International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

A critical review of emerging cybersecurity threats in financial technologies

Uchenna Joseph Umoga [1], Enoch Oluwademilade Sodiya [2,*], Olukunle Oladipupo Amoo [3] and Akoh Atadoga [4]

[1] *Independent Researcher, Seattle, Washington, USA.*
[2] *Independent Researcher, UK.*
[3] *Department of Cybersecurity University of Nebraska at Omaha USA.*
[4] *Independent Researcher, San Francisco, USA.*

International Journal of Science and Research Archive, 2024, 11(01), 1810–1817

Publication history: Received on 03 January 2024; revised on 11 February 2024; accepted on 13 February 2024

Article DOI: https://doi.org/10.30574/ijsra.2024.11.1.0284

Abstract

The rapid evolution of financial technologies (FinTech) has revolutionized the financial landscape, providing unprecedented convenience and efficiency. However, this technological advancement has also exposed the financial sector to an escalating array of cybersecurity threats. This paper presents a critical review of emerging cybersecurity threats in FinTech, analyzing the challenges and vulnerabilities faced by financial institutions in an era of increasing digitalization. The study delves into the complex landscape of cyber threats, exploring the spectrum from traditional threats, such as phishing and malware attacks, to sophisticated and evolving threats like ransomware, supply chain attacks, and artificial intelligence-driven cyber threats. The analysis highlights the interconnectedness of FinTech platforms, making them susceptible to systemic risks and cascading failures. Furthermore, the paper evaluates the impact of regulatory frameworks and compliance measures on mitigating cybersecurity risks in the FinTech domain. It assesses the effectiveness of current strategies and suggests potential enhancements to address the dynamic nature of cyber threats. A significant portion of the review focuses on the role of human factors in cybersecurity, emphasizing the need for robust training and awareness programs to empower financial professionals and users alike. Social engineering attacks, insider threats, and the exploitation of human vulnerabilities are discussed in detail, underscoring the importance of a holistic approach to cybersecurity. This critical review aims to provide a comprehensive understanding of the emerging cybersecurity landscape in FinTech. By shedding light on the evolving threats and vulnerabilities, the paper contributes to the ongoing discourse on safeguarding the integrity and security of financial technologies. As the financial industry continues to embrace technological innovations, a proactive and adaptive cybersecurity strategy is imperative to ensure the resilience of the financial ecosystem in the face of evolving cyber threats.

Keywords: Cybersecurity; Financial; Technologies; Cyber Threats; Review

1. Introduction

Financial technology (FinTech) has rapidly evolved, revolutionizing the financial sector through the integration of technology into financial services. The evolution of FinTech has significantly impacted the financial sector, leading to increased efficiency, accessibility, and innovation. The significance of FinTech in the financial sector is evident in its ability to enhance financial inclusion, streamline operations, and improve customer satisfaction. However, the rapid integration of technology in financial services has also brought about emerging cybersecurity threats and vulnerabilities, necessitating a critical review of these challenges.

The purpose of this critical review is to address the growing need for cybersecurity in FinTech and to analyze the emerging threats and vulnerabilities that accompany the integration of technology in financial services. Effective cybersecurity risk management is crucial for financial institutions to defend against cyber-attacks and safeguard their

* Corresponding author: Enoch Oluwademilade Sodiya

operations (Urus & Mohamed, 2021). Additionally, the FinTech revolution poses significant risks, including cybersecurity threats and data privacy concerns (Singhvi & Dadhich, 2023). Therefore, this critical review aims to provide insights into the cybersecurity challenges faced by the FinTech industry and offer an analysis of the emerging threats and vulnerabilities that have the potential to disrupt financial services.

The evolution of FinTech has transitioned through distinct eras, signifying the continuous advancement and integration of technology in the financial sector (Arner et al., 2015). This evolution has led to the positive outcomes of FinTech-driven transformations, including increased financial inclusion, streamlined operations, and improved customer satisfaction (Awaliyah, 2023), but has also introduced new risks, particularly in the area of cybersecurity. The critical review will delve into the historical evolution of FinTech and its impact on the financial sector, providing a comprehensive understanding of the context in which emerging cybersecurity threats have emerged.

