e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:02/February-2024 Impact Factor- 7.868 www.irjmets.com

FUTURE TRENDS IN CYBERSECURITY: EXPLORING EMERGING TECHNOLOGIES AND STRATEGIES

Arkan A. Ghaib*1

*1Department Of Information Technologies, Management Technical College, Southern Technical University, Basrah, Iraq.

DOI : https://www.doi.org/10.56726/IRJMETS49530

ABSTRACT

As technology advances, cybersecurity risks also adapt. This study examines upcoming developments in cybersecurity, emphasizing new technology and techniques designed to combat advancing cyber threats. Key areas of focus are advancements in artificial intelligence (AI) and machine learning for threat detection, the potential of quantum cryptography for securing communication channels, the integration of blockchain technology for decentralized and tamper-proof data management, and the adoption of zero trust architecture to improve network security. The paper also analyzes the difficulties and possibilities related to Internet of Things (IoT) security, secure multiparty computation, and post-quantum cryptography. This research intends to analyze trends in cybersecurity and their implications to offer insights into the changing landscape of cybersecurity and to direct future research and development activities in the sector.

Keywords: Cybersecurity, Denial Of Service, Internet Of Things, Cyber-Attacks, Blockchain.

I. INTRODUCTION

Cyber-attacks conducted over the Internet have increased significantly in recent years, and it is anticipated that new tactics may emerge in the future. Cyber-attacks encompass many techniques employed by individuals to exploit vulnerabilities in electronic systems and networks, typically to cause harm or gain unauthorized access to sensitive data.

Please provide information from sources 1 to 6. These attacks could originate from several websites, including those containing deceptive links, counterfeit content, or harmful code. They have been shown to impact a broad range of businesses [7-12]. Any electronic attack poses a substantial threat to the security of enterprises, organizations, and individuals as it can lead to the unauthorized collection of data and information from their devices. Furthermore, these attacks are known for their capacity to interrupt services, company operations, and other elements inside the digital realm. Enterprises must implement practical solutions to mitigate this issue and minimize its detrimental effects on their digital operations. Organizations and institutions rely on monitoring, detection, prevention, and response measures as the primary means to prevent cyber-attacks. They are consistently enhancing these tactics and broadening their capacity to recognize and understand electronic threats. Cyberattacks are deliberate and harmful actions aimed at computer systems, networks, and devices via the Internet to compromise or harm sensitive information [13-20]. Unauthorized individuals are attracted to computer systems due to the valuable information they hold. These attacks can be conducted by people or groups for purposes such as financial profit, political objectives, or personal agendas. Figure 1 shows that the expenditures associated with cybercrime are projected to exceed $23 trillion by 2027.

Cyberattacks employ a range of methods including viruses, malware, phishing, and denial-of-service (DoS) attacks. Viruses and malware have the ability to deeply penetrate computer systems. Hinder their functioning, pilfer valuable data, and obliterate vital files. These tactics are commonly disseminated via emails, instant chats, or illicit websites. Phishing is a deceptive social engineering assault aimed at deceiving people into disclosing their login passwords, credit card details, or other confidential information.

Throughout this procedure, there is a possibility of unauthorized individuals obtaining full control of all sensitive data. These assaults can manifest as fraudulent emails, phone calls, or websites that mimic a trustworthy source (see to Figure 2). Denial of Service (DoS) assaults flood a website or network with overwhelming traffic, making it unreachable to users in the digital environment. The assaults are executed through a network of infected computers referred to as bots. The bots collaborate to generate a significant volume of traffic and control the distribution of information among users. The attacks have significant

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:02/February-2024 Impact Factor- 7.868 www.irjmets.com

consequences for individuals, groups, and institutions. Cyberattacks in cyberspace can lead to unwanted access to sensitive data such as passwords and financial information, as well as the loss or misplacement of vital files kept on computers. Institutions or groups may face significant financial losses, damage to their reputation, and possibly legal liability.

