Mesopotamian journal of Cybersecurity
Vol.2023, **pp.** 57–63
DOI: https://doi.org/10.58496/MJCS/2023/010; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/CyberSecurity

Review Article

Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview

Maad M. Mijwil[1,*], Omega John Unogwu[2,3], Youssef Filali[4], Indu Bala[5], Humam Al-Shahwani[6]

[1] *Computer Techniques Engineering Department, Baghdad College of Economic Sciences University, Baghdad, Iraq*

[2] *Space Geodesy and Systems Division, Centre for Geodesy and Geodynamics, National Space Research and Development Agency, Nigeria*

[3] *Department of Computer Science, Azteca University, Chalco, Mexico*

[4] *Department of Computer Science, Faculty of Sciences Dhar-Mahraz, University of Sidi Mohamed Ben Abdellah, Fez, Morocco*

[5] *School of Electrical and Electronics Engineering, Lovely Professional University, Punjab, India*

[6] *Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka, Malacca, Malaysia*

ARTICLE INFO

Article History

Received 22 Dec 2022
Accepted 3 Mar 2023
Published 6 March 2023

Keywords

Cybersecurity

Sensitive information

Artificial intelligence

Cyberattacks

Digitization

ABSTRACT

The term cybersecurity refers to an environment capable of protecting digital devices, networks and information from unauthorized access and preventing data theft or alteration. It is composed of a collection of carefully crafted techniques, processes, and practices to protect sensitive information and deterring cyber-attacks. In the recent period, the domain of cybersecurity has undergone rapid growth in response to the increasing cyber threats. Cybersecurity includes important tactics that help protect the digital environment, which are firewalls, encryption, secure passwords, and threat detection and response systems. Employees must be trained on these tactics. This article will discuss the five most pressing challenges facing the cybersecurity industry today that must be taken into account by businesses, organizations, and individuals in order to secure their confidential data from cybercrime. The conclusion of the article highlighted the significance of growing awareness about cybersecurity risks in order to effectively handle digital environments and protect them from any electronic threats.

1. INTRODUCTION

In recent years, there has been substantial growth in electronic attacks over the Internet, and it is expected that there will be new strategies in the future. Cyber-attacks are a set of tactics carried out by individuals with the ability to exploit gaps in electronic systems and networks, often with the intent of damaging systems or accessing and viewing sensitive information [1-6]. These attacks can be carried out from a variety of different websites (unnatural links or fake) or malicious applications and are known to affect a wide range of different types of industries [7-12]. Every form of electronic attacks poses a major threat to the security of companies, institutions and even individuals because they can lead to the theft of data and information from their devices. Moreover, these attacks are characterized by the ability to disrupt services, business processes, and other things within the digital environment. Consequently, it is important for organizations to adopt a set of practical tactics to address this issue in order to prevent it from having a harmful impact on their operations in the digital environment. Organisations or institutions depend on monitoring, detection, prevention and response techniques, which are the most widely used methods to prevent cyber-attacks. They are continually seeking to develop these strategies and make them more effective and able to know the behaviour of electronic attacks. Cyberattacks can be described as malicious activities that target computer systems, networks, and devices over the Internet, intending to endanger or damage sensitive information [13-20]. Computer systems are among the most desirable systems to be controlled by unauthorized persons because the information included within these systems is very necessary to them [21]. These attacks can originate from a single individual or a group of individuals who may be motivated by financial gain, political activity, or even personal motives. Figure 1 shows that the costs of cybercrime will rise to more than $23 trillion by 2027.