In conclusion, the critical review of emerging cybersecurity threats in FinTech is essential to understand the implications of technology integration in financial services. By addressing the need for cybersecurity in FinTech and analyzing the emerging threats and vulnerabilities, this review aims to contribute to the development of effective risk management strategies and the safeguarding of financial systems in the digital era.

2. Traditional Cybersecurity Threats in FinTech

Traditional cybersecurity threats in the FinTech industry, such as phishing and malware attacks, pose significant risks to financial institutions and their customers. Phishing attacks involve various methods and techniques, including fake emails and websites designed to steal user credentials (Gupta et al., 2017; Orieno et al., 2024). These attacks can lead to financial damages, identity theft, loss of private information, and damage to brand reputation, affecting both individuals and financial institutions (Mohammad et al., 2015). Additionally, phishing attacks have been identified as a major problem in the cyber world, causing financial losses for industries and individuals (Jain & Gupta, 2017; Ezeigweneme et al., 2024).

Malware attacks targeting FinTech encompass various types of malicious software, each with its own consequences and countermeasures. These attacks often result in the loss of confidential customer information, financial loss, and the weakening of trust in financial institutions (Ozcan et al., 2021; Ohenhen et al., 2024). Countermeasures against malware attacks include the use of advanced detection techniques and intelligent decision support systems to prevent illicit activities such as identity theft and fraud perpetuated by cybercriminals (Adebowale, 2021; Adeleke et al., 2019).

In response to these threats, research has focused on developing detection and prevention techniques. Machine learning and data mining methods have been explored for detecting phishing websites, with the aim of raising awareness and protection techniques against phishing attacks (Ali, 2017; Ilugbusi et al., 2020). Furthermore, the use of hybrid models combining deep learning and recurrent neural networks has been proposed for detecting phishing URLs, highlighting the need for advanced technological solutions to combat these threats.

In conclusion, traditional cybersecurity threats, particularly phishing and malware attacks, continue to pose significant challenges to the FinTech industry. These threats have far-reaching impacts, including financial losses, identity theft, and damage to brand reputation. As a result, there is a growing emphasis on developing advanced detection and prevention techniques, leveraging machine learning, data mining, and intelligent decision support systems to enhance cybersecurity in the FinTech sector.

3. Advanced and Evolving Cyber Threats

Ransomware attacks have indeed seen a significant increase in recent years, posing a growing threat to financial institutions (Zakaria et al., 2017; Vincent et al., 2021). These attacks can lead to severe implications for financial institutions, including financial losses, reputational damage, and regulatory scrutiny. Additionally, the rise in ransomware incidents has targeted cloud storage, necessitating the development of hypervisor-level ransomware detection using machine learning (Purnaye, 2024). This highlights the evolving nature of ransomware attacks and the need for advanced detection and prevention mechanisms.

Supply chain attacks, particularly in the FinTech sector, have exposed vulnerabilities in the supply chain, making it imperative for financial institutions to implement robust strategies for prevention and response (Niekerk, 2023; Abrahams et al., 2023). The interconnected nature of the FinTech supply chain has made it susceptible to exploitation, emphasizing the need for proactive measures to mitigate these risks. Artificial intelligence (AI) is increasingly being

exploited in cyber attacks, posing future implications for FinTech security (Çatal et al., 2021; Anamu et al., 2023). The application of deep learning for mobile malware detection has revealed the dominance of ransomware as a significant threat, necessitating the development of advanced detection techniques. Furthermore, the exploitation of AI in cyber attacks underscores the need for continuous advancements in cybersecurity to counter these evolving threats.

In conclusion, the rise in ransomware incidents, vulnerabilities in the FinTech supply chain, and the exploitation of AI in cyber threats collectively highlight the advanced and evolving nature of cyber threats facing financial institutions. Addressing these challenges requires a multi-faceted approach, encompassing advanced detection technologies, robust supply chain security measures, and continuous advancements in cybersecurity to ensure the resilience of FinTech systems.

