Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
ISSN:2521-3504(online) ISSN:2074-0204(print)

A Review on Cyber Security and Cyber Attacks

Duaa Fadhel Najem[1], Suhad Muhajer Kareem[2]

[1,2]University of Basrah, College of computer science and information technology, Department of Cyber Security, Iraq. duaa.najem@uobasrah.edu.iq:

suhad.kareem@uobasrah.edu.iq

ARTICLE INFO

Article history:
Received: 19/03/2025
Rrevised form: 08/04/2025
Accepted : 15/05/2025
Available online: 30/06/2025

Keywords:

Cyber-attacks, Cyber security, Cyber threats, network security, Information technology

ABSTRACT

As technology has advanced, data protection has gotten more challenging. Information security now depends on cyber security. These days, protecting information is one of the biggest problems. Unquestionably, the Internet has created a new avenue for exploitation known as cybercrime because of the limitless amount of free websites. To combat these cybercrimes, both the public and business sectors are implementing a number of initiatives. Managing cyber security is a major challenge. In addition to presenting new trends and issues in the realm of cyber security, this research study focuses on upcoming technologies. It is anticipated that the thorough review study offered to scholars studying IT and cyber security will be beneficial. This analysis examines current advancements, difficulties, and new technology in the cybersecurity space. We concentrate on important ideas like cyber threats, and cyber threat intelligence. The relevant literature from 2020 to 2024 is evaluated using a systematic review methodology. This study aims to explore current trends, challenges, and future directions in cybersecurity and identify major cyber threats.

https://doi.org/10.29304/jqcsm.2025.17.22195

1. Introduction

The Internet has grown in significance during the past 20 years and permeated people's lives worldwide, facilitating global contact. Around 3 billion people utilize the Internet globally today Because of advancements and reasonably priced access in this industry, which have significantly increased its availability, functionality, and use [1]. Most covers interactions among people, governments, governmental institutions, and non-governmental groups now occur online [2]. The development of cyberspace has led to the emergence of modern challenges in the field of security that countries are currently facing. Threats including cyberwarfare, cybercrime, cyberterrorism, and cyberespionage have been brought about by the ease of access at low cost, the advantage of anonymity, the unpredictability of risk areas, the strong influence, and the lack of public transparency in cyberspace. Governments, criminal organizations, terrorist organizations, and even private citizens are examples of both strong and weak players [3].

∗Corresponding author: Suhad Muhajer Kareem

Email addresses: *suhad.kareem@uobasrah.edu.iq*

Communicated by 'sub etitor'

Cyber threats are different from traditional national security issues in that they are less secretive than core security issues that involve identifiable governments and states in a particular area. As a result, traditional national security is being challenged and losing its effectiveness in this area [4].

Experts have been considering the potential repercussions of cyberattacks over the course of nearly a decade. Various situations can arise that may cause significant financial or physical losses, and may even have a wide-ranging impact [5]. Therefore, if governments cannot formulate a comprehensive definition of cyberattack that is accepted and supported by the international community, this will remain a major challenge. Specialists must address the different aspects of the problem, provide legal advice and conduct the necessary assessments. Thus, the issue of what qualifies as a cyberattack arises. What are its traits, and is it essentially any Cyberattacks can be categorized as a specific type of attack, whether in the conventional or classic meaning. A methodical strategy was taken in this literature study. We used major academic databases like Google Scholar, IEEE Xplore, SpringerLink, Science Direct, and Scopus. "Cybersecurity," "Cyberthreats," "AI in Cybersecurity," "Threat Intelligence," and "Zero Trust Architecture" were among the keywords.

Peer-reviewed English-language research directly pertaining to cybersecurity from 2020–2024 is a requirement for inclusion. Non-peer-reviewed sources, out-of-date publications, and non-technical viewpoints are all excluded.

This is how the remainder of the study is organized. A thorough discussion of cyber security is reviewed in Section 2. We next went into cybercrimes in section 3. The history of cybercrime and the use of cyber security instruments in our study are illustrated in Section 4. The kinds of Cyber Attacks are described in Section 5. Section 6 discusses Cyber Ethics Cybersecurity in detail and in Section 7 we display recent studies in cybersecurity from 2020 to 2024, while Section 8 offers the conclusion.

