0.7143	0.5385
Epoch 9/10	0.8571	0.7691
Epoch 10/10	0.8571	0.7800
Epoch 11/10	0.8725	0.6441
Epoch 12/10	0.8765	0.7651
Epoch 13/10	0.8974	0.6524
Epoch 14/10	0.9278	0.6441
Epoch 15/10	0.9351	0.6441

VII. CONCLUSIONS

In this research paper, numerous research papers on ant species classification and other topics have been examined, and these papers have then been compared. In this study, we use a convolutional neural network to

ISSN 2394 - 7780

study how to classify ant species. In comparison to other machine learning techniques, the Convolution Neural Network method with data augmentation has been shown to be more effective for image processing. The suggested model has ache approaching ever greater validation accuracy than any other current model. In order to classify species, we considered numerous ant species. The purpose of this project is to construct ant species classification system based on convolution neural network (CNN) with data augmentation.

REFERENCES

[1] Paul Tresson, Philippe Tixier, William Puech, Dominique Carval. Insect interaction analysis based on object detection and CNN. MMSP 2019 - IEEE 21st International Workshop on Multimedia Signal Processing, Sep 2019, Kuala Lumpur, Malaysia. 10.1109/MMSP.2019.8901798 . hal-02361210

[2] Wilson EO. Taxonomy as a fundamental discipline. Philosophical Transactions of the Royal Society B:Biological Sciences. 2004; 359(1444):739.

[3] Gaston KJ, O'Neill MA. Automated species identification: why not? Philosophical transactions of the Royal Society of London Series B, Biological sciences. 2004; 359(1444):655–667.

[4] Marques ACR, M. Raimundo M, B. Cavalheiro EM, F. P. Salles L, Lyra C, J. Von Zuben Gaston KJ, O'Neill MA. Automating the identification of insects: a new solution to an old problem. Bulletin of Entomological Research. 1997; 87(02):203–211.

[5] Dyrmann M, Karstoft H, Midtiby HS. Plant species classification using deep convolutional neural network. Biosystems Engineering. 2016; 151(2005):72–80.

[6] Chen G, Han TX, He Z, Kays R, Forrester T. Deep convolutional neural network based species recognition for wild animal monitoring. In: 2014 IEEE International Conference on Image Processing (ICIP); 2014. p. 858862.

[7] Zhu LQ, Ma MY, Zhang Z, Zhang PY, Wu W, Wang DD, et al. Hybrid deep learning for automated lepidopteran insect image classification. Oriental Insects. 2016; 5316(November):1–13.

[8] F (2018) Ant genera identification using an ensemble of convolutional neural networks. PLoS ONE 13(1): e0192011.

[9] Drew LW. Are We Losing the Science of Taxonomy? BioScience. 2011; 61(12):942–946.

[10] Hopkins GW, Freckleton RP. Declines in the numbers of amateur and professional taxonomists: implications for conservation. Animal Conservation. 2002; 5:245– 249.

[11] Weeks PJD, Gauld ID,

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.

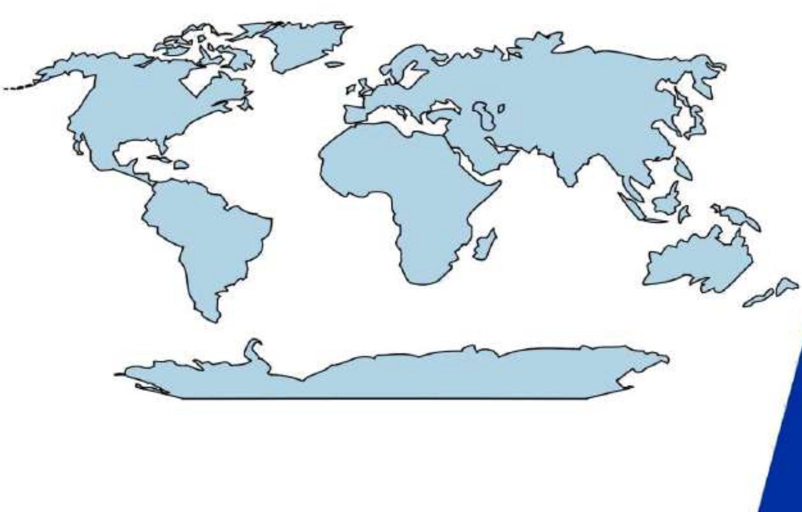
8. Decision of the Editorial Board regarding selection/rejection of the articles will be final.

