Essentials in Cyber Defence

Editors:

Dr.S.U. Aswathy

Dr.J. Gladson Maria Britto

Periodic Series in Multidisciplinary Studies

Title of the book: *Essentials in Cyber Defence*

Volume: *5*

This book is a part of the "**Periodic Series in Multidisciplinary Studies**", designed to showcase interdisciplinary research and academic contributions from various fields including science, humanities, technology, education, and more.

The goal of this series is to create a platform for both established and emerging scholars to present their findings in a way that transcends traditional academic silos. By promoting interdisciplinary collaboration and integrated thinking, the series contributes to the advancement of knowledge and the resolution of complex global challenges that require multi-perspective approaches. We believe that sharing diverse voices and research methodologies can catalyse meaningful progress across fields and foster a more informed and connected scholarly community.

This volume offers unique insights and case studies contributed by experts and researchers from around the world. Each chapter reflects the authors' individual perspectives and scholarly expertise. Readers are encouraged to engage critically with the content, reflect on the findings, and explore how these insights may apply to their own fields of interest or professional practice.

ISBN: 978-81-986418-6-1

Preface of the Series

In a world where digital systems underpin almost every aspect of modern life from government and finance to healthcare and critical infrastructure cybersecurity has emerged as one of the defining challenges of our time. The rapid evolution of cyber threats, combined with the increasing sophistication of attackers, demands not only reactive measures but proactive, strategic defense frameworks. It is in this context that **Essentials in Cyber Defence** has been developed.

This volume brings together foundational concepts, practical techniques, and current best practices in the field of cyber defence. The aim is to provide readers with a clear, accessible, and comprehensive understanding of the key elements required to defend against digital threats effectively. Topics span across network security, threat intelligence, incident response, endpoint protection, encryption, and the human factors that so often play a critical role in cyber incidents.

As the editor, my intent has been to ensure that this work serves as both a primer and a reference suitable for students beginning their journey in cybersecurity, professionals seeking to strengthen their defensive capabilities, and decision-makers looking to shape cyber-resilient organizations. Each chapter is authored by experts who bring not only theoretical knowledge but also valuable practical insights from the field.

In an age of growing cyber dependence, knowledge is perhaps the most powerful defense we have. It is my hope that the material presented here equips readers with the essential tools and perspectives to better understand, anticipate, and respond to the challenges of the cyber domain.

I am deeply grateful to the contributors for their commitment, and to the readers who continue to advance the conversation and practice of cybersecurity. May this volume serve as a meaningful step forward in our shared mission to secure the digital future.

Editor of the Series

Dr.S.U. Aswathy,
Marian Engineering College, India.
draswathy.cs@marian.ac.in

Dr.J. Gladson Maria Britto,
Malla Reddy College of Engineering, India.
hodcsd@mrce.in

TOC

Chapter-I

AUTOMATED INCIDENT RESPONSE SYSTEMS FOR CYBERSECURITY

Dr. Ananya Rajan, Professor of Cybersecurity, Indian Institute of Technology (IIT) Bombay, India.

Dr. Karthik Srinivasan, Professor of Cybersecurity, Indian Institute of Technology (IIT) Bombay, India.

Abstract--- Cybersecurity is challenging to manage. The people and resources to deal with the growing number of threats to their company are not available in most businesses. Most threats are investigated due to this inability to cope with the number of signals. Due to this, businesses are at risk of critical attacks. Cybersecurity teams are overwhelmed. Companies everywhere are detecting and clearing network security attacks in the highly evolving industry of cybersecurity. Human effort and intervention are now no longer enough owing to cyber threats complexity and perpetuity of changes. Automated response programs fuelled by artificial intelligence are evermore significant when it comes to network security as well as to thwarting cyberattacks. The research investigates AI and network security-powered automated incident response systems. These systems are able to detect, evaluate, and respond to security incidents instantaneously using AI algorithms, machine learning, and threat intelligence. With automated decision-making and orchestration, AI systems are capable of discovering and controlling security breaches, reacting faster, and restricting cyberattacks on businesses' networks and activities. AI-powered automated incident response systems need to have intelligent decision-making, adaptive response, and sophisticated threat detection. Such systems process vast amounts of data, identify anomalies, and identify security vulnerabilities through supervised, unsupervised, and reinforcement learning. This paper proposes AI-based systems learn from new data and threat situations; they can rapidly adapt to emerging cyber threats.

Keywords--- Cybersecurity, Cyberthreats, Machine Learning.

1. INTRODUCTION

With the increasing rate and sophistication of cyberattacks, there is a need for real-time threat mitigation. Companies can outsmart attackers and enhance system security through automated incident response, which gives the timely and targeted response necessary to counter threats as they emerge Goyal et al., (2024). An active approach is needed for successful safety measures in today's digital world. Humans have traditionally used fences, locks, signatures, strict rules, and a certain way of life to physically defend and secure their property and privacy Papastergiou et al., (2019). Hackers now have greater opportunities to compromise vital systems and bring down services, such as intercepting messages delivered to airplanes, freezing bank accounts, manipulating satellite data, and taking down military control systems, thanks to the development of networked electronic automation systems Abiade (2024). Computer system security has emerged as a top global and societal concern that must be addressed in today's cyber dependent society. The Internet's rapid growth has led to an increase of custom web-based applications, such as e-commerce, government, and other mission-critical services. However, external threats like Internet attacks can now affect the networked systems. The necessity for networked computer and information system security has significantly increased as a result of this situation. To protect networked information systems and services from attackers, it is now essential to fortify their security Armor. The purpose of intrusion detection systems (IDS) (Aravid, 2025) is to prevent malicious users from interfering with the regular operation of information systems in production Reddy & Reddy (2020).

Although nothing has really transformed incident response or firefighting, artificial intelligence (AI) in automated incident response has gained a lot of attention recently. Summers and Paxson's (2010) alarming findings demonstrated the limitations of traditional intrusion detection systems (IDS) and suggested using machine learning techniques to improve threat identification. Their study's practical findings demonstrated that machine learning was far more accurate at identifying anomalies and that it could be used to lower the frequency of false positives, allowing businesses to know for sure (as opposed to making informed guesses) whether an occurrence was genuine or just noise. This body of research has been further developed, examining different AI methodologies and their potential applications at various phases of the incident response lifecycle (Karlzen & Sommestad, 2023).

The usefulness of supervised, unsupervised, and semi-supervised learning methods for the detection of zero-day attacks was also investigated by Elsayed et al. (2023). According to their study, biassed or insufficient data may impair performance, underscoring the significance of utilizing sizable, varied datasets for AI training. An increasing number of people are worried about adversarial attacks on AI models. Goodfellow and associates. Prior research has demonstrated that adversarial examples can easily trick machine learning methods, as even minor modifications to the input data can alter the model's prediction (Hubara et al., 2018; Nutalapati, 2024; Trifonov et al., 2019; Leow, 2025)

2. Rise of the Internet Security Incidents

In addition to attracting hackers, the abundance of content-rich websites has raised the frequency and severity of security events. These days, Internet connectivity is ubiquitous, and its use is unavoidable. Users can choose from a variety of flexible and reasonably priced Internet connectivity alternatives offered by telephone companies. In actuality, this has become a gathering place for the hacker community, where they exchange current information on known vulnerabilities in the newest gear and software. The expansion and accessibility of the Internet itself coincide with an increase in Internet security events. Numerous avenues of entry into a business networked facility are made possible by the inherent flaws in the current operating systems and network protocols. For example, some system software flaws are used to create root shells on individual hosts, which are then used to run privileged commands (Charyyev & Gavirova 2024).

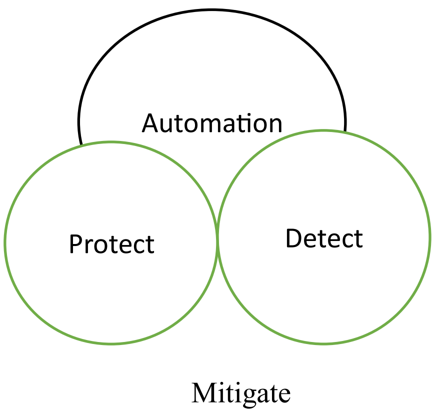


Figure 1: Incident Response Systems

Many IP packets can be created at the same time to stop a victim in a network range that is well-manipulated. Automated attack tools are created by the hacker community to take advantage of known weaknesses in target systems that provide essential services like mail servers, web servers, database servers, and more. The tools they created are freely accessible on their community websites. Both novice and expert hackers utilize these tools to break into and take over the victim machines. In actuality, compromised computers have specific programs installed that allow them to launch coordinated attacks against victims. To fix known vulnerabilities, operating system vendors frequently release patches and upgrades. Exploits have included poorly maintained personal PCs and servers, ignorant users, and application software vulnerabilities.

3. Need for Intrusion Detection Systems

The term "intrusion" describes an attack on a networked computer facility that aims to violate Confidentiality, Integrity, and Availability (CIA) or cause harm. Intrusions can take many different forms, including malware launches, network-based attacks on susceptible services, and user privilege escalation on hosts.

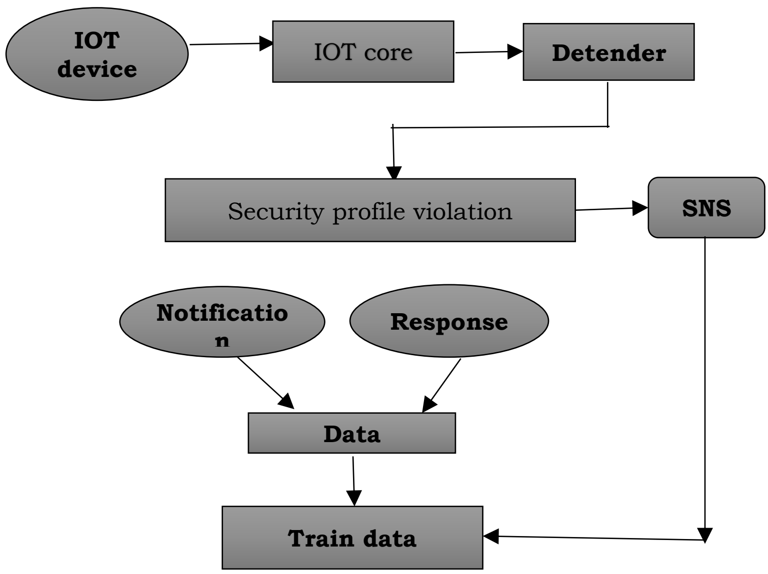


Figure 2: Mitigate IOT Risks

The technique of identifying non-compliant information system use or attacks on networks and computing facilities is known as intrusion detection. An intrusion detection system (IDS) is an automated instrument used to identify intrusions that can be installed in software, hardware, or a mix of the two. Among the many different alternative processes used to secure company networks, an intrusion detection system (IDS) appears to be one of the most popular security technology solutions. The IDS is a useful device that may be used as a burglar alarm or security camera Anayat (2024). This intrusion detection system can be set up to record events, which can then be utilized as forensic proof to hold the enemy accountable. However, a large number of IDS cause a higher number of false alarms, which might be problematic. The two main components that help secure a network are visibility and control, both of which are offered by an IDS. Visibility assists with decision-making by making network traffic visible, which has a direct impact on the creation of security policies. Control is then used to enforce adherence to the security policy by preventing access to privileged sections of computer networks. As seen in Figure 1.3, an intrusion detection system is often positioned behind a firewall in a computer network. It is at the second and last layer of protection and is carefully built to search for harmful network traffic. The firewall and IDS work together, and neither can take the place of the other.

While the email server is used to give university staff members the ability to send emails, the web server is used to broadcast information about the university to the wider public. Confidential information is shared via email with government officials and outside organizations. The university campus is large, with numerous departments distributed across far-flung buildings housing well-connected nodes. The campus network, which only allows public access to a select few services like the web server, email server, and Domain Name Server (DNS), is protected by the firewall. Using a variety of tools and methods, an attacker gains access to the university campus network and discovers that the CMAIL 2.4.9 mail server is used for email. Knowing that this specific program is susceptible to buffer overflow attacks, the criminal takes use of this vulnerability to launch a command shell with administrator privileges.

4. Components of Automated Incident Response Systems

Data Collection and Monitoring

To keep an up-to-date picture of the network environment, AIR systems continuously collect data from network devices, apps, and security tools. To find irregularities or questionable trends, they employ techniques like log aggregation and real-time traffic monitoring. This data, which provides a framework of normal and atypical actions, serves as the foundation for additional investigation Uzoma et al., (2023).

Machine learning is employed by monitoring solutions to further improve anomaly detection. The algorithms are better able to detect deviations that show potential threats through learning normal behaviour patterns. Ongoing monitoring enhances the quality of future threat predictions and response actions by aiding in the early identification of incidents and contributing to a more affluent dataset.

Automated Detection and Analysis

Applying algorithms to analyze data and identify any security breaches is referred to as automated analysis and detection.

Improved Uptime

One issue response tool that proves useful for small- and medium-sized businesses is Better Uptime. You can get threat alerts by phone call, email, or a Slack integration after quick setup. The software includes standard network utilities such as ping and uptime. Amazon Web Services (AWS), Heroku, Microsoft Teams, and numerous other business applications have plugins. Better Update provides businesses of all sizes with competitive pricing and a free version.

Check Point Incident Response

A well-known cybersecurity supplier, Check Point is well-known for its firewall and VPN products. Network traffic monitoring, threat analysis, and email scanning are just a few of the many incident management and response features that Check Point Incident Response provides. On the Check Point Incident Response website, you can request a demo.

Digital Risk Protection

Digital Risk Protection is a user-friendly incident response platform that includes tools for data gathering and log analysis. It is mostly intended for businesses who want to shield their brands against infringement or repeated harm. But because of how easy it interfaces with incident response platforms through APIs, it's also a versatile tool. You can ask Group IB for a demo.

FireEye Mandiant

Data science and common cybersecurity procedures (Manco, 2022) are combined in Mandiant, a threat intelligence and incident response solution. Each organization is given specialized protection by the tool. With more than 15 years of industry experience, FireEye contributes seasoned knowledge to this product. To get you started with Mandiant, they provide a free edition

Varonis Data Alert

Varonis Data Alert offers analytics and notifications about the infrastructure, data usage, and users of a company. Additionally, it is an incident response tool that identifies and addresses questionable activity. According to Varnish, it gathers billions of data points to aid Data Alert in comprehending the threat environment. The Varonis website does not offer pricing; however, you can request a demo.

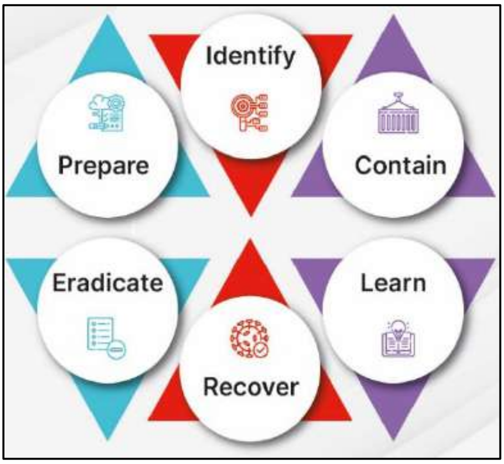


Figure 3: 6 Steps of AIR

5. Benefits of Automated Incident Response

Automate Manual Security Processes

Security teams would be better suited looking into and reacting to real and significant security occurrences rather than squandering time on manual incident response chores. That's precisely what automated incident response allows them to do. By automating these processes, analysts can concentrate on areas where their expertise and contributions are most needed, from alarm notification and correlation to initial investigation, triage, ticket generation, and report generation Abdul (n.d).

More Efficient Security Operations

Automation improves incident identification, response, and mitigation through increased speed, consistency, and proactivity. Analysts can concentrate on preventing attacks before they inflict irreversible harm rather than painstakingly copying and pasting proof of a threat. As security operations increase mean-time-to-resolution (MTTR), they also become more efficient.

Generate Critical Insights in Real Time

Security staff may prioritize incident response tasks and efficiently handle security alerts at scale with the help of an automated incident response platform that can report pertinent information in a centralized dashboard. Various security information sources can be automatically added to notifications to enhance incident response and give more insight into the threat environment.

No More Alert Fatigue

Many organizations receive an excessive number of alerts from security tools. Analysts must manually examine each warning to ascertain whether it pertains to real threats or false positives. This is acceptable as long as there aren't many alerts, but for the majority of companies and organizations, SOC teams can spend days locating all of the warnings from a single day. We refer to this as alert weariness. Because of alert fatigue, real problems are frequently overlooked, leaving the company far more susceptible. This issue is resolved by automated incident response, which does away with the human factor entirely in alarm processing and reaction. Additionally, by allowing security teams to analyse and address more threats, this advantage enhances enterprise security.

Improved Decision Making

Everyone's involvement during an event is clearly defined in an automated incident response plan. This expedites the process and guarantees that, in the event of a threat, the proper decision-makers are involved.

Reduced Damages

When a true cyberattack occurs, automated IR helps your company respond more effectively and quickly, minimizing the impact on your company.

Internal and External Coordination

An effective automated IR plan aids in coordinating interactions with external parties, including as partners and suppliers, as well as internal departments and units inside an organization in the event of a security crisis. In order to control brand reputation and damage after a security event, it is essential to bring together all relevant stakeholders.

Better MTTD and MTTR

Your Mean Time to Detect, or MTTD, is the average amount of time it takes to identify a security issue or incident. On the other hand, Mean Time to Respond (MTTR) is the average amount of time needed to mitigate and contain the threat. By distinguishing genuine threats from false positives, automated incident response enables organizations to identify and address risks more quickly.

Lower Operational Costs for SOCs

SOCs can devote their time to more productive work because automated IR handles the majority of warnings and expedites repetitious procedures. As a result, SOCs' operating expenses are decreased.

To prevent further intrusions into the workstation where the CMAIL is installed, the attacker proactively installs a backdoor. The attacker uses this unlawfully obtained privilege to install tools and utilities, such sniffers, that expose real data. With increased privileges, the attacker can now change important information like finances, research, intellectual property, and the personal lives of all employees and students, which could have an impact on the university's growth and reputation. The scenario under discussion makes it clear that the conventional security mechanism has not been able to prevent the attacker from taking advantage of the known weaknesses. As a second line of defines in networked information system infrastructure, the intrusion detection system (IDS) steps in to save the day. An intrusion detection system (IDS) is designed to explicitly identify and report different types of intrusions in the host and network where it is placed. Installing intrusion detection systems (IDS) on a business network results in a secure infrastructure and timely notification of the administrator during the intrusion. This enables the administrator to take prompt action to prevent the hacker from accessing other areas of the network Manda (2021).

Patches have been installed to address the detected inherent vulnerabilities in the software and hardware in an effort to guarantee network security. In the modern, dynamic, and susceptible world, the traditional, reactive, and aftermath method of protecting IT facilities is no longer infallible.

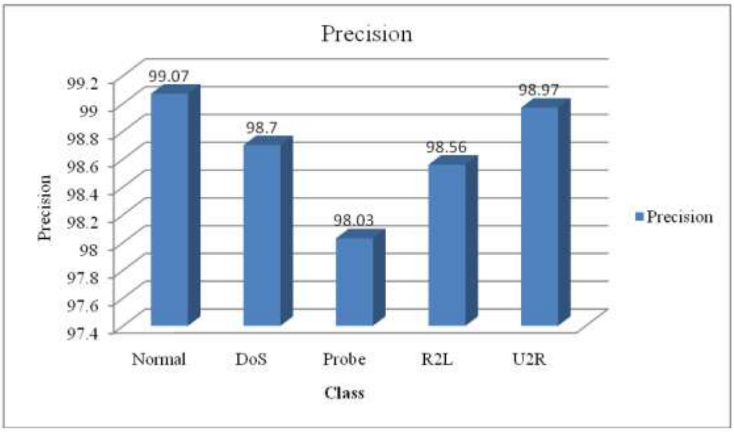


Figure 4: Precision Values

It is necessary to take a more thorough, proactive strategy that incorporates the necessary security elements even while the software and hardware of the information technology infrastructure are being researched, designed, and developed. Despite the technological progress made in IDS operation, it is evident that certain significant issues remain unresolved.

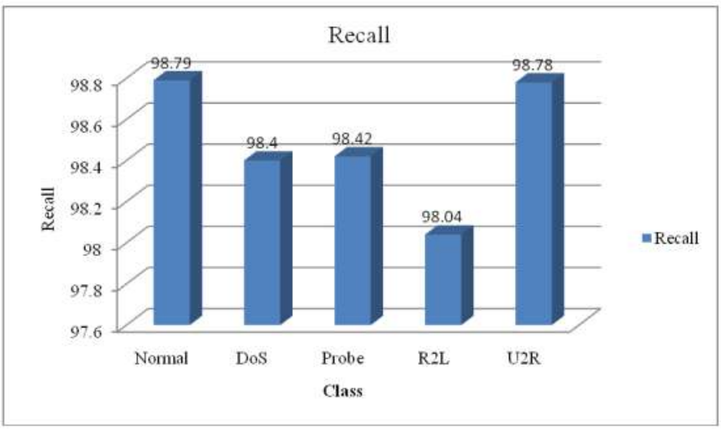


Figure 5: Detection Rates of Various Classes in the Training Data

The process of precisely identifying an intrusion takes a lot of time since it involves a lot of computing work. The invaders continue to succeed in their mission because they are constantly improving their intrusion strategies to fool the IDS.

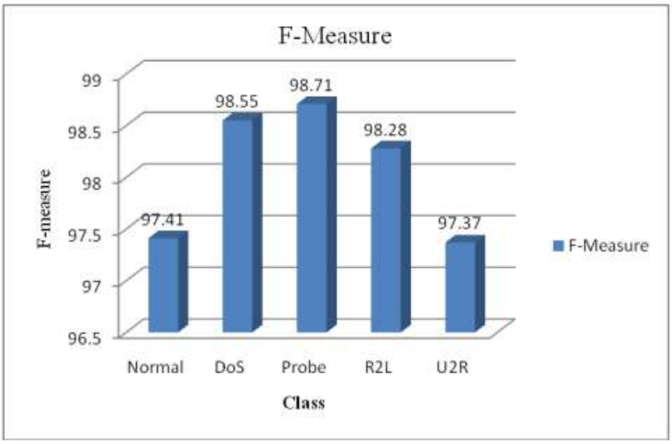


Figure 6: F-measure of Various Classes for Training Dataset

The current situation is made even more dangerous by the Internet's unrelentingly complicated expansion and the several kinds of end-host software that are vulnerable. The creation of false positives is yet another significant obstacle to the design and deployment of IDS, even though standard privacy and security standards impedes the detection process. IDS, which were created utilizing a variety of approaches, have been commercially available for the past 20 years.