*Corresponding author. Email: mr.maad.alnaimiy@baghdadcollege.edu.iq

A variety of tactics are utilised to execute cyberattacks, including viruses, malware, phishing attempts, and denial-of-service (DoS) assaults [23][24]. Viruses and malware are powerful tools that have the practical ability to infect computer systems, disable their services, steal sensitive information and destroy necessary files. These methods are often spread through emails, instant messages, or malicious websites. One of the most dangerous operations is phishing, which is a social engineering attack that tricks users into revealing login credentials, credit card numbers, or other sensitive information. During this procedure, it is possible for unauthorized individuals to gain control of all sensitive information. These attacks can take the form of fake emails, phone calls, or websites that appear to come from a delegated source (see Figure 2). In addition, there are other harmful assaults, which are the DoS attacks, which are the most common electronic attacks that overload a website or network with traffic, making it unavailable to users in the digital environment. These attacks are executed utilising a network of compromised computers, which are commonly referred to as bots. The bots collaborate to produce a large volume of traffic and influence the flow of information between users. These attacks have devastating consequences for individuals, organisations, and institutions. For individuals in the cyber environment, cyberattacks can lead to the theft of sensitive information, such as passwords and financial information, or the loss of essential files from computers. As for institutions or organisations, they may be exposed to large financial losses, reputational damage, and even legal liability.

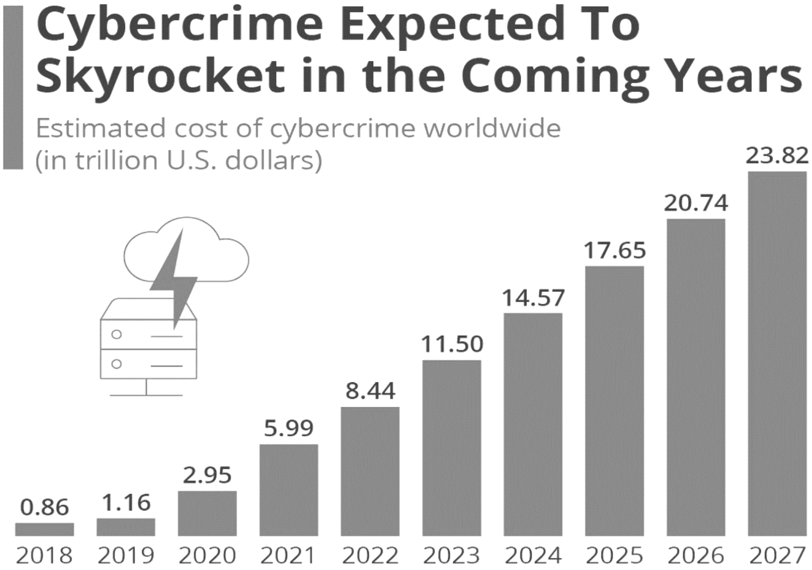


Fig. 1. The Estimated costs of cybercrime from 2018 to 2027 [22].

To counter these cyberattacks, following the soundest practices for online security, such as utilising strong passwords, avoiding emails from suspicious parties, and keeping the software and operating systems up-to-date is essential. In addition, institutions and organisations must implement cybersecurity criteria, such as firewalls, antivirus software, and intrusion detection systems to protect their networks and data from any cyber-attack. With the rise of cyber threats in the digital world, it is essential for both individuals and organizations to take preventative measures against cyber-attacks and malware. This can be accomplished by keeping up-to-date with the most recent dangers and employing efficient security measures while devising appropriate strategies to thwart them [25-29]. Section 2 of this article will cover the five most sophisticated cybersecurity threats.

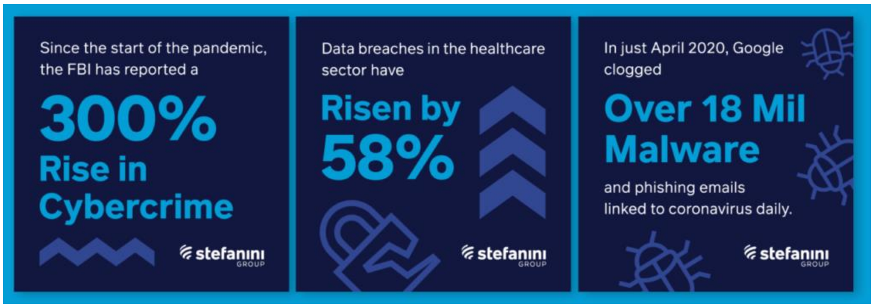

Since the start of the pandemic, the FBI has reported a
300%
Rise in Cybercrime
stefanini GROUP
Data breaches in the healthcare sector have
Risen by 58%
stefanini GROUP
In just April 2020, Google clogged
Over 18 Mil Malware
and phishing emails linked to coronavirus daily.
stefanini GROUP