2. Cyber Security

Cybersecurity should be an essential part of any organization's infrastructure. In short, it should be a cornerstone of any organization that places a high priority on cyber security can succeed greatly and accomplish big things because of its capacity to shield customer and private data from rivals. Providing this protection must be a top priority for a business or organization in order to develop and expand [6]. Cybersecurity involves the measures taken to defend against attacks, whether from outside or inside, on data and networks. Cybersecurity professionals protect computer systems, internal networks, servers, and networked systems. Cybersecurity ensures controlled access to information so that only authorized individuals can view it [7]. Understanding the many types of cyber security is crucial for improving safety. The several types of cyber security are listed in Fig. 1.

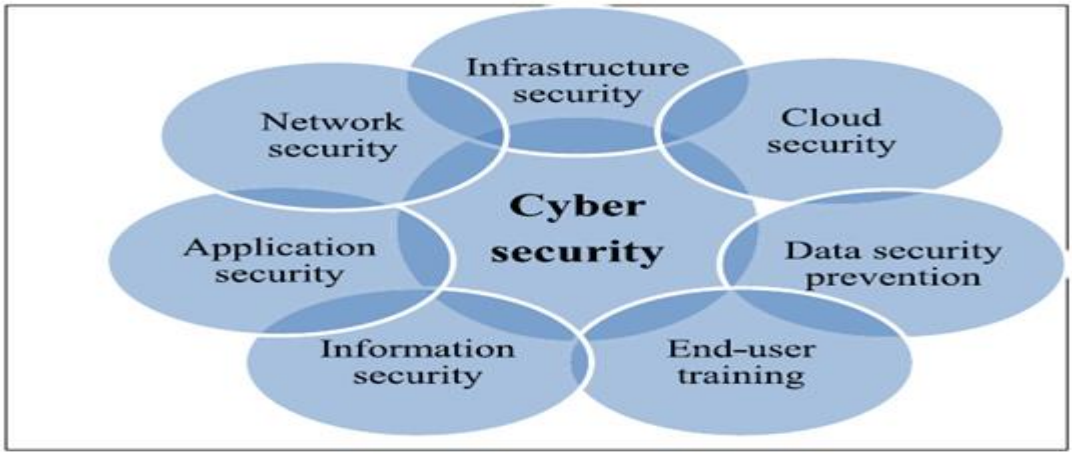

Fig. 1 Various forms of cyber security

3. Cyber Crimes

Any unlawful behavior that primarily involves stealing from a computer is referred to as cybercrime. The idea of cybercrime has been enlarged by the US Department of Justice to cover any illegal behavior involving the storing of evidence on a computer. The concept of cybercrime has been broadened by the US Department of Justice to encompass any illegal behavior including the storing of evidence on a computer. Cybercrimes include crimes that are made possible by computers, including network intrusions and computer virus transmission, as well as crimes that are computer-based incarnations of crimes that already existed, like terrorism, identity theft, stalking, and bullying. Both the public and the government now consider these crimes to be serious problems. To put it simply, cybercrime is when someone sells illegal goods, pursues people, steals someone's identity, or employs malicious software to interfere with business activities. The increasing significance of technology in people's lives will lead to an increase in cybercrime. The intersection of attack, crime, and breach is depicted in Fig. 2 [8].