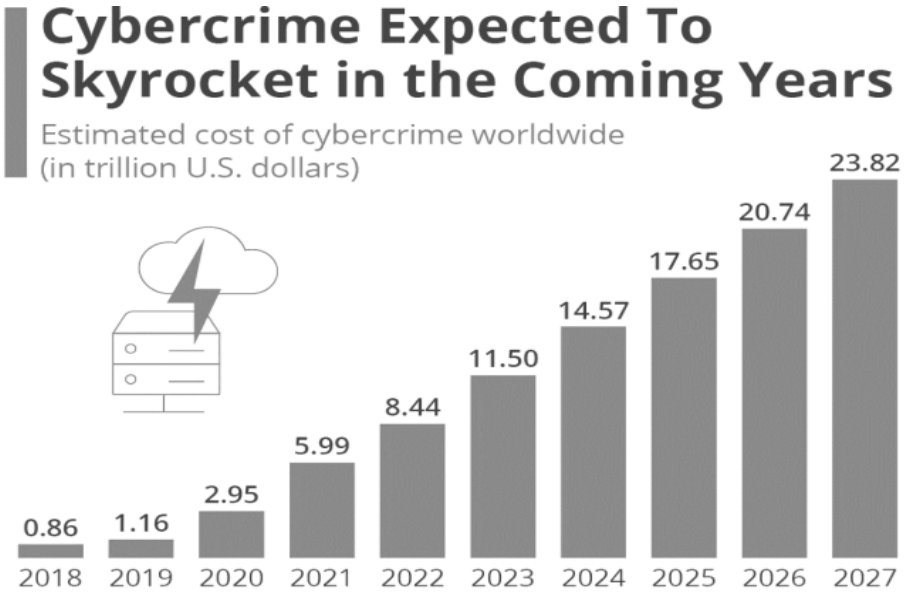

Figure 1: The projected expenses associated with cybercrime spanning from 2018 to 2027 [22].

II. TOP FIVE CYBERCRIMES

Here are five significant evolving threats in cybercrime:

1. **Ransomware Attacks:** Ransomware remains a top concern, with cybercriminals continually refining their tactics. They not only encrypt files but also increasingly engage in double extortion, threatening to release sensitive data unless the ransom is paid. Additionally, ransomware attacks are becoming more sophisticated, with threat actors targeting larger organizations and critical infrastructure [23].

Method and analysis which is performed in your research work should be written in this section. A simple strategy to follow is to use keywords from your title in first few sentences.

Figure 2: Example of Ransomware Attacks

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:02/February-2024 Impact Factor- 7.868 www.irjmets.com

2. **Supply Chain Attacks:** Supply chain attacks have gained prominence, with attackers exploiting vulnerabilities in the software supply chain to infiltrate target systems. This involves compromising a trusted supplier or vendor to gain access to the intended target's network. Such attacks can have far-reaching consequences, affecting numerous organizations connected to the compromised supply chain [24].