www.iaraedu.com

Journal

ISSN 2322 - 0899

INTERNATIONAL JOURNAL OF RESEARCH IN MANAGEMENT & SOCIAL SCIENCE



Volume 8, Issue 2
April - June 2020

www.iaraedu.com

Journal

ISSN 2394 - 9554

International Journal of Research in Science and Technology

Volume 6, Issue 2: April - June 2019

Indian Academicians and Researchers Association

www.iaraedu.com

INDIAN ACADEMICIANS AND RESEARCHERS ASSOCIATION

Membership No: M / M – 1365

Certificate of Membership

This is to certify that

XXXXXXXXXXX

is admitted as a

Life Member

of

Indian Academicians and Researchers Association

in recognition of commitment to Educational Research

and the objectives of the Association

INDIAN ACADEMICIANS AND RESEARCHERS ASSOCIATION ★

Date: 27.01.2020

Director

President

INDIAN ACADEMICIANS AND RESEARCHERS ASSOCIATION

Membership No: M / M – 1365

Certificate of Membership

This is to certify that

XXXXXXXX

is admitted as a

Member

of

Indian Academicians and Researchers Association

in recognition of commitment to Educational Research

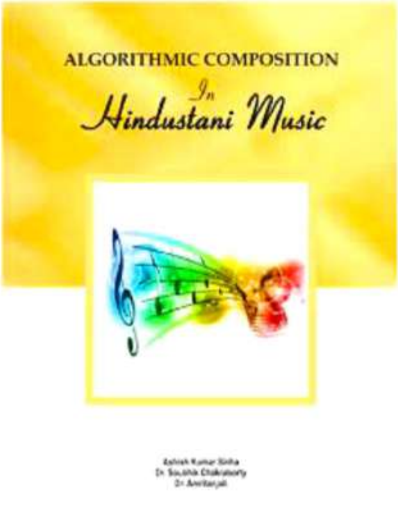
and the objectives of the Association

Date: 27.01.2020

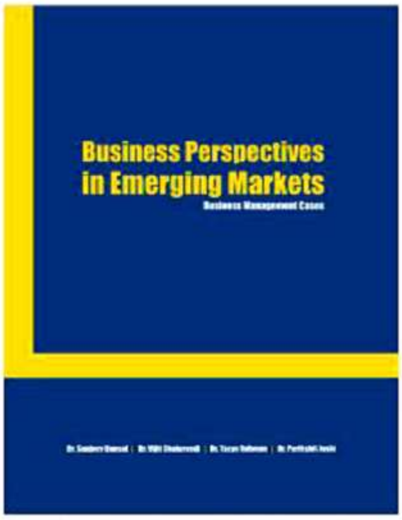
Director

President

IARA Organized its 1st International Dissertation & Doctoral Thesis Award in September'2019

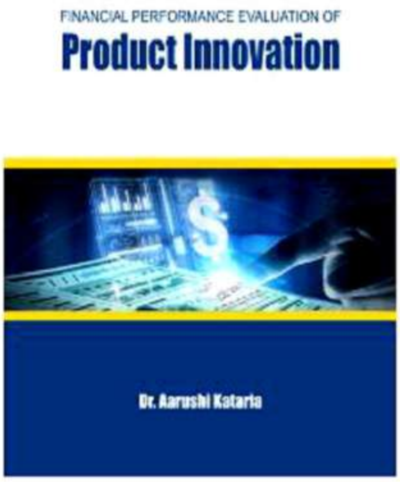


Ashish Kumar Sinha, Dr. Soubhik Chakraborty
Dr. Amritanjali
ISBN : 978-81-930928-8-0

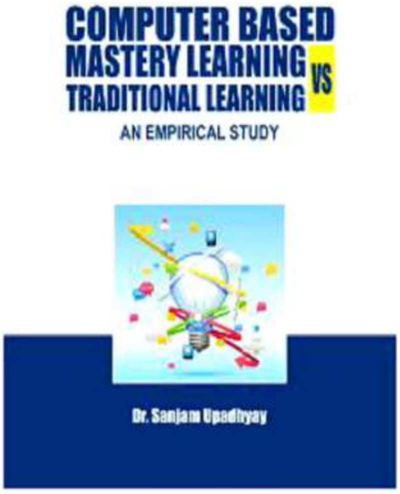


Dr Sanjeev Bansal, Dr. Vijit Chaturvedi
Dr. Tazyn Rahman, Dr. Parikshit Joshi
ISBN : 978-81-936264-0-5

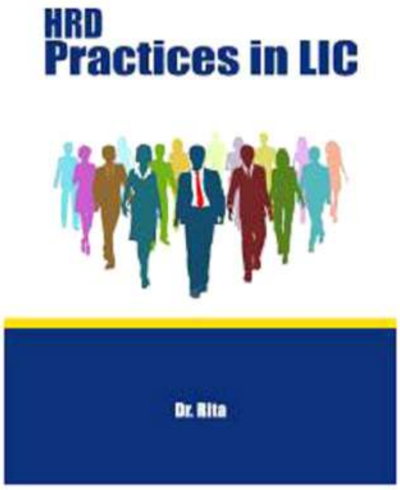
Dr. Jyotsna Golhar
Dr. Sujit Metre
ISBN : 978-81-936264-6-7



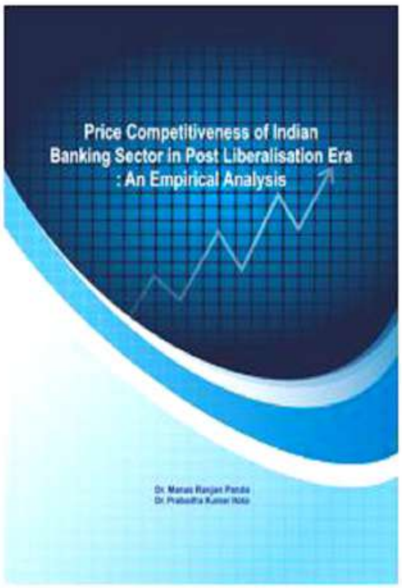
Dr. Aarushi Kataria
ISBN : 978-81-936264-3-6



Dr. Sanjam Upadhyay
ISBN : 978-81-936264-5-0



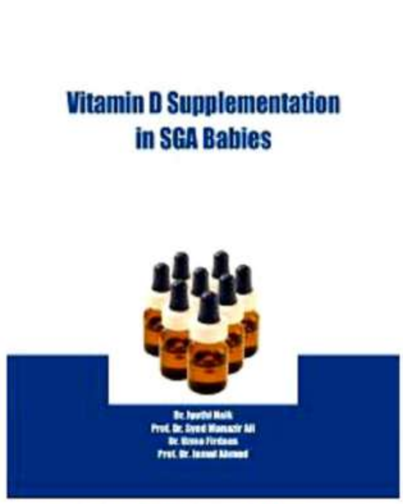
Dr. Rita
ISBN : 978-81-930928-7-3



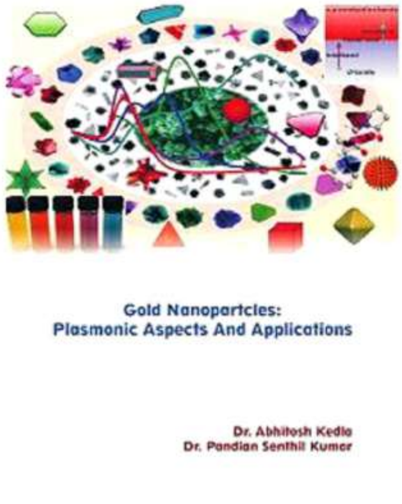
Dr. Manas Ranjan Panda, Dr. Prabodha Kr. Hota
ISBN : 978-81-930928-4-2