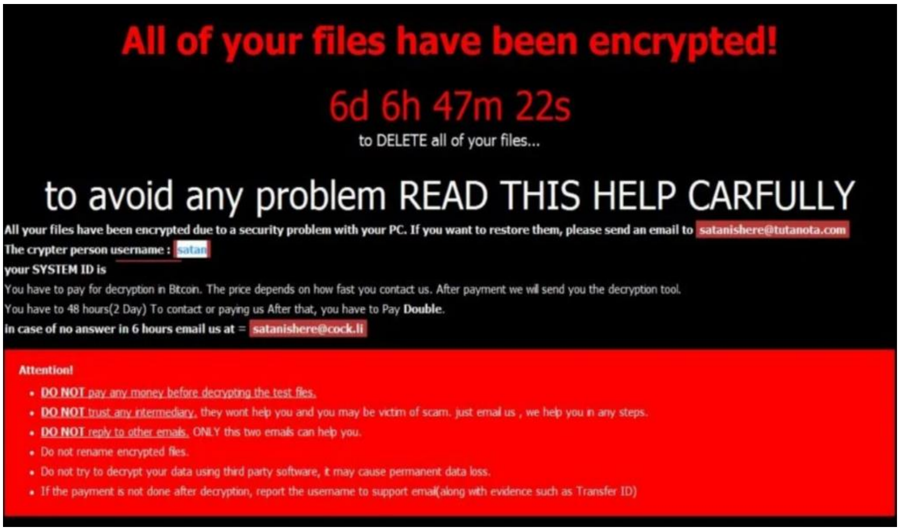
Fig. 2. Cybersecurity statistics for the period 2021-2022 [30]

2. TOP FIVE EVOLVING THREATS

Cyber-attacks are complicated procedures as they use advanced tools and techniques to penetrate systems and computer networks. These attacks have the ability to bypass firewalls and antivirus programs in order to steal sensitive information [31-33]. Examples of advanced cyber threats include advanced persistent threats (APTs), ransomware, and zero-day exploits .The 5 most famous threats that exist now are as follows:

- Ransomware Attack

A ransomware attack is one of the most advanced types of malicious cyber-attacks, where the attacker performs a series of actions with the purpose of encrypting the victim's computer files or the entire system and demands payment in dollars or another currency in exchange for providing the victim with a decryption key or code. Ransomware attacks can be delivered through multiple channels, including phishing emails, social engineering, and exploit kits, which are favoured by the attacker. The loss of information or data can have a significant impact on its users, leading to potential financial losses or damage to their reputation. Therefore, they are forced to follow the instructions of the attacker and satisfy them in order not to lose their data. Maintaining regular backups of data, implementing protective software, and providing proper user training to prevent falling prey to phishing scams are crucial. The years 2021 and 2022 witnessed a significant development in ransomware, as a large number of these attacks appeared, and these attacks are still developing until now in February 2023 in infiltrating systems, encrypting them, and stealing sensitive information. Figure 3 demonstrates a sample of a hacker encrypting a victim's data and providing a deadline. If the victim fails to yield to the hacker's requests, all their files will be completely wiped out.



All of your files have been encrypted!

6d 6h 47m 22s

to DELETE all of your files...

to avoid any problem READ THIS HELP CARFULLY

All your files have been encrypted due to a security problem with your PC. If you want to restore them, please send an email to satanishere@tutanota.com

The crypter person username : satan

your SYSTEM ID is

You have to pay for decryption in Bitcoin. The price depends on how fast you contact us. After payment we wil send you the decryption tool.

You have to 48 hours(2 Day) To contact or paying us After that, you have to Pay **Double**.

in case of no answer in 6 hours email us at = satanishere@cock.li

Attention!

