International Journal of Advances in Engineering and Management (IJAEM)
Volume 5, Issue 2 Feb. 2023, pp: 733-741 www.ijaem.net ISSN: 2395-5252

Cyber Security Threats and Predictions: A Survey

Amilia Abu Bakar[1], Mohamad Fadli Zolkipli[2]
Hospital Kulim, Kedah, Malaysia[1]
School of Computing, University Utara Malaysia, Sintok, Kedah,Malaysia[2]

Date of Submission: 05-02-2023 Date of Acceptance: 20-02-2023

ABSTRACT: Cyber security threats are becoming more sophisticated and widespread as the world becomes increasingly dependent on technology. The increasing interconnectedness of devices, networks, and systems has created new opportunities for hackers to exploit vulnerabilities in order to steal data, disrupt operations, and cause damage. As technology continues to evolve, it is predicted that threats will become more complex and difficult to detect. Cybercriminals have learned to hack, attack, and breach data with the aid of innovative ways and powerful tools. The introduction of Artificial Intelligence (AI) technology into cyberspace has enabled the development of intelligent models for system defence. Adapting quickly to new conditions, AI technologies have the potential to become indispensable tools for the cybersecurity industry. In this paper, we highlight several research in terms of cyber security predictions using Artificial Intelligence (AI). In addition, emerging trends and recent developments of cyber security threats and challenges are presented. Overall, the ultimate goal of this paper is to serve as a reference point and guidelines for the academia and professionals in the cyber industries, especially from the learning point of view.

KEYWORDS: Cyber Security, Threats, Artificial Intelligence, Cyber Attacks, Predictions

I. INTRODUCTION

The internet, also known as the World Wide Web, has transformed the way people communicate globally over the past 20 years and has become increasingly integrated into their daily lives. With approximately 5.16 billion internet users worldwide, the internet has reached a staggering 64.4% of the world's population [17]. The internet's affordability and advancements have significantly improved its availability, performance, and ease of use, creating a huge global network that contributes billions of dollars to the world economy each year. However, the increased reliance on the internet has also made businesses, government agencies, and financial institutions more vulnerable to cyberattacks. Cyberattacks, which target businesses, military installations, government agencies, or financial institutions such as banks, are illicit attempts to access protected data or extort a ransom [15].Cyber threats are becoming a rapidly increasing menace to the online community, as the frequency of attacks and public awareness of the underlying technology continue to rise. Cyber threats are so prevalent because they are less expensive, more convenient, and less risky than physical attacks, as cybercriminals need only a computer and an internet connection and are not constrained by location or distance [9]. The anonymity of the internet makes it difficult to identify and prosecute cybercriminals, leading to a growing concern about the frequency and complexity of cyber threats. As a result, cybersecurity has become the most important field of study, as it aims to preserve the confidentiality, accessibility, and integrity of data in cyberspace. Althoughcybersecurity is a singular concept, it requires the cooperation of various other industries to ensure its safety.

We will present this paper on Cyber Security threats and prediction by firstly define Cyber Security, follows by Cyber Security Threats definition and type. The remainder section organized as follows. Section 3 introduces Cyber Security Threats Predictions and related work on Cyber Security Threats Predictions. Section 4 summarizes this article in the conclusion part and follows with acknowledgement and references.

II. LITERATURE REVIEW

In today's world, cyber culture has become a widely used and necessary source of information exchange and other professional activities, such as commerce, shopping, bank transactions, advertisements, and services. This exponential increase in online usage has resulted in an exponential increase in cybercrime. This increase is primarily due to the widespread usage of Web applications in almost all areas of life. These Web applications have design vulnerabilities that are exploited by cybercriminals to gain unauthorised access to computers. As a result, cyber security has become a top priority for researchers and practitioners. The growing dependence on the Internet has made it an attractive target for cybercriminals. The pervasiveness of online activities such as e-commerce, social media, and online banking has increased the likelihood of cyber attacks. Cyber security is critical in safeguarding the confidentiality, integrity, and availability of information in cyberspace. Due to the evolving nature of cyber threats, continuous research and development of security measures are necessary.

2.1 DEFINITION OF CYBER SECURITY

There has been significant advancement in cyber security research aimed at supporting cyber applications and mitigating key security vulnerabilities faced by these applications. Cyber Security involves the study of various cyber threats and the development of security strategies (countermeasures) that maintain the confidentiality, integrity, and availability of digital and information technology, according to a study by [9] depicts and explain in Figure 1.