4. Systemic Risks and Interconnectedness

The interconnectedness of FinTech platforms has indeed transformed the financial landscape, creating a complex web of relationships and dependencies (Haldane & May, 2011). This interconnectedness has led to the emergence of systemic risks, particularly concerning cyber threats. Cyber threats pose a significant systemic risk to financial networks, as demonstrated by the potential for contagion in financial systems (Gai & Kapadia, 2010; Adaga et al., 2024). The interconnected nature of financial systems amplifies the impact of cyber threats, leading to potential cascading failures that can disrupt the entire financial ecosystem.

Cascading failures in interconnected financial networks can have severe consequences, affecting the stability and functioning of the entire financial system. Mitigating these cascading failures requires a comprehensive approach that addresses the complex interdependencies within the network (Smolyak et al., 2020; Abrahams et al., 2024). Furthermore, understanding cascading failures as continuous phase-space transitions provides valuable insights into the dynamics of systemic risk in interconnected financial systems (Yang & Motter, 2017; Hassan et al., 2024).

In conclusion, the interconnectedness of FinTech platforms has introduced systemic risks, particularly in the face of cyber threats. These risks can lead to cascading failures within the financial ecosystem, necessitating robust mitigation strategies to ensure the stability and resilience of the interconnected financial networks.

5. Regulatory Frameworks and Compliance

Regulatory frameworks and compliance are crucial in ensuring the security and integrity of various sectors, including cybersecurity and FinTech. Existing cybersecurity regulations are essential for governing cybersecurity measures, as revealed by (Mwelu et al., 2018; Balogun et al., 2024). The study highlights the positive impact of sanctions, inefficiency of the public procurement regulatory framework, and contractors' resistance to non-compliance on compliance within a regulatory framework. Additionally, Kharlamov & Pogrebna (2019) develop a new framework linking cross-cultural human values, regulation, and governance in the area of cybersecurity, emphasizing the importance of understanding cultural commitment toward regulation and governance.

In the FinTech sector, compliance measures are central to cooperation and delegation of authority, as indicated by (Buvik, 2013). Furthermore, Biasin (2023) examines the new cybersecurity requirements for medical devices in the EU, emphasizing the need for compliance with evolving regulatory frameworks. Additionally, Aliyu et al. (2020) propose a Holistic Cybersecurity Maturity Assessment Framework for Higher Education Institutions in the United Kingdom, incorporating security and privacy regulations, and best practices that institutions must comply with.

To enhance regulatory frameworks, it is crucial to address fragmented authority and reliance on existing frameworks, as highlighted by (Lewallen, 2020). Furthermore, Walton et al. (2020) emphasize the importance of guidance on the disclosure of cybersecurity risks and incidents, along with potential internal control solutions, to enhance regulatory frameworks. Additionally, Schmitz & Cole (2022) discuss the proposals for a NIS 2.0 Directive and a Cyber Resilience Act, outlining how these initiatives will complement existing regulatory gaps and contribute to a more efficient and coherent regulatory framework in the EU.

In conclusion, the synthesis of these studies underscores the significance of existing cybersecurity regulations, the evaluation of compliance measures in the FinTech sector, and the recommendations for enhancing regulatory frameworks. By addressing inefficiencies, cultural values, and proposing new assessment frameworks, the regulatory landscape can be strengthened to ensure robust cybersecurity and compliance in various sectors.

6. Human Factors in Cybersecurity

Social engineering attacks are a significant threat in cybersecurity, exploiting human vulnerabilities to gain unauthorized access to sensitive information. These attacks employ various tactics, including persuasion, social influence, and deception, to manipulate individuals into divulging confidential data or performing actions that compromise security (Wang et al., 2021). Tactics used in social engineering attacks encompass a wide range of human factors, such as cognitive biases, emotions, and personality traits, which can be exploited by skilled attackers to create security vulnerabilities (Wang et al., 2021; Akindote et al., 2023). Human-based attacks are sophisticated and hard to detect, making their mitigation necessary (Salahdine & Kaabouch, 2019). Mitigation strategies for social engineering attacks involve building a resilient insider threat program, creating a culture of cybersecurity awareness, and implementing user awareness training programs for financial professionals and users (Airehrour et al., 2018; Akindote et al., 2024). These strategies aim to enhance individuals' ability to recognize and resist social engineering tactics, thereby reducing the success rate of such attacks.