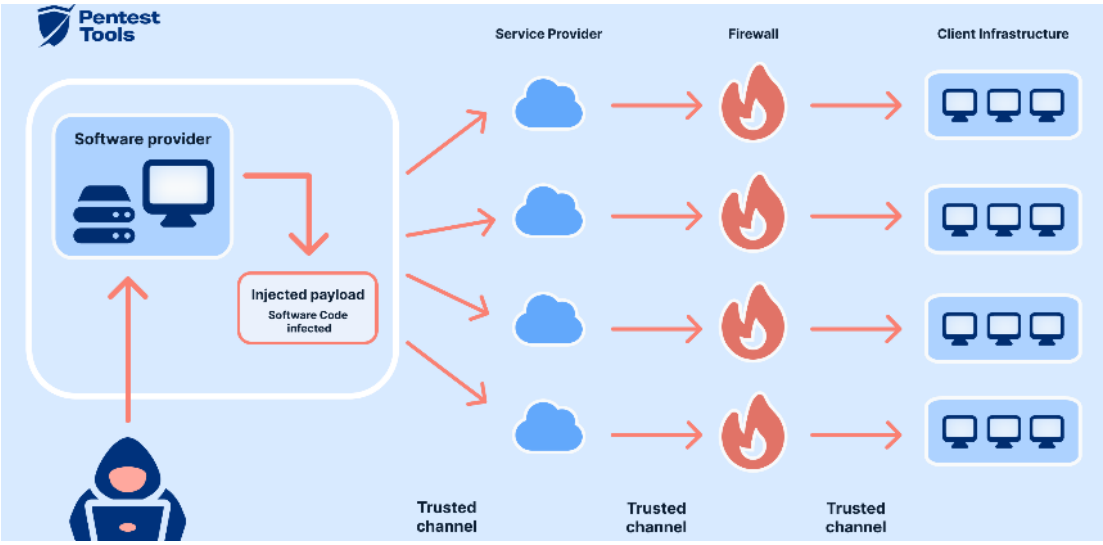

Figure 3: Example of supply chain attacks

3. **Zero-Day Exploits and Vulnerabilities:** The identification and utilization of zero-day vulnerabilities continue to pose a substantial risk. Zero-day exploits specifically target software vulnerabilities that are either unknown to the vendor or lack a viable patch, rendering them exceptionally hazardous. Cybercriminals and nation-state actors alike exploit these vulnerabilities to gain unauthorized access to systems and networks [25].

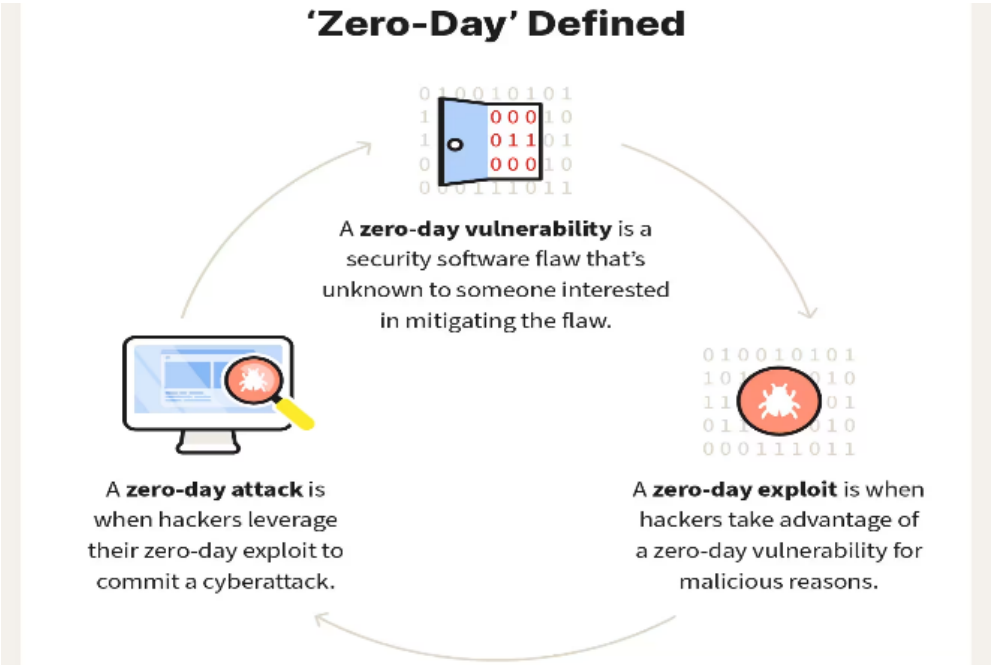

Figure 4: Zero Day Attack [2]

4. **Social Engineering and Phishing:** Social engineering assaults, such as phishing, continue to be a common danger vector. Cybercriminals occupy complex approaches to trick individuals into revealing confidential info, such login credentials or bank information. Phishing tries frequently disguise themselves as genuine emails, websites, or communications, which preserve make them tough to identify. [26].