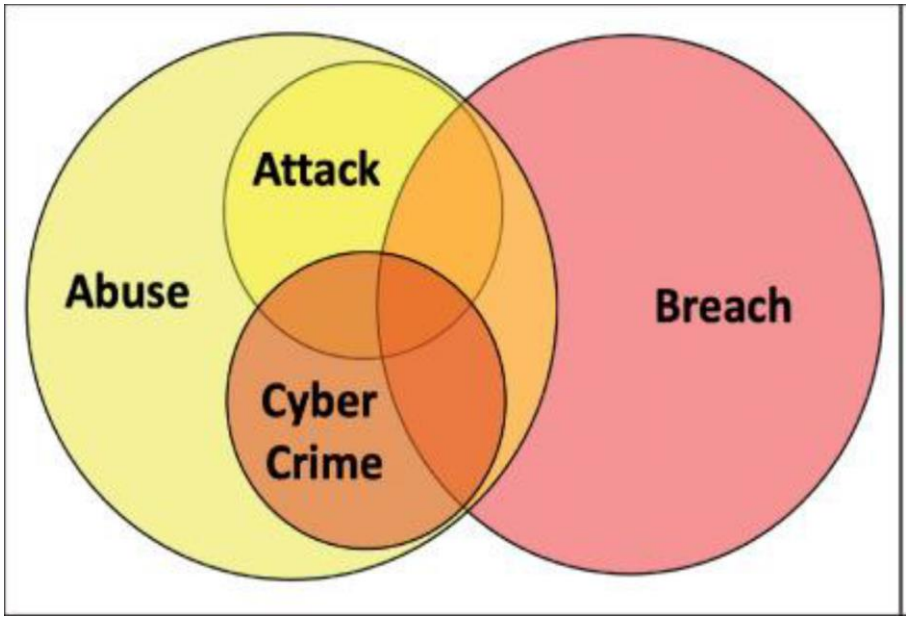

Fig. 2: Intersection of attack, crime and breach

4. History of Cybercrime and Cyber Security

This organized table (1) highlights significant occasions, turning points, and advancements throughout the history of cybersecurity and cybercrime:

Table 1 - History of Cybercrime and Cyber Security

Year/Period	Event/Development	Description
1940s	Early Computer Hacking	In the earliest computing experiments, systems were manipulated, but not intentionally.
1950s-1960s	Birth of Computer Viruses	From John von Neumann, theoretical concepts of self-replicating programs were developed.
1971	First Recognized Virus: "Creeper"	As an ARPANET experiment, "Creeper" shown "I'm the creeper, catch me if you can."
1981	First Personal Computer Virus	The "Elk Cloner" virus infected Apple II computers through floppy disks.
1986	First PC Virus: "Brain"	It was the first virus to infect IBM PCs and was created by two brothers from Pakistan.
1988	The Morris Worm	The CERT/CC (Computer Emergency Response Team) was established as a result of the extensive disruption caused by one of the first significant Internet-distributed worms.
1990s	Rise of Phishing and Malware	As personal computing increased, bad malware and email frauds became more prevalent.
1991	Birth of Antivirus Software	The launch of Norton Antivirus signified the beginning of the commercialization of cybersecurity products.
1995	Growth of Cybercrime Organizations	For financial gain, organized crime groups started to take advantage of the internet.
1998	First Major Government Cyberattack	The Solar Sunrise hack exposed weaknesses in national security by focusing on US military networks.
2000	"ILOVEYOU" Virus	A huge email worm caused billions of dollars' worth of harm by infecting millions of machines worldwide.
2003	Creation of the Anonymous Hacker Group	The emergence of the hacktivist collective Anonymous led to the commencement of political campaigns and cyberattacks.
2007	Estonia Cyberattacks	The Estonian government, banks, and media outlets were rendered inoperable by a string of DDoS strikes.
2009	Operation Aurora	Chinese actors were accused of launching a cyber-espionage campaign against Google and other businesses.
2010	Stuxnet Worm	Cyberwarfare began when a very advanced cyberweapon struck Iranian nuclear installations.
2014	Sony Pictures Hack	Sensitive company communications and data were made public by a North Korean-attributed cyberattack.

5. Kinds of Cyber Attacks

The attacker often begins by flooding the targeted systems with various messages, blocking legitimate data flow and preventing any communication between the system and other systems or the network. The main categories of cyber-attacks, as shown in Fig. 3, include denial-of-service attacks, logic bombs, abuse tools, spyware, Trojans, worms, viruses, spam, and botnets. If a denial-of-service attack is carried out, authorized users cannot access the system, and vice versa. A different method is called broad denial of service, in which numerous distributed systems launch an attack at once rather than starting from a single source. Sometimes, in order to attack the victim, worms spread across several computers. There are publicly available abuse tools that enable network vulnerabilities to be identified and exploited with varying degrees of expertise [9].