Poornima University
ISBN : 978-8193-6264-74

Institute of Public Enterprise
ISBN : 978-8193-6264-4-3



Dr. Jyothi Naik, Prof. Dr. Syed Manazir Ali
Dr. Uzma Firdaus, Prof. Dr. Jamal Ahmed
ISBN : 978-81-936264-9-8



Dr. Abhitosh Kedia
Dr. Pandian Senthil Kumar
ISBN : 978-81-939070-0-9

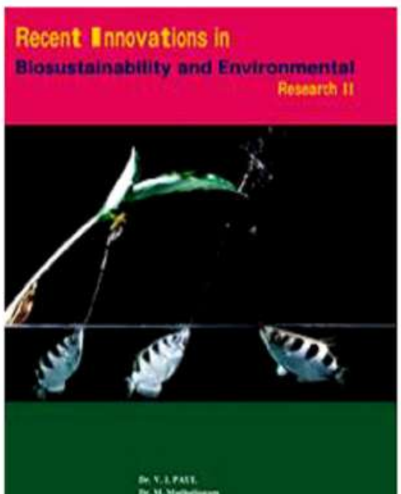
Dr. Vinod
S. Chandwani
ISBN : 978-81-939070-2-3

Prof. Dr. Dhananjay
Awasarikar
ISBN : 978-81-939070-1-6

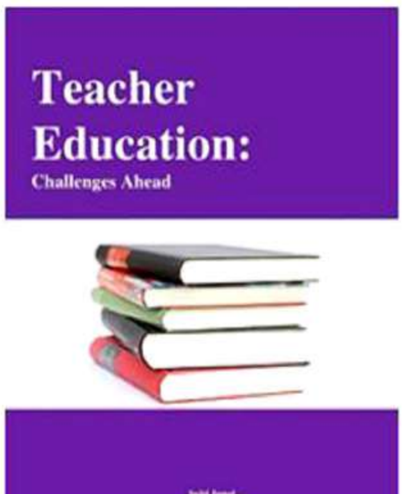
Dr. C. Samudhra Rajakumar, Dr. M. Ramesh
Dr. C. Kathiravan, Dr. Rincy V. Mathew
ISBN : 978-81-939070-4-7

Dr. C. Samudhra Rajakumar, Dr. M. Ramesh
Dr. C. Kathiravan, Dr. Rincy V. Mathew
ISBN : 978-81-939070-6-1

Dr. C. Samudhra Rajakumar, Dr. M. Ramesh
Dr. C. Kathiravan, Dr. Rincy V. Mathew
ISBN : 978-81-939070-7-8



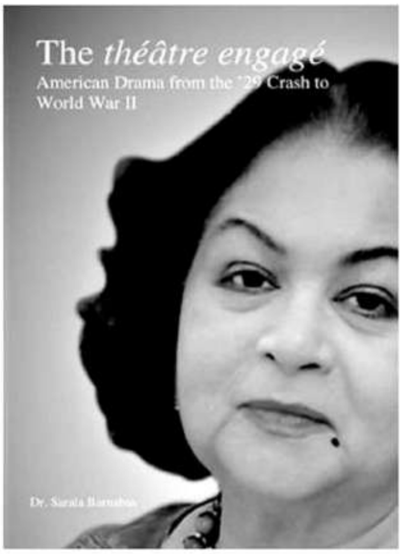
Dr. V. I. Paul, Dr. M. Muthulingam
Dr. A. Elangovan, Dr. J. Nelson Samuel Jebastin
ISBN : 978-81-939070-9-2