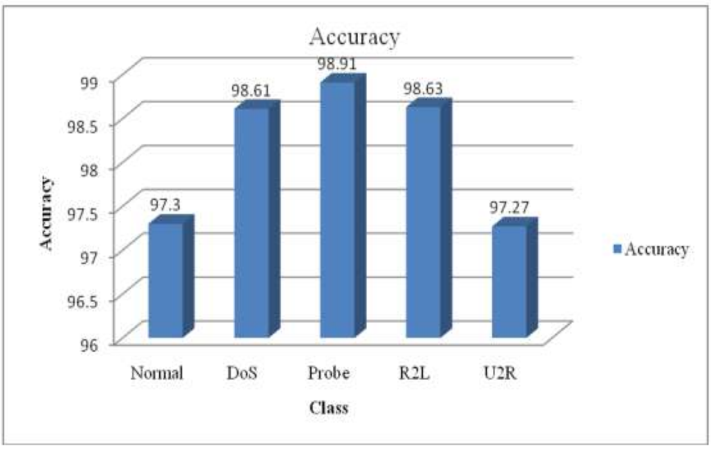


Figure 7: Detection Accuracy of Training Dataset

When it comes to identifying a particular class of attacks, they perform better than one another. For the other classes, their accuracy levels are comparatively lower.

Because of their flexibility, the students were able to act swiftly, ensuring that each real-time intervention was carried out in an average of 1.5 seconds per threat:

reduces the time it takes to identify malicious software and implement immediate actions."

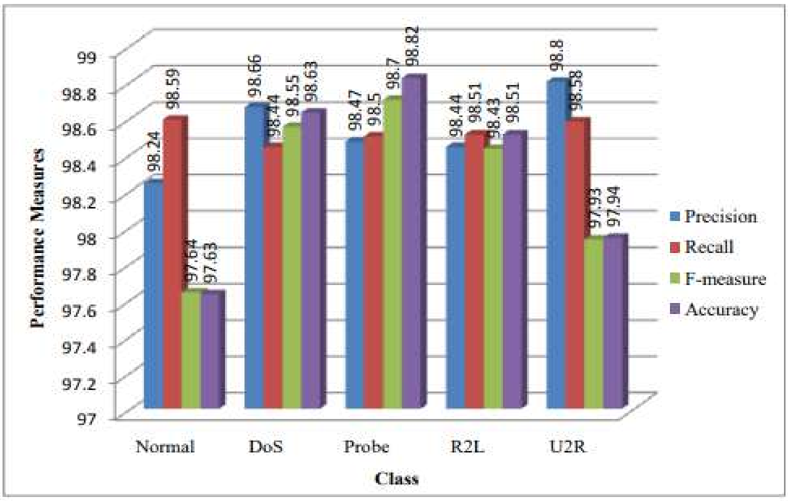


Figure 8: Performance evaluation

In order to engage the dynamic nature of cyber threats and enable a learned-improve mechanism, this dynamic responsiveness is crucial. Even while these developments are encouraging, there are still a number of issues, most notably the higher false positive rate in unsupervised models and the resilience of AI systems against hostile attacks. Future efforts will focus on enhancing model generalization and including multi-modal attacks to create a more comprehensive threat detection system.

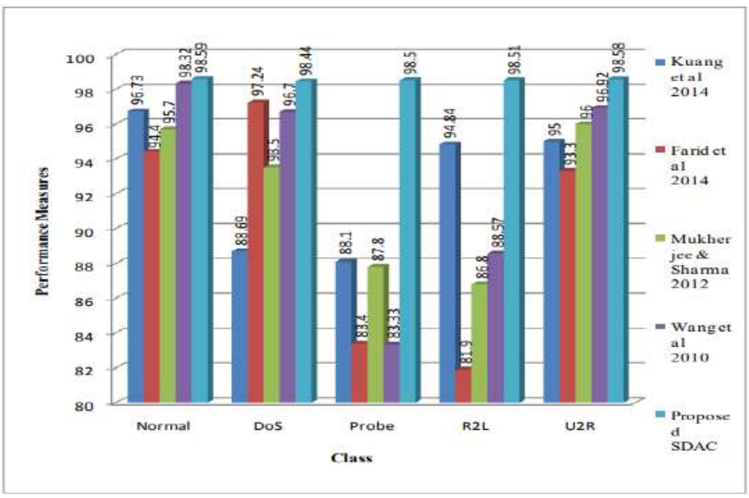
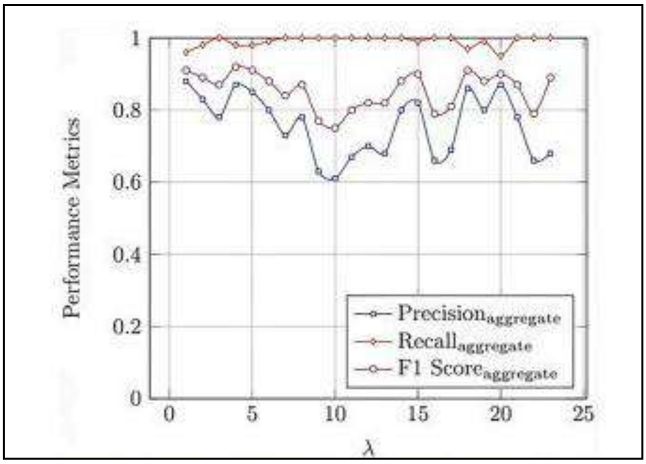
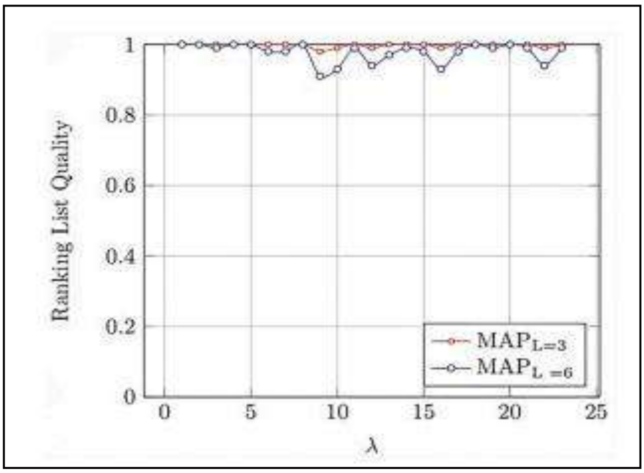


Figure 9: Comparison of Detection Rate

Furthermore, the responsible implementation of such systems necessitates adherence to moral and legal requirements, which supports initiatives for more explicable and transparent AI models.



(a)



(b)

Figure 10: Performance Evaluation

Our findings collectively add to a growing body of research supporting AI's application as a revolutionary tool in cybersecurity with outstanding advantages for threat identification and response. RTLR. Response systems driven by AI Properly analysed information also requires a system that can use an efficient cybersecurity strategy for AI reaction to be feasible! In conclusion Automated incident response systems driven by AI are a remarkable development in cybersecurity. Adamant leverages the advantages of machine learning and reinforcement learning to create quick, accurate, and flexible defensive countermeasures for cyber security. To get beyond the remaining challenges and keep improving the technologies that are available with digital infrastructures, further research and development will be required.

6. Conclusion

Either internal or external factors might lead to network assaults. Many traditional security methods, including as firewalls, proxy servers, data encryption, and user authentication, can prevent internal attackers, but they are unable to manage bigger network servers. Internal assaults can access and exploit the system without the genuine person's consent because they are aware of the original network characteristics, policies, and breakdown techniques. By taking advantage of the original system, external attackers can pose as authorized users and create external attacks. As a result, an extra wall is required to defend systems such as Intrusion Detection Systems (IDS), which can effectively manage both insider and outer threats, as well as implement extensive applications and supply the data required for prompt countermeasures.

References

[1] Goyal, D., Gandhi, Y., Dongre, D., Shailesh, Bhagat, G. P., & Pawar, R. (2024, June). Decision Systems for Adaptive Cybersecurity Incident Response. In *International Conference on Frontiers of Intelligent Computing: Theory and Applications* (pp. 543-563). Singapore: Springer Nature Singapore.

[2] Papastergiou, S., Mouratidis, H., & Kalogeraki, E. M. (2019, May). Cyber security incident handling, warning and response system for the european critical information infrastructures (cybersane). In *International Conference on Engineering Applications of Neural Networks* (pp. 476-487). Cham: Springer International Publishing.

[3] Aravid, J. (2025). Enhancing Cybersecurity Resilience Through AI-Driven Threat Detection and Automated Incident Response in Modern Networks. *International Journal of Advanced Research in Cyber Security*, *6*(2), 1-6.

[4] Manco, D. I. (2022). *Automation in the Cybersecurity Incident Handling Process* (Doctoral dissertation, Politecnico di Torino).

[5] Abiade, O. (2024). TOPIC: Cybersecurity Automation: Streamlining Incident Response.

[6] Reddy, A. R. P., & Ayyadapu, A. K. R. (2020). Automating Incident Response: Ai-Driven Approaches to Cloud Security Incident Management. *Chelonian Research Foundation*, *15*(2), 1-10.

[7] Karlzen, H., & Sommestad, T. (2023, August). Automatic incident response solutions: a review of proposed solutions' input and output. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (pp. 1-9).

[8] Nutalapati, P. (2024). Automated Incident Response Using AI in Cloud Security. *Journal of Artificial Intelligence, Machine Learning and Data Science*, *2*(1), 1301-1311.

[9] Trifonov, R., Manolov, S., Tsochev, G., & Pavlova, G. (2019). Automation of cyber security incident handling through artificial intelligence methods. *WSEAS Transactions on Computers*, *18*(2), 274-280.

[10] LEOW, E. (2025). Employing Automation for Incident Response Planning. *ISACA Journal*, (1).

[11] Charyyev, S., & Gavirova, O. (2024). Incident Response Automation System. *Innovative Science*, (12-2-1), 36-37.

[12] Anayat, R. (2024). Cybersecurity Automation with AI: Reducing Human Error and Improving Incident Response.

[13] Uzoma, J., Falana, O., Obunadike, C., Oloyede, K., & Obunadike, E. (2023). Using artificial intelligence for automated incidence response in cybersecurity. *International Journal of Information Technology (IJIT)*, *1*(4).

[14] Abdul, S. (2023). AI for Cyber Security: Automated Incident Response Systems.

[15] Manda, J. K. (2021). Cybersecurity Automation in Telecom: Implementing Automation Tools and Technologies to Enhance Cybersecurity Incident Response and Threat Detection in Telecom Operations. *Advances in Computer Sciences*, *4*(1).

Chapter-II

DESIGN OF ADVANCEMENTS IN AI FOR CYBER THREAT DETECTION

Dr. Neha Chopra, Cyber Forensics Specialist, Delhi Technological University (DTU), India.

Dr. Vikram Patil, Cyber Forensics Specialist, Delhi Technological University (DTU), India.

Abstract--- The field of artificial intelligence (AI) has the potential to fundamentally change how society uses technology, particularly in terms of how personal information is connected and how hackers can access people's private lives. Future AI software systems are anticipated to be customized by profit-driven criminals to their operations, further complicating ongoing cybercrime investigations. This thesis examines the potential use of developing AI technology by cybercriminals and multinational criminal organizations to carry out ever-more complicated criminal activities, as well as the preparations that the homeland security sector should make. Using a future scenario methodology, four scenarios were developed to forecast how hackers would take advantage of AI systems and what steps should be taken immediately to protect the US from dangerous AI use. Automotive technology has advanced in many ways. These developments have led to the development of a complex automotive technology ecosystem and have brought autonomous cars closer to commercialization. Like any other technology, these developments have benefits but also provide a number of risks. One of these issues in the automotive sector is cybersecurity risks. These security flaws in cars have the potential to cause fatalities as well as enormous costs and disastrous outcomes. Therefore, some of the cybersecurity problems in the automotive ecosystem are resolved by carrying out a comprehensive threat analysis, assessment, and detection. This dissertation will accomplish this by developing a three-step framework for assessing, identifying, and evaluating risks using machine learning techniques.

Keywords--- Cybersecurity, Artificial Intelligence, Software Systems.

1. INTRODUCTION

The way people perform a variety of tasks has significantly improved since the 1990s due to technology improvements. Intelligence is the ability to acquire and apply a variety of knowledge and abilities to solve problems. The application of general mental skills to solve problems, reason, and learn from various situations is another aspect of intelligence. Cognitive abilities such as language, perception, planning, memory, and attention are all associated with intelligence (Ijiga et al., 2024). In general, the last ten years can be used to analyse how intelligence has developed. Both artificial and human intelligence have a role in intelligence. As a science, AI was more akin to science fiction. But AI is already a reality that permeates our daily lives and is no longer a work of science fiction. Thus, artificial intelligence (AI) makes it possible for computers to analyse complex data and provide accurate information by using neural networks that mimic the real neurons' functions (Bécue et al., 2021).

A subfield of science and engineering known as artificial intelligence (AI) studies the theory and application of building systems that exhibit human-like intelligence. In the twenty-first century, artificial intelligence (AI) has emerged as a prominent research issue in a wide range of fields, including business, accounting, finance, marketing, economics, engineering, science, education, health, the stock market, and law, to mention a few. Thanks to advancements in AI, the golden age of AI has come. Artificial intelligence is now the most advanced technology as a result. It will therefore continue to take centre stage in the technical spotlight for a long time to come. The fact that artificial intelligence has improved people's lives must be emphasized. In example, integrating AI technology has a direct correlation with improving people's daily activities (Aminu et al., 2024).

Since the intelligence of computers with machine learning capabilities has had a substantial impact on industry, society, and government, the field of artificial intelligence (AI) has grown significantly. The artificial intelligence areas are broadly divided into 16 groups. Programming, artificial life, belief revision, data mining, distributed AI, expert systems, genetic algorithms, neural networks, theorem proving, constraint satisfaction, knowledge representation, machine learning, learning natural language, and theory of computation are some of the topics covered (Sharma, 2024; Vaddadi et al., 2023; Galla et al., 2022; Madhavram et al., 2022).

2. REVIEW OF LITERATURE

In recent years, a variety of cyber security applications have experimented with AI approaches (Zhimin et al., 2021). This paper so reviews the current research on

AI applications in aberrant traffic detection, network situation awareness, user access authentication, and hazardous behavior monitoring. This study presents a conceptual human-in-the-loop intelligence cyber security model based on the findings, while also pointing out a number of limits and difficulties (Reddy, 2021).

In the context of cybersecurity, want to give a general overview of how artificial intelligence may be used in both attack and defence. The study claims that significant progress in information technology has led to the emergence of new cybersecurity issues. The computational complexity of cyberattacks calls for new approaches that are more flexible, scalable, and resilient. This essay focuses on applying the AI-based approach to cybersecurity issues. We specifically demonstrate the potential applications of AI in APT, malware detection, intrusion detection, and other domains such as spam and phishing detection. Additionally, our research illustrates a scenario where artificial intelligence could be employed maliciously. While research on AI's potential to solve cybersecurity challenges is ongoing, some of the problems with implementing AI-based defences are equally significant. For instance, the creation of autonomous intelligent malware or the hostile attack against AI models. Therefore, more study should be done to identify solutions to these risks (Lekkala et al., 2022).

To enhance cyber security is examined by Shidawa Baba Atiku et al. (2020). In fields like data analytics, artificial intelligence has become so sophisticated that it can now perform tasks more effectively than humans. For this study, which employed the thematic literature review approach, data was collected from a variety of sources, including academia, scientific direct, research portals, and Google Scholar. The study demonstrated that while there are advantages and disadvantages to utilizing AI to stop cyberattacks, the advantages outweigh the disadvantages. According to this report, because AI systems require quick and effective technology to operate, they are expected to improve the security of businesses and customers online. The increasing use of AI engines in cyber security as opposed to conventional scanning engines is evidence of this. Among the challenges of AI applications for cyber security are the threat of adversarial AI attacks and the complacency of the human component. It is still believed that the advantages of using AI in cyber security outweigh the risks, even with its drawbacks. Human interaction is still necessary for cyber security. As a result, more industry experts are advocating that AI should be incorporated into each company's cyber security operation centre's systems (Srinivasulu & Venkateswaran, 2023).

Cyber security, according to Kaspersky Lab (2018), is a method for stopping destructive, unauthorized attacks on computers, servers, mobile devices, electronic systems, networks, and data. Cybersecurity is a broad word that includes anything from end-user training and disaster recovery to the protection of personal computer information. Cybersecurity and artificial intelligence are closely related. Lord (2017) defines cyber security as the technology, protocols, and policies designed to protect networks, devices, programs, and data against harm, unauthorized access, or attack. Cybersecurity is also known as information technology security. Consequently, a growing number of industry experts are suggesting that AI should be incorporated into the cyber security operation center systems of every company

Cybersecurity, according to Kaspersky Lab (2018), is a method for stopping damaging, unauthorized attacks on computers, servers, mobile devices, electronic systems, networks, and data. "Cybersecurity" is a comprehensive phrase that includes everything from protecting personal computer data to disaster recovery and end-user training. Cybersecurity and artificial intelligence are closely related. The technology, procedures, and regulations known as cybersecurity were developed to protect networks, devices, software, and data against harm, unauthorized access, and attacks (Lord, 2017). Cybersecurity is also known as information technology security.

Buczkowski (2017) A wide range of technologies can be referred to by the general term "artificial intelligence." Its objective is to enable computers to think and behave like people, as well as to solve problems more quickly and efficiently than people. AI can perform a wide range of tasks, such as planning, speaking, moving, identifying sounds and objects, and interacting with people in social and professional contexts. Tasks may be accomplished using machine learning, deep learning, recommendation systems, text mining, natural language processing (NLP), evidence-based methods, and predictive and prescriptive analytics. The aforementioned techniques can also be applied to cyber security concerns (Manoharan & Sarker, 2023).

Lehto, (2015) System resilience, vulnerability patching, and risk management are all related to cyber security practices. Among the primary study areas are methods for spotting viruses and other anomalies in network behaviour, as well as IT problems associated with IT security. To put it briefly, cyber security is a collection of actions taken to guard against cyberattacks and their consequences, including implementing the required defences. Cyber security is based on a threat analysis of an organization or institution. Threat and risk assessments serve as the foundation for a company's cyber security strategy's components and structure as well as its implementation program. A company may frequently need to create several targeted cyber security plans and standards. The essential element is that required dangers will be prepared for, and enough protection against threats' harmful consequences will be tried to be established.

Cyber Threats: The Need to Tame the Surge

Cyberthreats can take many different forms. They include assaults that aim to obtain data, corrupt data, conceal data, or interfere with digital processes. Hacktivists, spies, terrorist organizations, criminal gangs, nation-states, irate workers, or lone hackers may start them. Cyber risks are categorized as 'Cyber Crime', 'Cyber Terrorism', and 'Cyber Attack', depending on the attack's origin and goal (Ijiga et al., 2024). Additionally, they are usually grouped according to the kind of threat, as illustrated in Figure 1.

Seldom are the cyberthreats depicted in Figure 1.1 above isolated. They are typically polymorphic and multi-vector, meaning they combine multiple attack kinds and alter their forms to evade detection. In actuality, the majority of episodes end with the injection of malware at the exploitation stage, regardless of the type of attack vector employed. As a result, the most prevalent and pervasive cyberthreat that impacts the majority of Internet users is "malware." As previously mentioned in Figure 1, all of these malwares can be introduced. 'Drive-by-Download' is the most popular method of attack for hackers on web-based systems (Salem et al., 2024). 'Application Security' is the most important of these because so many programs are utilized on various devices all over the world. Application security is security that is measured at the application level and guards against malicious code injection or data theft. Web security and mobile app security are subsets of application security. Since the majority of applications nowadays are either web-based or mobile-based, web security and mobile app security both address the majority of application security issues. As it aims to address the growing danger on web applications like browsers, hybrid mobile apps, etc., the thesis covers the most important part of the cybersecurity paradigm by concentrating on web security and mobile app security.

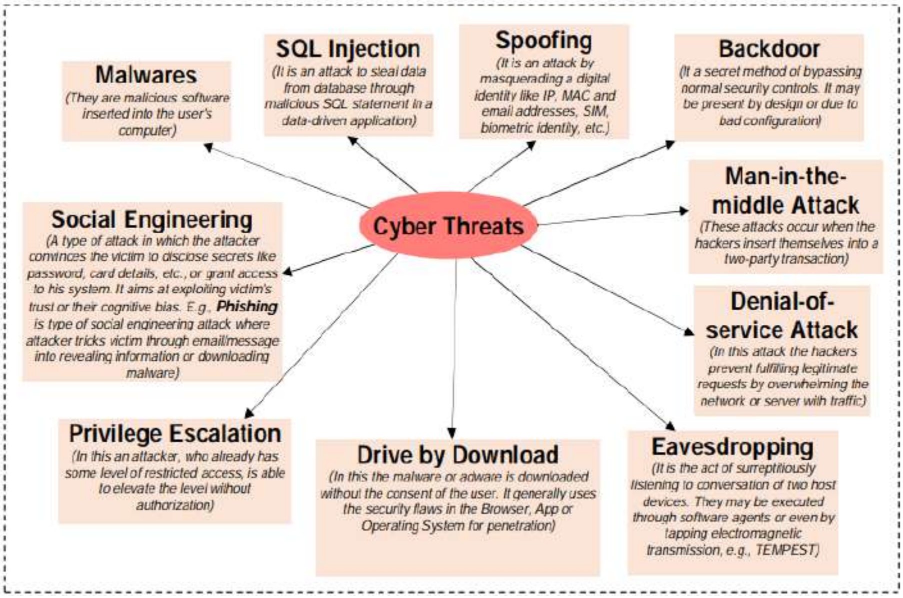


Figure 1: Types of Cyber Threats

2.1. Problem Statement

Despite the fact that cybersecurity in automotive systems is a thoroughly researched subject, intrusion detection techniques in V2X BSM datasets have not yet been examined. Since connected car technology hasn't been widely adopted and sold, there aren't many thorough research on V2X cybersecurity in terms of threat analysis, evaluation, and detection. Numerous threat assessment and characterisation models are available, such as OCTAVE, HEAVENS, NHTSA, EVITA, and others. Although there is no defined framework that uses and includes the results in the design of other security systems (such as intrusion detection systems), these threat assessment techniques are essential for private organizations attempting to determine the seriousness of a threat. Finding a connection between threat assessment and intrusion detection techniques is the aim of this study. All risk or danger assessments in this study will be conducted subjectively using scores or tables. Throughout this process, no discrete variables will be used to determine threat category. From the viewpoint of the users, they will frequently be assessed using linguistic considerations and non-discrete definitions. Due to its fuzzy character, this threat assessment method frequently produces inaccurate assessments and ineffective scoring. This work is among the first to attempt to use fuzzy logic to overcome threat assessment inefficiencies. There aren't many findings because there aren't enough V2X or DSRC datasets that are available to the public. One of the most recent datasets in the field will be utilized in this study. Due to high false positive rates or costly processing requirements, intrusion detection systems in the automotive V2X market are sometimes written off as a bad choice. This study's objective is to develop a feasible IDS for deployment.