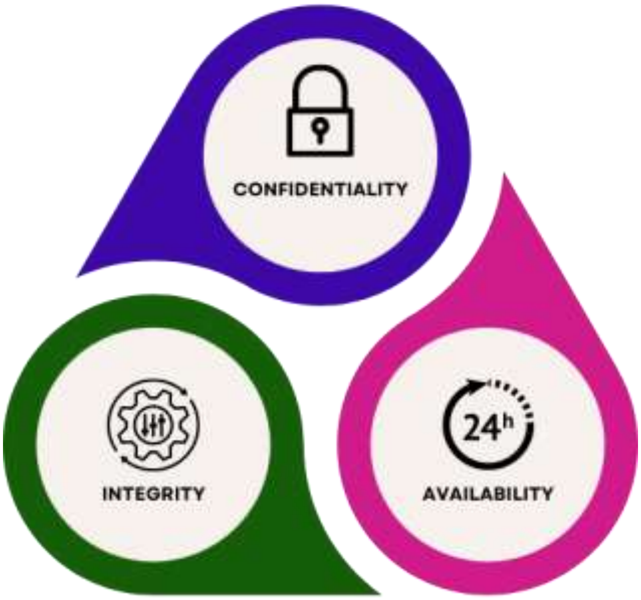

Figure 1: CIA Triad in Cyber Security

- Confidentiality refers to the practice of preventing the disclosure of information to unauthorized individuals or computer systems.
- Integrity refers to term used to prevent any modification or deletion in an authorized manner
- Availability ensures that the systems responsible for providing, storing, and processing information can be accessed when needed and by those who require it.

The goal of cyber security is to safeguard computer systems and networks from cyber threats such as hacking, viruses, and malware.Cyber security research is essential in developing effective measures to counter these threats and enhance the overall security posture of computer systems. Cyber Security, as defined in the research paper by [16], is the protection of internet-connected hardware, software, and data from cyber attacks. It is an essential aspect of businesses' security posture, along with physical security measures to prevent unauthorized access to their data centre and other electronic equipment. According to [7], Cyber Security encompasses a collection of tools, tactics, policies, security measures, security guidelines, risk mitigation strategies, actions, training, best practices, security assurance, and innovative technologies used to secure cyberspace and the assets of users. Cyber security is not limited to a single domain but involves the coordination of multiple other domains to ensure security, as mentioned in research papers by [15] and [12] as depicts in Figure 2.

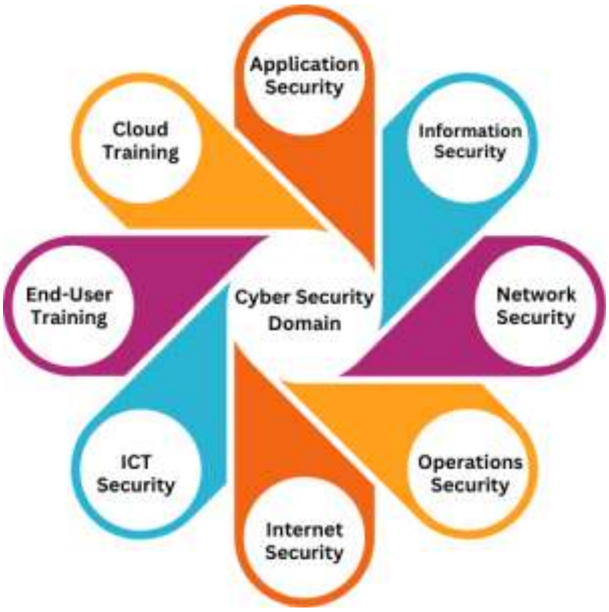

Figure 2: Cyber Security Domain

Cyber Security Domain	Focused Aspects
Application Security	Application security refers to the protection of software applications from external threats and attacks by implementing various security measures. It involves identifying and addressing potential security vulnerabilities throughout the software development lifecycle to ensure that the application is secure from unauthorized access, theft, or damage.
Information Security	Information security refers to the practice of protecting sensitive and confidential information from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves implementing measures to ensure the confidentiality, integrity, and availability of information, and mitigating risks to information security through the use of policies, procedures, and technologies.
Network security	Network security refers to the set of measures taken to protect computer networks and their data from unauthorized access, modification, theft, or destruction. It includes technologies and policies designed to prevent and monitor unauthorized access to a network, detect and respond to security incidents, and ensure the confidentiality, integrity, and availability of network resources.
Operations security	Information security is the practice of protecting sensitive and confidential information from unauthorized access, use, disclosure, disruption, modification, or destruction. It involves the implementation of various security measures to ensure the confidentiality, integrity, and availability of information, including policies, procedures, and technologies.
Internet security	Internet security refers to the measures taken to protect computer systems, networks, and data from unauthorized access, theft, or