Insider threats pose a significant risk in the FinTech sector, where malicious insiders can exploit their access to sensitive financial data for personal gain or to inflict harm on the organization. Building a resilient insider threat program is crucial to effectively mitigate these risks. Such a program should encompass comprehensive monitoring of user activities, implementing strict access controls, and conducting regular security awareness training to educate employees about the potential dangers of insider threats (Siddiqi et al., 2022; Babarinde et al., 2023).

User awareness plays a pivotal role in mitigating social engineering attacks and insider threats. Training programs for financial professionals and users are essential to equip individuals with the knowledge and skills to identify and respond to potential security threats effectively. Creating a culture of cybersecurity awareness within organizations fosters a proactive approach to security, encouraging employees to remain vigilant and report any suspicious activities promptly (Syafitri et al., 2022; Ogundairo et al., 2023).

In conclusion, human factors play a critical role in cybersecurity, particularly in the context of social engineering attacks and insider threats. Understanding the tactics used in social engineering, implementing mitigation strategies, addressing insider risks in FinTech, and emphasizing the importance of user awareness are essential components of a comprehensive cybersecurity approach.

7. Future Outlook

The evolving landscape of cyber risks in financial technologies is crucial to understand. Several studies have provided valuable insights into the challenges and opportunities that lie ahead. Raban & Hauptman (2018) conducted a long-term foresight study to identify major threat drivers and emerging technologies likely to impact defense and attack capabilities in cybersecurity. Their study emphasizes the importance of understanding emerging technologies that could shape the future cybersecurity landscape. Furthermore, Sadik et al. (2020) focused on the cybersecurity of smart grids and emerging trends such as using blockchain in the Internet of Things (IoT). This highlights the growing significance of integrating advanced technologies into cybersecurity frameworks to mitigate emerging threats. Moreover, Lee (2020) emphasized the increasing importance of cybersecurity in the Internet of Things (IoT) and the growing threat of cyberattacks, indicating a shift in focus towards securing interconnected devices and systems.

Additionally, Osak et al. (2020) highlighted the acute aspects of cybersecurity in the energy systems of the future, particularly in the era of total digitalization. Their study underscores the need to address large-scale cyber attacks on critical infrastructure, including power systems, reflecting the evolving nature of cyber threats in essential sectors.

These studies collectively underscore the growing significance of understanding emerging technologies, securing interconnected systems, and addressing critical infrastructure vulnerabilities in shaping the future outlook of cybersecurity threats in financial technologies.

8. Recommendation and Conclusion

Based on the critical review of emerging cybersecurity threats in financial technologies (FinTech), several key findings have been identified that necessitate urgent attention and strategic response. The increasing sophistication of cyber threats poses a significant risk to the integrity and security of financial systems. To address these challenges effectively, the following recommendations are proposed; the review highlights the dynamic and evolving nature of cyber threats in the FinTech sector. Threat actors are constantly adapting their tactics, techniques, and procedures to exploit

vulnerabilities and circumvent traditional security measures. Data breaches continue to be a prevalent threat, compromising sensitive financial information and eroding public trust. The review underscores the need for robust data protection measures to safeguard customer information and maintain the confidentiality of financial transactions. The interconnected nature of FinTech ecosystems introduces vulnerabilities in the supply chain. Cybersecurity risks extend beyond individual organizations, requiring a collaborative and holistic approach to address potential weaknesses in the broader financial infrastructure.

Given the dynamic nature of cyber threats in FinTech, it is imperative for financial institutions, regulatory bodies, and technology providers to adopt a proactive and adaptive cybersecurity strategy. Implementing real-time monitoring systems and leveraging threat intelligence to identify and respond to emerging threats promptly. Embracing cutting-edge technologies such as artificial intelligence and machine learning to enhance anomaly detection, threat prediction, and automated response mechanisms. Recognizing the role of human factors in cybersecurity, organizations should invest in comprehensive training programs to educate employees on cybersecurity best practices and promote a culture of security awareness. Encouraging collaboration among industry stakeholders, sharing threat intelligence, and collectively addressing cybersecurity challenges can strengthen the overall resilience of the FinTech ecosystem.