Sajid Jamal
Mohd Shakir
ISBN : 978-81-939070-8-5

Dr. R. Emmaniel

ISBN : 978-81-939070-3-0

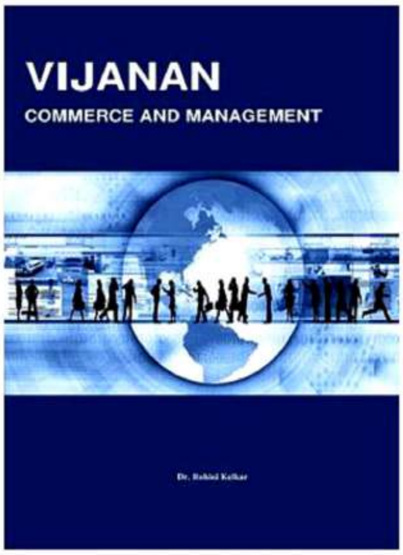


Dr. Sarala Barnabas

ISBN : 978-81-941253-3-4

Dr. M. Banumathi
Dr. C. Samudhra Rajakumar

ISBN : 978-81-939070-5-4

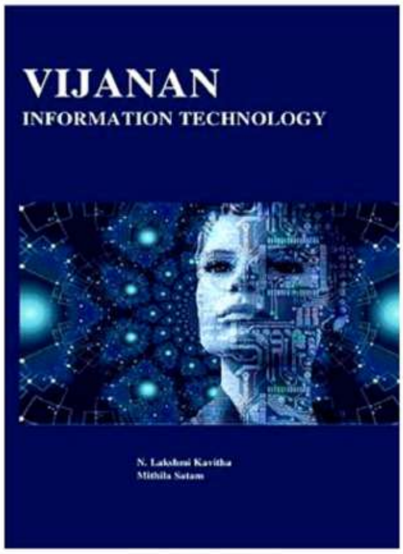


Dr. (Mrs.) Rohini Kelkar

ISBN : 978-81-941253-0-3

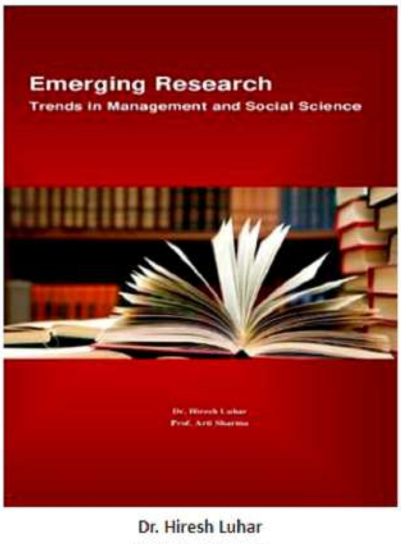
Dr. Tazyn Rahman

ISBN : 978-81-941253-2-7



Dr. N. Lakshmi Kavitha
Mithila Satam

ISBN : 978-81-941253-1-0



Dr. Hiresh Luhar
Prof. Arti Sharma

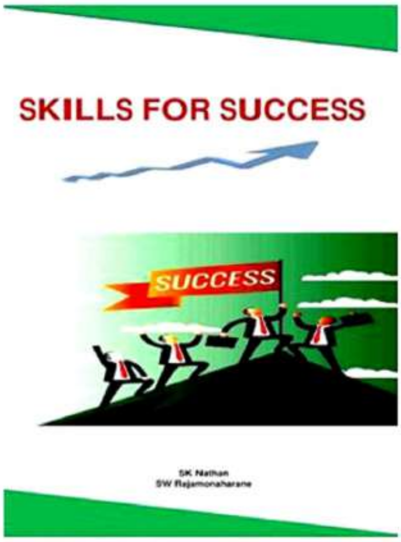
ISBN : 978-81-941253-4-1

Dr. Hiresh S. Luhar
Dr. Ashok S. Luhar

ISBN : 978-81-941253-5-8

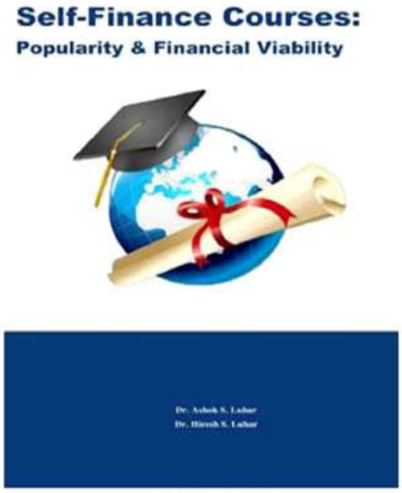
Dr. Babita Kanojia
Dr. Arvind S. Luhar

ISBN : 978-81-941253-7-2

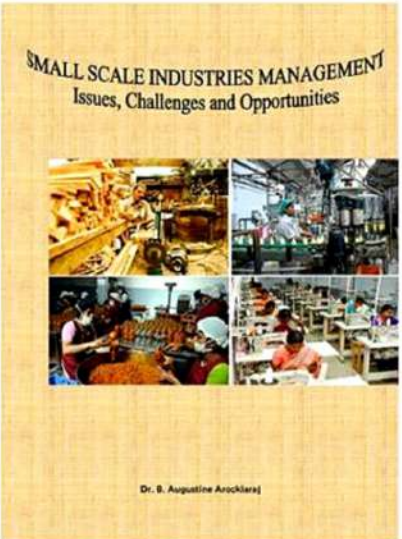


Dr. Sw Rajamonaharane
SK Nathan
ISBN : 978-81-942475-0-0

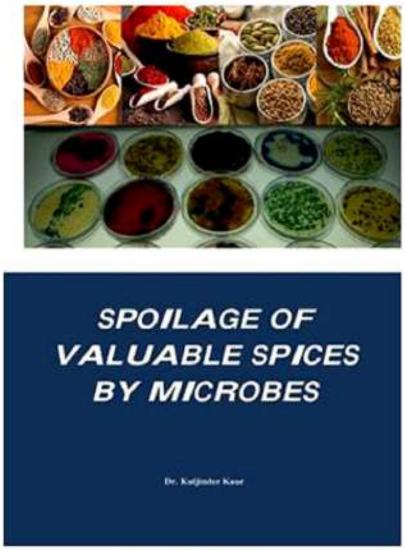
Aditi Sharma
ISBN : 978-81-941253-8-9



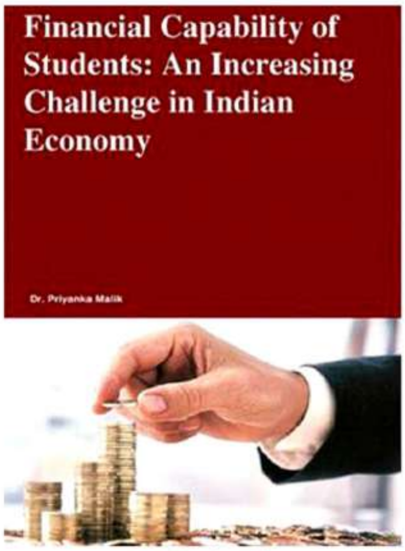
Dr. Ashok S. Luhar
Dr. Hiresh S. Luhar
ISBN : 978-81-941253-6-5



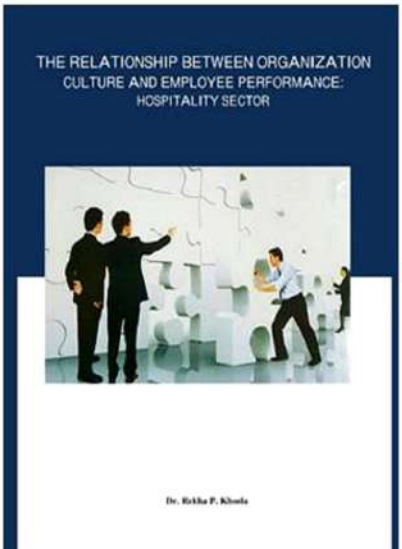
Dr. B. Augustine Arockiaraj
ISBN : 978-81-941253-9-6



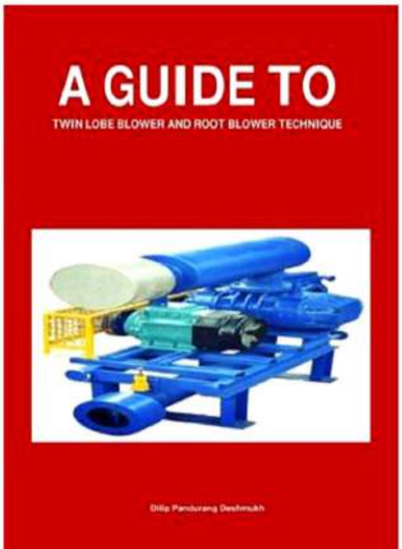
Dr. Kuljinder Kaur
ISBN : 978-81-942475-4-8