3. ARTIFICIAL INTELLIGENCE

The way people perform a variety of tasks has significantly improved since the 1990s due to technology improvements. Intelligence is the ability to acquire and apply a variety of knowledge and abilities to solve problems. The application of general mental skills to solve problems, reason, and learn from various situations is another aspect of intelligence. Cognitive abilities such as language, perception, planning, memory, and attention are all associated with intelligence. In general, the last ten years can be used to analyse how intelligence has developed. Both artificial and human intelligence contribute to intelligence. As a science, AI was more akin to science fiction. However, artificial intelligence (AI) is already a reality that permeates our daily lives rather than a work of science fiction. As a result, AI makes it possible for computers to comprehend complex data and provide accurate information by using neural networks that mimic the real neurons' functions (Yaseen, 2023).

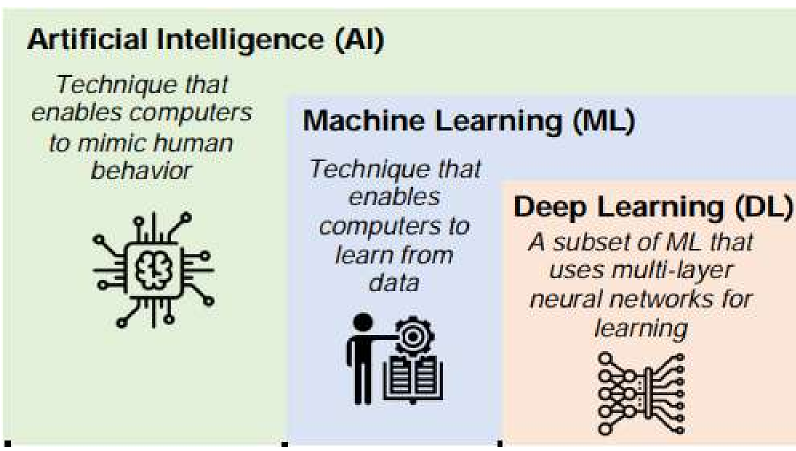


Figure 2: Evolution

The theory and practice of developing systems that exhibit human-like intelligence in behaviour are the focus of the scientific and technical field known as artificial intelligence (AI). In the twenty-first century, artificial intelligence (AI) has emerged as a prominent research issue in a wide range of fields, including business, accounting, finance, marketing, economics, engineering, science, education, health, the stock market, and law, to mention a few. Thanks to advancements in AI, the golden age of AI has come. Artificial intelligence is now the most advanced technology as a result. It will therefore continue to take center stage in the technical spotlight for many years to come.

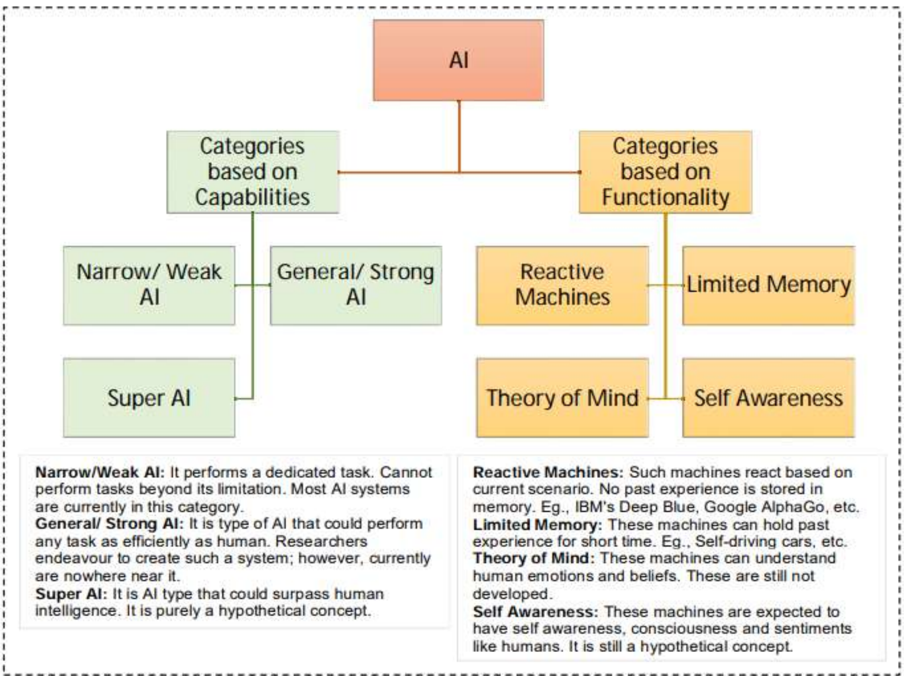


Figure 3: Illustration of AI

The fact that artificial intelligence has improved people's lives must be emphasized. In example, integrating AI technology has a direct correlation with improving people's daily activities. Since the intelligence of computers with machine learning skills has had a substantial impact on industry, governments, and society, the field of artificial intelligence (AI) has expanded dramatically. The artificial intelligence areas are broadly divided into 16 groups. Programming, artificial life, belief revision, data mining, distributed AI, expert systems, genetic algorithms, neural networks, theorem proving, constraint satisfaction, knowledge representation, machine learning, learning natural language, and theory of computation are some of the topics covered. Most AI systems are developed as components of sophisticated programs that lend intelligence in a number of ways, including processing natural language, reasoning with information, and learning and adapting. Nonetheless, certain developed systems, such as planning or expert systems, fall into the category of pure AI applications. The wide, diverse area of artificial intelligence is built on the foundations and connections of numerous disciplines, including mathematics, languages, psychology, neurology, mechanical engineering, statistics, economics, control theory and cybernetics, philosophy, and many more. Despite the fact that many ideas and techniques have been lifted from these domains.

4. CYBERSECURITY

In many respects, the internet has made the globe smaller, but it has also exposed us to difficult and diverse influences that were previously unknown. "The world of hacking grew at the same pace as security." There are two methods to tackle the problem of cyber security. First, the most cutting-edge encryption technology will provide them with strong protection because cloud computing firms only do that. Since online transactions currently account for more than 60% of all commercial transactions, this sector needed a high level of security to ensure efficient and transparent transactions.

Figure 4: Categories of Cyber Security

Consequently, cyber security has gained popularity. Cybersecurity covers a wide range of topics, including cyberspace, in addition to safeguarding data in the IT industry. High levels of security are necessary for cutting-edge technologies like online banking, cloud computing, mobile computing, and e-commerce. These technologies' security has become a top concern since they hold private data about individuals. Sensitive information is among the various types of data that are being stored as a result of the digitization of many aspects of human life, including business, education, and healthcare. Protecting digital data from theft or physical damage while maintaining its availability and confidentiality is known as security. But as technology develops, cybercrime becomes more prevalent and sophisticated. This enormous rise in cybercrime is being caused by a number of factors, including the use of inadequate software, out-of-date security measures, design flaws, programming errors, easily accessible internet hacking tools, a lack of public awareness, high financial return rates, and more. To find the target's flaws and launch an assault on the victim, technical attackers develop ever-more-advanced attack tools. New attacks have emerged as a result, taking many different forms that are challenging to identify. The decentralization of data repositories, the digital nature of the vast amounts of data that accumulate through online transactions, and the growing reliance on the internet in all facets of life have all contributed to the creation of effective security algorithms (Tanikonda et al., 2022). The dynamic nature of cybercrime makes it difficult to anticipate and stop emerging threats. It is the most difficult and stressful profession since internet is full of sophisticated threats. Therefore, learning about security defensive mechanisms, different approaches, and current information security challenges is crucial. Cybersecurity is a set of techniques that have been documented with the goal of safeguarding an organization's or user's online environment. It is in charge of the techniques used to prevent unauthorized access to data, networks, and applications. Since it covers a broad range of technologies and processes, it may also be called information technology security. As people become more dependent on computer systems, including TVs, smartphones, and the numerous little devices that comprise the Internet of Things, the field is growing in significance. These days, cybersecurity is essential to maintaining the safety of our society. On the other hand, cybersecurity is neither a straightforward term nor a clearly defined area of study. Over time, it has developed into a highly cross-border and dynamic field that is impossible to fully understand with a single glance. Protecting critical information infrastructures and enhancing cyber security are essential to the security and economic well-being of any country. Making the Internet safer (and safeguarding Internet users) has become a key component of new service development and government regulation. To tackle cybercrime, a more comprehensive and secure strategy is required. Since technology alone cannot prevent crime, law enforcement organizations must have the tools necessary to properly investigate and punish cybercrime. Many countries and governments are increasingly enacting stringent cyber security legislation to stop the leakage of private information. Everyone needs to learn about cyber security in order to protect oneself from the growing number of cybercrimes.

5. AI FOR CYBERSECURITY

Similar to how AI-systems need new cybersecurity techniques and tools to become more resilient and reliable, cybersecurity may leverage AI to raise awareness, react instantly, and enhance overall effectiveness. This necessitates self-adaptation and adaptability in the face of persistent attacks that change the existing attacker-defender asymmetries. Artificial intelligence (AI) can be used to categorize different attack types, apply observation tactics, and collect lessons learned in strategies that use AI to teach adaptive responses (e.g., notice discrepancies fast and know how to resolve them) at scale.

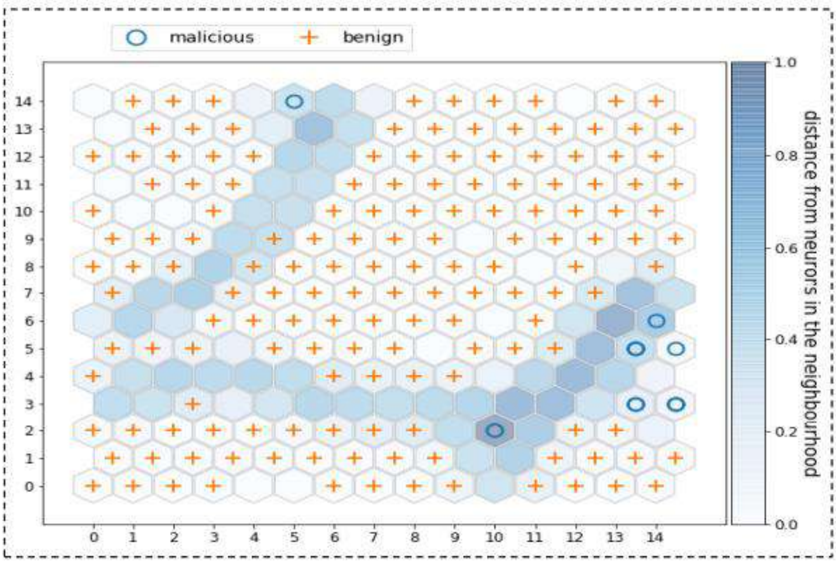


Figure 5: Hexagonal Plot of Webpages Dataset

It is commonly known that networks with tens of thousands of users can be effectively secured by a small team of highly qualified cyber defenders. In addition to offering the domain expertise required to address problems like quality-of-service constraints and system degradation behaviours, AI may expand that same level of system security, making it ubiquitous. In cyber defensive circumstances, AI is likely to be utilized by both attackers and defenders, in contrast to other effective AI uses (such as spam filtering). The incorporation of AI changes the conventional approach of removing vulnerabilities or raising the cost of an attack. Autonomous and semiautonomous (human-in-the-loop) systems must be prepared for the worst-case scenarios, as well as anticipate, react to, and evaluate possible and actual risk events. AI-based judgments affect a wide range of stakeholders, including data owners, service providers, and system administrators. Important issues include how stakeholders are consulted and informed about autonomous operations, as well as how decision-making is allocated and limited.

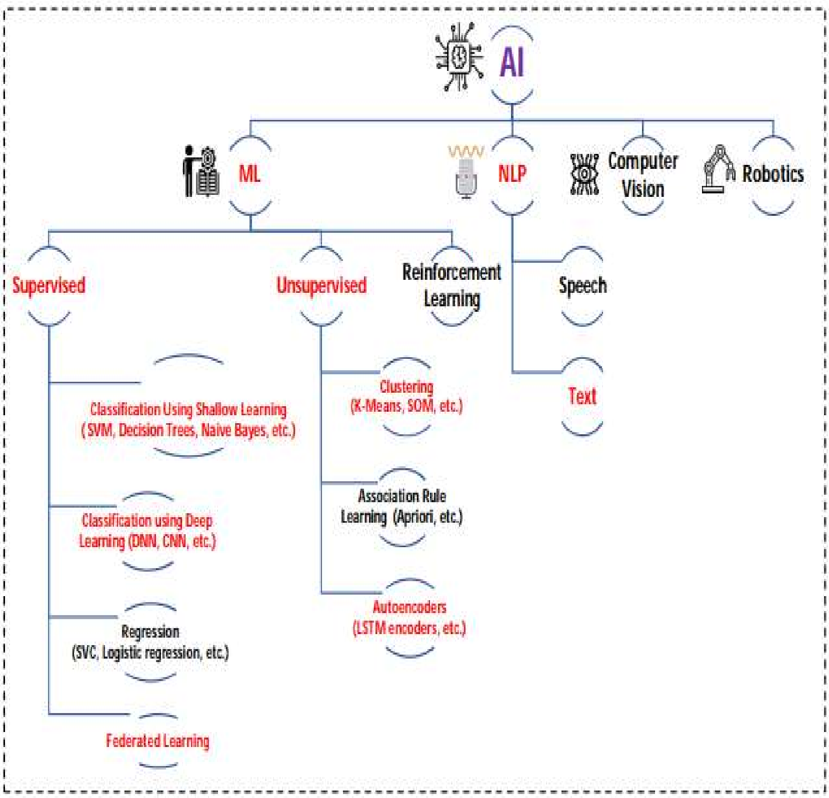


Figure 6: Components of AI in Cyber security

Attackers may employ traditional deterministic planning in a stable cyber environment, planning under uncertainty in an uncertain cyber environment, and artificial intelligence (AI) to learn how to attack, conduct reconnaissance, gather information, and formulate strategies when little is known about the environment. Today's technology systems generate vast volumes of data, which artificial intelligence can gather and evaluate (Kavitha & Thejas, 2024).

AI has the potential to reduce hazards and increase accuracy in biometric authentication systems. On the other hand, privacy violations could arise from AI's surveillance of behavioural patterns. To develop strategies that address the technological and ethical aspects of AI-assisted identity management, as well as the possibility of abuse, more research is needed.

6. IMPORTANCE OF THE STUDY

In order for a computer to solve a problem, an algorithm that is sufficiently effective must first be created and then included into the hardware or software. Not every problem has a direct algorithm, and in those situations where the algorithm cannot be found, a direct programming approach cannot be used to solve the problem. By offering the opportunity to solve issues in situations where methods cannot be manually constructed, machine learning (ML) broadens the scope of computer work. It is possible to define an algorithm as non-constructive by using examples of appropriate behaviour. ML algorithms are thus described as a meta-algorithm for creating algorithms from given information that describes what they should produce (Kavitha & Thejas, 2024).

Because these algorithms simply provide computing data rather than computing algorithms, they provide a far superior method for interacting with computers. Increasing the ability to solve computer problems is a good enough reason to study machine learning, but it's not the only one. Understanding what can be practically calculated is encouraged by learning, and studying computation can also help people understand learning. As a scientific field, machine learning (ML) studies the computer underpinnings of learning. In addition to providing insight into our understanding of the mind, attempting to address problems using computational models of learning can also serve as inspiration for the creation of machine learning models. Researching machine learning (ML) provides scientific importance as a way to comprehend learning and computation together. However, science must have a positive impact on the world in order to be meaningful. Possibilities for expanding ML research include improving the world, which can be achieved by consistently maintaining a connection with pressing real-world issues. Numerous specific problems of practical and commercial significance can be resolved by ML approaches. Our only goal as researchers is to advance science, so perhaps we can start with a novel approach and then look for a problem it can answer, or we can start with a problem and then take the required actions to address it. Excellent study will be conducted in both situations, allowing us to recognize the key elements of the issue and comprehend the benefits, drawbacks, and constraints of current frameworks. The use of deep learning (DL) techniques to address cyber security issues is covered in the body of this thesis. Testing the limits of models based on DL architectures on a variety of cyber security problems, comparing the results with traditional machine learning algorithms, figuring out how well successful recipes generalize across problems, and expanding the techniques as necessary to make them effective by introducing new approaches where appropriate are the objectives of the research work documented in this thesis. The primary goal of the research project is to apply AI systems to a variety of cyber security issues that are deemed realistic and challenging enough to be of practical importance.

6.1. Scope of Study

There are serious concerns about how artificial intelligence may affect crime and criminal justice given its growing capabilities and apparent proficiency at tasks that were previously only performed by humans. AI has the potential to change not just how crimes are committed but also how the criminal justice system and law enforcement are run. Naturally, as AI will affect every aspect of human behaviour, these significant changes are not limited to the administration of justice. Concerns regarding the gaps between criminals and law enforcement as a result of offenders engaging in high-tech crimes necessitated that criminal justice be equally prepared and equipped to use technology like artificial intelligence (AI) to promote crime prevention and control.

6.2. Application of AI in Cyber Security

AI as a Legal Personality

When considering the legal and regulatory ramifications of adopting artificial intelligence, the primary question to consider is whether new laws are necessary to regulate these technologies or if the existing legal structure is sufficient to handle any potential legal issues. For example, who will be responsible for any criminal culpability resulting from AI's actions? Under the current legal system, a robot or artificial intelligence program cannot be held responsible or liable if a third party is hurt as a result of any action or inaction on the program's part. Let's take an example where an artificial intelligence program controls a self-driving automobile and it gets into an accident. Two guys lost their lives in an autonomous Tesla vehicle crash in November 2021. In this case, how will the culpability be divided? An entity's personhood is a crucial legal consideration when allocating rights and responsibilities. Personhood can be legal or natural, and anything in between is a tool, an instrument, an agent, etc. From the perspective of determining who would ultimately be responsible for the consequences of an act or omission, personhood attribution is crucial.

AI Forensics for Crime Detection

The process of trying to determine whether or not specific crimes are being or have been committed is known as crime detection. AI is capable of resolving this issue. In an attempt to extract DNA profiles and ascertain if a DNA sample was inadvertently transferred or directly from an individual present at the crime scene, more sophisticated artificial intelligence (AI) algorithms are being developed. However, since it is now hard to determine how this AI comes to its judgments, there may have been a breach of the fundamental legal requirement that evidence be subject to inspection.

Gunshot Detection

Witnesses and roving police officers frequently hear "shots fired!" but determining the precise location of the gunfire takes important time when every second counts. The goal of gunshot detection software is to identify when gunfire occurs and pinpoint the exact position of the shot. In order to identify and isolate the staccato sounds of gunfire, acoustic gunshot detection systems usually employ a collection of microphones placed across densely populated regions. These noises can then be verified by people, who may subsequently alert law enforcement to the location of the gunshot. When police in Fresno, California, used Shot Spotter to apprehend a killer in 2017, it had a significant impact. Thanks to technology, authorities were able to trace down the murderer and capture him in 4 minutes and 13 seconds.

Predictive Policing

Artificial intelligence technology supports the application/tool known as predictive policing. These tools are currently being used by law enforcement agencies and investigative teams worldwide to stop crimes from occurring. These programs use sets of data amounts that have undergone analytical processing to analyse the data from the accessible criminal records. Through such data analysis, the goal is to foresee crimes and areas that are vulnerable to them, as well as to identify the likely targets of threats in order to reduce potential dangers. Therefore, to accomplish the goal, these systems analyse copious amounts of police data, including past crime data, which is gathered to identify potential crime hotspots.

Following the identification of hotspots or possible criminals (individuals or groups) who may commit crimes, law enforcement agencies are deployed to stop crimes from happening. Therefore, rather than repairing the harm caused after a crime has been committed, the goal of these tools utilized in law enforcement is to prevent the crime from happening in the first place. By offering risk evaluations, predictive policing seeks to deter crime; yet, these risk assessments are not without their own hazards. One of the worries is that because risk analyses frequently lack transparency and the capacity to explain, it is impossible to appropriately balance the risks of crime prevention with the risks of crime prevention. This could result in disproportionate violations of the right to privacy and the related rights to equal treatment in equal circumstances as well as protection from stigmatization, discrimination, and stereotyping.

Bail Proceedings and Predictive

The foundation of India's bail regulations is judicial discretion. Many different people have criticized the use of discretion and judgment in bail proceedings. Some have criticized the courts for giving the "gravity" of the offense too much weight. In the 2012 case of Sanjay Chandra vs. CBI16, the Supreme Court ruled that an accused person's request for bail should not be denied only on the basis of the seriousness and gravity of the offense. However, when determining whether to grant or refuse bail, consideration should be given to elements crucial to carrying out an effective investigation and whether the accused constitutes a flight risk. It was recently reaffirmed by the Supreme Court in Prabhakar Tewari v. State of U.P. & Ors17. The 2017 Law Commission Report on Bail in the Code of Criminal Procedure states that when performing a risk assessment during the bail process, the kind and gravity of an offense should not be considered. However, in their risk assessment, various sessions courts, high courts, and even the Supreme Court usually ignore this legislative requirement in bail jurisprudence and prioritize the nature of the offense.