To stay ahead of emerging cybersecurity threats in FinTech, future research should focus on the following areas; given the potential threat posed by quantum computing to traditional encryption methods, exploring and adopting quantum-safe cryptographic techniques is crucial for securing financial transactions in the future. As blockchain technology continues to play a pivotal role in FinTech, research should delve into enhancing the security of distributed ledger systems and smart contracts. Developing and refining regulatory frameworks that adapt to the evolving cybersecurity landscape, ensuring that they are effective, enforceable, and facilitate innovation without compromising security.

In conclusion, the critical review of emerging cybersecurity threats in FinTech underscores the importance of a proactive and adaptive approach to cybersecurity. Organizations must invest in advanced technologies, employee training, and collaboration to stay resilient against evolving threats. Future research should focus on quantum-safe cryptography, blockchain security, and regulatory frameworks to ensure the continued security and stability of financial technologies. By implementing these recommendations, stakeholders can contribute to a more secure and resilient FinTech ecosystem.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Abrahams, T.O., Ewuga, S.K., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O., 2023. Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security.

[2] Abrahams, T.O., Ewuga, S.K., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O., 2024. MASTERING COMPLIANCE: A Comprehensive Review Of Regulatory Frameworks In Accounting And Cybersecurity. *Computer Science & IT Research Journal*, *5*(1), pp.120-140.

[3] Adaga, E.M., Egieya, Z.E., Ewuga, S.K., Abdul, A.A. and Abrahams, T.O., 2024. Philosophy In Business Analytics: A Review Of Sustainable And Ethical Approaches. *International Journal of Management & Entrepreneurship Research*, *6*(1), pp.69-86.

[4] Adebowale, M. (2021). Intelligent decision support system.. https://doi.org/10.5772/intechopen.95252

[5] Adeleke, O.K., Segun, I.B. and Olaoye, A.I.C., 2019. Impact of internal control on fraud prevention in deposit money banks in Nigeria. *Nigerian Studies in Economics and Management Sciences*, *2*(1), pp.42-51.

[6] Airehrour, D., Nair, N., & Madanian, S. (2018). Social engineering attacks and countermeasures in the new zealand banking system: advancing a user-reflective mitigation model. Information, 9(5), 110. https://doi.org/10.3390/info9050110

[7] Akindote, O.J., Adegbite, A.O., Dawodu, S.O., Omotosho, A. and Anyanwu, A., 2023. Innovation In Data Storage Technologies: From Cloud Computing To Edge Computing. *Computer Science & IT Research Journal*, *4*(3), pp.273-299.

[8] Akindote, O.J., Adegbite, A.O., Omotosho, A., Anyanwu, A. and Maduka, C.P., 2024. Evaluating The Effectiveness Of It Project Management In Healthcare Digitalization: A REVIEW. *International Medical Science Research Journal*, *4*(1), pp.37-50.

[9] Ali, W. (2017). Phishing website detection based on supervised machine learning with wrapper features selection. International Journal of Advanced Computer Science and Applications, 8(9). https://doi.org/10.14569/ijacsa.2017.080910

[10] Aliyu, A., Μαγλαράς, Λ., He, Y., Yevseyeva, I., Cook, A., Janicke, H., … & Boiten, E. (2020). A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. Applied Sciences, 10(10), 3660. https://doi.org/10.3390/app10103660

[11] Anamu, U.S., Ayodele, O.O., Olorundaisi, E., Babalola, B.J., Odetola, P.I., Ogunmefun, A., Ukoba, K., Jen, T.C. and Olubambi, P.A., 2023. Fundamental design strategies for advancing the development of high entropy alloys for thermo-mechanical application: A critical review. *Journal of Materials Research and Technology*.

[12] Arner, D., Barberis, J., & Buckley, R. (2015). The evolution of fintech: a new post-crisis paradigm?. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2676553

[13] Awaliyah, T. (2023). The impact of financial technology innovation on banking service transformation: a case study in the fintech industry. Global, 1(3), 306-313. https://doi.org/10.59613/global.v1i3.47

[14] Babarinde, A.O., Ayo-Farai, O., Maduka, C.P., Okongwu, C.C., Ogundairo, O. and Sodamade, O., 2023. Review of AI applications in Healthcare: Comparative insights from the USA and Africa. International Medical Science Research Journal, 3(3), pp.92-107.