- **DO NOT** pay any money before decrypting the test files.
- **DO NOT** trust any intermediary, they wont help you and you may be victim of scam. just email us , we help you in any steps.
- **DO NOT** reply to other emails. ONLY this two emails can help you.
- Do not rename encrypted files.
- Do not try to decrypt your data using third party software, it may cause permanent data loss.
- If the payment is not done after decryption, report the username to support email(along with evidence such as Transfer ID)

Fig. 3. Example of ransomware attack [34].

- IoT Attacks

Through the IoT environment which encompasses various devices embedded in the environment of things such as lights, washing machines, televisions, etc. Many devices connect to the Internet on a daily basis to communicate with each other and share data that is controlled by users. In recent years, IoT devices have seen numerous attacks ranging from physical attacks on IoT devices to social engineering attacks on IoT devices. Through these attacks, users' devices are fully controlled, data is infiltrated, all the movements of these users are viewed and misused for malicious purposes, as well as their movements are monitored within the digital environment. The attacker can gather information about the victim's behaviour, find out full details about him/her, and exploit it to carry out malicious operations against the user, destroy his reputation, or steal money. In addition, social engineering is widely employed to make attacks against users. In this type, the attacker exploits the trust relationships established between users and IoT devices to obtain sensitive information from the devices and pass it on to them or others without the command or approval of these users. Internet of Things devices is the most vulnerable devices to hacking and cyber threats. In general, every smart and digital device that transmits data via the Internet, for instance, laptop computers, is vulnerable to threats and electronic crimes in order to access sensitive information and control user behaviour. Figure 4 shows the statistics of the types of attack on devices in the IoT environment.

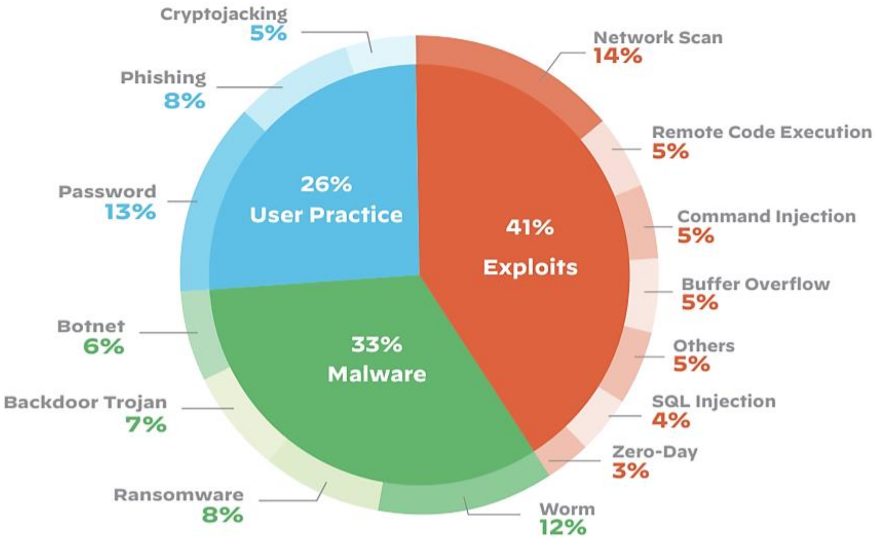


Fig. 4. Statistics of attacks on IoT [35].

- Cloud Attacks

Cloud computing is the modern era of new technologies, as it revolutionised the physical world to store all data and files in large sizes. Large and small companies always seek to back up their files and data in the digital cloud. In addition, the digital cloud is utilised to transfer files easily between companies or individuals. On the other hand, cloud computing is characterized by its low cost and high efficiency in storing and transmitting data, but this also increases the chances of data security breaches. The primary motivation for compromised data security is a lack of encryption and authentication and incorrect configuration of cloud settings. As a result, it is necessary to execute mechanisms and tactics in maintaining many considerations for cloud security, protecting all files and data, as well as preserving sensitive information. Cyber-attacks take different forms targeting cloud computing systems and infrastructure. These attacks seek to find vulnerabilities that would allow hackers to gain access to sensitive information stored in the cloud and disrupt the regular operation of applications and services that rely on cloud computing. Companies frequently resort to digitisation by converting all data into digital data and storing it in computers and cloud computing in order to deal with it efficiently [36]. Through this process, electronic attacks are generated to control the cloud, unauthorized access to cloud resources, data breaches, denial of service attacks, and access to all files stored within this cloud. To prevent cloud attacks, it is crucial to execute strong security measures, including access controls, encryption, monitoring and detection systems, and regularly assess the security of cloud environments.