Improving the Efficiency of Prisons & Correctional Services

In order to reform prisoners and reintegrate them into society at large, correctional facilities are essential. However, it has been noted that jails are increasingly being used by criminals and mafias as a location to plot and carry out crimes. Cell phones, firearms, cigarettes, and other items are being accessed by prisoners without authorization. The jail administration finds it difficult to keep a careful eye on these kinds of activities. However, activity within the jail premises can be closely watched with the use of UAVs and an AI-powered surveillance system.

7. CONCLUSION

The Internet has ushered in the information age and surpassed human civilization over the last 20 years. These days, cyberspace is a vital and necessary component of our ecology and our daily lives. But as more people use the Internet, it has also turned into a haven for hackers who are always posing new and dangerous risks to computer systems. Numerous computing platforms, including PCs, laptops, tablets, smartphones, Internet of Things devices, etc., are the focus of these threats. Despite their best efforts, security organizations around the world are unable to keep up with the increasing complexity and diversity of these threats. The development of clever cognitive systems over the past ten years, signalled by artificial intelligence (AI), gives cybersecurity organizations hope that cyber-attacks can be contained. A step in that direction is this effort. This thesis's study focuses on the nexus between cybersecurity and artificial intelligence. It investigated a number of traditional machine learning and deep learning techniques for classifying webpages, including the use of both structured and unstructured raw web content as input. It created effective machine learning models for identifying fraudulent websites, outperforming earlier comparable methods in terms of classification outcomes. The thesis uses machine learning to analyse the security of hybrid apps on mobile platforms. Recommendations are made to enhance these apps' security architecture in light of this stud.

REFERENCES

[1] Ijiga, O. M., Idoko, I. P., Ebiega, G. I., Olajide, F. I., Olatunde, T. I., & Ukaegbu, C. (2024). Harnessing adversarial machine learning for advanced threat detection: AI-driven strategies in cybersecurity risk assessment and fraud prevention. *J. Sci. Technol*, *11*, 001-024.

[2] Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: Challenges and opportunities. Artificial Intelligence Review, 54(5), 3849-3886.

[3] Aminu, M., Akinsanya, A., Oyedokun, O., & Tosin, O. (2024). A Review of Advanced Cyber Threat Detection Techniques in Critical Infrastructure: Evolution, Current State, and Future Directions.

[4] Sharma, B. P. (2024). Evaluating the Role of Artificial Intelligence in Enhancing Cyber Threat Detection and Response Mechanisms. *Journal of Digital Transformation, Cyber Resilience, and Infrastructure Security*, *8*(12), 1-10.

[5] Vaddadi, S. A., Vallabhaneni, R., & Whig, P. (2023). Utilizing AI and machine learning in cybersecurity for sustainable development through enhanced threat detection and mitigation. *International Journal of Sustainable Development Through AI, ML and IoT*, *2*(2), 1-8.

[6] Galla, E. P., Rajaram, S. K., Patra, G. K., Madhavram, C., & Rao, J. (2022). AI-Driven Threat Detection: Leveraging Big Data for Advanced Cybersecurity Compliance.

[7] Madhavram, C., Galla, E. P., Sunkara, J. R., Rajaram, S. K., & Patra, G. K. (2022). AI-Driven Threat Detection: Leveraging Big Data for Advanced Cybersecurity Compliance.

[8] Reddy, A. R. P. (2021). The role of artificial intelligence in proactive cyber threat detection in cloud environments. *Neuro Quantology*, *19*(12), 764-773.

[9] Lekkala, S., Avula, R., & Gurijala, P. (2022). Big Data and AI/ML in Threat Detection: A New Era of Cybersecurity. *Journal of Artificial Intelligence and Big Data*, *2*(1), 32-48.

[10] Srinivasulu, A., & Venkateswaran, R. (2023). Enhancing cybersecurity through advanced threat detection: a deep learning approach with cnn for predictive analysis of ai-driven cybersecurity data. *Journal of Research in Engineering and Computer Sciences*, *1*(5), 65-77.

[11] Manoharan, A., & Sarker, M. (2023). Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection.

[12] Salem, A. H., Azzam, S. M., Emam, O. E., & Abohany, A. A. (2024). Advancing cybersecurity: a comprehensive review of AI-driven detection techniques. *Journal of Big Data*, *11*(1), 105. https://doi.org/10.1186/s40537-024-00957-y

[13] Yaseen, A. (2023). AI-driven threat detection and response: A paradigm shift in cybersecurity. International Journal of Information and Cybersecurity, 7(12), 25-43.

[14] Tanikonda, A., Pandey, B. K., Peddinti, S. R., & Katragadda, S. R. (2022). Advanced AI-Driven Cybersecurity Solutions for Proactive Threat Detection and Response in Complex Ecosystems. *Journal of Science & Technology*, *3*(1).

[15] Kavitha, D., & Thejas, S. (2024). Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation. *IEEE Access*.

Chapter-III

NEXT-GENERATION FIREWALLS: ARCHITECTURE AND EFFECTIVENESS

Dr. Meera Arvind, Professor of Information Security, Vellore Institute of Technology (VIT), Vellore, India.

Dr. Arjun Nair, Professor of Information Security, Vellore Institute of Technology (VIT), Vellore, India.

Abstract--- IT is developing at an astonishing rate, which has significantly altered the distributed network's perimeter. Therefore, the conventional ideas of security are insufficient. Port-based firewalls are now essentially worthless since smart cyber threats are emerging to take advantage of the weaknesses in traditional security tools as more and more companies use analytics, cloud computing, and other automation tools to accelerate the development of new goods and services to satisfy consumer demand. Advanced firewalls such as Web Applications firewalls (WAFWs) and next generation firewalls (NGFWs) have been developed to address these issues. With an emphasis on extra features like DPI, application filtering, and AI implementation, this article aims to explain how NGFWs evolved and integrated with cloud solutions. Accordingly, this study evaluates the effectiveness of AI-based firewalls in fending off contemporary cyberthreats by utilizing advanced techniques such as machine learning and deep learning. The study looks at AI-based firewalls' ability to provide consistent performance in dynamic networks and focuses on how well they work in the cloud. This study illustrates the real performance of various AI-based firewall architectures, including their capacity to identify threats, false positives, and time consumption, without any theoretical simulation. Along with discussing potential disadvantages and potential changes, the article also examines the problems associated with using these advanced firewalls in cloud systems. In order to defend the current complex enterprise environments, including the usage of cloud services, this research provides a literature evaluation of the NGFWs and WAFWs and their relevance. The results broaden our understanding of cyber security management and point to AI's potential as a crucial facilitator of resource management, growth, and detection in the context of cloud security.

Keywords--- Artificial Intelligence, Firewall, Security, Cloud, Cyber Security.

1. INTRODUCTION

The fast digitization of information and the growing popularity of cloud computing are reflected in two main changes in security. The idea of a distinct network border is thus becoming less evident as more businesses store their data in the cloud and use it to process big data. Everyone working in the fields of information security and maintaining the integrity of digital environments now faces a new level of difficulty as a result. Conventional security measures, particularly firewalls, have significant shortcomings when it comes to containing emerging dangers and characteristics of contemporary cyberthreats (Jaggernauth & Rocke, 2021). The cyber security sector has developed Next-Generation (NGFWs) to address these issues. NGFW integrates more in-depth analyses including deep packet analysis, application filtering, and IPS systems, in contrast to traditional firewall systems, which are primarily concerned with filters based on rules and ports. These characteristics allow NGFWs to function as more advanced layers for managing network traffic and providing improved detection and defence against cutting-edge cyberthreats (Liang & Kim, 2022). The other essential element of NGFWs that provides real-time defence against both known and unknown threats is an intrusion prevention system (IPS). IPS features are essential for gradually detecting, let alone stopping, network unwanted traffic before it has a chance to cause significant harm in the cloud, where the "addressable space" is much larger. Apart from their email security characteristics, NGFWs also prevent malware and phishing, which are still frequent attack methods (Gudimetla et al., 2017). On the opposite end of the spectrum, NGFWs contain anti-malware and web filtering features that safeguard people browsing the internet from websites that are harmful to cloud-based users. Because Threat Intelligence may provide real-time information on newly-formed threats that can be integrated into the NGFW, it also enhances the performance of firewalls. Last but not least, Deep Packet Inspection (DPI) enables NGFWs to see the data being transferred over the network and have an opportunity to remove any malicious traffic, even when it is encrypted. The entire world is now separated into different networks for communication, information sharing, financial transactions, and other purposes (Audin, 2004). The enormous expansion of computer networks and systems has made people and businesses more reliant on the data that is saved and shared through these systems. As a result, it becomes essential to safeguard not only the computers, the data they contain, and the different resources that are connected to them, but also to guarantee legitimacy and prevent attacks on the network and computers (Thu et al., 2023). To put it simply, a computer network is an interconnection of digital telecommunications that allows the different nodes to share resources. Any device that can transfer data, such as computers, routers, switches, etc., can serve as a node. For data to flow between these nodes, a data link is necessary. Wireless media or a cable can be used to connect the nodes to one another. Another way to think of a network is as an anthology of connected entities (Lei, 2024).

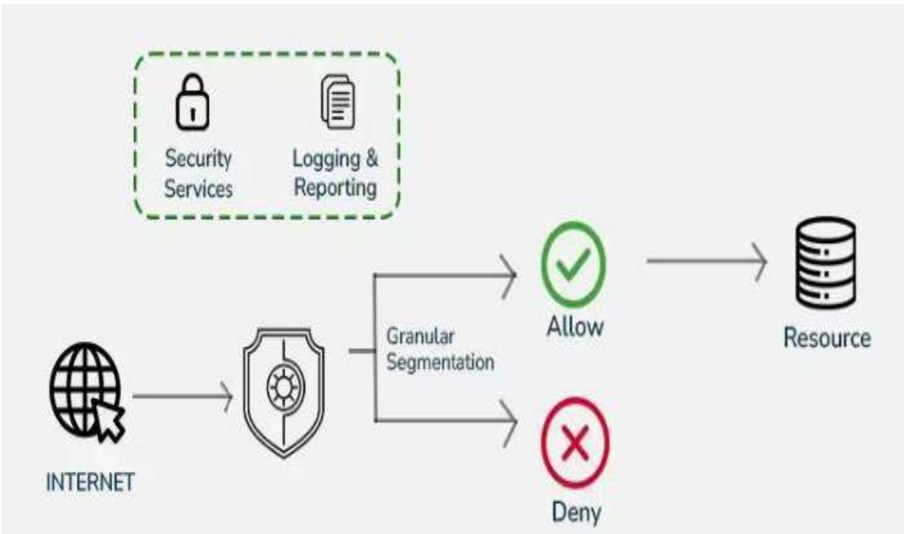


Figure 1: Next Generation Firewall

In a more straightforward manner, packets are sent over these established channels from one device to another. A packet is sent by one device and received by the other. If these packets are not interfered with, there is no issue; however, this is not always the case. Our concerns about the security of data packets and, consequently, networks from numerous dangers were heightened by the transmission of data across these communication channels. Using a firewall is the most fundamental and straightforward method of protecting our computer systems and network (Thu et al., 2023). Firewalls have been the first line of defines for the required safety and protection ever since we became concerned about protecting our networks and systems. A computer firewall is used to guard against deliberate intrusions that could jeopardize confidentiality, cause data corruption, or cause a denial of service on a computer, whether it is networked or standalone. The security mechanisms known as firewalls are in charge of guarding our networks and personal computers against malicious malware, hackers, and intruders. They shield us and our networks against malicious malware that could infiltrate our computers or from snoopy hackers (Singh & Singh, 2023).

2. REVIEW OF LITERATURE

Yao, (2013) created a lightweight multicast authentication system for small-scale Internet of Things applications and updated the original Nyberg's fast one-way accumulator.

SE-AKA, a safe and effective Authentication and Key Agreement (AKA) protocol, was suggested by Lai, (2013) and is compatible with all group authentication scenarios in LTE networks. In particular, SE-AKA implements an asymmetric key cryptosystem to safeguard user privacy and employs Elliptic Curve Diffie-Hellman (ECDH) to provide KFS/KBS (Fathia, 2024).

The extent of the DDoS flooding assault issue and efforts to mitigate it were examined by Zargar, (2013). Based on where and when they stop, identify, and react to DDoS flooding attacks, it categorized the attacks and ranked the current countermeasures.

Thus, RSA, the most popular public key cryptography technique, serves as the foundation for Kothmayr's, (2013) suggested security strategy. It is intended to operate on common communication stacks for Low Power Wireless Personal Area Networks (6LoWPAN) using UDP/IPv6 networking.

The Fuzzy Attribute-Based Signcryption (FABSC), a unique security technique that appropriately balances security and elasticity, was created (Hu Chunqiang, 2013; Ilyasov, 2024).

Zhou, (2013) suggested a secure and effective routing system for WSNs that relies on authentication and encryption. By shifting routing-related responsibilities to the BS, BEARP specifically reduces the burdens on sensor nodes. This not only preserves network-wide energy equivalency and increases network lifetime, but it also enhances the security mechanism that the secure BS performs exclusively.

Shin et al., (2015) suggested a simple method of authentication. Additionally, in order to fend against potential attacks in ubiquitous networks, the technique offers secure password updates, session key agreement, and mutual authentication between entities (Islam et al., 2023).

Imran Memon et al. (2015) suggested using an asymmetric cryptographic approach to protect user privacy and provide safe connection. Because the asymmetric cryptography scheme is strong against this kind of attack by providing mutual authentication, the authors were able to tackle the wireless communication problem in the A3 algorithm, such as eavesdropping, and make the system more secure.

Gope et al. (2015) suggested an enhanced protocol of Wen et al. (2013) that is resistant to a number of known attack types, including replay, forgery, known session key, backward, and forward secrecy, among others.

For safe data transmission in military heterogeneous wireless sensor networks (MHTWSN), Kumar et al. (2017) suggested a new secure multipath routing protocol (NSRP). To find trusted neighbour nodes and create secure multiple routes for dependable data delivery in MHTWSN, NSRP employs elliptic curve cryptography (ECC) (Freet & Agrawal, 2016).

A new method was presented by Pandi Vijayakumar et al., (2017) to enhance VANETs' current authentication functionality. The first privacy-preserving method in this suggested framework is anonymous authentication, which not only authenticates the vehicle user anonymously but also maintains the integrity of the communications being transmitted.

In order to implement Secure Multiparty Computation (MPC) and Fully Homomorphic Encryption (FHE) in Smart Grid (SG) Advanced Metering Infrastructure (AMI) networks that are constructed utilizing wireless mesh networks, SametTonyali et al. (2018) suggested new protocols. By encrypting the data (FHE) or calculating its shares on a randomly generated polynomial (secure MPC), the suggested methods hide the smart meters' (SMs') reading data (Kokko, 2017).

The suggested approach by Sravani Challa et al. (2018) covers functionality aspects such the inclusion of dynamic sensor nodes, password and biometric updates, smart card revocation, and other standard capabilities needed for user authentication in wireless sensor networks.

Using intelligent software agents, neural networks, genetic algorithms, neuro-genetic algorithms, fuzzy techniques, rough sets, and particle swarm intelligence, Sannasi Ganapathy et al. (2013) conducted a survey on intelligent methods for feature selection and classification for intrusion detection in networks (Manda et al., 2023).

By identifying attack characteristics, Louvieris et al., (2013) introduced a novel anomaly detection technique that can be utilized to identify hitherto unidentified network attacks. To improve the situational awareness of cyber network operators, this effects-based feature identification technique integrates k-means clustering, Naive Bayes feature selection, and C4.5 decision tree classification in a unique way to identify cyberattacks with high accuracy.

3. DIFFERENT APPROACHES FOR THREATS

Deep Learning Approaches for Threat Detection:

Choosing the most cutting-edge AI models and algorithms, particularly those based on deep learning, is the first step towards the launch of next-generation AI-based firewalls. CNNs and RNNs are selected to evaluate high-level temporal and spatial characteristics and to identify indications of the emergence of new threats. These deep learning techniques aid in improving real-time threat detection capability, which in turn raises accuracy.

Integration with Cloud Infrastructure for Real-Time Analysis

The models and AI algorithms that have been chosen are seamlessly integrated into cloud platforms to enable real-time network traffic analysis. Its scalability, data processing skills, and capacity to start integration on various cloud platforms are some of the problems that need to be resolved in this regard. The deployment ensures that AI-based firewalls can maintain a continuous level of protection against threats while also utilizing cloud flexibility to scale up or down in response to demand.

Auto-Scaling Based on Network Traffic Patterns

Intelligent scaling techniques are used to scale the AI firewalls dynamically based on traffic volumes in order to handle the cloud's ever-changing nature. Additionally, the system loads and balances incoming network traffic and boosts the firewall's power in case of a spike. This adaptive scaling feature enables the firewall to minimize resource consumption when not in use and operate at peak efficiency during periods of high traffic (Pavlović et al., 2023).

Dynamic Allocation of Resources for Optimal Performance

In order to improve AI firewall performance, it also adjusts additional dynamic resource allocations on top of the implementation. This means that CPU, memory, and network resources can be dynamically allocated based on the risks and load at any given time. The firewall operates at its best when resources are allocated flexibly, accommodating any network modifications without compromising its functionality.

Real-Time Threat Intelligence Integration

Among these is continuous monitoring, which is the implementation's main component and is aided by real-time threat intelligence feeds. As new threats emerge, the AI-based firewalls are aware of them and employ innovative tactics to combat them. By addressing newly developing cybersecurity risks, the integration of real-time threat intelligence enhances system performance.

Automated Updates to Ensure Protection against Emerging Threats

Automated update features are also included in the implementation. The threat database, security updates, and new algorithms can be downloaded and updated on a regular basis by an AI-based firewall. Without additional human intervention, this automation guarantees that the firewalls remain proactive in the face of emerging threats. Updating ensures both the longevity of the security structures and their general productivity.

Adaptability to New Threats

The NGFW is one of the most valuable resources in the current cyber environment, particularly with the move to the cloud. Since NGFWs have extra layers of functionality that are novel and solve current security challenges, this runs counter to standard firewalls. NGFWs are essential in the context of the cloud because cloud solutions have increased the demand for all-encompassing security solutions for distributed and dynamic infrastructures. VPN technology, which provides safe remote access to cloud solutions, is another facet of NGFW. This is crucial because it protects data transmission procedures from being intercepted by unauthorized users, which is especially critical for businesses with employees from several locations. Furthermore, only authorized apps can access additional sensitive data or network zones thanks to Application Control, which enables NGFWs to regulate the apps running in the cloud environment. Other fundamental components of NGFWs that address the prompt identification and mitigation of known or emerging threats include Intrusion Prevention Systems (IPS). The typical IPS capability to detect and stop malicious activity before it happens is crucial in the cloud, where the attack surface is much greater. Along with the characteristics outlined in E-mail Security, NGFWs protect against malware and phishing attacks, which are commonly disseminated via email, which is still one of the most efficient attack vectors (Rao et al., 2022).

4. ANALYSING VARIOUS AI-BASED FIREWALL STRATEGIES

Numerous significant flaws were discovered through the analysis of different AI-based firewall tactics, which must be noted in order to progress the development of AI-based cybersecurity products. For this reason, comprehension of the outcomes of specific deep learning structures is one of the most notable deficiencies. These models include CNNs and RNNs, which are very accurate and flexible. However, it is challenging to understand how these large neural networks make decisions. Future problems and difficulty in determining the specific cause of false positive results or how the models arrived at particular hazard ratings are presented by such opacity. Because interpretability and accountability are essential in such circumstances, it is necessary to overcome this weakness if the trustworthiness of AI-based firewalls is to be decreased. One of the aforementioned drawbacks is that machine learning techniques are susceptible to the idea drift phenomena, particularly those that make use of substantial volumes of data from prior experiences. The underlying nature of threats has changed as a result of shifting cyber security conditions; new strategies and directions have emerged. It is clear from analysing these kinds of situations that machine learning, which relies on data from earlier situations, can cause models to react slowly to novel dangers, potentially leading to a large rise in false negatives. This shortcoming highlights the need for dynamic retraining, sometimes continuous model updates, and real-time threat intelligence integration to combat the ever-evolving nature of these attacks in the context of contemporary AI-based firewalls (Neupane et al., 2018).

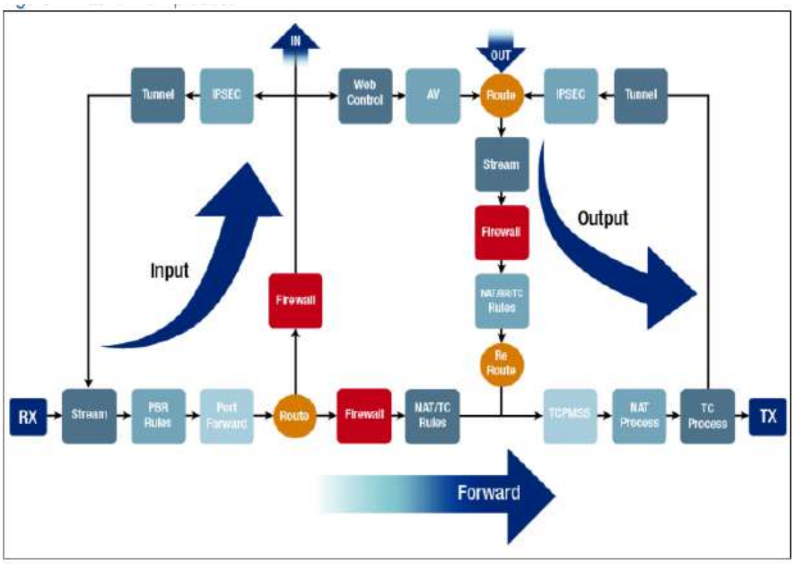


Figure 2: Packet Flow Process

Furthermore, the study exacerbated problems related to the use of specific machine learning algorithms in extensive networks. Some machine learning algorithms are unable to manage the Volume, Variety, and Velocity features of increasingly complex network structures, which results in a bottleneck and jeopardizes real-time threat identification. The practical implementation of AI-based firewalls and the adaptation of anti-malware measures to the ever-increasing demands of contemporary networks depend heavily on the issues surrounding scalability; therefore, technological advancement is required to create an AI-based firewall that can function in large and complex networks (Patel et al., 2024).