	damage over the internet. It aims to ensure the confidentiality, integrity, and availability of information transmitted over the internet through the use of various security measures such as firewalls, encryption, and intrusion detection systems.
ICT security	ICT security, also known as information and communication technology security, is the practice of safeguarding computers, networks, and information from unauthorized access, theft, or damage. It involves implementing various security measures to ensure confidentiality, integrity, and availability of information, such as firewalls, encryption, and access controls. Effective ICT security is essential for protecting sensitive and critical information in modern organizations.
End-User Training	End-user training refers to the process of educating and instructing individuals who use software or technology systems to ensure they can operate them efficiently and securely. It aims to provide individuals with knowledge on the proper usage and handling of technology systems, and best practices for cybersecurity and data privacy.
Cloud Security	Cloud security is the set of measures and technologies used to protect cloud-based infrastructure, applications, and data from unauthorized access, theft, or damage. It involves implementing security controls and policies to ensure confidentiality, integrity, and availability of information stored in the cloud. Effective cloud security is essential to prevent data breaches, comply with regulations, and maintain trust in cloud computing services.

Table 1 : Description on Domain in Cyber Security

Recently, many private firms and government organizations across the worldwide have been confronted with the dilemma of cyber attacks[12]. Protecting this data from cyber attacks is a challenging issue in today's technologically dependent world.

2.2 OVERVIEW OF CYBER SECURITY THREATS

According to [12], cyber threats are incidents that can cause disruptions to missions, tasks, individuals, and national cyber assets through unauthorized access, manipulation of information, destruction, disclosure, or disruption of services. In today's interconnected world, it is difficult for countries to disconnect from cyberspace due to its crucial role in communication and influence. The global nature of the software and hardware supply chain makes it impossible to guarantee their security. Cybersecurity concerns can have a broad impact as they can affect actual operations, unlike a physical bomb with limited range. Access to and control of cyberspace is limited to a few individuals, leaving users unable to manage or modify the software and hardware they use.

2.3 TYPES OF CYBER SECURITY THREATS

Technology is rapidly advancing in a society fuelled by social networks, internet transactions, cloud computing, and automated operations. Cyber criminals are continuously devising new attack techniques, tools, and approaches that enable them to penetrate more complex or tightly controlled environments, cause more harm, and even evade detection. By using unique methods to gain unauthorized access to networks, applications, and data, attackers attempt to compromise the confidentiality, integrity, and availability of information. Their targets range from individuals to small and medium-sized businesses to multinational corporations. With the total number of attacks increasing each year, cyber threats pose a risk to the security of large businesses, jeopardizing information security, business continuity, and customer confidence. Hackers, sabotage groups, organized hackers, terrorists, internal dissatisfied factors, and foreign countries are the six sources of cyber threats [12].

The similarity in international literature [12], [16], [15], [7], [9], [4] listed in Table 2 below as types of Cyber Security Threats :