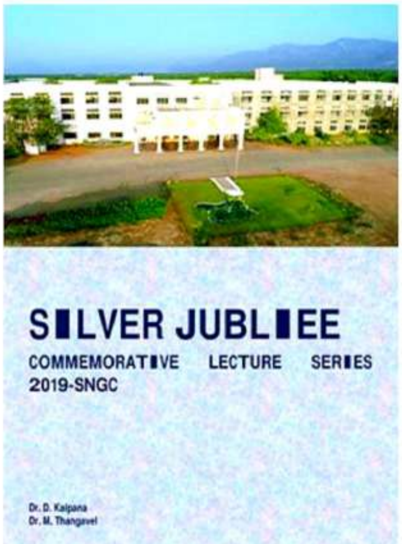
Dr. Priyanka Malik
ISBN : 978-81-942475-1-7



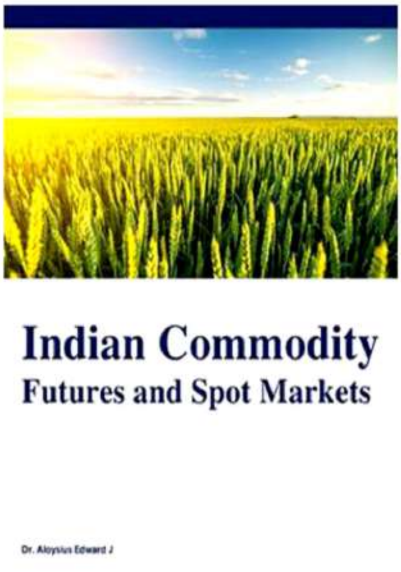
Dr. Rekha P. Khosla
ISBN : 978-81-942475-2-4



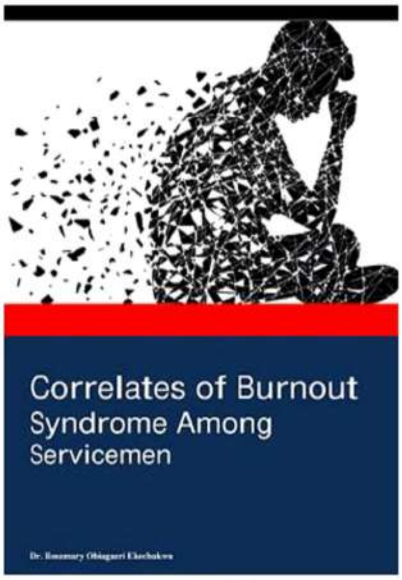
Dilip Pandurang Deshmukh
ISBN : 978-81-942475-3-1



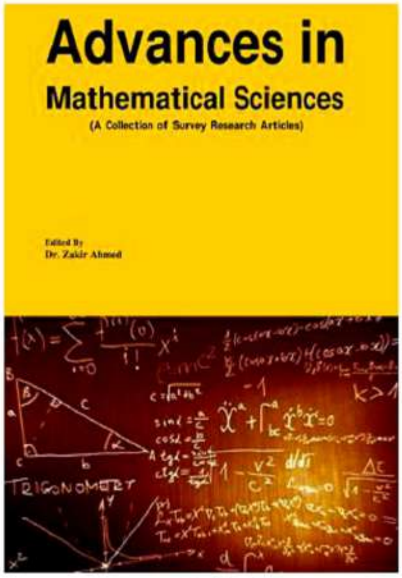
Dr. D. Kalpana, Dr. M. Thangavel
ISBN : 978-81-942475-5-5



Dr. Aloysius Edward J.
ISBN : 978-81-942475-7-9

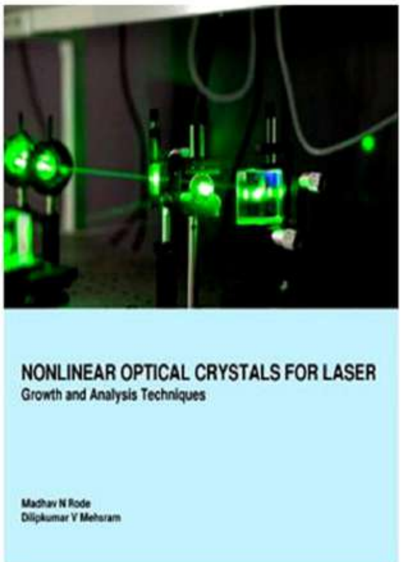


Dr. R. O. Ekechukwu
ISBN : 978-81-942475-8-6

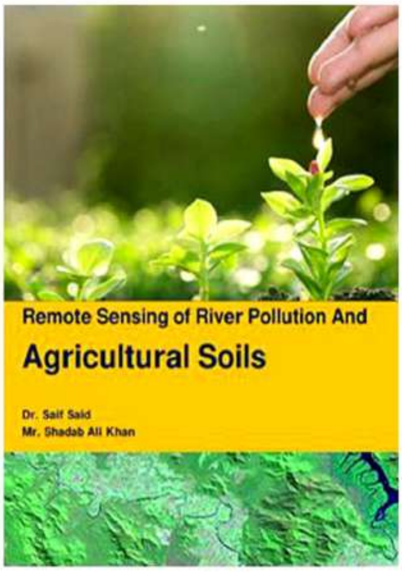


Dr. Zakir Ahmed
ISBN : 978-81-942475-9-3

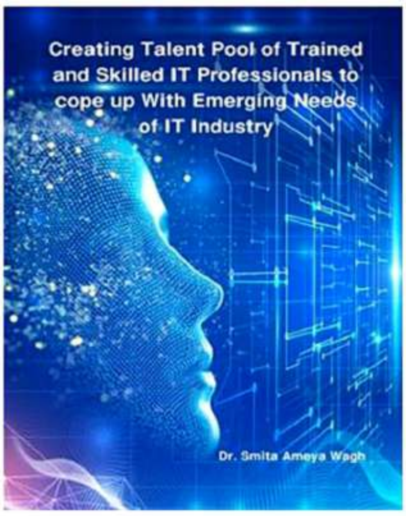
Dr. (CA) Ajit S. Joshi
Dr. Arvind S. Luhar
ISBN : 978-81-942475-6-2