A different kind of assault known as a logic bomb is a situation where a programmer enters code into a program, and when a specific event occurs, a destructive action is automatically executed. In addition, a program called a 'Sniffer' is used to intercept data and analyze each packet in the data stream for information such as passwords. Trojans hide malicious code inside programs that the user wants to run. Furthermore, the virus creates copies of itself inside frequently used system files, disabling them. By loading these infected files into memory, the virus is able to infect other files. Unlike worms, the virus requires human intervention to spread. In contrast, a worm is a program that has the ability to spread by jumping from one computer to another within a network [10].

A group of systems that have been hacked and are under remote control is known as a "botnet." used for message theft, spam, virus distribution, and attack planning.

In order to achieve their malicious goals, Botnets are typically installed covertly on a target device, allowing an attacker to remotely access the system without authorization. Another name for botnets is electronic troops. To analyze the cybersecurity threats and their impact on WAMS-based FFR control, [11] adopted a unique CNN scale to handle the forgery data extracted from two scales. In addition, they investigated the cybersecurity protection framework using time and frequency in the FFR system. Higher accuracy and resilience were demonstrated by the results while using real synchrophasor data.

Makrove's hidden knowledge-based model is adopted to design a unified approach to respond to a cyber-attack. They also looked at an updated HMM approach for approximating security states. By conducting a case, the developed method's validity has been proven. Zhang and Malakaria developed a decision support system in the field of cybersecurity to assist in selecting the optimal security portfolio for preventing multistage cyberattacks [12]. To identify persistent threats, such system had preventive and online optimizations backed by an LM. To choose the most successful solutions, they determined that the online game was a Bayesian STACKELBERG.

[13] Investigated the factors that could lead to a cyberattack on NPPs. Both AHP and FA were used to determine the relative importance of variables associated with NPP potential. They discovered that there was a higher chance of adoption for the Korean cyber security strategy.

Tosun asserts that cyberattacks generate sudden, negative shocks to a company's reputation [14].

As a result of additional comebacks, financial markets also respond adversely to corporate security breaches. The trading rate also increased as a result of increased liquidity and selling pressure. As target corporations continue to pay their CEOs, R&D and dividends gradually decrease.

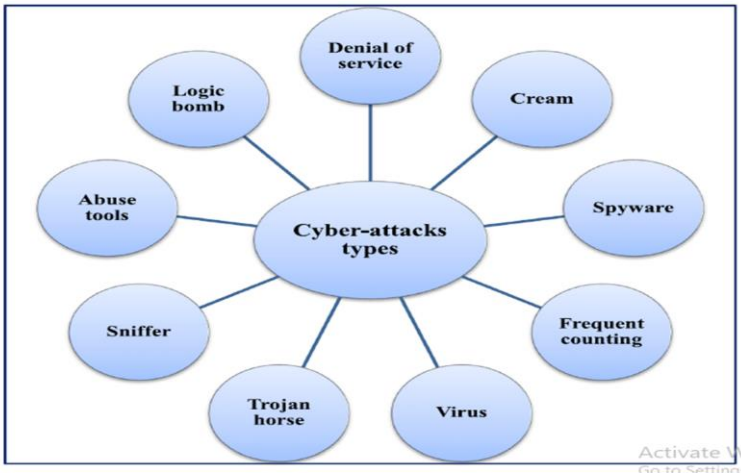

Fig. 3. Main cyber-attacks types.

The methods that hackers most commonly use are listed in Table 2. The three pillars of availability, integrity, and secrecy form the foundation of any organization's security. Since the development of computers, the industry standard for systems security has been the security triangle, or CIA, since the development of computers, the industry standard for systems security has been the security triangle, or CIA, which consists of these three components.

"The CIA triad—comprising Confidentiality, Integrity, and Availability—serves as a foundational analytical framework in cyber security. In this review, it is used to categorize different types of cyber threats and evaluate the effectiveness of various security measures. For instance, ransomware attacks predominantly affect availability, while phishing and data breaches target confidentiality." For more information, see [15].