- Phishing Attacks

Phishing attacks are one of the most expected electronic crimes on the Internet, where the attacker tries to get sensitive information such as passwords, credit card numbers, and other personal information from individuals in the digital environment. Usually, these attacks include the use of fake emails that seem to come from a trustworthy source, such as a well-known site, well-known platform, or bank, in order to reassure the victim of the incoming messages. These messages contain fake links designed to look real but intended to steal the victim's information without their knowledge. Moreover, in these attacks, well-designed malware is employed to infect computer systems or applications that run immediately once installed with the possibility of stealing sensitive information or controlling the victim's computer. To safeguard against these attacks, individuals should be very cautious of unwanted emails (Spam) or fake messages, especially those that ask for personal information or contain suspicious links. It's also crucial to use robust passwords and regularly monitor bank and credit card accounts for suspicious activity. Besides, utilising antivirus software and keeping all software and operating systems updated can assist in preventing phishing attacks and other types of cybercrime.

- Cryptocurrency and Blockchain Attacks

Cryptocurrency and blockchain attacks refer to various forms of cyberattacks targeting cryptocurrency wallets, exchanges, and blockchain networks [37-40]. Phishing is one of the most common styles of cryptocurrency attacks. Attackers send scam emails or messages to cryptocurrency users, often impersonating an authorised source, in an attempt to steal their login credentials or other sensitive information. Utilising malware, where attackers infect computers or mobile devices with malware prepared to steal cryptocurrency wallets or other sensitive data. In addition to attacks on individual users, cryptocurrency exchanges and wallets can also be targeted by hackers who utilise distributed denial-of-service (DDoS) attacks to flood the network and access sensitive information.

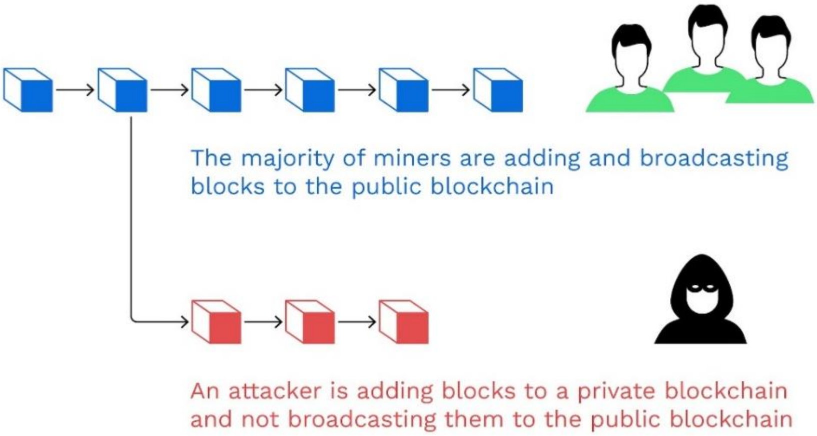

The majority of miners are adding and broadcasting blocks to the public blockchain
An attacker is adding blocks to a private blockchain and not broadcasting them to the public blockchain

Fig. 5. Statistics of attacks on IoT [35].

Blockchain networks can be targeted by attackers trying to take control of the network, known as a 51% attack (see Figure 5), or exploiting vulnerabilities in the code to steal or manipulate data. To safeguard against cryptocurrency and blockchain attacks, users should use robust passwords, enable two-factor authentication, and keep their software and operating systems contemporised. Exchanges and other service providers must also utilise robust security measures, such as encryption, firewalls, and intrusion detection systems. Likewise, the community as a whole can work to enhance the security of blockchain networks by conducting regular code audits and executing the most useful practices for network governance and security.