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:06/Issue:02/February-2024 Impact Factor- 7.868 www.irjmets.com

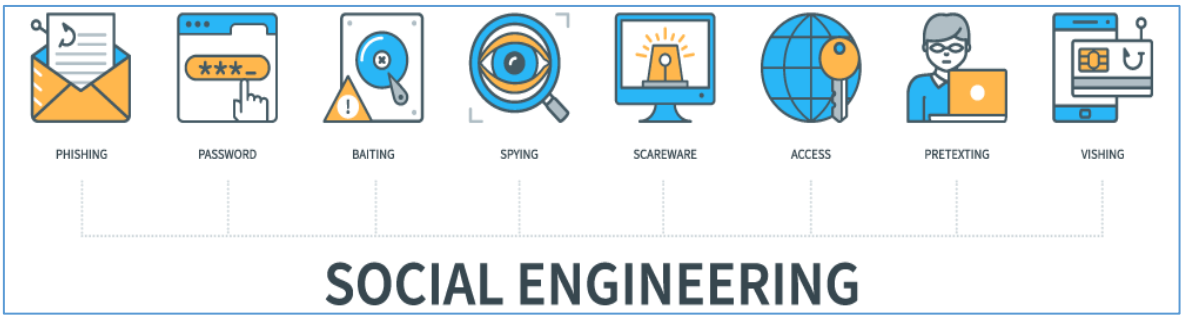

Figure 5: Examples of social engineering attacks [2]

5. **Deepfake and AI-based Attacks:** The general use of deepfake tools presents new obstacles in adopting cyber-attacks. Deepfake technology may change audio, video, and photos to produce realistic yet fraudulent content. This can be applied for wicked objectives such as impersonation, deception campaigns, and fraud, which can wear away trust and authenticity in digital channels [27].

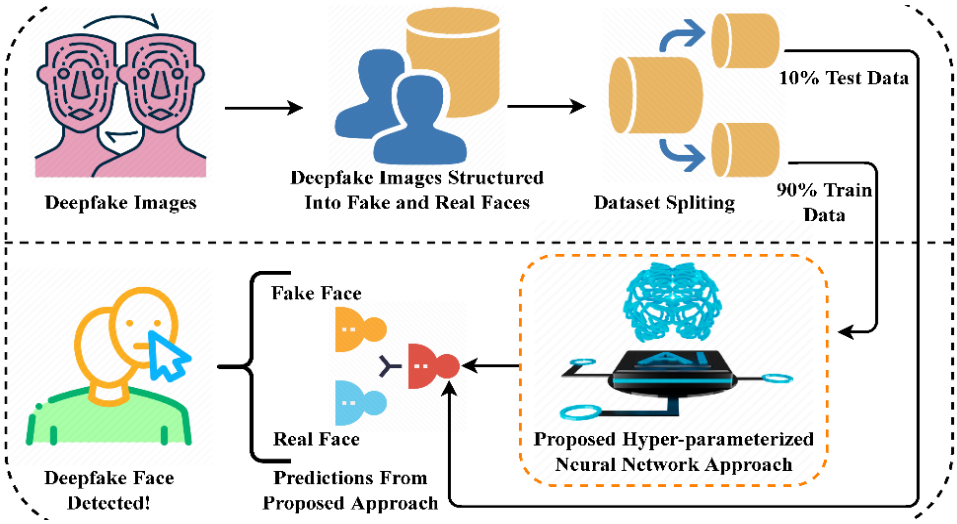

Figure 6: AI and Deep Fake attacks [1]

These developing risks emphasize the importance of robust cybersecurity measures, like standard software keeping informed and thorough staff educating, is extremely important. Sharing threat details and implementing modern security technology to successfully reduce risks. Collaboration between governments, industry stakeholders, and cybersecurity experts is crucial to effectively tackle these modifying threats. [28].

III. EMERGING TECHNOLOGIES IN CYBERSECURITY

When discussing emerging technologies in cybersecurity, it is crucial to highlight the innovative tools and techniques that are shaping the future of cyber defense. Here are some notable forthcoming technologies. [29].