Table 2- Cybercriminals' standard methods

Technique	Overview	Reference
Denial of Service	Because a hacker has used up all of the server's resources, system users are unable to access the service.	(Alghamdi, M.I., 2021)
The Man in the Middle	Occurs when a hacker places himself between the router and the victim's device to intercept or change data packets.	(Huang, J., et al., 2020)
Malware	Malware may infect users' devices when they come into contact with viruses or worms.	(Ma, L., et al., 2021)
Phishing	This technique involves a hacker acting as a legitimate email sender and seeking users to disclose sensitive information.	(Saxena, R., Gayathri, E., 2021)

The idea of secrecy states that sensitive information and characteristics, such as military secrets, should only be accessed by those who have been granted authorization (Confidentiality). The integrity principles state that only authorized resources and individuals may add, modify, or delete sensitive information and features. False information entered into a database (Integrity) is one example. Systems, functions, and data must meet certain requirements in order to be made available on demand by the SLA service level (Availability), in accordance with availability principles [16].

The best cybersecurity practices go against the aforementioned guidelines. This is a simple defense that a skilled hacker could easily overcome. The larger a corporation is, the more complicated cyber-security becomes. Another cyber-security limitation is the growing involvement in both the real and virtual worlds of data exchange. One key difficulty in the realm of cyber-security is the shortage of qualified staff. Many persons at the lower end of the cyber-security spectrum have general capabilities. A comprehensive strategy considers all of these elements and excludes none [17].

The main infrastructure in the world functions as both physical and cyber. We gain greatly from this amazing facility. However, putting a system online makes it more susceptible to hackers and cyberattacks. Decision-makers in the organization must include the potential impact of assaults on their performance in their agenda. Web application security is viewed by many of the top new hackers as the most vulnerable area for an assault on a business. The first line of defense for application security is robust encryption [18].

Every strategy needs to be specially created and applied in a unique way for every company. Information hacking and infiltration are thus less common. The complexity of cyber-security is rising. Organizations need to approach cybersecurity from a "security perspective." To stay ahead of hackers, you must thus always maintain good security. As security measures improve, the same applies to investing in cybersecurity services and systems. According to Trend Micro, and Snowe, McAfee, Cisco, and Chandra are one of three prominent companies in the industry [19].

6. Cyber Ethics Cybersecurity

Cyber has effectively communicated information and increased community yield over time. Cyber is utilized in a variety of industries and applications, but boosting output has always been taken into consideration. Rapid data transport to the internet generally results in a reduction of system security [20].

The term "cyber ethics" in cybersecurity refers to the moral standards and directives that regulate how people, groups, and governments behave online. It entails being aware of how digital behavior affects security, privacy, and the general welfare of people and society [21].

Below is a summary of its main components:

1. Privacy: - Ethical Management of Personal Data: One of the main issues in cybersecurity is safeguarding people's privacy. This entails making certain that people's consent is acquired when necessary and that personal data is gathered, stored, and treated appropriately. Data Protection: Making sure solutions are built and put into place to stop unwanted access to private and sensitive data is part of ethical cybersecurity practices.

2. Integrity: - Information system security: It is essential to make sure that the data in systems is correct, unchangeable, and shielded from manipulation. This is essential to preserving organizations' and users' faith in the systems' integrity.

Ethical Hacking: Experts who perform vulnerability assessments or penetration tests must do it with the organization's permission, without causing harm, and with the intention of enhancing security.

3. Accountability: - Accountability for activities**:** Those who create, oversee, or operate with digital systems are responsible for their actions, particularly if they lead to security lapses, invasions of privacy, or harm to their reputation.

Monitoring and Enforcement: To preserve public confidence in cybersecurity, procedures for identifying ethical transgressions and making sure that there is a system of accountability for them must be put in place.

4. Access and Equity: - Equal Access to Technology: Another aspect of cybersecurity ethics is making sure that everyone has equitable access to the tools and technology required for online safety.

5. Confidentiality: - Protecting Sensitive Information: One of the main ethical responsibilities in cybersecurity is to make sure that private, business, or financial information is protected from unwanted disclosure.

NDAs, or non-disclosure agreements: Professionals in the sector must adhere to confidentiality agreements and nondisclosure agreements in order to keep sensitive information private.