Types of Cyber Security Threats	Characteristics
Denial of Services Attacks	A denial of service (DoS) attack is a type of cyberattack in which an attacker floods a network or website with traffic, rendering it inaccessible to users. The goal of a DoS attack is to disrupt the normal functioning of a system or network. Instead of launching a single attack against the target, the attacker performs a distributed denial-of-service attack (DDoS).
Ransomware	Ransomware is a type of malicious software designed to block access to a computer system or its data until a ransom is paid to the attacker. It typically encrypts the victim's files and demands payment in exchange for a decryption key. Payment is often demanded in cryptocurrency to avoid traceability.
Malware	Malware is a type of software that is specifically designed to harm, disrupt, or infiltrate a computer system or network without the user's consent or knowledge. It can take various forms such as viruses, worms, trojans, spyware, ransomware, and adware. Malware can steal data, damage systems, and compromise security. Malware infects a system or network when a user clicks on a malicious link, opens an email attachment, or installs risky software. When malware connects with another system or device, it propagates or replicates. Restricting network access, installing extra dangerous software, and collecting data are some of the causes.
Social Engineering	Social engineering is a method of manipulating people to obtain sensitive information or gain access to secure systems by exploiting their trust, naivety, or lack of awareness. It involves using psychological techniques, deception, and impersonation to trick individuals into divulging confidential information, performing actions, or granting access to resources.
Phishing	Phishing is a type of cyber attack where criminals use fake emails, websites, or other electronic communications to trick people into revealing sensitive information such as passwords, bank account details, or credit card numbers. It is typically done by posing as a trustworthy entity to steal personal or financial information.
Man-in-the-middle Attack	A man-in-the-middle (MITM) attack is a type of cyber attack where an attacker intercepts communication between two parties to secretly eavesdrop, modify, or impersonate messages. The attacker relays messages between the legitimate parties without their knowledge, enabling them to read, alter, or inject new content, such as malware or spyware.
Cryptojacking	Cryptojacking is a type of cyber attack where an attacker uses a victim's computer or other device to mine cryptocurrency without their consent or knowledge. The attacker injects a script or malware onto the victim's computer, using its processing power to solve complex mathematical problems and generate cryptocurrency rewards, while causing performance degradation or overheating.

Sql Injection	SQL injection is a type of cyber attack where an attacker exploits security vulnerabilities in a web application's input validation mechanisms to inject malicious SQL code into a database. This allows the attacker to retrieve or modify sensitive data, execute unauthorized actions, or even take control of the entire system.
Zero Day Exploit	A zero-day exploit occurs after a network vulnerability is disclosed but before a patch or solution is put in place. During this time period, attackers target the disclosed vulnerability. Detecting zero-day vulnerability threats necessitates constant awareness.
Spam	Spam refers to unsolicited, unwanted, and often mass-produced messages, typically sent via email, text messages, social media, or instant messaging. These messages are often sent for commercial or fraudulent purposes and can contain malware or phishing links. Spam can also refer to unsolicited comments or posts on websites or forums.
Cross-site scripting (XSS)	A malicious attacker attempts to execute JavaScript code in the client's browser in order to steal sensitive data from the client. It is a widespread vulnerability recently discovered on websites.
Drive-by-Downloads	Concerns unintended malware downloads through the Internet and is increasingly exploited by cybercriminals to rapidly propagate malware. When a user visits a website, opens an email message, or clicks on a deceptive pop-up window, drive-by downloads may occur. Nonetheless, the vast majority of drive-by downloads occur when users visit websites. An increasing number of websites are compromised with a variety of malware.
Brute force attack	Consists of multiple attempts to access protected information (passwords, encryption, etc.) until the correct key is discovered and the information can be accessed.

Table 2 : Types of Cyber Security Threats

III. CYBER SECURITY THREATS PREDICTIONS

As a result of the rapid growth of computer networks, the quantity of cyber attacks has increased significantly. Information technology (IT) solutions and computer networks are crucial to all aspects of our society, such as the administration, the economy, and crucial infrastructures. As a result, they are highly susceptible to cyberattacks. A cyberattack involves the use of one or more computers to assault other computers or networks. The goal of such an assault is generally to render the target computer inoperable, incapacitate its services, or gain access to its information. Indeed, upholding cybersecurity has emerged as one of the most challenging responsibilities in the realm of computer science, and it is anticipated that cyberattacks will continue to advance in complexity and pervasiveness.

3.1 OVERVIEW OF CYBER THREATS PREDICTIONS

Predictive analysis may therefore give organisations an advantage in correctly allocating their limited defence resources. Although the practise of anticipating assaults is not new, automating attack forecasts and predictions was not a common practise in the past. Instead, the majority of attack estimates were based on the opinions of knowledgeable specialists from the cyber-threat landscape. The availability of knowledgeable professionals is limited, and their time is much more so. By reducing biases in predictions and reducing the amount of time specialists spend on forecasts, automation of attack forecasting and prediction will significantly reduce attackers' first mover advantage. To project the continuance of an assault and predict next occurrences, document the attackers' conduct and create a description of an attack for future use.