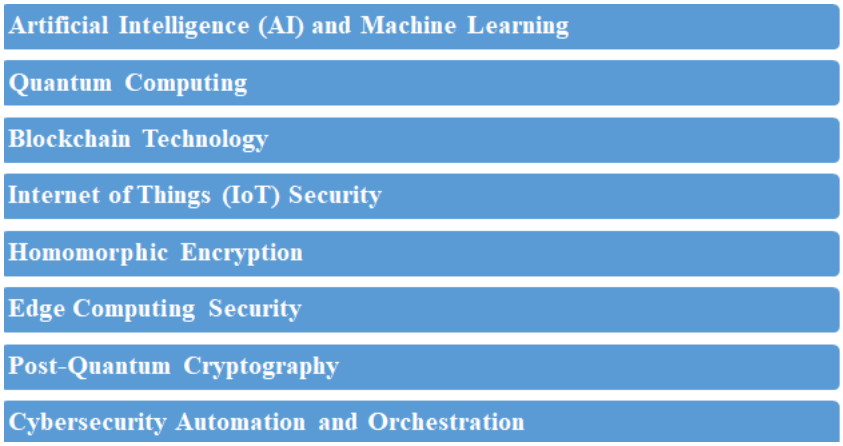

Figure 7: Emerging Technologies in Cybersecurity

1. Artificial Intelligence (AI) and Machine Learning (ML) are transforming cybersecurity by enhancing threat detection, identifying anomalies, and analyzing behavioral patterns. 30. These systems have the capability to scan large datasets in order to identify patterns and irregularities, allowing for immediate detection and reaction to cyber threats. Machine learning algorithms can enhance the accuracy of virus detection, spam filtering, and fraud detection systems.
2. Quantum computing can potentially undermine current encryption algorithms, posing a significant challenge to traditional cryptography methods. Quantum-resistant encryption is being created to protect sensitive information from possible breaches by quantum computers, guaranteeing security in the future. [31].
3. Blockchain technology provides a decentralized and tamper-proof method for data storage, improving the security and reliability of digital transactions and records. Blockchain technology can be used in cybersecurity for secure identity management, secure supply chain management, and decentralized threat intelligence sharing.
4. Internet of Things (IoT) Security is crucial as IoT devices become more widespread to protect against cyber threats and prevent assaults on key infrastructure and personal privacy. Modern IoT security measures encompass device authentication, encryption, secure firmware updates, and network segmentation to separate compromised devices [33].
5. Homomorphic encryption is a method that enables computations to be carried out on encrypted data without the need for decryption. This technique ensures the preservation of data privacy and security. This technology enables secure computation outsourcing, where sensitive data can be processed by third parties without exposing it to potential adversaries [34].
6. Edge Computing Security: Edge computing enhances data processing by reducing latency and enhancing efficiency through the proximity of processing capacity to the data source. However, securing edge computing environments against cyber threats requires implementing robust security measures at the network edge, including encryption, access control, and intrusion detection [35].
7. Post-Quantum Cryptography, sometimes known as quantum-resistant cryptography, encompasses cryptographic methods specifically developed to withstand attacks from quantum computers. These algorithms are being developed to replace current cryptographic standards, Securing encrypted data for an extended period in the quantum era. [36].
8. Cybersecurity Automation and Orchestration: Automation and orchestration technologies streamline security operations by automating repetitive tasks, orchestrating workflows, and integrating security tools. This allows security teams to respond to threats faster, minimize human error, and allocate resources more efficiently [37].
9. By leveraging these emerging technologies, organizations can enhance their cybersecurity posture and stay ahead of evolving cyber threats in an increasingly complex digital landscape.