7. Cybersecurity vs. Cybercrime: -

Stopping Cybercrime: Ethical cybersecurity is supporting law enforcement when needed and preventing unlawful activities such as ransomware attacks, phishing, hacking, and identity theft. Hacking for malevolent intents or without permission is regarded as immoral and unlawful, whereas ethical hacking is a valid and essential technique for detecting vulnerabilities.

7. Transparency: - Clear Disclosure of Security Risks: Companies have an ethical obligation to alert users to security concerns and breaches as soon as possible. This includes disclosing specifics about these flaws and the steps being taken to address them.

8. Making Ethical Choices Despite Emerging Technologies:-Automation and AI: As automated systems and artificial intelligence (AI) become more prevalent in cybersecurity, ethical choices about the application of AI systems must be made to prevent bias, discrimination, or negative consequences.

9. Balancing Security and Freedom: - Freedom of Expression: Protecting people's rights to free speech and information access while maintaining system security is a crucial component of ethical cybersecurity. In conclusion, the goal of cyber ethics in cybersecurity is to protect networks and systems while preserving people's rights, privacy, and freedoms. Decisions about risk, security, and the wider impact on society should be made in accordance with ethical standards.

8. Recent Studies in Cybersecurity (2020–2024)

1- **Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., Bisztray, T., & Debbah, M. (2024) [22]:** The future of cybersecurity using large language models (LLMs) and generative artificial intelligence (AI) is thoroughly reviewed in this study. We investigate LLM applications in a number of fields, including as software engineering, design verification, intrusion detection, malware detection, phishing detection, cyber threat intelligence, and hardware design security. We give a summary of the development and status of LLM, emphasizing improvements in models such LLaMA, BERT, Falcon2, Mixtral-8x7B, GPT-4, GPT-3.5, and BERT.

2- **Rios, T. N., and Mendes, C. (2023) [23]:** In order to determine which XAI approaches have been used in cybersecurity and which fields, this paper aims to examine the present research scenario on XAI applied to cybersecurity. Already profited from this technique in the field of cybersecurity.

3- **Vasoya, S., Bhavsar, K., & Patel, N. (2022) [24]:** Cybersecurity is really important in the field of information technology. One of the top concerns of our day is information security. When we think of cybersecurity, the first thing that comes to mind is cyberattacks, which are becoming more frequent and include ransomware. Many governments and businesses use a variety of tactics to combat cybercrime. Even with various cybersecurity precautions, ransomware still frightens people.

4- **Podder, P., Bharati, S., Mondal, M. R. H., Paul, P. K., & Kose, U. (2021) [25]:** This study provides a comprehensive examination of the application of deep learning (DL) methods in cybersecurity. This paper provides a quick overview of deep belief networks, generative adversarial networks, recurrent neural networks, and other DL approaches used in cybersecurity. The differences between shallow learning and deep learning are then illustrated. The effectiveness of DL approaches in preventing cyberattacks is also covered, as well as the current status of cyberattacks in IoT and other networks.

5- **Lee, I. (2020([26]:** A four-layer approach for IoT cyber risk management is presented in this study. Additionally, a linear programming approach is used in this research to distribute funds across several IoT cybersecurity initiatives. As a proof of concept, an example is given.

9. Conclusion

Procedures that prevent security threats, data breaches, and cyberattacks are referred to as cybersecurity. In general, the word "cybersecurity" raises several questions, such as: What types of risks and difficulties do businesses face? What can be done to reduce these attacks? Who is most at risk? What steps must be taken to lower risks of cyberattacks? However, many questions remain unanswered. This analysis examines current advancements, difficulties, and new technology in the cybersecurity space. We concentrate on important ideas like cyber threats, and cyber threat intelligence. The relevant literature from 2020 to 2024 is evaluated using a systematic review methodology. This study aims to explore current trends, challenges, and future directions in cybersecurity and identify major cyber threats.

References

[1] Tan, S., et al., 2021. Attack detection design for dc microgrid using eigenvalue assignment approach. Energy Rep. 7, 469–476.