According to[8] the steps in the anatomy of cyber attacks are defines as follows:

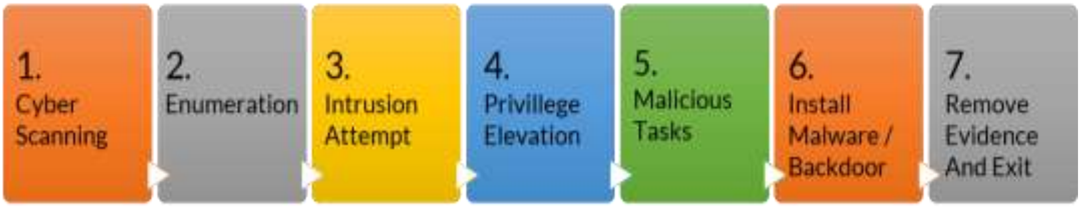

Figure 3: Anatomy of Cyber Attacks

Many different types of cyber attacks follow this simple series of events, which can be seen in network traffic or on the target system, where intrusion detection systems can be detected.

3.2 RELATED WORK

The swift evolution of our society is attributed to the progressions in computing technology, which have had an enormous impact on people's daily routines and professions. Certain technologies have resulted in the creation of machines that can reason, learn, make decisions, and solve problems similarly to humans. Artificial intelligence (AI), for example, emulates intelligence and is capable of performing real-time analysis and decision-making while processing extensive amounts of data to solve problems. Numerous scientific and technological domains can take advantage of AI techniques. The internet contains vast amounts of personal data, presenting numerous cybersecurity challenges. The large volume of data makes manual analysis almost impractical, while the dangers continue to increase, including AI-based attacks. Additionally, the high costs of hiring professionals elevate the expense of preventing hazards. Developing and implementing algorithms that identify these dangers necessitates a substantial amount of time, resources, and effort. One solution for these challenges is to employ AI-based techniques. AI can quickly, accurately, and effectively analyse vast amounts of data. Using the history of threats, an AI-based system can predict similar attacks in the future, even if their patterns change. According to [13], AI can be utilized in cyberspace for the following reasons: AI can detect new and significant changes in attacks, AI can manage enormous amounts of data, and AI security systems can continuously adapt to respond more effectively to attacks.

Typically, this is achieved by establishing a framework to scrutinize enormous datasets of cybersecurity events and detect hazardous behavioral trends. The approach employs data surveillance from past incidents and recorded Indications of Compromise (IOC) to oversee, identify, and counter threats in real-time. Consequently, if similar actions are observed, they are recognized automatically based on the models [13]. Machine Learning (ML) classification techniques utilize IOC datasets to identify and categorize the distinct actions of malwares in datasets. Additionally, behavior-based analysis uses machine learning-based clustering and classification methods to evaluate the conduct of hundreds of malwares. The patterns can further be employed to automate the identification and classification of new threats, allowing security analysts and other automated systems to receive considerable advantages. By examining a historical dataset comprising specific WannaCry-related incidents, ML systems can learn to automatically recognize ransomware attacks that resemble WannaCry. The comparison of Prediction Techniques from relevant publications is shown in Table 3.

Authors	Year	Approach/Model /Technique	Evaluation / Implementation	Findings
[5]	2021	Data Mining	Virus Corpus Dataset	Detection with high precision and less time
[14]	2020	Data Mining	IDS Data Set	Highlight the superiority of the model and its capacity to detect any future cyber-attacks

[3]	2020	Deep Learning Framework	CTF Dataset	Positive prognosis on the outcome of attacks
[19]	2020	Data Mining	National Vulnerability Database	High degree of accuracy and precision in evolutionary patterns
[18]	2019	Data Mining	Various Datasets	Customizing the model to meet the needs of the project and developing domain-specific NLP tools to achieving higher performance cybersecurity incident prediction and discovery approaches.
[6]	2019	Deep Learning Framework	Low interaction honey-pot	Accommodate difficult dataset phenomena, such as long-range dependence and extreme nonlinearity.
[1]	2019	Data Mining	Algorithm called "Time Series" and the model called "SARIMA".	Considerable output accuracy.
[2]	2018	Bayesian State Space Model	CPSS Dataset	Ability to predict cyber-attacks over time