3. CONCLUSIONS

Sensitive information is the primary mark for attackers who want to steal, manipulate, or delete it from the victim's devices. The process of stealing this information takes place through several methods of attack and exploitation of individuals or institutions in order to complete the interests of the attackers. Cybercrimes are constantly growing, and modern strategies are being utilised to commit crimes operating computers and the Internet, such as hacking, phishing, identity theft, cyberstalking, and online fraud. These crimes cause significant harm to individuals and institutions and exploit them in order to take large sums of money and publish private information to the public. Unfortunately, these crimes are challenging to verify due to the global and unspecified nature of the Internet. Therefore, it is preferable to use artificial intelligence techniques that have a significant role in analysing the behaviour and practices of malicious software. In addition, practical prevention and response to cybercrime require a combination of technological solutions, legal frameworks and international cooperation.

Funding

Non.

Conflicts Of Interest

The authors declare no conflicts of interest.

Acknowledgment

Authors would like to thank the anonymous reviewers for their efforts.

References

[1] F. Fauziyah, Z. Wang, and G. Joy, "Knowledge Management Strategy for Handling Cyber Attacks in E-Commerce with Computer Security Incident Response Team (CSIRT)," Journal of Information Security, vol. 13, no. 4, pp. 294-311, Oct. 2022. doi: 10.4236/jis.2022.134016.

[2] M. M. Mijwil, R. Doshi, K. K. Hiran, A. H. Al-Mistarehi, and M. Gök, "Cybersecurity Challenges in Smart Cities: An Overview and Future Prospects," Mesopotamian journal of cybersecurity, vol. 2022, pp. 1-4, 2022. doi: 10.58496/MJCS/2022/001.

[3] M. M. Mijwil, E. Sadıkoğlu, E. Cengiz, and H. Candan, "Siber Güvenlikte Yapay Zekanın Rolü ve Önemi: Bir Derleme," Veri Bilimi, vol. 5, no. 2, pp. 97-105, Dec. 2022.

[4] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework," Sensors, vol. 21, no. 9, pp. 1-14, May 2021. doi: 10.3390/s21093267.

[5] M. M. Yamin, M. Ullah, H. Ullah, and B. Katt, "Weaponized AI for cyber attacks," Journal of Information Security and Applications, vol. 57, p. 102722, Mar. 2021. doi: 10.1016/j.jisa.2020.102722.

[6] M. M. Mijwil, M. Aljanabi, and A. H. Ali, "ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information," Mesopotamian journal of cybersecurity, vol. 2023, pp. 18-21, Feb. 1, 2023. doi: 10.58496/MJCS/2023/004.

[7] S. Acharya and S. Joshi, "Impact of cyber-attacks on banking institutions in India: A study of safety mechanisms and preventive measures," PalArch's Journal of Archaeology of Egypt/Egyptology, vol. 17, no. 6, pp. 4656-4670, 2020.

[8] Z. Hasan, H. R. Mohammad, and M. Jishkariani, "Machine Learning and Data Mining Methods for Cyber Security: A Survey," Mesopotamian journal of cybersecurity, vol. 2022, pp. 47-56, Nov. 2022. doi: 10.58496/MJCS/2022/006.

[9] M. M. Mijwil, M. Aljanabi, and ChatGPT, "Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime," Iraqi Journal For Computer Science and Mathematics, vol. 4, no. 1, pp. 65-70, Jan. 2023. doi: 10.52866/ijcsm.2023.01.01.0019.

[10] M. M. Mijwil, I. E. Salem, and M. M. Ismaeel, "The Significance of Machine Learning and Deep Learning Techniques in Cybersecurity: A Comprehensive Review," Iraqi Journal For Computer Science and Mathematics, vol. 4, no. 1, pp. 87-101, Jan. 2023. doi: 10.52866/ijcsm.2023.01.01.008.

[11] S. N. F. N. B. Mustaffa and M. Farhan, "Detection of False Data Injection Attack using Machine Learning approach," Mesopotamian journal of cybersecurity, vol. 2022, pp. 38-46, July 2022. doi: 10.58496/MJCS/2022/005.