Proposed Improvements

Improving Interpretability and Transparency: Deep learning models' decision-making process can be better understood by incorporating explain ability approaches like layer-wise relevance propagation or attention mechanisms. Generally speaking, cybersecurity experts can have confidence in the choices made by AI firewalls when they see visualizations that offer more information about the characteristics influencing the model's output.

Mitigating Concept Drift

The robustness of the AI-based firewall can be increased with the use of dynamic retraining of the model using recent datasets, continuous learning mechanisms, and the integration of threat intelligence data. Additionally, there are self-tuning algorithms that adjust the model parameters in response to new threats.

Improving Scalability

By utilizing innovative solutions created by parallel processing and computing dispersion, some of the scalability problems can be addressed. Machine learning algorithms must be developed with parallel processing in mind, utilizing cloud and edge computing technologies, in order to increase their scalability.

Fortifying Against Adversarial Attacks

AI-based firewalls would be more resilient to hostile activities if they used a range of defense techniques, regularly updated the adversarial database, and used adversarial training procedures.

Human-Centric AI Models

Through the use of AI models that mimic human behaviour patterns, threat detection becomes more accurate and employs fewer false positive modes.

Ensuring Regulatory Compliance

It would be easier to comply with the established regulatory standards if AI-based firewalls have integrated reporting and auditing functionalities. When constructing AI firewalls, legal and ethical considerations may be eliminated with the assistance of legal and regulatory experts.

4.1. Types of Attacks on a Network

Although they present some risks, networks—both intranet and internet—offer incredible opportunities. Information is vulnerable to various threats or attacks in the absence of appropriate controls. Viruses, worms, and trojans were major threats in the early days of computers, but these slowly developing threats have since been replaced by threats that spread quickly—within 15 minutes. Current attacks are far more covert than they were in the past due to the way that today's online threats are evolving. Attackers are drawn to the network's information and resources, which make them desirable targets. A network is considered secure if all of its systems and resources can withstand attacks of any kind. In the event of an attack, a system or network must be able to minimize the harm and quickly recover. Communication surveillance (passive attacks), active network assaults, close-in attacks, exploitation by the systems within the network, and attacks via the service provider are some examples of attack classifications. Below, many attack kinds are covered (Lamdakkar et al., 2024).

Passive Attacks

Unencrypted communication is watched for sensitive data and cleartext passwords in these types of attacks. Monitoring unsecured communications, traffic analysis, gathering authentication data, and decrypting traffic that has been inadequately encrypted are a few examples. Adversaries are able to predict future activities through passive interception of network processes. Without the user's consent, it could lead to the disclosure of data files or information to the attacker. Adversaries are able to predict future activities through passive interception of network processes. Such attacks are typically an effort to exploit the data that is accessible through the system. It won't negatively impact the system's resources.

Active Attack

In these types of assaults, attempts are made to get around or compromise the systems that are part of the secured networks. Trojan horses, worms, viruses, and stealth can all be used to do this. In order for the available information to be stolen or altered, attempts are made to circumvent the security measures and install harmful code. These attacks attempt to intercept data while it is in transit or attempt to gain access to the target network by a remote user who has been granted permission. It could lead to data tampering, Denial of Service, or the distribution of data files. Usually, the goal of such assaults is to damage the system's resources and interfere with its functionality.

5. PROXY FIREWALL

In contrast to packet filter firewalls, which only examine packets without changing them, proxy firewalls serve as a mediator in all connections that are made through them between the internal and external networks. As a result, it prevents direct communication between the machine or device making the request and the one providing it. On behalf of the asking machine, the proxy server instead obtains the data from the providing machine. Additionally, it has the ability to store these data in its memory, allowing it to supply the same data upon request from another internal network device without physically visiting the computer in question. Stated differently, an internal network's systems are all represented by a single address. Other computer systems within a network can use a shared Internet connection thanks to a hardware device on the network. Clients generate requests, which are then accepted by the proxies and either sent to the server or handled by the cache. These proxies are also known as "gateway" or "server.".

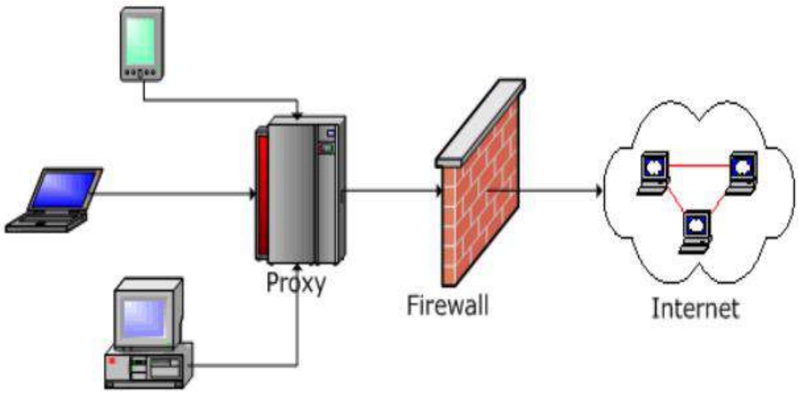


Figure 3: Proxy Firewall

Its primary purpose is to offer security from the outside network. It controls the packets entering and leaving the network. Client requests are filtered, cached, logged, and managed by firewall proxy servers. It is employed to limit connections from a proxy to the source server within the local area network (LAN) or to the external network (internet). It differs from a traditional firewall in that it only offers one address and limits connections from the outside world. To put it simply, a proxy essentially performs the following tasks:

1) Sends the request to the server located in the external network or
2) non-trusted zone after receiving it from a system within the internal network or trusted zone (intranet).
3) Reads the server's answer to the request after receiving it.
4) Returns this response to the client if it is safe to do so.

The two primary operating layers of a proxy server are the application layer and the transport layer. As a result, they fall into two categories: circuit-level gateways, which are proxy servers that operate at the transport layer, and application gateways, which are proxy servers that operate at the application layer.

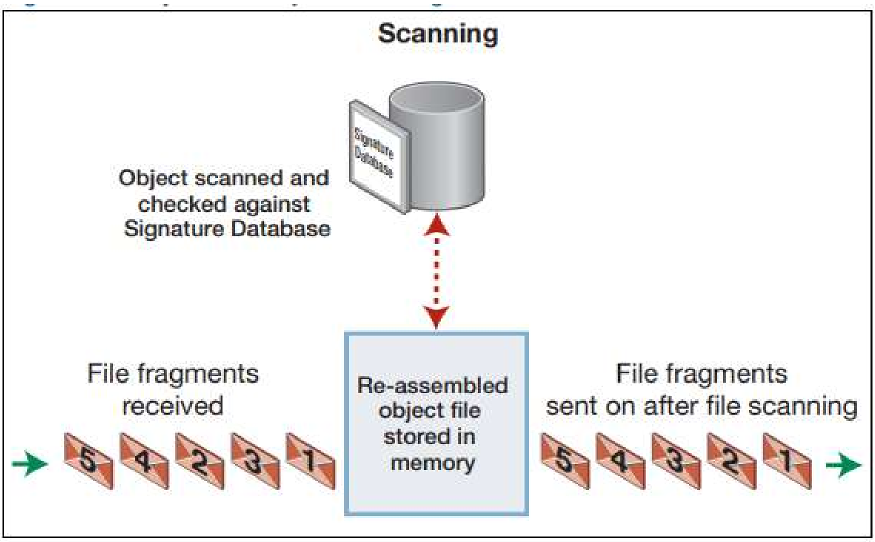


Figure 4: Proxy-based Object Scanning

5.1. Circuit Level Proxy

Similar to application-level proxy firewalls, they always establish a new connection after receiving connections from clients, rejecting some and accepting others in accordance with the policies. Although users perceive this procedure to be transparent, it is actually not as transparent as it may be. The circuit level proxy firewall was created to get around this and boost speed. Because the proxy establishes an end-to-end connection between the client and the target application, the connection between the client and the server is a virtual circuit. TCP connection relays are provided by circuit level firewall proxies. These circuit level proxies finish the handshake procedure by intercepting the TCP connections being made to a host behind them. Traffic begins to move from the server to the client and vice versa as soon as the firewall allows a connection to be made. The firewall is in charge of making sure that only the authentic packets from the established connection pass through. Because circuit level firewalls don't verify any data or the packet's payload, they are sufficiently quick. In essence, circuit level firewalls make sure that the handshake procedure is correctly finished before the connection is established. These firewalls do not allow the use of payload data in the higher-layer conventions to restrict access, nor do they allow access confinements to be imposed on conventions other than TCP (Mukkamala et al., 2020).

5.2. Application-level Proxy

This particular proxy server firewall allows application-layer admission control. They capture the requirements that the network's applications are requesting and carry out the necessary actions to fulfil the request. All of the results are then returned to the application that made the request, verifying that it was handled correctly. As a result, the different apps are given a high degree of security without having to communicate directly with servers that are not part of the network. A separate proxy is required for service. It can thoroughly examine incoming and outgoing data packets even at the application level because it is there and functions at that level. Some apps may even be prohibited from accessing the computer network. Every communication and network action carried out by the apps is also recorded in a log. The application-level proxy flow scenario is shown in detail in figure 1.18. The firewall interprets any client request as though it were coming from the serving device.

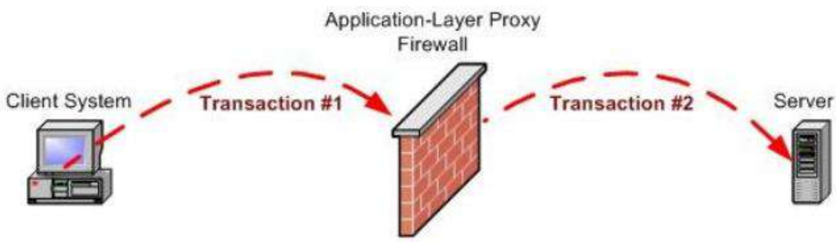


Figure 5: Application-Level Proxy Firewall

6. LATEST TECHNOLOGIES AND FIREWALL

We are no longer restricted to wired networks alone. Various technologies have been developed for network formation. Some of them have been covered below:

Wireless Sensor Networks

In order to monitor certain ecological, physical, or medical conditions, WSNs (Wireless Sensor Networks) are composed of specialized wireless sensor nodes that are spatially circulated throughout the environment. These nodes may include cameras for vision, mouthpieces for sound, and temperature sensors. WSN nodes are typically wireless, albeit they may or may not be mobile over time. A sensor, communication antenna, microprocessor, and power source make up a WSN node. A wireless sensor network is made up of these nodes that communicate with one another on the fly to send the data they have collected to a base station that serves as the network's command and control center. There are two possible modes of communication between the nodes and the base station: one-way, or simply from the nodes to the base station, or two-way. Since WSNs are frequently utilized in fields like environmental/earth sensing, air pollution monitoring, forest fire detection, health monitoring, etc., they are the most useful kind of ad hoc networks available today. WSNs serve as the foundation for many smart city initiatives and the Internet of Things which is thought to be the next major advancement in ICT after the creation of the internet, www, and smartphones. By combining data from multiple sensors, WSNs are able to gather accurate and varied environmental data across a vast area. Furthermore, the UC's scope zone and application domain are expanded by the combination of Smart WSNs with a larger network, such as the Internet. Any object that moves or is placed immobile could have sensors attached to it. Security has always been a fundamental concern in the field of networking, and wireless sensor networking scenarios are no exception. In actuality, security in this kind of setting necessitates greater emphasis than has been observed in conventional systems. Compared to typical computing scenarios, there is a far higher chance of security threats being introduced as wireless networks and other system scenarios have been integrated into computer processing environments. Security is risk management, according to. The assessment of threats, vulnerabilities, and attacks, the determination of costs associated with the threats and the evaluation of all the different attacks given the vulnerabilities, and the development of appropriate safeguards and countermeasures are the primary areas of security attention. All of this is done based on the cost versus the likely loss that the risk will produce. The majority of experts categorize security issues into three groups. They are availability, integrity, and secrecy. Although it will take some work, it is very possible to secure these locations in distributed systems.

Cloud Computing

When data centers began offering web services like server hosting and storage, cloud computing was born. As the internet grew and increasingly large-scale client web administrations appeared, specialized cooperatives like Google, Microsoft, and Amazon realized that:

1) They are able to rent out storage that would otherwise be unnecessary.
2) Any designer can now create a dynamic biological system of uses thanks to open-source application programming interfaces (APIs), which are likely impossible for a single firm to create on its own.

The primary advantage of cloud computing is that users don't need any technical knowledge or experience with the supporting infrastructure. The goal of cloud computing is to enable the identification of computer resources (such as servers, networks, storage, apps, and services) that require little administrative work and can be rapidly and simply configured. "The National Institute of Standards and Technology (NIST) states that the service provider can also accomplish this by posting a shared pool of configurable, on-demand network access to interactive mode." Since they are the best single coherent computer with a computer server, cloud computing devices are connected to the network. Emphasis on cloud service providers in browser-based program versions to give clients total control, doing away with the requirement for ongoing computer equipment management or client licensing version upgrades.

Internet of Things

The term "ubiquitous computing" was originally used to describe what is now known as the "Internet of things." As a result, we use both terms interchangeably in this work. One way to conceptualize ubiquitous computing is as though there are computers everywhere. After centralized computer registering and PC registering, which were introduced by at Xerox's Palo-Alto [Parc] research center in 1988, this is the third wave of processing. It is common to omit Mark Weiser as the originator of ubiquitous computing. Ubiquitous computing envisions a smart environment with autonomous computer systems and smooth communication between system entities. This processing mechanism can provide humanity with an unparalleled level of convenience and profitability. In a world known as ubiquitous computing (UC), computers are everywhere, but we are unaware of their existence. In order to allow machine-to-machine (M2M) communications and disseminate a wide range of protocols, places, and applications, ubiquitous computing is essential for recommending propelled amalgamation of devices, frameworks, and services. This idea can lead to a wide range of products, such as heart monitoring monitors, cars with built-in sensors, or field operation tools that assist firefighters in their search and protection. By making these processing devices invisible to the user, the concept of ubiquitous computing aims to promote constant collaboration with the atmosphere and available resources by making a large number of registering devices available throughout the physical world. All types of devices and sensors are seamlessly linked to wireless networks to provide users with communication and computing services. Security is primarily concerned with evaluating potential attacks in light of vulnerabilities and creating suitable defences and counters. The majority of this is carried out by weighing the cost against the possible harm that the risk could cause. The majority of experts categorize security issues into three groups. They are availability, integrity, and secrecy. Although it will take some work, it is very possible to secure these locations in distributed systems. There are restrictions on ubiquitous systems that do not apply to conventional computing. They drastically alter the security of ubiquitous computing. These limitations include energy as a source, computational power, and connectivity. Three security areas are reviewed below from the standpoint of ubiquitous computing. In the world of ubiquitous computing, most security solutions for portable devices now use a predefined configuration of algorithms and administration protocols that are insufficient.

7. IMPORTANCE OF FIREWALL

In the past, hackers were thought to be extremely talented programmers who knew every little element about the network. They succeeded in taking advantage of the weaknesses in the networks. Nowadays, though, anyone can become a hacker in a matter of minutes by using a variety of online tools. Because of this, the network had to be secured, necessitating the use of security policies that could be updated on a regular basis. Since those networks are still vulnerable to internal dangers, we cannot declare that a network that is isolated from the outside world is secure. Cutting off contact with the outside world is also not a solution. Given that firewalls are the first line of protection, security and dependability are crucial for analysing all network traffic. Networks and businesses are protected by the use of firewalls. As a result, it became the attackers' first option for investigating firewall vulnerabilities and fully exploiting them. To take advantage of its weaknesses, one must determine how the firewall, firmware, etc., is implemented. Understanding how attackers can fingerprint a firewall is essential for network security as it can aid in the development of countermeasures for firewall tactics. Additionally, how the administrator confirms that the high-level policy is enforced by the firewall policy. For instance, "the people of a department should not be able to access the database of other departments" could be the policy. This can help with firewall analysis and debugging. It is difficult to confirm that a firewall accurately verifies a policy. First, it makes sense that standards conflicts and the ensuing request affectability would ensnare the guidelines in a firewall setup. Second, a firewall approach could include innumerable components. In extreme circumstances, an Internet firewall may consist of hundreds or even thousands of standards. Third, an endeavour firewall strategy frequently includes historical decisions that were made by different chairmen for different reasons, at different periods, and for different causes. This makes it much more difficult to examine firewall arrangements. Humans are incapable of verifying several intricately linked rules. Therefore, effective methods and tools for validating firewall tactics are essential to firewall success. However, the lack of firewall arrangement checks devices severely under-assists firewall executives. The majority of firewalls on the Internet suffer from strategy errors, according to quantitative studies. Firewall errors can be extremely costly and harmful. As a result, they might entice hackers to use these security flaws to target the network and result in large losses for companies. Firewalls have played a significant part in cloud environments as well as traditional networks. We must ensure that security and trust are upheld because cloud computing is also quickly growing in the commercial sector. In these kinds of situations, we must establish and preserve confidence. Nowadays, the majority of information is stored on the cloud and can be accessed via WSN or conventional networks. This has also drawn in hackers, who are constantly attempting to infiltrate networks and use their resources without permission, in addition to authorized users. It can occasionally result in issues for the network's authorized users. Since firewalls are the first line of defines in terms of security, security professionals have always been interested in their architecture and deployment.

8. CONCLUSION

Security is a basic concern for any computer system or network, particularly in this day and age when practically everything and everyone has some sort of network access. Unauthorized access must be prevented to host systems, network resources, user data, etc. Various firms are implementing security techniques in their computer systems for this reason. One of the simplest instruments in this section is a firewall. At the several entrance points, security policies are being established and put into effect. Their primary focus is on the availability, confidentiality, and integrity of user data and network resources. In order to guarantee the security of a network or isolated system, every incoming and departing data packet must adhere to the whole security policy or set of rules. If the data packet complies with all security regulations, it can pass over the security barrier; if not, it must be dropped. Basic firewall technology checks the source and destination IP addresses, as well as the port and packet numbers. However, as network requirements grow, firewall advancements also become essential. As a result, numerous firewall kinds have developed. such as NAT PAT VPN, stateful firewall, stateless firewall, etc. Because technology has advanced so rapidly, firewalls now play an important role. Because of this, firewalls have a lot of work to do. In some way, this has made firewalls less effective.

REFERENCES

[1] Jaggernauth, E., & Rocke, S. (2021). Effectiveness of Paired Next Generation Firewalls in Securing Industrial Automation and Control Systems: A Case Study. *West Indian Journal of Engineering*, 4-10.

[2] Liang, J., & Kim, Y. (2022, January). Evolution of firewalls: Toward securer network using next generation firewall. In *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0752-0759). IEEE.

[3] Gudimetla, S., & Kotha, N. (2017). Firewall Fundamentals-Safeguarding Your Digital Perimeter. *Neuro Quantology*, *15*(4), 200-207.

[4] Audin, G. (2004). Next-gen firewalls: what to expect. *Business Communications Review.*, *34*(6), 56-61.

[5] Thu, S. L. (2023, November). Evaluation of the Next Generation Firewall with Breach and Attack Simulation. In *Conference on Innovative Technologies in*

Intelligent Systems and Industrial Applications (pp. 253-271). Cham: Springer Nature Switzerland.

[6] Lei, S. (2024, June). Synergizing next-generation firewalls and defense-in-depth strategies in a dynamic cybersecurity landscape. In *International Conference on Computer Network Security and Software Engineering (CNSSE 2024)* (Vol. 13175, pp. 143-149). SPIE.

[7] Thu, S. L. (2023, November). Evaluation of the Next Generation Firewall with Breach and Attack Simulation. In *Conference on Innovative Technologies in Intelligent Systems and Industrial Applications* (pp. 253-271). Cham: Springer Nature Switzerland.

[8] Singh, L., & Singh, R. (2023). Comparative Analysis of Traditional Firewalls and Next-Generation Firewalls: A Review. *Latest Trends in Engineering and Technology*, 15-27.

[9] Fathia, A., & Blessing, E. (2024). Machine Learning Algorithms for Anomaly Detection in Next-Gen AI-Based Firewalls: A Performance Analysis.

[10] Ilyasov, I. (2024). Deploying Firewall Protection and Security Protocols. *Innovative Science*, (12-2-1), 50-52.

[11] Islam, M. S., Uddin, M. A., Hossain, D. M. D., Ahmed, D. M. S., & Moazzam, D. M. G. (2023). Analysis and evaluation of network and application security based on next generation firewall. *International Journal of Computing and Digital Systems*, *13*(1), 193-202.

[12] Freet, D., & Agrawal, R. (2016). Network security and next-generation firewalls. In *Proceedings of International Conference on Technology Management (ICTM 2016)* (p. 23).

[13] Kokko, K. (2017). Next-generation firewall case study.

[14] Manda, J. K. (2023). Next-Generation Firewall Technologies for Telecom: Evaluating Advanced Firewall Technologies and Their Role in Protecting Telecom Networks from Evolving Cyber Threats.

[15] Pavlović, M., Zajeganović, M., & Milivojević, M. Implementation of Next-Generation Firewalls in Modern Networks.

[16] Rao, S. D. P. (2022). Mitigating Network Threats: Integrating Threat Modeling in Next-Generation Firewall Architecture.

[17] Neupane, K., Haddad, R., & Chen, L. (2018, April). Next generation firewall for network security: a survey. In *SoutheastCon 2018* (pp. 1-6). IEEE.

[18] Patel, U. (2024). The role of next-generation firewalls in modern network security: a comprehensive analysis. *International Journal of Advanced Research in Engineering and Technology (IJARET)*, *15*(4), 135-154.

[19] Lamdakkar, O., Ameur, I., Eleyatt, M. M., Carlier, F., & Ait Ibourek, L. (2024). Toward a modern secure network based on next-generation firewalls: recommendations and best practices. *Procedia Computer Science*, *238*, 1029-1035.

[20] Mukkamala, P. P., & Rajendran, S. (2020). A survey on the different firewall technologies. *International Journal of Engineering Applied Sciences and Technology*, *5*(1), 363-365.