Table 3: Comparison on Prediction Methods

IV. CONCLUSIONS

Enhancing defensive capabilities in the digital realm to enhance cybersecurity is one of the most critical issues to be addressed to enable robust societies and modern living that is becoming increasingly reliant on information technology. It is essential to scrutinize past events and predict the future to devise new security measures and software to safeguard socially sensitive data and crucial infrastructure from assailants. Anticipating future cyberattacks can provide benefits to individuals, organizations, and society. Thus, minimizing the attackers' first-mover advantage must be a research priority. In this analysis, we provided a survey of the literature on cyber threats, attack prediction methods, and types. The results indicate that most researchers prefer Artificial Intelligence (AI) techniques, such as Data Mining and Deep Learning, for predicting attacks. To summarize, the issue of predicting cyberattacks is an intriguing research challenge that has been tackled by numerous scholars. The features of the data sets affect how well the current machine learning algorithms for cyber-security work. The attack variety of today's must be correctly reflected in data sets. Existing data sets must be updated often for this. The findings have made AI approaches an essential component of cyber-security, but it's important to be aware of their disadvantages. Although artificial intelligence technologies have made detections more self-sufficient, it still doesn't seem viable to ensure comprehensive security without human supervision [18].

ACKNOWLEDGEMENT

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Ethical Hacking & Penetration Testing Research Project. This work was supported by Universiti Utara Malaysia.

REFERENCES

[1]. Amarasinghe, A. M. S. N., Wijesinghe, W. A. C. H., Nirmana, D. L. A., Jayakody, A., & Priyankara, A. M. S. (2019). AI Based Cyber Threats and Vulnerability Detection, Prevention and Prediction System. International Conference on Advancements in Computing (ICAC) (pp. 363-368). IEEE.

[2]. Bakdash, J. Z., Hutchinson, S., Zaroukian, E. G., Marusich, L. R., Thirumuruganathan, S., Sample, C., & Das, G. . (2018). Malware in the future? Forecasting of analyst detection of cyber events. Journal of Cybersecurity, 4(1), tyy007.

[3]. Ben Fredj, O., Mihoub, A., Krichen, M., Cheikhrouhou, O., & Derhab, A. (2020). CyberSecurity attack prediction: a deep learning approach. 13th International Conference on Security of Information and Networks, (pp. 1-6).

[4]. Bendovschi, A. (2015). Cyber-attacks–trends, patterns and security countermeasures. Procedia Economics and Finance, 28, 24-31.

[5]. Desai, V., Oza, K., & Naik, P. (2021). Data mining approach for cybersecurity. . International Journal of Computer Applications Technology and Research, 10, 035-041.

[6]. Fang, X., Xu, M., Xu, S., & Zhao, P. (2019). A deep learning framework for predicting cyber attacks rates. EURASIP Journal on Information security, 1-11.

[7]. Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. . (2020). Cyber security threats and vulnerabilities: a systematic mapping study. Arabian Journal for Science and Engineering, 45, 3171-3189.

[8]. Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. . (2018). Survey of attack projection, prediction, and forecasting in cyber security. . IEEE Communications Surveys & Tutorials, 21(1), 640-660.

[9]. Julian Jang-Jaccard, Surya Nepal. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences,, 973-993.

[10]. Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. . Energy Reports, 7, 8176-8186.

[11]. Morovat, K., & Panda, B. (2020). A survey of artificial intelligence in cybersecurity. International Conference on Computational Science and Computational Intelligence (CSCI), (pp. 109-115).

[12]. Rahman, M. A., Al-Saggaf, Y., & Zia, T. . (2020). A data mining framework to predict cyber attack for cyber security. 15th IEEE Conference on Industrial Electronics and Applications (ICIEA) (pp. 207-212). IEEE.

[13]. Saravanan, A., & Bama, S. S. . (2019). A review on cyber security and the fifth generation cyberattacks. Oriental journal of computer science and technology, 12(2), 50-56.

[14]. Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. International Journal of Advanced Research in Computer and Communication Engineering, 7(11), 125-128.

[15]. Statista. (2023, January). Retrieved from https://www.statista.com/statistics/617136/digital-population-worldwide/

[16]. Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. . (2018). Data-driven cybersecurity incident prediction: A survey. IEEE communications surveys & tutorials, 21(2), 1744-1772.

[17]. Williams, M. A., Barranco, R. C., Naim, S. M., Dey, S., Hossain, M. S., & Akbar, M. (2020). A vulnerability analysis and prediction framework. Computers & Security,92.

[18]. Ahmetoglu, H., & Das, R. (2022). A comprehensive review on detection of cyber-attacks: Data sets, methods, challenges, and future research directions. Internet of Things, 100615.