IV. FUTURE TRENDS AND PREDICTIONS IN CYBER SECURITY

Emerging technologies are reshaping the landscape of cybersecurity, offering innovative tools and approaches to defend against evolving threats. Artificial Intelligence (AI) and Machine Learning (ML) are at the forefront, empowering advanced threat detection and behavior analysis through real-time anomaly detection[38][39]. Quantum Computing poses challenges to traditional encryption methods. Advancing the creation of quantum-resistant cryptography to protect valuable information. Blockchain technology provides decentralized and immutable data storage, which improves the security of digital transactions and records. In the field of Internet of Things (IoT) security, actions like device authentication and encryption help reduce dangers linked to the increasing number of connected devices. Homomorphic encryption allows computations to be carried out on encrypted data without requiring decryption, thereby maintaining privacy in outsourced computations. Edge computing involves moving data processing closer to where the data is generated, requiring strong security protocols at the edge of the network. Post-Quantum Cryptography is being developed to create encryption techniques that can withstand quantum computer attacks, ensuring the long-term security of encrypted data. Cybersecurity automation and orchestration improve efficiency by allowing quicker responses to attacks and reducing the occurrence of human errors. Organizations can strengthen their cybersecurity defenses and adjust to the ever-changing threat environment of the digital era by adopting these new technologies [40].

V. CONCLUSION

Exploring future trends in cybersecurity shows an environment characterized by fast technology progress and changing threat vectors. Cutting-edge technologies such as Artificial Intelligence (AI), Blockchain, Quantum Computing, and IoT security solutions provide substantial potential to enhance cybersecurity and mitigate risks. These technologies facilitate sophisticated threat detection, distributed data storage, and encryption that is immune to quantum attacks, allowing enterprises to outpace advanced cyber attackers. Innovative tactics such as cybersecurity automation, zero-trust frameworks, and threat intelligence sharing work along with technical improvements to create a comprehensive approach to cybersecurity. Organizations must stay attentive, agile, and collaborative to combat evolving cyber threats. Organizations may protect their assets, data, and infrastructure against new cyber threats by using new technologies and implementing proactive security measures in the digital age.

ACKNOWLEDGEMENTS

The authors would like to express their thanks to Southern Technical University (https://www.stu.edu.iq) Basrah, Iraq for its support in the present study.

VI. REFERENCES

[1] Raza, A.; Munir, K.; Almutairi, M. A Novel Deep Learning Approach for Deepfake Image Detection. *Appl. Sci.* 2022, *12*, 9820. https://doi.org/10.3390/app12199820

[2] Norton. (2023, July). norton.com.

[3] Mijwil, M., Unogwu, O. J., Filali, Y., Bala, I., & Al-Shahwani, H. (2023). Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. Mesopotamian journal of cybersecurity, 2023, 57-63.

[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] Nahi, A. A., Ghaib, A. A., & Ali, A. A. A. A. (2023, December). Metaverse Applications and Its Use in Education. In International Multi-Disciplinary Conference-Integrated Sciences and Technologies (pp. 61-80). Cham: Springer Nature Switzerland.

[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] Dawood, H. A., & Jassim, K. F. (2013, December). Mitigating IPv6 security vulnerabilities. In 2013 International Conference on Advanced Computer Science Applications and Technologies (pp. 304-309). IEEE.

[22] Jasim, K. F., Ghafoor, K. Z., & Maghdid, H. S. (2022). Analysis of Encryption Algorithms Proposed for Data Security in 4G and 5G Generations. In ITM Web of Conferences (Vol. 42, p. 01004). EDP Sciences.

[23] Jasim, K. F., Ismail, R. J., Al-Rabeeah, A. A. N., & Solaimanzadeh, S. (2021). Analysis the Structures of Some Symmetric Cipher Algorithms Suitable for the Security of IoT Devices. Cihan University-Erbil Scientific Journal, 5(2), 13-19.

[24] Jasim, K. F., & Al Shaikhli, I. F. (2014, November). Comparative study of some symmetric ciphers in mobile systems. In The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M) (pp. 1-5). IEEE.

[25] Jasim, K. F., & Al-Shaikhli, I. F. (2015, December). Mobile technology generations and cryptographic algorithms: analysis study. In 2015 4th International Conference on Advanced Computer Science Applications and Technologies (ACSAT) (pp. 50-55). IEEE.