Chapter-IV

ZERO TRUST ARCHITECTURE FOR ENHANCED CYBERSECURITY

Dr. Priya Kapoor, Senior Researcher in Cyber Law and Defense, Symbiosis International University, Pune.

Dr. Rohan Malhotra, Senior Researcher in Cyber Law and Defense, Symbiosis International University, Pune.

Abstract--- Information security is threatened by traditional-based security concepts, which are thought to be inadequate and unable to control the dynamics of information system trust. In an effort to bridge the trust gap in information security, a novel framework known as Zero Trust Architecture (ZTA) combines identity-based policies with ongoing authentication and verification. In an effort to bridge the trust gap in an information system, this architecture is based on a number of trust nodes and logical elements. This framework's acceptance is still in its infancy due to a number of incorrect presumptions and conclusions. We make an effort to investigate the framework's complexities and fill up the current knowledge gap. Although we don't criticize other approaches, this article examined the benefits and features of the zero-trust security architecture in an effort to give a general overview of the model and fill the knowledge gap on the efficacy of implementing a zero-trust philosophy. Therefore, in order to establish a zero-trust architecture, organizations need to continuously check and verify that a user and their device have the correct rights and characteristics. It requires the development of a policy that considers user and device risk in addition to compliance or other requirements to be considered before permitting the transaction. In addition to being aware of all their services and privileged accounts, the organization must be able to control what and where they connect. One-time validation is insufficient since user traits and threats can change at any time.

Keywords--- Cybersecurity, Threats, Zero Trust Architecture.

1. INTRODUCTION

Globally, cybersecurity threats continue to be a significant issue and are only growing. Malicious attacks and incursions on servers and other hardware components have resulted in data theft for corporations worldwide, putting people at danger. It stands to reason that this matrix would not contain the government (Rebouças Filho, 2025). The most frequent target is still, surprisingly, the government; in 2021, there were approximately 1862 breaches, a 68% rise from 2020. When major security breaches were made public in January 2022, mostly impacting the governments of Canada, Australia, and Belarus, similar situations occurred for the US Department of Homeland Security in 2021 (Hubbard et al., 2021). Because users' perceptions of the security and privacy of their data are so negative, this entropy keeps spreading mistrust. People's perceptions of information technology are hence constrained. While there are many more types of these threats, some of the more current trends and attacks include ransomware, data breaches, identity fraud, phishing, cloud vulnerability, insider threats, and the internet of things (Zanasi et al., 2024). Both individuals and businesses are impacted by these actions; for instance, ransomware attacks have been connected to decreased productivity, slow response times, and disruptions in information systems. This has had a major impact, reducing the capacity of institutions such as hospitals and other essential infrastructure. In another scenario, the victims of the attack are threatened with losing their data or being forced to pay, which often damages the organization's reputation (Roy et al., 2024). Porous network surfaces and insiders are two types of weak surfaces that hackers try to exploit by getting past an organization's weakest point. Numerous studies have shown that insiders are the information security attack surface that is most vulnerable (Stafford, 2020; Sharma, 2022).

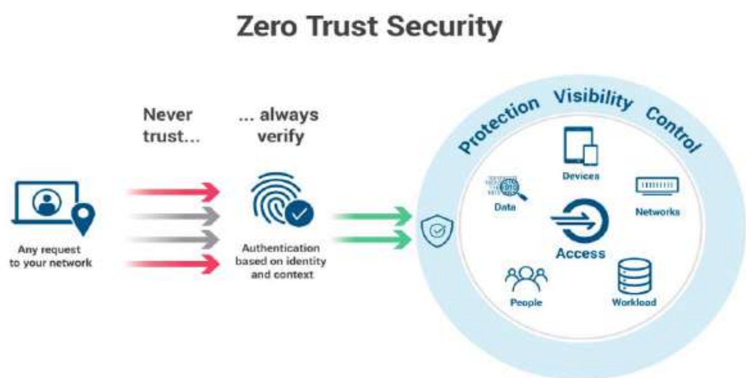


Figure 1: Zero Trust Architecture for Enhanced Cybersecurity

As technology develops and virtual working becomes more prevalent, organizations must take proactive measures to safeguard their resources and assets because a perimeter-based security framework is not enough to meet the demands of the dynamism in information security, especially with regard to cloud computing where data may be accessed remotely (Ogendi, 2024). Therefore, a preventive framework and an effective countermeasure are required to meet these goals. A more comprehensive strategy that prioritizes user identification, validation, verification, and sporadic security checks is needed for information security assurance. Hackers still exploit an organization's weakness despite the fact that there are several security architectures that try to mitigate the effects of an attack. As a result, a comprehensive framework is required in this regard, and the Zero-Trust Architecture (ZTA) has recently drawn increasing interest. This will therefore eliminate any uncertainty regarding the implementation of ZTA and provide a conceptual understanding of it (Khan et al., 2023).

2. LITERATURE REVIEW

There is a dearth of thorough study on ZTA's long-term operational impact, despite the fact that several studies emphasize its immediate security benefits. Few research has examined how ZTA increases operational efficiency over time, notwithstanding Marc's (2023) demonstration of a decrease in security breaches. More thorough research is needed in this area, but Shah et al. (2022) showed a 25% gain in efficiency as a result of automation and decreased manual oversight. This study fills that vacuum by looking at the long-term operational gains made possible by ZTA in actual case studies (Chokkanathan et al., 2024).

ZTA adoption is nevertheless hampered by legacy system integration, especially in sectors that depend on antiquated infrastructure. Many businesses have technological challenges when attempting to adopt micro-segmentation and continuous verification on older systems, according to Arachchige et al. (2020). There aren't many real-world instances of how these difficulties are resolved, though. This report makes a contribution by offering thorough case studies on the time and money needed to manage ZTA integration with legacy systems in healthcare and financial institutions (Kim et al., 2024). ZTA's capabilities are being improved by emerging technologies like artificial intelligence (AI) and machine learning (ML), especially in automating threat identification and response. Although there is little research on AI's measurable effects (Tiwari et al., 2022), Marc (2023) talked about how it aids in real-time anomaly detection. This study builds on this by illustrating how AI-driven solutions in the financial services sector cut down on manual monitoring efforts by 45%, indicating the possibility of additional ZTA optimization through the integration of AI and ML (Manda et al., 2022).

In order to overcome the drawbacks of conventional perimeter-based approaches, Zero Trust Architecture (ZTA) has become a crucial cybersecurity architecture. Its fundamental ideas—continuous authentication, micro-segmentation, and least-privileged access—have been successful in reducing security risks in a variety of sectors. Although Ghasemshirazi et al., (2023) highlighted ZTA's broad applicability, there aren't many industry-specific insights, especially in fields like healthcare and financial services. According to a literature review, there aren't many (Bashir et al., 2024; Abbas & Gul, 2025) models that adhere to the Zero Trust principle and meet all of the aforementioned IoT requirements. The relevant work's specifics are covered in the corresponding chapters. By creating a blockchain-based access control system and hardware-based device identities for authentication, the thesis aims to address the difficult security requirements of IoT networks. In the network, measures are taken to isolate and lessen Byzantine attacks. When combined, these two methods aid in achieving each of the aforementioned goals. By taking these steps, the organization improved security in a number of ways, including:

1) Enhanced visibility into network traffic, improving threat detection and response.
2) Strengthened security posture, reducing the risk of data breaches and unauthorized access.
3) Improved access control policies and encryption, safeguarding sensitive data at rest and in transit.

The agency's security resilience has been greatly improved by adhering to the White House's Zero Trust policies, which have decreased vulnerabilities in its networks, apps, and data. effectiveness in hybrid and cloud contexts.

3. IMPORTANCE OF NETWORK SECURITY

For many different applications, system and network technology is essential. Applications and networks depend on security. Despite the fact that network security is an essential necessity for developing networks, there aren't many readily implementable security techniques. Network developers and security technology developers are separated by a "communication gap." The Open Systems Interface (OSI) concept serves as the foundation for the well-established process of network design (Patel et al., 2024). When developing networks, the OSI model offers a number of benefits. It provides standardization of protocols, ease of usage, flexibility, and adaptability. It is simple to combine the protocols of several levels to create stacks that enable modular development. Individual layer implementation can be altered at a later time without requiring further changes, providing development flexibility. Secure network design is a less evolved method than network design. The intricacy of security requirements cannot be managed using any methodology. The benefits of network design are greater than those of secure network design (Hung-Jen, 2013). The fact that the entire network is secure must be underlined while discussing network security. The security of the computers at each end of the communication chain is not the only aspect of network security. The communication channel shouldn't be open to intrusions when data is being transmitted. The communication channel might be targeted by a potential hacker, who would then take the data, decode it, and reintroduce a fake message. Encrypting the communication and protecting the network are equally crucial as protecting the computers (Alagappan et al., 2022).

Figure 2: Flow of the Work

4. BACKGROUND AND MOTIVATION FOR ZERO TRUST

IoT connects many devices and networks, which present risks on multiple fronts, whereas traditional M2M applications are usually targeted. It is difficult to safely move several data streams between chosen networks when there is a mix of diverse devices, networks, platforms, and users. Trust boundaries must therefore cover protocol security and all possible communication routes for the devices involved. In an intricately linked Internet of Things, a strong foundation of trust in security begins at the device level and extends across platforms, networks, and the cloud. To guarantee end-to-end security and integrity, each agent in the IoT system must uphold a certain degree of trust. To identify IoT-specific intrusions and assaults, a thorough investigation by IoT security analytics will be necessary. An adversary can compromise nodes when they are deployed in unsupervised, potentially hostile environments without physical protection. Low power IoT nodes cannot employ traditional security measures because they were not created for the Internet of Things and need a lot of resources. Since users (or devices) are no longer limited to a network's perimeter, the traditional method of categorizing them as internal and external to thwart an attack is no longer applicable. A device must be trusted based on its identification and past conduct rather than the network to which it belongs, as we have learned from the IoT assaults previously discussed. If appropriate steps are not taken to stop it, even legitimate nodes in the network could be the source of a significant attack. Therefore, a Zero Trust (Sharma, 2022) approach should be used by the new security mechanism.

In the past, the majority of networks adhered to the security concept "verify, then trust." This suggests that the person or device is trusted and granted network access once its credentials have been validated. The device is blindly trusted, particularly if it has been confirmed to be a part of the internal network. But according to the Zero Trust mechanism put forth by the analyst at Forrester Research, a network should not presume that any user requesting access to a resource, whether inside or outside its boundaries, is trustworthy; rather, it should confirm whether or not the access is necessary. The Zero Trust framework's three fundamental tenets are:

1) Never trust, always verify;
2) Principle of Least Privileges; and
3) Assume there is an impending breach.

Every time a device wishes to connect to the network, it should be authenticated and granted only the minimal amount of access necessary to carry out its intended role. This is crucial given the evolving security landscape of today, particularly with regard to IoT networks. Imagine a situation where a conference room's smart TV serves as the display screen. It can end up being a bot that launches a DDoS attack or a spying gadget that compromises data or privacy. There is a great deal of risk because it is linked to the same network as the company that houses sensitive information like finances and human resources. Therefore, greater duty to prevent data misuse accompanies increased capabilities (Ghasemshirazi et al., 2023). Every effort is being made to minimize human involvement in order to improve the Quality-of-Experience (QoE) in a seamless manner. An exploit's risk surface grows as a result. When an attack targets medical, emergency, or mission-critical communication systems—where communication must be dependable—the casualties are devastating. The loss could be financial, private, or life-threatening. Therefore, fine-grained access control must be put in place and each device requesting access to a resource must first be authenticated. The emphasis is now on selectively protecting the data or resources based on the potential harm they could create, rather than protecting the network's perimeter.

5. CHALLENGES IN TRUST

It is likely that researchers are aware of the many beneficial services that cloud computing has provided. It also takes into account a lot of security risks and challenges. Since a lot of data is sent over networks and kept in cloud resources, malicious components can cause a number of vulnerabilities. In this study, we analyze the security status of cloud scenarios that are divided into seven types based on a Singh et al. (2016) study (Ahmadi et al., 2024). It should be noted that each of this area's subsections corresponds to a distinct security attribute. As seen in Fig. 2, cloud protection challenges can be divided into seven categories: trust and conviction, security policies, client management issues, operating system base issues, application security, data storage security, and network security. Starting with the trust and conviction issue, which aids in making a reliable decision, the classification covers all seven security difficulties. This section also focuses on issues at the application level. These security rules ought to safeguard the workplace. We outline several actual cluster flaws and a simulated cluster assault on the network cloud to demonstrate how clustering issues and all operating systems commonly affect the cloud. There are still a number of flaws in the desktop operating system that make network servers and cellphones susceptible to serious attacks.

5.1. Security

Cloud data security is becoming increasingly important as we move our gadgets, data centers, corporate activities, and more to the cloud. The quality of cloud data security is ensured by comprehensive security policies, cloud security solutions, and enterprise security culture. Cloud security, also known as cloud computing security, is the result of combining a number of policies, processes, controls, and technologies to protect cloud-based systems, data, and infrastructure. These security measures are in place to protect cloud data, help with regulatory compliance, protect client privacy, and set up authentication rules for certain individuals and devices. Every facet of cloud security, including traffic filtering and access authentication, can be tailored to the specific requirements of the company. The development of a workable cloud application security engineering that provides control and remediation is further examined by the ElasticaQ2 2015 and CSA. Furthermore, according to the International Organization for Standardization (ISO), data security issues that can be resolved with cloud computing are essential security requirements for an effective and safe cutting-edge technical solution.

Trust and Conviction

Regarding trust, we calculated it as the belief that leverages the company's experience and sticks to the trustworthy selection of cloud partners, virtualization, web-based access, storage hardware, and the computational algorithm that has been proven to be trustworthy. Assessing trust is a complex, multi-phase process that depends on the multidimensional factor that Chen, D. et al. (2012) identified (Tiwari et al., 2022). Actually, the TCP protocol has security, which means that the service provider is protecting the confidentiality and integrity of the data.

Security Policies Security

Policies include the rules necessary to prevent attacks by adopting preventative measures. According to a 2019 study by Asma Shaikh et al., these guidelines should guarantee the cloud workspace without sacrificing its dependability and performance (Manda et al., 2022). Security policies, which include service-level agreements (SLAs), forerunner trust, and service-client management challenges, are dependent on authorities. SLAs also fulfil customer requests and validate the terms that exempt suppliers from liability for outages or problems with execution. SLA is unable to guarantee that a certain task will be completed.

Client Management Issue

From a security standpoint, one of the major concerns with cloud computing is client administration. Information in the client organization system is not available in the open cloud.

Application Issues

The weakest aspect of a software program is its security. The more important components of the apps are front-end, back-end, parallelism, structure, and a variety of platforms with a variety of flaws. The software is written by a variety of developers in a variety of languages, and many programming dialects have flaws.

Cloud Data Storage Issue

Data storage is one of the most important aspects of cloud computing. Information storage and cloud computing security are major concerns as a result of the proliferation of online apps and devices (Rhoads & Smith, 2024). Network Cloud computing has faced a major challenge known as network security because it has always been essentially dependent on the network. A developing subfield of computer security, network security, and information security is the main connection between network and cloud security. In practice, there are several security issues with networks. According to R. Buyya et al. (2017) (Syed et al., 2022, network administrators must thus implement preventive components and administrations and adopt suitable security ways to safeguard the data and cloud infrastructure. Regrettably, network security has encountered significant association accessibility threats, such as flooding attacks, denial of service (DoS), distributed denial of service (DDoS), and flaws in internet conventions.

Operating System Base Issue

A number of virtual computers are used in cloud computing. Numerous operating system collaboration groups and server classifications in intra- and inter-networks have led to a number of security problems.

5.2. Webpages Dataset: Importance and Relevance

Building machine learning models to perform a variety of webpage analyses is made easier with the help of the Webpages dataset. Both supervised and unsupervised learning models can be developed. However, it is important to keep in mind that there isn't yet a large enough dataset in the public domain to facilitate research in this field.

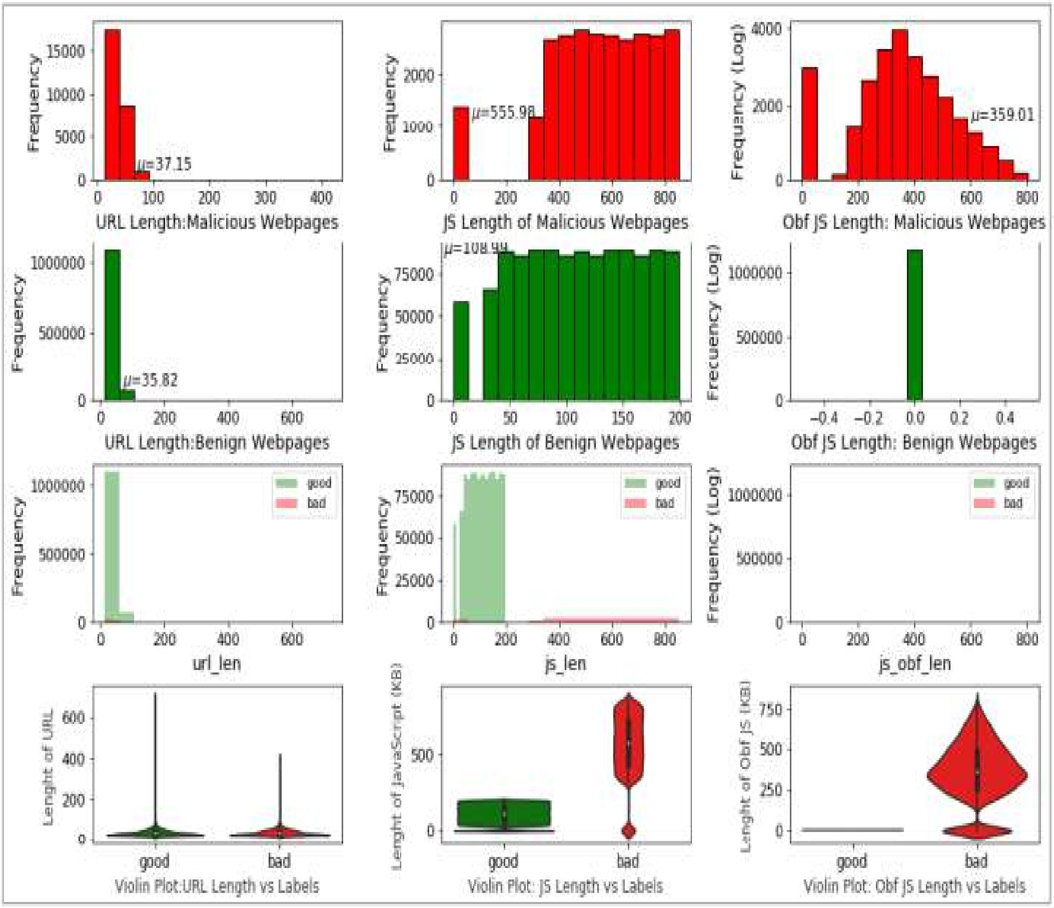


Figure 3: Plots of Univariate

All researchers working in the field of online security will gain from it. Additionally, cyber security and anti-virus organizations might utilize this data to model their security products. It has enough qualities to provide more understanding. In order to support future study, Additionally, this data contains processed raw web content, including JavaScript code, which can be used to extract additional attributes if needed. It is helpful for the Internet security research community, cyber security firms, and Cyber Law Enforcement agencies when they are creating policies. The dataset was created with the downstream purpose of classifying webpages as benign or harmful in mind.

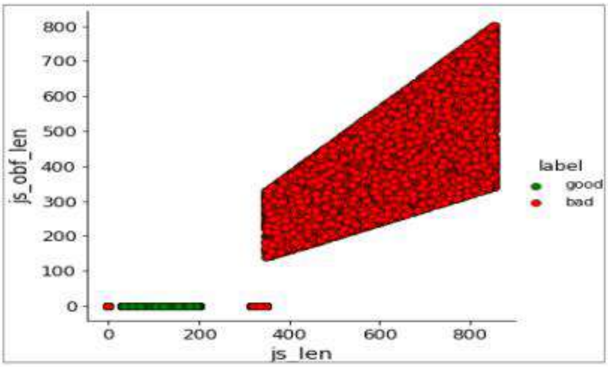


Figure 4: Bivariate Pairwise Plot

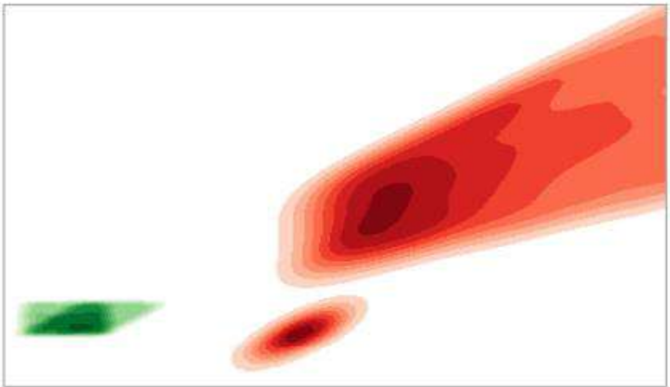


Figure 5: Bivariate Density Plot

Nonetheless, this dataset has enough data to be applied to any machine learning application involving webpage analysis. A webpages dataset is essential to Zero Trust Architecture (ZTA) because it makes it possible to gather and examine a variety of web page features, content, and structures, which aids in the creation of strong cybersecurity defences. Researchers and developers can improve threat detection, prevention, and incident response capabilities by examining webpages to find trends, abnormalities, and possible vulnerabilities. Additionally, ZTA's defences can be strengthened and a culture of constant monitoring and trust verification can be fostered by using webpage datasets to train machine learning models to identify and categorize harmful web content, such as phishing sites or malware-infected pages.