[15] Balogun, O.D., Ayo-Farai, O., Ogundairo, O., Maduka, C.P., Okongwu, C.C., Babarinde, A.O. and Sodamade, O.T., 2024. The Role Of Pharmacists In Personalised Medicine: A Review Of Integrating Pharmacogenomics Into Clinical Practice. *International Medical Science Research Journal*, *4*(1), pp.19-36.

[16] Biasin, E. (2023). New cybersecurity requirements for medical devices in the eu: the forthcoming european health data space, data act, and artificial intelligence act. Law Technology and Humans, 5(2), 43-58. https://doi.org/10.5204/lthj.3068

[17] Buvik, A. (2013). An empirical analysis of coercive means of enforcing compliance in public procurement. Journal of Public Procurement, 13(2), 243-273. https://doi.org/10.1108/jopp-13-02-2013-b004

[18] Çatal, Ç., Giray, G., & Tekinerdoğan, B. (2021). Applications of deep learning for mobile malware detection: a systematic literature review. Neural Computing and Applications, 34(2), 1007-1032. https://doi.org/10.1007/s00521-021-06597-0

[19] Ezeigweneme, C.A., Umoh, A.A., Ilojianya, V.I. and Adegbite, A.O., 2024. Review Of Telecommunication Regulation And Policy: Comparative Analysis USA AND AFRICA. *Computer Science & IT Research Journal*, *5*(1), pp.81-99.

[20] Gai, P. and Kapadia, S. (2010). Contagion in financial networks. Proceedings of the Royal Society a Mathematical Physical and Engineering Sciences, 466(2120), 2401-2423. https://doi.org/10.1098/rspa.2009.0410

[21] Gupta, B., Arachchilage, N., & Psannis, K. (2017). Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommunication Systems, 67(2), 247-267. https://doi.org/10.1007/s11235-017-0334-z

[22] Haldane, A. and May, R. (2011). Systemic risk in banking ecosystems. Nature, 469(7330), 351-355. https://doi.org/10.1038/nature09659

[23] Hassan, A.O., Ewuga, S.K., Abdul, A.A., Abrahams, T.O., Oladeinde, M. and Dawodu, S.O., 2024. Cybersecurity In Banking: A Global Perspective With A Focus On Nigerian Practices. *Computer Science & IT Research Journal*, *5*(1), pp.41-59.

[24] Ilugbusi, S., Akindejoye, J.A., Ajala, R.B. and Ogundele, A., 2020. Financial liberalization and economic growth in Nigeria (1986-2018). *International Journal of Innovative Science and Research Technology*, *5*(4), pp.1-9.

[25] Jain, A. and Gupta, B. (2017). Phishing detection: analysis of visual similarity based approaches. Security and Communication Networks, 2017, 1-20. https://doi.org/10.1155/2017/5421046

[26] Kharlamov, A. and Pogrebna, G. (2019). Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity†. Regulation & Governance, 15(3), 709-724. https://doi.org/10.1111/rego.12281

[27] Lee, I. (2020). Internet of things (iot) cybersecurity: literature review and iot cyber risk management. Future Internet, 12(9), 157. https://doi.org/10.3390/fi12090157

[28] Lewallen, J. (2020). Emerging technologies and problem definition uncertainty: the case of cybersecurity. Regulation & Governance, 15(4), 1035-1052. https://doi.org/10.1111/rego.12341

[29] Mohammad, R., Thabtah, F., & McCluskey, T. (2015). Tutorial and critical analysis of phishing websites methods. Computer Science Review, 17, 1-24. https://doi.org/10.1016/j.cosrev.2015.04.001

[30] Mwelu, N., Davis, P., Ke, Y., & Watundu, S. (2018). Compliance within a regulatory framework in implementing public road construction projects. Construction Economics and Building, 18(4), 1-23. https://doi.org/10.5130/ajceb.v18i4.6362

[31] Niekerk, B. (2023). Vulnerability of south african commodity value chains to cyber incidents. Scientia Militaria South African Journal of Military Studies, 51(3). https://doi.org/10.5787/51-3-1430

[32] Ogundairo, O., Ayo-Farai, O., Maduka, C.P., Okongwu, C.C., Babarinde, A.O. and Sodamade, O.T., 2023. Review On MALDI Mass Spectrometry And Its Application In Clinical Research. *International Medical Science Research Journal*, *3*(3), pp.108-126.