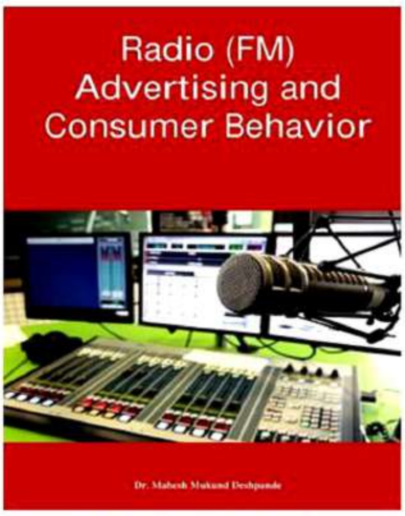
Madhav N Rode
Dilip Kumar V Mehsram
ISBN : 978-81-943209-6-8



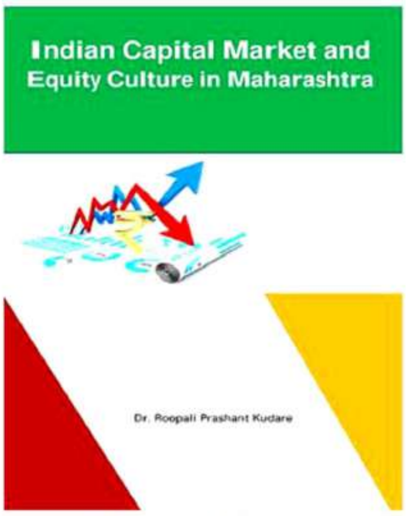
Dr. Saif Said
Shadab Ali Khan
ISBN : 978-81-943209-1-3



Dr. Smita Ameya Wagh
ISBN : 978-81-943209-9-9

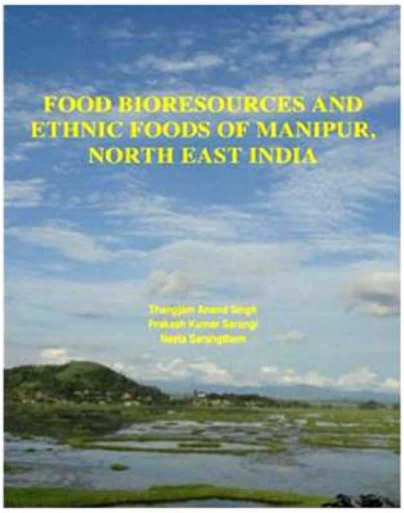


Dr. Mahesh Mukund Deshpande
ISBN : 978-81-943209-7-5

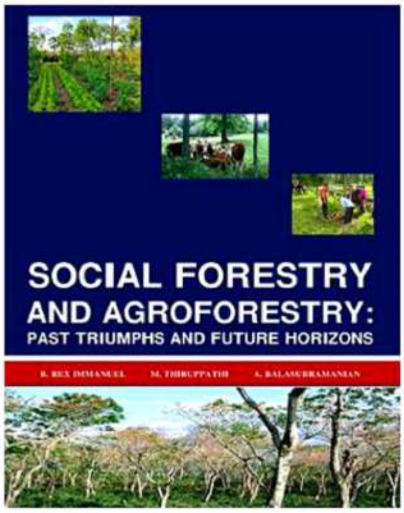


Dr. Roopali Prashant Kudare
ISBN : 978-81-943209-3-7

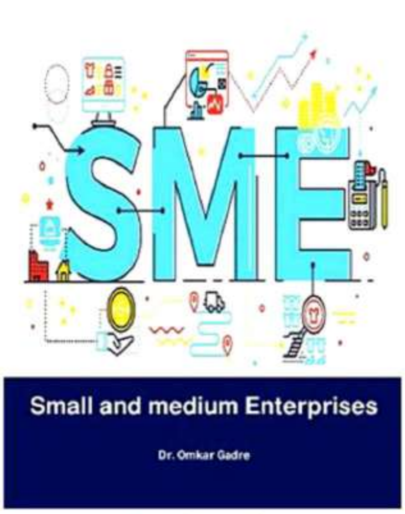
M. Thiruppathi
R. Rex Immanuel
K. Arivukkarasu
ISBN : 978-81-930928-9-7



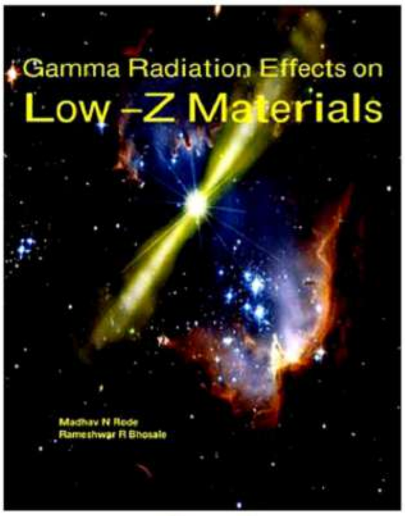
Dr. Th. Anand Singh
Dr. Prakash K. Sarangi
Dr. Neeta Sarangthem
ISBN : 978-81-944069-0-7



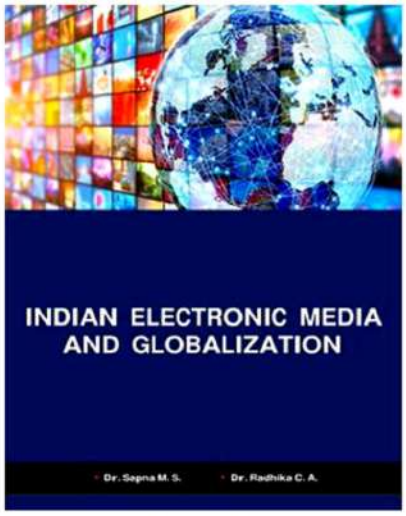
R. Rex Immanuel
M. Thiruppathi
A. Balasubramanian
ISBN : 978-81-943209-4-4