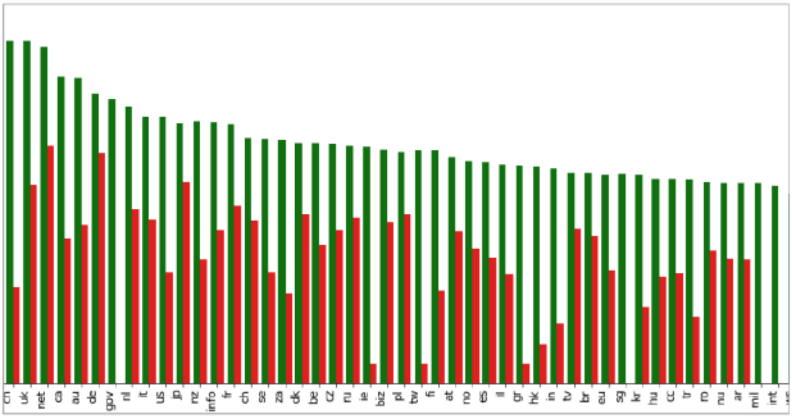


Figure 6: Plot of Top-Level Domain ('tld') Attribute

'tld', the seventh attribute, provides the webpage's Top Level Domain Name. Figure 7 shows a visualization of this property. This dataset includes webpages from a wide variety of domains, as the graph illustrates.

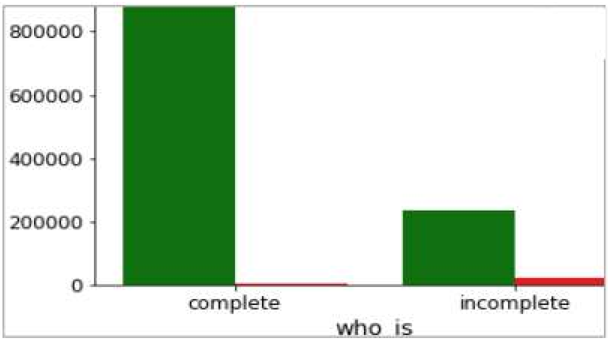


Figure 7: Registration Plot

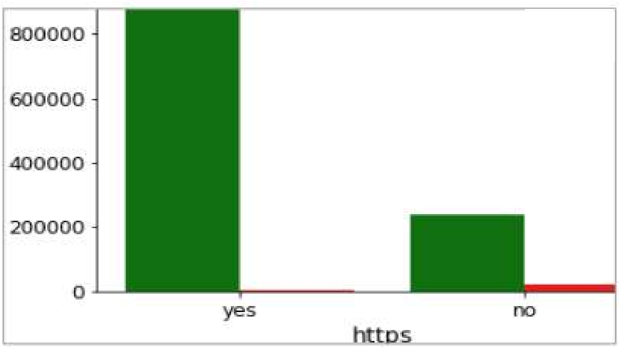


Figure 8: HTTPS Plot

'Who is' and 'https' are the eighth and ninth attributes in the collection, respectively, and they indicate if the webpage uses HTTPS and whether its WHOIS information is complete. Both of these attributes are categorical. The 'who is' property provides the completeness of domain registration information for websites hosted with domain registrars. The 'https' element indicates whether or not the web server delivers the webpage using the HTTP secure protocol. These two characteristics are shown in Figures 8 and 9.

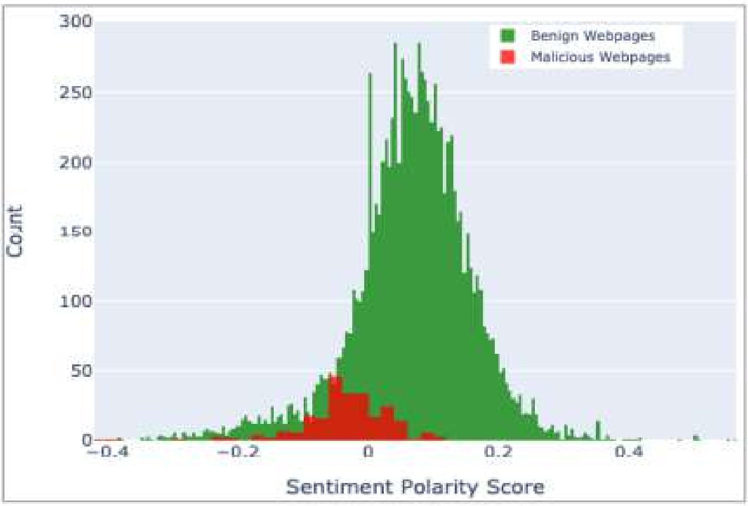


Figure 10: Web Content: Sentiment Score

Figure 11: Web Content: Profanity Score

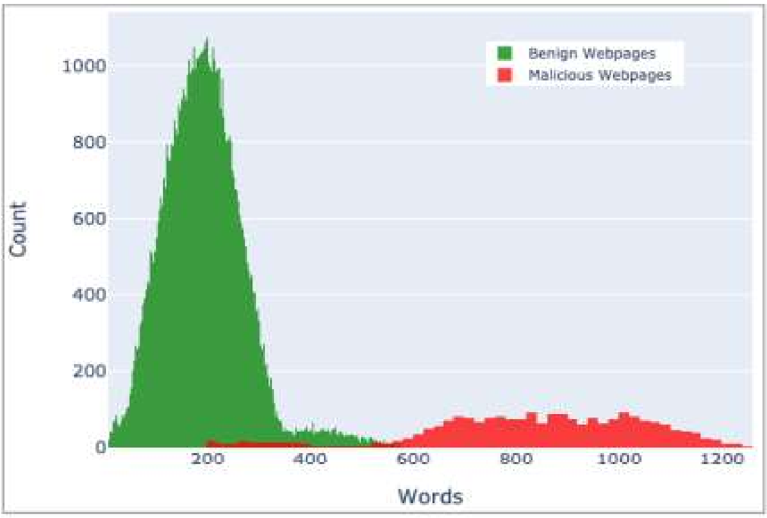


Figure 12: Web Content- Word Count

'content' is the dataset's eleventh attribute. JavaScript code and other raw web content are contained in this property; they have been cleaned and filtered to minimize their size. This attribute was included in the dataset with the intention of facilitating more attribute extraction from the dataset, should that be needed in subsequent studies. Additionally, this unstructured web content can be used directly for experiments with some machine learning approaches, such as deep learning (see Chapter 6 for an example of this). Figures 10, 11, and 12 below display this raw content's vectorized plot.

6. DISCUSSION

Every time a device wishes to connect to the network, it should be authenticated and granted only the minimal amount of access necessary to carry out its intended role. This is crucial given the evolving security landscape of today, particularly with regard to IoT networks. Imagine a situation where a conference room's smart TV serves as the display screen. It can end up being a bot that launches a DDoS attack or a spying gadget that compromises data or privacy. There is a great deal of risk because it is linked to the same network as the company that houses sensitive information like finances and human resources. Therefore, greater duty to prevent data misuse accompanies increased capabilities. Every effort is being made to minimize human involvement in order to improve the Quality-of-Experience (QoE) in a seamless manner. An exploit's risk surface grows as a result. When an attack targets medical, emergency, or mission-critical communication systems—where communication must be dependable—the casualties are devastating. The loss could be financial, private, or life-threatening. Therefore, fine-grained access control must be put in place and each device requesting access to a resource must first be authenticated. The emphasis is now on selectively protecting the data or resources depending on the potential harm they could do if lost or compromised, rather than protecting the network's perimeter. The information might be readings from various Internet of Things devices or each device's credentials, which are needed for access control. Due to their inherent resource limitations, IoT devices will need to rely on an external agent, such as cloud storage, in order to handle data on a big scale. Resource-constrained gadgets are those that have limited processing and storage power and frequently rely on batteries (poor energy budget) (Chokkanathan et al., 2024). However, there is always a chance of a privacy violation when you entrust sensitive information to an outside authority. Any leak of personally identifiable information, including a user's location or identity, is considered a privacy breach. It is necessary to handle the data such that it cannot be associated with the user. The IoT system becomes centralized when a single authority controls all network access control, which has an impact on the system's scalability. Additionally, it exposes the system to a single point of failure. In IoT networks, access control and authentication should ideally be limited to the objects from which they originate, making it impossible to steal their identity by removing the essential components. When nodes are engaging for the first time, this fosters trust, particularly in a foreign network.

7. CONCLUSION

Traditional architectures are fundamentally different from zero trust. It secures direct access to IT resources rather than networks. It controls access according to context and risk rather than identification, which is susceptible to theft. The architecture is delivered as a service and at the edge by a dedicated cloud, which serves as an intelligent switchboard that permits safe, one-to-one connections between users, devices, workloads, branches, and applications, regardless of where they are located. To put it another way, zero trust separates network connectivity and security. It enables businesses to use the internet as their corporate network in an efficient manner. In order to replicate these actions, the Zero Trust Security

Model takes stringent steps to verify the identity and intent of users, devices, and the interdependent factors in the system environment. These rules are considered economical and effective since they outperform the latency in the conventional security model. The perimeter-based deployment of the old security framework has led to ransomware, malware, intrusion, and data theft. As a result, the ZTA meets this goal; nevertheless, because to the lack of knowledge on this design, its adoption is restricted. We offer a literature-based assessment of the ZTA architecture's effectiveness and efficiency along with a conceptual overview of it. ZTA, therefore, removes the trust vulnerability in an organization's information system, and the model may be combined with various security frameworks and put into practice. From the standpoint of policy, the architecture is founded on the principle of "never trust" and attempts to identify and verify individuals and devices prior to granting them access to infrastructure and resources. The rapid pace of digital transformation requires a security architecture that can keep up. Traditional perimeter-based tactics are no longer sufficient due to their inherent shortcomings. Today's cybersecurity problems can be solved with zero trust architecture's emphasis on dynamic, context-based laws and secure, any-to-any connections.

REFERENCES

[1] Rebouças Filho, W. L. (2025). The Role of Zero Trust Architecture in Modern Cybersecurity: Integration with IAM and Emerging Technologies. *Brazilian Journal of Development*, *11*(1), e76836-e76836.

[2] Hubbard, T., Klimavicz, J. F., Wong, S., & Steinhoff, J. C. (2021). Zero trust in a virtual cybersecurity world. *The Journal of Government Financial Management*, *70*(2), 12-19.

[3] Zanasi, C., Russo, S., & Colajanni, M. (2024). Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures. *Ad Hoc Networks*, *156*, 103414. https://doi.org/10.1016/j.adhoc.2024.103414

[4] Roy, A., Dhar, A., & Tinny, S. S. (2024). Strengthening IoT Cybersecurity with Zero Trust Architecture: A Comprehensive Review. *Journal of Computer Science and Information Technology*, *1*(1), 25-50.

[5] Stafford, V. (2020). Zero trust architecture. *NIST special publication*, *800*(207), 800-207.

[6] Sharma, H. (2022). Zero Trust in the Cloud: Implementing Zero Trust Architecture for Enhanced Cloud Security. *ESP Journal of Engineering & Technology Advancements (ESP-JETA)*, *2*(2), 78-91.

[7] Ogendi, E. G. Leveraging Advanced Cybersecurity Analytics to Reinforce Zero-Trust Architectures within Adaptive Security Frameworks.

[8] Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews*, *19*(3), 105-116.

[9] Chokkanathan, K., Karpagavalli, S. M., Priyanka, G., Vanitha, K., Anitha, K., & Shenbagavalli, P. (2024, November). AI-Driven Zero Trust Architecture: Enhancing Cyber-Security Resilience. In *2024 8th International Conference on Computational System and Information Technology for Sustainable Solutions (CSITSS)* (pp. 1-6). IEEE.

[10] Kim, Y., Sohn, S. G., Jeon, H. S., Lee, S. M., Lee, Y., & Kim, J. (2024). Exploring Effective Zero Trust Architecture for Defense Cybersecurity: A Study. *KSII Transactions on Internet and Information Systems (TIIS)*, *18*(9), 2665-2691.

[11] Tiwari, S., Sarma, W., & Srivastava, A. (2022). Integrating Artificial Intelligence with Zero Trust Architecture: Enhancing Adaptive Security in Modern Cyber Threat Landscape. *International Journal of Research and Analytical Reviews*, *9*, 712-728.

[12] Manda, J. K. (2022). Zero Trust Architecture in Telecom: Implementing Zero Trust Architecture Principles to Enhance Network Security and Mitigate Insider Threats in Telecom Operations. *Journal of Innovative Technologies*, *5*(1).

[13] Bashir, T. (2024). Zero Trust Architecture: Enhancing cybersecurity in enterprise networks. *Journal of Computer Science and Technology Studies*, *6*(4), 54-59.

[14] Abbas, G., & Gul, S. (2025). Zero Trust Architecture: Revolutionizing Cybersecurity in the Era of Advanced Threats.

[15] Patel, R., Müller, K., Kvirkvelia, G., Smith, J., & Wilson, E. (2024). Zero trust security architecture raises the future paradigm in information systems. *Informatica and Digital Insight Journal*, *1*(1), 24-34.

[16] Alagappan, A., Venkatachary, S. K., & Andrews, L. J. B. (2022). Augmenting Zero Trust Network Architecture to enhance security in virtual power plants. *Energy Reports*, *8*, 1309-1320.

[17] Ghasemshirazi, S., Shirvani, G., & Alipour, M. A. (2023). Zero trust: Applications, challenges, and opportunities.

[18] Ahmadi, S. (2024). Zero trust architecture in cloud networks: Application, challenges and future opportunities. *Journal of Engineering Research and Reports*, *26*(2), 215-228.

[19] Rhoads, J., & Smith, A. (2024). Effectiveness of Continuous Verification and Micro-Segmentation in Enhancing Cybersecurity through Zero Trust Architecture.

[20] Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. *IEEE access*, *10*, 57143-57179.

Chapter-V

MACHINE LEARNING IN MALWARE ANALYSIS AND PREVENTION

Dr. Sneha Deshmukh, Digital Forensics and Incident Response Expert, University of Mumbai, India.

Dr. Ashwin Menon, Digital Forensics and Incident Response Expert, University of Mumbai, India.

Abstract--- Strong and proactive internet security measures must be put in place since digital threats are becoming more frequent and sophisticated. The integration of AI techniques for predicting and detecting cyberattacks is examined in this study. We use unaided approaches for inconsistency discovery and administered learning calculations for break expectation on a variety of datasets, such as network logs, client behaviors, and framework exercises. To improve the precision and usefulness of danger-distincting evidence, social analysis and continuous observation frameworks are combined. Traditional detection techniques face several difficulties since malware is become more varied and complicated. This study looks at how well the Machine Learning algorithm, a potent machine learning tool, recognizes and categorizes malware samples. Emerging approaches such as behavior-based detection and semantic malware descriptions have shown promise and are deployed in commercial software. However, new techniques must be developed to keep pace with the development of malware.

Keywords--- Malware Analysis, Machine Learning, Software Defined Networks.

1. INTRODUCTION

The security landscape calls for innovative approaches to counter more sophisticated malware in a world of expanding cyberattacks. Due to their centralized and programmable nature, which offers more control and visibility over network functions, SDNs are a strategic advantage (Faruk et al., 2021). Information technology is ubiquitous and improvements to this information technology's security are needed to ensure a secure future. As critical infrastructures increasingly rely on both public and private networks, there also exists a greater potential for widespread impact as a result of disruption or failure of such networks. To safeguard critical infrastructures means not only protecting their physical infrastructures but also the cyber aspects of the systems upon which they depend. With today's use of the Internet to facilitate the communications, monitoring, operations, and business systems supporting many critical infrastructures, there is greater opportunity for intentional, malicious compromise. Cyber-attacks are growing in number and severity. Attackers wishing to disrupt key infrastructures are motivated by various reasons and consider cyber-space as a potential tool to be able to have much more effect, e.g., to endanger humans or bring about extensive economic harm. While so far, no cyber-attack has significantly affected critical infrastructures, past attacks proved that there are wide vulnerabilities in information systems and networks that can cause serious harm. The consequences of a successful attack could involve severe economic impact through effects on key economic and industrial sectors, threats to infrastructure components like electric power, and disruptions that interfere with the response and communication abilities of first responders in emergency situations (Anderson et al., 2017; Nath & Mehtre, 2014; Saad et al., 2019).

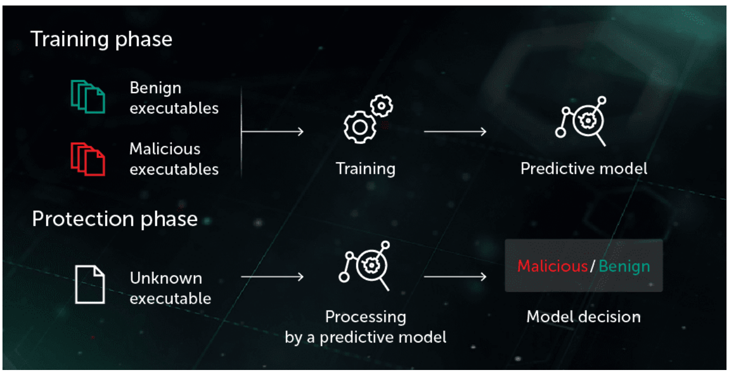


Figure 1: Machine Learning in Cybersecurity

Malware is a generic category of attack software or hardware loaded onto machines, generally unknowingly to the legitimate owner, which subverts the machine for the advantage of an attacker. Current classes of malware include viruses, worms, Trojan horses, spyware, and bot executables. Spyware is a type of malware utilized to track and/or forward information to an unauthorized third party covertly. Bots (short for "robots") are malware applications that are secretly installed on a targeted computer, enabling an unauthorized user to take control of the infected computer remotely for a number of malicious intents. Botnets are collections of machines that have been infected by bot malware so that they are controlled by an attacker. Malware can be introduced at any stage in the system life cycle. The World Wide Web is now an important vehicle for spreading malware. Malware, for example, is remotely injected into otherwise innocent websites, where it can then go on to infect users of those so-called "trusted" sites (Dada et al., 2019; (Urooj et al., 2021).

2. REVIEW OF LITERATURE

The Significant Permission Identification (SigPID) method was developed by Li et al. and employs permissions as features to detect malware. In order to find the necessary rights that actually categorize the apps as safe or harmful, they mined the permission information (Udayakumar et al., 2017). The newest methods currently employed were contrasted with the authors' results. The outcomes illustrated the fact that SigPID is more efficient at identifying malware, with the accuracy of 91.4% gained by unknown malware. Zhu et al. have suggested a method (termed DroidDet) to mine APIs, permissions, permission rate, and system events as a crucial part. To develop a model for classifying whether an application is malware-infected, they employed ensemble rotation forest. The trial results proved that the proposed method was superior to other existing methods with accuracy of 88.26%. Kim and others have published a malware detection tool. The authors refine the numerous feature types they have extracted using existence-based or similarity-based feature extraction methods (Djenna et al., 2023).

The significance of Android intents and permissions as a discriminator to detect fraudulent applications has been studied by Feizollah et al. In the course of the research, 7,406 applications were utilized, out of which 1,846 were malicious and 5,560 were benign. The findings proved that the union of both the features yields a high recognition rate of 95.5% compared to solo characteristics. Agrawal and Trivedi have used various machine learning classifiers to study various malware detection methods. The outcomes demonstrated that RF outperformed other ML classifiers. Using dynamic behaviour features, Feng et al. have developed an effective dynamic framework called EnDroid that can identify malware with high accuracy. To extract key features and remove unnecessary and noisy ones, they used a feature selection technique. Additionally, EnDroid used a stacking ensemble technique to differentiate between malicious and benign programs. The studies' findings demonstrated that stacking enhanced performance and provided a workable technique for virus identification (Haque et al., 2023).

Mahindru and Sangal introduced a system for detecting malware on mobile devices called ML-Droid. This system used dynamic analysis to find mobile malware. Furthermore, a number of machine learning approaches incorporate dynamic features to make model creation easier. In the experiment, five million Android apps were used. The results demonstrated that the recommended approach had a 98.8% accuracy rate.

Qaisar and Li have offered a multimodal study of hazardous applications. The authors employed information fusion to identify the malicious programs based on their visual, static, and dynamic properties. They use a semi-supervised method for classifying and identifying malware. The findings demonstrated that their method outperformed other conventional methods with a 95% accuracy rate. Mad4a is a hybrid malware analysis method developed by Kabakus and Dogru. This strategy makes use of both static and dynamic methods. This method's significance lies in exposing the covert actions of Android malware (Faruk et al., 2022).

Ibrahim et al. presented a method based on static analysis and the key components of Android applications, such as two recently suggested features. An API DL model created especially for this use case then uses these features as input. The proposed method is implemented and evaluated on a classified dataset of Android apps. They focused on extracting features related to broadcast receivers, opcode sequences, services, permissions, and API requests. They also included two new static features: application size and fuzzy hash.

Patil and Deng demonstrated a neural networks-based malware analysis framework with high accuracy, demonstrating how using DL networks instead of conventional ML models may increase accuracy. The results of the experiment showed how accurately the DL-based malware classification method classifies malware. Furthermore, they suggested that DL's gradient descent and backpropagation processes enhance accuracy, reduce false positives, and raise true positives.

2.1. Malware Detection Methods

The most popular approach among all antivirus software is the signature-based approach. This method compares the signature of the application to an existing database signature. A disadvantage of this approach is its incapacity to detect new, undiscovered malware, sometimes known as zero-day malware. Researchers have started using machine learning approaches that use both static and dynamic malware analysis to get around this method's drawbacks.

2.2. Machine Learning

Computers can learn without explicit programming thanks to machine learning. It has been used in many different industries and has been a popular area of study in recent years. Medical data processing, false news categorization, and speech analysis or recognition are a few examples of these domains. Researchers start using machine learning techniques with both static and dynamic malware analysis (Sharma et al., 2023).

2.3. Types of Machine Learning

Three categories of machine learning exist: reinforcement learning, supervised learning, and unsupervised learning. The different ML categories are displayed in Figure 2.