[2] Aghajani, G., Ghadimi, N., 2018. Multi-objective energy management in a micro-grid. Energy Rep. 4, 218–225.

[3] Xu, H., Sun, L., Zhai, E., & Huang, J. 2024. Large language models for cyber security: A systematic literature review. arXiv. https://arxiv.org/abs/2405.04760

[4] Nazario, M., & Alghazzawi, D. 2023. Cyber Threat Intelligence for Security Decision-Making: A Review and Research Agenda. Computers & Security, 133, 103392.

[5] Cao, J., et al., 2021. Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks. Inform. Sci. 548, 69–84.

[6] Vaddadi, S. A., Syed, T. A., & Waghmare, L. M. 2023. A comprehensive review study of cyber-attacks and cyber security. International Journal on Recent and Innovation Trends in Computing and Communication, 11(5(.

[7] Ahmed Jamal, A., et al., 2021. A review on security analysis of cyber physical systems using machine learning. Mater.

[8] Alqarni, M., Alshamrani, A., Khan, R., & Zaman, N. 2024. Economic impact of cyber attacks and effective cyber risk management strategies: A light literature review and case study analysis. Procedia Computer Science, 228, 392–400.

[9] Amet, R. 2023. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333. https://doi.org/10.3390/electronics12061333.

[10] Aziz, A.A., Amtul, Z., 2019. Developing Trojan horses to induce, diagnose and suppress Alzheimer's pathology. Pharmacol. Res. 149, 104471.

[11] Qiu, W., et al., 2021. Time-frequency based cyber security defense of wide-area control system for fast frequency reserve. Int. J. Electr. Power Energy Syst. 132, 107151.

[12] Zhang, Y., Malacaria, P., 2021. Bayesian Stackelberg games for cyber-security decision support. Decis. Support Syst. 148, 113599.

[13] Kim, Y.S., et al., 2020. Development of a method for quantifying relative importance of NPP cyber attack probability variables based on factor analysis and AHP. Ann. Nucl. Energy 149, 107790.

[14] Tosun, O.K., 2021. Cyber-attacks and stock market activity. Int. Rev. Financ. Anal. 76, 101795.

[15] Pfleeger, C. P., & Pfleeger, S. L.2012. Security in computing (5th ed.). Prentice Hall.

[16] Nguyen, D.C.L., Golman, D.W., 2021. Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'. Comput. Law Secur. Rev. 40, 105521.

[17] Associated Press. 2024. Europe's cybersecurity chief says disruptive attacks have doubled in 2024, sees Russia behind many.

[18] The Times. 2024. The Times view on hackers: Cybermen. https://www.thetimes.co.uk/article/the-times-view-on-hackers-cybermen-n9stm26ls

[19] Katrakazas, C., et al., 2020. Cyber security and its impact on CAV safety: Overview, policy needs and challenges. In: Milakis, D., Thomopoulos, N., van Wee, B. (Eds.), Advances in Transport Policy and Planning. Academic Press, pp. 73–94 (Chapter 3).

[20] Cybersecurity and Infrastructure Security Agency (CISA). 2023. CSRB year in review 2023. https://www.cisa.gov/resources-tools/resources/csrb-year-review-2023

[21] Doe, A. 2021. "The Rise of Ransomware: Challenges and Solutions." Journal of Cybersecurity, 14(2), 123-134.

[22] Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., Bisztray, T., & Debbah, M. 2024. Generative AI in Cybersecurity: A Comprehensive Review of LLM Applications and Vulnerabilities.

[23] Mendes, C., & Rios, T. N. 2023. Explainable Artificial Intelligence and Cybersecurity: A Systematic Literature Review. arXiv.

[24] Vasoya, S., Bhavsar, K., & Patel, N. 2022. A systematic literature review on ransomware attacks. ArXiv.

[25] Podder, P., Bharati, S., Mondal, M. R. H., Paul, P. K., & Kose, U. 2021. Artificial neural network for cybersecurity: A comprehensive review. arXiv.

[26] Lee, I. 2020. Internet of Things (IoT) Cybersecurity: Literature Review and IoT Cyber Risk Management. Future Internet, 12(9), 157.