Dr. Omkar V. Gadre
ISBN : 978-81-943209-8-2

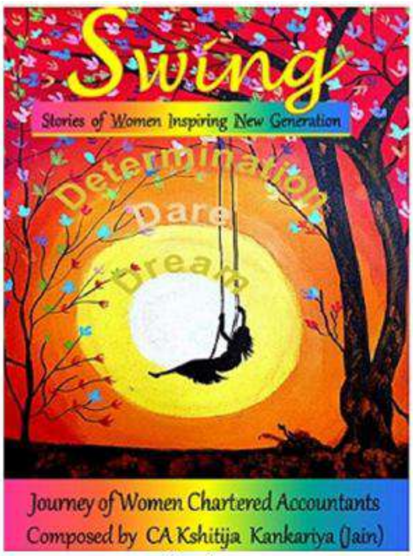


Madhav N Rode
Rameshwar R. Bhosale
ISBN : 978-81-943209-5-1

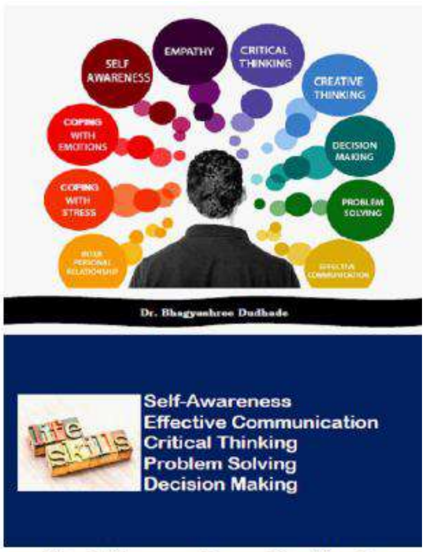


Dr. Sapna M S
Dr. Radhika C A
ISBN : 978-81-943209-0-6

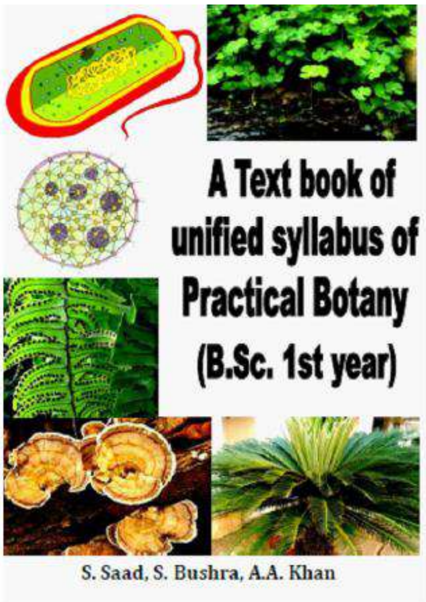
Hindusthan College
ISBN : 978-81-944813-8-6



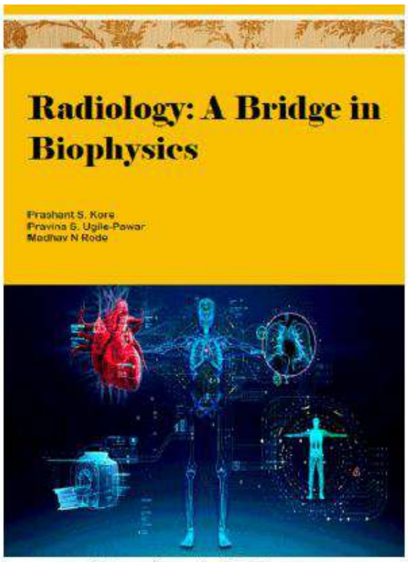
Swing
ISSN: 978-81-944813-9-3



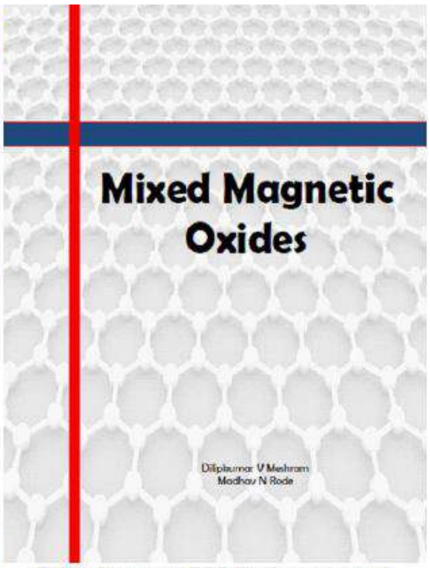
Dr. Bhagyashree Dudhade
ISBN : 978-81-944069-5-2



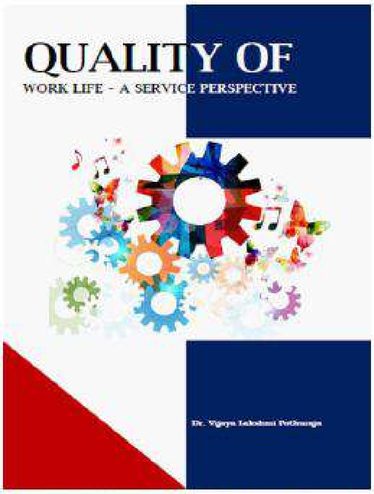
S. Saad, S. Bushra, A. A. Khan
ISBN: 978-81-944069-9-0



Prashant S. Kore
Pravina S. Ugile-Pawar
Madhav N Rode
ISSN: 978-81-944069-7-6



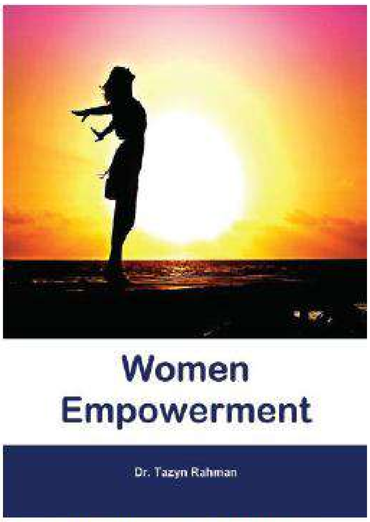
Dilipkumar V Meshram and Madhav N Rode
ISSN: 978-81-944069-6-9