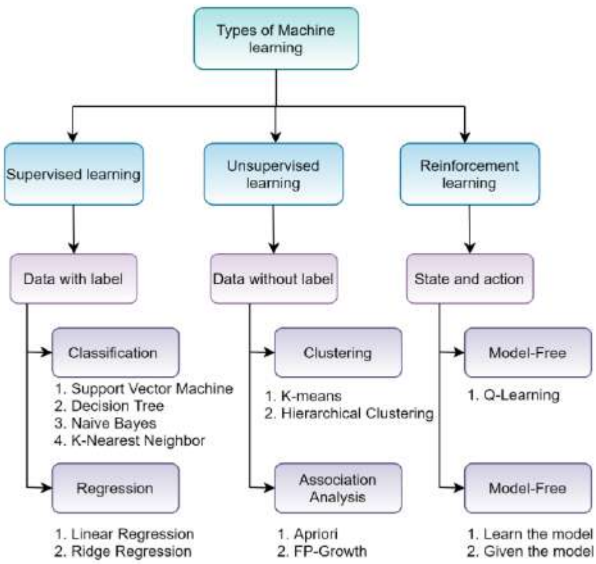
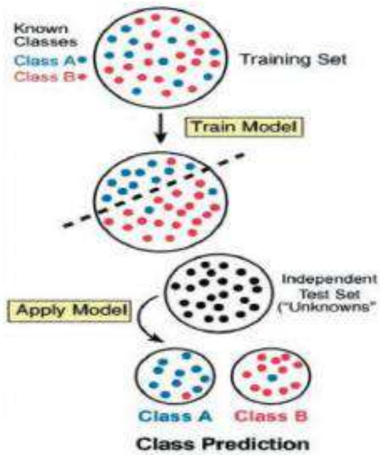


Figure 2: Various categories of ML

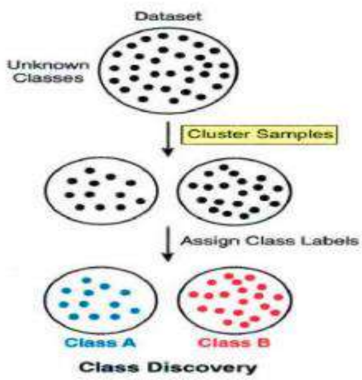
1) Supervised learning is divided into two categories: regression and categorization.

2) Classification- It involves classifying the cases into distinct groups. There are categorical values in the output attribute.

- Binary classification: This divides a set of instances into two categories, such as "malware" and "benign.""
- Multiclass classification: This divides a set of occurrences into two or more classes, such as "malware family classification.""
- Regression: Real values, such as "weights" and "heights," make up the output attribute."



(a)



(b)

Figure 3: Unsupervised and Supervised Classification

- Another name for unsupervised learning is "learn without examples." This learning does not require any prior knowledge of the predicted attribute. The two kinds of this learning are association and clustering.
- Association: This problem is based on market analysis. It presents the collection of objects' association rule. For instance, what is the likelihood that item B will be purchased along with item. The Apriori algorithm is one instance of association rule mining.
- The practice of organizing data points into groups whose members are similar in some way is known as clustering. K-means, partitioned clustering, hierarchical clustering, and others are a few instances of clustering.
- Reinforcement learning: This dynamic programming technique uses a system of rewards and penalties to train the model. It is employed to specify the optimal course of action that enables the agent to maximize a reward while resolving an issue. Q-learning and R-learning are two instances of reinforcement learning.

2.4. Motivation

Smartphones are getting more and more common in our daily lives in the modern era. Many people use smartphones for a number of things, such as banking, shopping, entertainment, and gaming. Numerous operating systems are available on the market, such as Windows Phone, iOS, Android, and BlackBerry. Of these, Android is the most widely used (Alraizza & Algarni, 2023). With over 3.04 million apps, it holds an 85% market share. There were one billion mobile subscribers as of December 2019, but during the COVID-19 epidemic, that number rose to seven billion. Users now use smart devices to access a variety of services due to the exponential rise of mobile technologies. The growth of the upcoming economy and mobile Internet is significantly influenced by the proliferation of Android apps. Attackers have been interested in Android apps due to their growing usage. Recently, the rapid development of mobile technology has given rise to a number of dangers, including financial loss, information leakage, and system damage. According to the MacAfee research, there will be about 121 million more Android malware cases in 2020. The rise in Android malware has made manually managing the malware samples more difficult. To avoid this issue, a more efficient and automated method of malware detection must be developed (Akhtar & Feng, 2022). The signature-based method is the foundation of the conventional malware detection techniques, which are ineffective at identifying novel viruses. In the past, the malware was created with straightforward goals in mind. It was therefore easier to identify. Conventional malware is the term for this kind of malware. Attackers are developing sophisticated malware that is more difficult to detect and can run in kernel mode. New generation malware is the term used to describe this kind of malware. The latest malware that is coming out is really intricate and smart. As a result, complex and sophisticated malware cannot be swiftly and precisely detected using traditional approaches. Therefore, techniques for enhancing malware identification and categorization need to be created.

3. PROPOSED METHODOLOGY

The focus is on addressing the shortcomings of traditional approaches and improving the overall hazard recognition and response capabilities while putting forth a high-level network safety framework that makes use of AI. Create a crossover strategy by utilizing a variety of AI models, such as controlled and solo learning computations. This might enhance general accuracy and lessen the drawbacks of particular models. Put mechanisms in place to make AI models more resilient to hostile attacks. To improve control efforts, adversarial preparatory techniques should be employed and models should be updated often. reaction systems that use posteriorizing to quickly address dangers that have been discovered. Computerized solutions that reduce reaction time and lessen the impact of safety events include disengaging compromised frameworks and altering security arrangements.

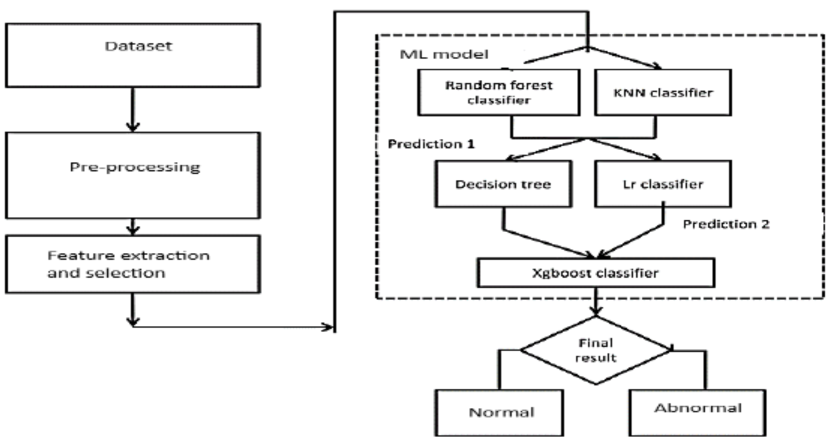


Figure 4: Basic Block diagram

Data Collection

It is typical practice to handle information assortment by obtaining testing of known malware variants from threat knowledge feeds and malware archives. Next, those examples are examined to remove structures that might be used to type and describe the behavior of malware, including byte sequences, procedure calls, page credits, and record hashes.

Scientists are also able to observe how malicious software tests perform in controlled experiments using dynamic probing methods like emulation and sandboxing. This allows experts to discover runtime exercises and obtain safe programming exams, which leads to a proper dataset for scheduling and evaluation. Even after static record inspection, malware recognition at times incorporates information collection, such as record changes, library modifications, network exchanges, and cycle injections (Lee et al., 2019).

Data Processing

Malware detection data processing is the methodical examination and modification of raw data to derive useful information for detection and prevention of malicious software threats.

Furthermore, labelling data helps in the effective training and assessment of supervised systems by labelling classes to specify whether a sample is benign or malignant. Operations such as data augmentation to extend the variety of datasets and separating data into train, validation, and test sets to accurately analyze model performance also fall under the category of data processing.

Feature Extraction

The process of identifying and removing relevant features or attributes from malware testing to assist in identification and description of malicious programming is referred to as highlight extraction for malware recognition.

These highlights allow AI systems to make the distinction between safe and malicious material by giving them important information about the features, patterns, and structure of malware.

Highlight extraction techniques for malware detection may vary based on the type of data being scanned, such as dynamic rules of behaviour, organization traffic, and static record credits. Common highlights extracted from malware tests are such as text, byte sequences, code development, metadata, direct programming interface calls, document size, record type, and record hashes.

Detection

The process of developing detection models which can differentiate between unwanted and harmless software using labelled datasets for training machine learning algorithms is referred to as model training in malware detection.

From the input features captured in the course of data processing, the model learns basic malware sample patterns and characteristics as the model trains. This involves exposing the algorithm to the training dataset and successively modifying its inbuilt configurations for the purposes of reducing the loss function or predictive error. Neural networks, support vector machines, decision trees, and random forests are some of the machine learning algorithms that are often used for malware detection (Akhtar & Feng, 2023).

Prediction

The GBA model can classify new unseen samples once it is trained on labelled data and tuned to minimize prediction errors. The trained GBA model is given the features which were excluded from the input sample in the prediction phase. The model then calculates the probability or confidence level with which the sample belongs to the malicious class. With the help of a judgment threshold, the sample is classified as benign or malicious depending on this score (Buriro et al., 2023).

4. EXPERIMENTAL ANALYSIS

As was mentioned in the preceding section, some research publications suffered from unbalanced datasets, while others employed very large datasets. This problem stems from the researchers' conviction that bigger datasets improve accuracy and lessen bias. Even though this is a widely held belief, it's crucial to keep in mind that extremely huge datasets could present some difficulties.

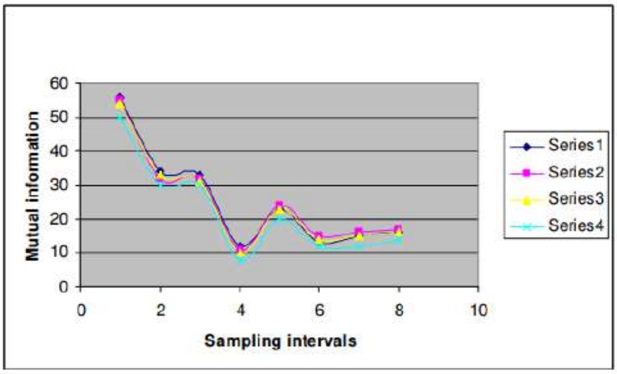


Figure 5: Normal Data

The time and processing power needed to train the model can be decreased by using a dataset of a manageable size. The use of current datasets is another issue that must be resolved in order to preserve the study's relevance and applicability in real-time circumstances.

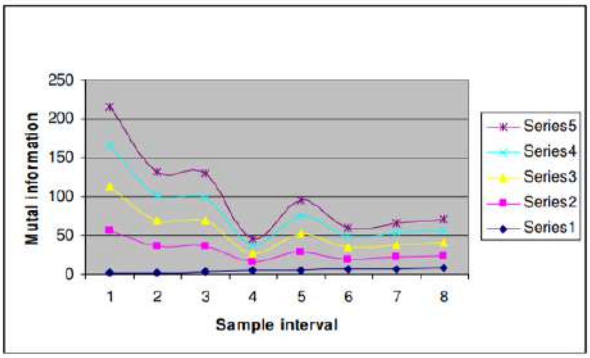


Figure 6: Attack Data

One popular preprocessing technique for dealing with unpredictable image sizes is resizing photos to a fixed size. Many machine learning models depend on the input photos having a consistent size and format, which is ensured by this step. But one must be aware of how information loss is affected by resizing. Therefore, more research is required to create resizing methods that reduce information loss while preserving an appropriate and consistent image size for processing (Awais et al., 2023).

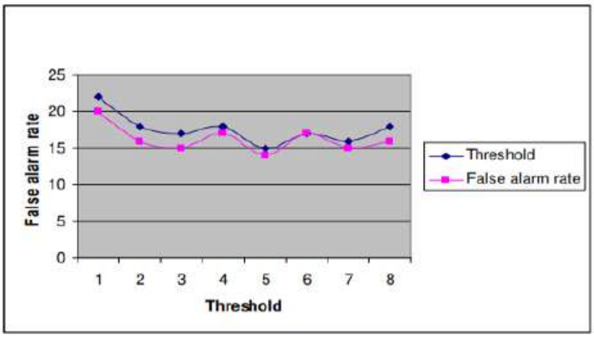


Figure 7: False Alarm Rate

Researchers may think about using distributed computing and parallelization approaches to expedite training and shorten the time needed to handle massive datasets.

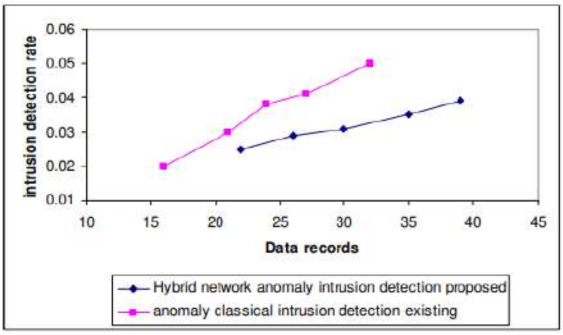


Figure 8: Performance of Anomaly Intrusion Detection in Combined Network

In order to train the model in parallel, this entails dividing the task among various computer resources, such as numerous PCs or GPUs. The time and memory resources needed for training can be greatly decreased with parallelization (Masum et al., 2022).

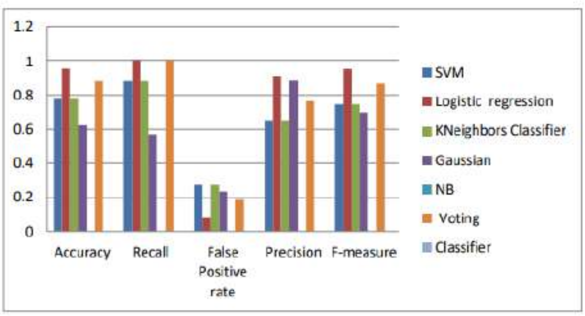


Figure 9: Performance Matrices of ML Algorithms on Mendeley Data

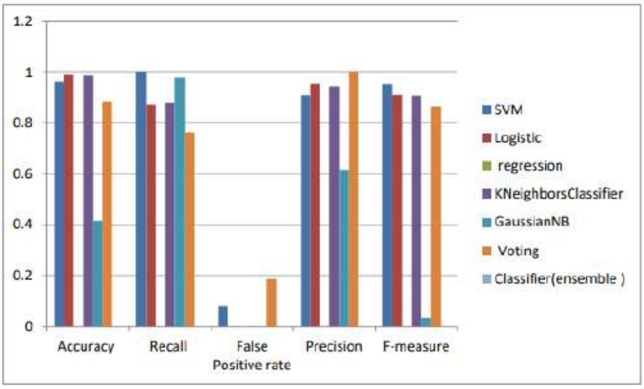


Figure 10: Performance Matrices of ML Algorithms on Figshare Dataset

Numerous trends in malware study and detection have surfaced over time, each having unique disadvantages. As a result, researchers have focused on other techniques that aim to increase detection and classification precision while identifying malware in real-time with few false positives (Bearden & Lo, 2017; (Cuan et al., 2018).

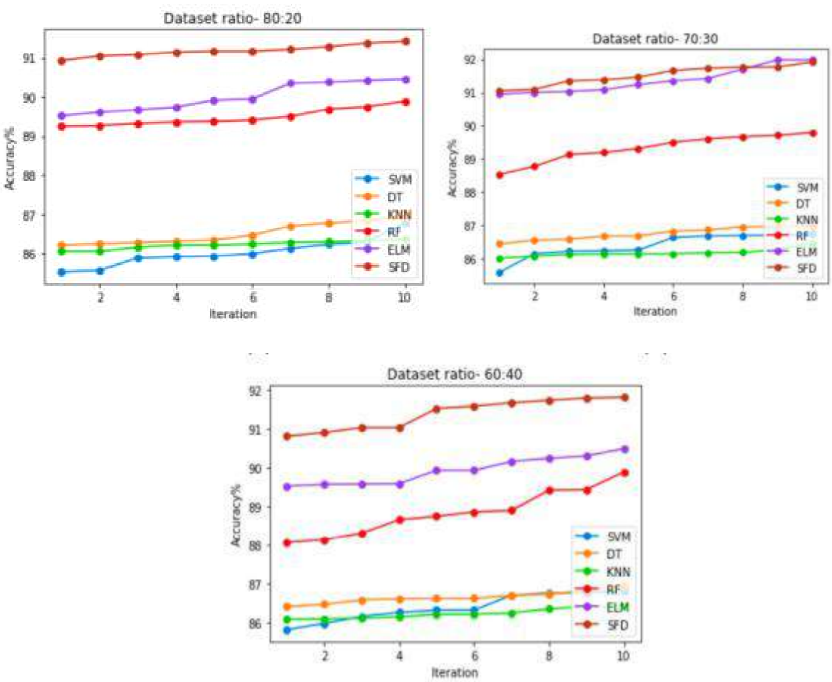


Figure 11: Evaluation of the Accuracy of Various Benign-to-malicious URL Ratios (a) 80:20, (b) 70:30, and (c) 60:40.

In any experiment involving classification or prediction, the dataset is crucial. The dataset includes information that gives the model a high degree of comprehension. To improve model training and produce the best possible output, only pertinent information from the input dataset can be utilized. Therefore, a dataset is essential for developing and evaluating the suggested techniques.

5. CONCLUSION

With the high complexity and occurrence of malicious software, malware analysis forms a critical component of cybersecurity. Creating good protection involves knowledge about malware. Malware analysis enhances the detection and prevention of future attacks by classifying and recognizing different types of malwares. Since machine learning (ML) can analyse enormous amounts of data and detect complex patterns, it is critical to malware analysis. We provide an overview of the latest trends in machine learning-based malware analysis in this paper, explaining each of them. The works analysed demonstrate the merits and efficacy of using XML, DL, and transfer learning methods in malware studies. These methods contribute to the accuracy, explainability, and transparency of malware analysis and detection. Each trend's limitation and challenge are also addressed. We further provide some directions of research that could influence malware analysis in the future based on the survey outcome. These areas are capable of showing interesting opportunities for the field to continue to push itself in the way that will enable it to get past the challenges the researchers are facing. Although this study provides useful insight, it is important to keep in mind that it has some limitations. The findings might not be as generalizable as they potentially could because of the infinitesimal sample size. Repeating these findings with larger samples should be aimed at by later research.

REFERENCES

[1] Faruk, M. J. H., Shahriar, H., Valero, M., Barsha, F. L., Sobhan, S., Khan, M. A., ... & Wu, F. (2021, December). Malware detection and prevention using artificial intelligence techniques. In *2021 IEEE international conference on big data (big data)* (pp. 5369-5377). IEEE.

[2] Anderson, H. S., Kharkar, A., Filar, B., & Roth, P. (2017). Evading machine learning malware detection. *black Hat*, *2017*, 1-6.

[3] Nath, H. V., & Mehtre, B. M. (2014, March). Static malware analysis using machine learning methods. In *International Conference on Security in Computer Networks and Distributed Systems* (pp. 440-450). Berlin, Heidelberg: Springer Berlin Heidelberg.

[4] Saad, S., Briguglio, W., & Elmiligi, H. (2019). The curious case of machine learning in malware detection.

[5] Akhtar, M. S., & Feng, T. (2022). Malware analysis and detection using machine learning algorithms. *Symmetry*, *14*(11), 2304. https://doi.org/10.3390/sym14112304

[6] Dada, E. G., Bassi, J. S., Hurcha, Y. J., & Alkali, A. H. (2019). Performance evaluation of machine learning algorithms for detection and prevention of malware attacks. *IOSR Journal of Computer Engineering*, *21*(3), 18-27.

[7] Urooj, U., Al-Rimy, B. a. S., Zainal, A., Ghaleb, F. A., & Rassam, M. A. (2021). Ransomware Detection Using the Dynamic Analysis and Machine Learning: A survey and Research Directions. *Applied Sciences*, *12*(1), 172. https://doi.org/10.3390/app12010172

[8] Udayakumar, N., Anandaselvi, S., & Subbulakshmi, T. (2017, December). Dynamic malware analysis using machine learning algorithm. In *2017 International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 795-800). IEEE.

[9] Djenna, A., Bouridane, A., Rubab, S., & Marou, I. M. (2023). Artificial intelligence-based malware detection, analysis, and mitigation. *Symmetry*, *15*(3), 677. https://doi.org/10.3390/sym15030677

[10] Haque, M. A., Ahmad, S., Sonal, D., Abdeljaber, H. A., Mishra, B. K., Eljialy, A. E. M., ... & Nazeer, J. (2023). Achieving organizational effectiveness through machine learning based approaches for malware analysis and detection. *Data and Metadata*, *2*, 139-139.

[11] Faruk, M. J. H., Masum, M., Shahriar, H., Qian, K., & Lo, D. (2022, June). Authentic learning of machine learning to ransomware detection and prevention. In *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 442-443). IEEE.

[12] Sharma, P., Kapoor, S., & Sharma, R. (2023). Ransomware detection, prevention and protection in IoT devices using ML techniques based on dynamic analysis approach. *International Journal of System Assurance Engineering and Management*, *14*(1), 287-296.

[13] Alraizza, A., & Algarni, A. (2023). Ransomware detection using machine learning: A survey. *Big Data and Cognitive Computing*, *7*(3), 143. https://doi.org/10.3390/bdcc7030143

[14] Akhtar, M. S., & Feng, T. (2023). Evaluation of machine learning algorithms for malware detection. *Sensors*, *23*(2), 946. https://doi.org/10.3390/s23020946

[15] Lee, K., Lee, S. Y., & Yim, K. (2019). Machine learning based file entropy analysis for ransomware detection in backup systems. *IEEE access*, *7*, 110205-110215.

[16] Buriro, A., Buriro, A. B., Ahmad, T., Buriro, S., & Ullah, S. (2023). MalwD&C: a quick and accurate machine learning-based approach for malware detection and categorization. *Applied Sciences*, *13*(4), 2508. https://doi.org/10.3390/app13042508

[17] Awais, M., Tariq, M. A., Iqbal, J., & Masood, Y. (2023, February). Anti-ant framework for android malware detection and prevention using supervised learning. In *2023 4th International Conference on Advancements in Computational Sciences (ICACS)* (pp. 1-5). IEEE.

[18] Masum, M., Faruk, M. J. H., Shahriar, H., Qian, K., Lo, D., & Adnan, M. I. (2022, January). Ransomware classification and detection with machine learning algorithms. In *2022 IEEE 12th annual computing and communication workshop and conference (CCWC)* (pp. 0316-0322). IEEE.

[19] Bearden, R., & Lo, D. C. T. (2017, December). Automated microsoft office macro malware detection using machine learning. In *2017 IEEE international conference on big data (Big Data)* (pp. 4448-4452). IEEE.

[20] Cuan, B., Damien, A., Delaplace, C., & Valois, M. (2018, July). Malware detection in pdf files using machine learning. In *SECRYPT 2018-15th International Conference on Security and Cryptography* (p. 8p).