[26] Hai, T., Dhahad, H. A., Jasim, K. F., Sharma, K., Zhou, J., Fouad, H., & El-Shafai, W. (2023). Deep learning-based prediction of lithium-ion batteries state of charge for electric vehicles in standard driving cycle. Sustainable Energy Technologies and Assessments, 60, 103461.

[27] Jasim, K. F., & Al-Shaikhli, I. F. (2017, March). Analysis of Confidentiality Algorithms in Different Mobile Generations. In Conference of Cihan University-Erbil on Communication Engineering and Computer Science (p. 55).

[28] Jasim, K. F., & Al Shaikhli, I. F. (2014, November). Comparative study of some symmetric ciphers in mobile systems. In The 5th International Conference on Information and Communication Technology for The Muslim World (ICT4M) (pp. 1-5). IEEE.

[29] Ghafoor, K. Z., Guizani, M., Kong, L., Maghdid, H. S., & Jasim, K. F. (2019). Enabling efficient coexistence of DSRC and C-V2X in vehicular networks. IEEE Wireless Communications, 27(2), 134-140.

[30] Al-Majdi, K., Salman, A., Abbas, N. A., Hashim, M. M., Taha, M., Nahi, A. A., & Saleh, S. (2022). MLCM: An efficient image encryption technique for IoT application based on multi-layer chaotic

maps. International Journal of Nonlinear Analysis and Applications, 13(2), 1591-1615.

[31] Al-Rabeeah, A. A. N., & Hashim, M. M. (2019). Social Network Privacy Models. Cihan University-Erbil Scientific Journal, 3(2), 92-101.

[32] Al-Rabeeah, A. A. N., & Saeed, F. (2017, May). Data privacy model for social media platforms. In 2017 6th ICT International Student Project Conference (ICT-ISPC) (pp. 1-5). IEEE.

[33] Hashim, M. M., Kareem, M. M., Al-Azzawi, W. K., Nahi, A. A., Taha, M. S., & Ali, A. H. (2022, August). Based Complex Key Cryptography: New Secure Image Transmission Method utilizing Confusion and Diffusion. In 2022 8th International Conference on Contemporary Information Technology and Mathematics (ICCITM) (pp. 59-65). IEEE.

[34] Hashim, M. M., & Al-Rabeeah, A. A. N. (2019). Social Network Privacy Models: A systematic literature review and directions for further research. Cihan University-Erbil Scientific Journal, 3(2), 92-101.

[35] Saleh, S., Al-Mufarrij, J., & Nahi Alrabeeah, A. A. (2023). On continuity and categorical property of interval-valued topological spaces. International Journal of Nonlinear Analysis and Applications.

[36] Hashim, M. M., Al-Hilali, A. A., Qasim, H. B., Salah, O. R., & Nahi, A. A. (2023, October). An Optimized Image Annotation Method Utilizing Integrating Neural Networks Model and Slantlet Transformation. In 2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI) (pp. 1-10). IEEE.

[37] Hashim, M. M., Al-Hilali, A. A., Safi, M. G. A., Salah, O. R., & Nahi, A. A. (2023, October). Sentence Reduction based on Automatic Document Text Summarization and Crossbred Framework. In 2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI) (pp. 1-10). IEEE.

[38] Qasim, H. B., Hasan, S. A., Nahi, A. A., Mohammed, A. H., Ghaib, A. A., Muslim, C. K., & Al-Hilali, A. A. (2023, October). Case Study: Fiber Optic network installation and Monitoring at Cihan University-Erbil. In 2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI) (pp. 1-8). IEEE.

[39] 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.

[40] Ghaib, A. A., Alsalhi, Y. E. A., Hayder, I. M., Younis, H. A., & Nahi, A. A. (2023). Improving the Efficiency of Distributed Utility Item Sets Mining in Relation to Big Data. Journal of Computer Science and Technology Studies, 5(4), 122-131.