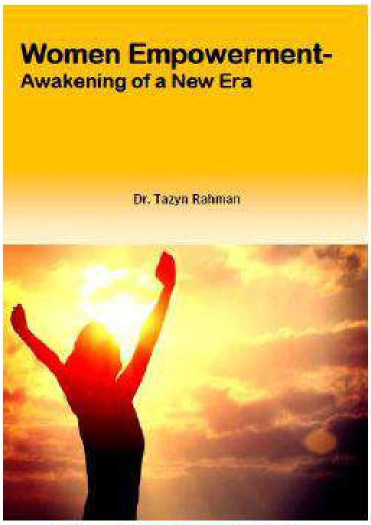
Dr. Vijaya Lakshmi Pothuraju
ISBN : 978-81-943209-2-0

Pratibha College
ISBN : 978-81-944813-2-4

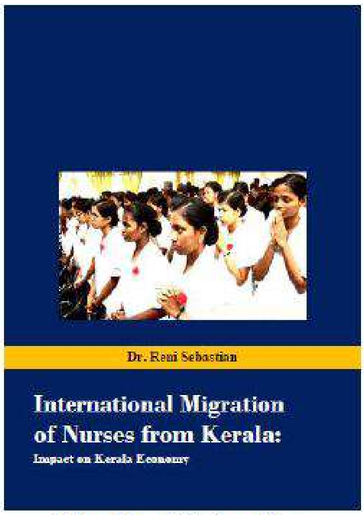
Pratibha College
ISBN : 978-81-944813-3-1



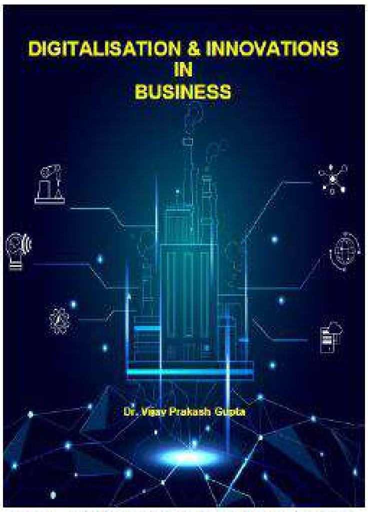
Dr. Tazyn Rahman
ISBN : 978-81-936264-1-2



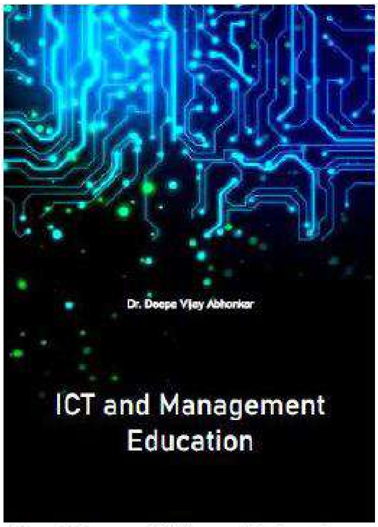
Dr. Tazyn Rahman
ISBN : 978-81-944813-5-5



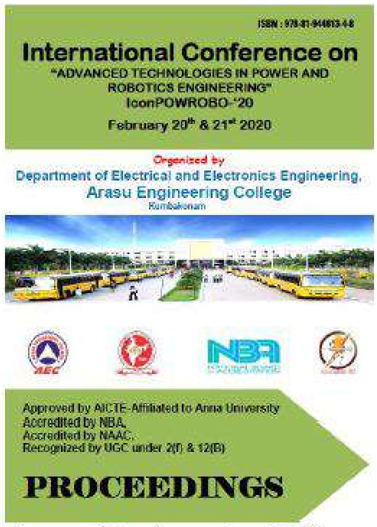
Dr. Reni Sebastian
ISBN : 978-81-944069-2-1



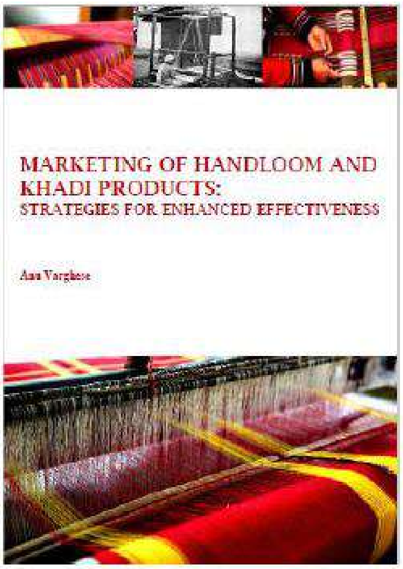
Dr. Vijay Prakash Gupta
ISBN : 978-81-944813-1-7



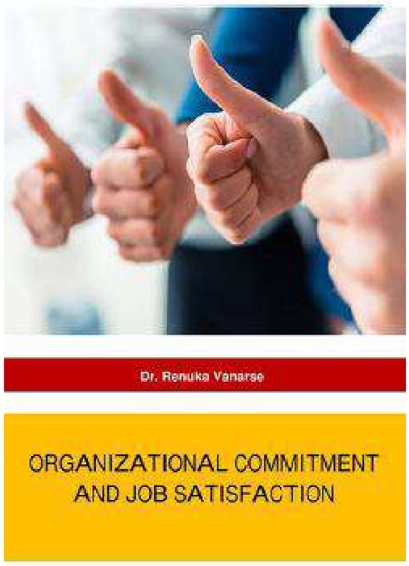
Dr. Deepa Vijay Abhonkar
ISBN : 978-81-944813-6-2



Arasu Engineering College
ISSN: 978-81-944813-4-8



Dr. Anu Varghese
ISBN : 978-81-944069-4-5



Dr. Renuka Vanarse
ISBN : 978-81-944069-1-4

Indian Academicians and Researchers Association
www.iaraedu.com