[12] Z. Hasan and N. S. Al-Ramadan, "Cyber-attacks and Cyber Security Readiness: Iraqi Private Banks Case," Social Science and Humanities Journal, vol. 5, no. 8, pp. 2312-2323, 2021.

[13] M. M. Mijwil, Y. Filali, M. Aljanabi, M. Bounabi, H. Al-Shahwani, and ChatGPT, "The Purpose of Cybersecurity in the Digital Transformation of Public Services and Protecting the Digital Environment," Mesopotamian journal of cybersecurity, vol. 2023, pp. 1-6, Jan. 2023. doi: 10.58496/MJCS/2023/001.

[14] K. Aggarwal, M. M. Mijwil, S. Sonia, A. H. Al-Mistarehi, S. Alomari, M. Gök, A. M. Alaabdin, and S. H. Abdulrhman, "Has the Future Started? The Current Growth of Artificial Intelligence, Machine Learning, and Deep Learning," Iraqi Journal for Computer Science and Mathematics, vol. 3, no. 1, pp. 115-123, Jan. 2022. doi: 10.52866/ijcsm.2022.01.01.013.

[15] I. E. Salem, M. M. Mijwil, A. W. Abdulqader, M. M. Ismaeel, A. Alkhazraji, and A. M. Z. Alaabdin, "Introduction to The Data Mining Techniques in Cybersecurity," Mesopotamian Journal of Cybersecurity, vol. 2022, pp. 28-37, May 30, 2022. doi: 10.58496/MJCS/2022/004.

[16] M. Shafiq, Z. Gu, O. Cheikhrouhou, W. Alhakami, and H. Hamam, "The Rise of 'Internet of Things': Review and Open Research Issues Related to Detection and Prevention of IoT-Based Security Attacks," Wireless Communications and Mobile Computing, vol. 2022, no. 8669348, pp. 1-12, Aug. 2022. doi: 10.1155/2022/8669348.

[17] A. Djenna, S. Harous, and D. E. Saidouni, "Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure," Applied Sciences, vol. 11, no. 10, pp. 1-30, May 2021. doi: 10.3390/app11104580.

[18] R. Mansoor, D. N. Hamood, and A. K. Farhan, "Image Steganography Based on Chaos Function and Randomize Function," Iraqi Journal For Computer Science and Mathematics, vol. 4, no. 1, pp. 71–86, Jan. 2023. doi: 10.52866/ijcsm.2023.01.01.007.

[19] O. J. Unogwu, R. Doshi, K. K. Hiran, and M. M. Mijwil, "Introduction to Quantum-Resistant Blockchain," In Advancements in Quantum Blockchain With Real-Time Applications, pp. 36-55. IGI Global, 2022. doi: 10.4018/978-1-6684-5072-7.ch002.

[20] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," International Journal of Critical Infrastructure Protection, vol. 25, pp. 36-49, Jun. 2019. doi: 10.1016/j.ijcip.2019.01.001.

[21] M. Aljanabi, M. Ghazi, A. H. Ali, S. A. Abed, and ChatGPT, "ChatGpt: Open Possibilities," Iraqi Journal For Computer Science and Mathematics, vol. 4, no. 1, pp. 62–64, Jan. 2023. doi: 10.52866/ijcsm.2023.01.01.0018.

[22] A. Fleck, "Cybercrime Expected To Skyrocket in Coming Years," Statista, 2022. [Online]. Available: https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/.

[23] A. Hernandez-Suarez, G. Sanchez-Perez, L. K. Toscano-Medina, H. Perez-Meana, J. Olivares-Mercado, et al., "ReinforSec: An Automatic Generator of Synthetic Malware Samples and Denial-of-Service Attacks through Reinforcement Learning," Sensors, vol. 23, no. 3, pp. 1231, Jan. 2023. doi: 10.3390/s23031231.

[24] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," Future Generation Computer Systems, vol. 92, pp. 178-188, Mar. 2019. doi: 10.1016/j.future.2018.09.063.

[25] N. A. Bajao and J. Sarucam, "Threats Detection in the Internet of Things Using Convolutional neural networks, long short-term memory, and gated recurrent units," Mesopotamian Journal of Cybersecurity, vol. 2023, pp. 22–29, Feb. 2023. doi: 10.58496/MJCS/2023/005.

[26] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, and B. Green, "Looking back to look forward: Lessons learnt from cyber-attacks on Industrial Control Systems," International Journal of Critical Infrastructure Protection, vol. 35, pp. 100464, Dec. 2021. doi: 10.1016/j.ijcip.2021.100464.

[27] R. Geetha and T. Thilagam, "A Review on the Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security," Archives of Computational Methods in Engineering, vol. 28, pp. 2861–2879, Sep. 2020. doi: 10.1007/s11831-020-09478-2.

[28] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," Energy Reports, vol. 7, pp. 8176-8186, Nov. 2021. doi: 10.1016/j.egyr.2021.08.126.

[29] S. Nifakos, K. Chandramouli, C. K. Nikolaou, P. Papachristou, S. Koch, et al., "Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review," Sensors, vol. 21, no. 15, pp. 5119, Jul. 2021. doi: 10.3390/s21155119.

[30] Stefanini Group, "Cyber Security Statistics For 2022: List Of Data And Trends," 2022. [Online]. Available: https://stefanini.com/en/insights/articles/cyber-security-statistics-for-2022-data-and-trends.

[31] M. M. Mijwil, K. Aggarwal, R. Doshi, K. K. Hiran, and M. Gök, "The Distinction between R-CNN and Fast R-CNN in Image Analysis: A Performance Comparison," Asian Journal of Applied Sciences, vol. 10, no. 5, pp. 429-437, Nov. 2022. doi: 10.24203/ajas.v10i5.7064.

[32] K. Kim, F. A. Alfouzan, and H. Kim, "Cyber-Attack Scoring Model Based on the Offensive Cybersecurity Framework," Applied Sciences, vol. 11, no. 16, pp. 7738, Aug. 2021. [Online]. Available: https://doi.org/10.3390/app11167738.

[33] M. M. Mijwil, "Malware Detection in Android OS Using Machine Learning Techniques," Data Science and Applications, vol. 3, no. 2, pp. 5-9, Dec. 2020.

[34] N. Bhatt, "What are the Top 10 Emerging Cybersecurity Challenges?," Sagenext, Oct. 2022. [Online]. Available: https://www.thesagenext.com/blog/emerging-cybersecurity-challenges.

[35] L. O'Donnell, "More Than Half of IoT Devices Vulnerable to Severe Attacks," Threat post, Mar. 2020. [Online]. Available: https://threatpost.com/half-iot-devices-vulnerable-severe-attacks/153609/.

[36] M. M. Mijwil, A. K. Faieq, and A. H. Al-Mistarehi, "The Significance of Digitalisation and Artificial Intelligence in The Healthcare Sector: A Review," Asian Journal of Pharmacy, Nursing and Medical Sciences, vol. 10, no. 3, pp. 25-32, Nov. 2022. [Online]. Available: https://doi.org/10.24203/ajpnms.v10i3.7065.

[37] S. Sayeed and H. Marco-Gisbert, "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack," Applied Sciences, vol. 9, no. 9, pp. 1-17, Apr. 2019. [Online]. Available: https://doi.org/10.3390/app9091788.

[38] S. Ramos, F. Pianese, T. Leach, and E. Oliveras, "A great disturbance in the crypto: Understanding cryptocurrency returns under attacks," Blockchain: Research and Applications, vol. 2, no. 3, pp. 100021, Sep. 2021. [Online]. Available: https://doi.org/10.1016/j.bcra.2021.100021.

[39] S. Sayeed and H. Marco-Gisbert, "Proof of Adjourn (PoAj): A Novel Approach to Mitigate Blockchain Attacks," Applied Sciences, vol. 10, no. 18, pp. 6607, Sep. 2020. [Online]. Available: https://doi.org/10.3390/app10186607.

[40] "What is a 51% attack and how is it prevented?," Bitpanda. [Online]. Available: https://www.bitpanda.com/academy/en/lessons/what-is-a-51-attack-and-how-is-it-prevented/.