[33] Ohenhen, P.E., Chidolue, O., Umoh, A.A., Ngozichukwu, B., Fafure, A.V., Ilojianya, V.I. and Ibekwe, K.I., 2024. Sustainable cooling solutions for electronics: A comprehensive review: Investigating the latest techniques and materials, their effectiveness in mechanical applications, and associated environmental benefits.

[34] Orieno, O.H., Ndubuisi, N.L., Ilojianya, V.I., Biu, P.W. and Odonkor, B., 2024. The Future Of Autonomous Vehicles In The US Urban Landscape: A Review: Analyzing Implications For Traffic, Urban Planning, And The Environment. *Engineering Science & Technology Journal*, *5*(1), pp.43-64.

[35] Osak, A., Panasetsky, D., & Buzina, E. (2020). Analysis of cyber vulnerabilities of the emergency control and relay protection to assess the reliability and survivability of electrical power systems in the era of total digitalization. E3s Web of Conferences, 216, 01040. https://doi.org/10.1051/e3sconf/202021601040

[36] Ozcan, A., Catal, C., Donmez, E., & Senturk, B. (2021). A hybrid dnn–lstm model for detecting phishing urls. Neural Computing and Applications, 35(7), 4957-4973. https://doi.org/10.1007/s00521-021-06401-z

[37] Purnaye, E. (2024). Hypervisor-level ransomware detection in cloud using machine learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11(9), 3186-3190. https://doi.org/10.17762/ijritcc.v11i9.9508

[38] Raban, Y. and Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. Foresight, 20(4), 353-363. https://doi.org/10.1108/fs-02-2018-0020

[39] Sadik, S., Ahmed, M., Sikos, L., & Islam, A. (2020). Toward a sustainable cybersecurity ecosystem. Computers, 9(3), 74. https://doi.org/10.3390/computers9030074

[40] Salahdine, F. and Kaabouch, N. (2019). Social engineering attacks: a survey. Future Internet, 11(4), 89. https://doi.org/10.3390/fi11040089

[41] Schmitz, S. and Cole, M. (2022). Towards an efficient and coherent regulatory framework on cybersecurity in the eu: the proposals for a nis 2.0 directive and a cyber resilience act. Applied Cybersecurity & Internet Governance, 1(1), 121-137. https://doi.org/10.5604/01.3001.0016.1323

[42] Siddiqi, M., Pak, W., & Siddiqi, M. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. Applied Sciences, 12(12), 6042. https://doi.org/10.3390/app12126042

[43] Singhvi, S. and Dadhich, M. (2023). Fintech revolution and future of sustainable banking: opportunities and risks analysis. International Journal of Management and Development Studies, 12(04), 12-21. https://doi.org/10.53983/ijmds.v12n04.003

[44] Smolyak, A., Levy, O., Vodenska, I., Buldyrev, S., & Havlin, S. (2020). Mitigation of cascading failures in complex networks. Scientific Reports, 10(1). https://doi.org/10.1038/s41598-020-72771-4

[45] Syafitri, W., Shukur, Z., Mokhtar, U., Sulaiman, R., & Ibrahim, M. (2022). Social engineering attacks prevention: a systematic literature review. Ieee Access, 10, 39325-39343. https://doi.org/10.1109/access.2022.3162594

[46] Urus, S. and Mohamed, I. (2021). A flourishing fintech ecosystem: conceptualization and governing issues in malaysia. Business and Economic Research, 11(3), 106. https://doi.org/10.5296/ber.v11i3.18729

[47] Vincent, A.A., Segun, I.B., Loretta, N.N. and Abiola, A., 2021. Entrepreneurship, agricultural value-chain and exports in Nigeria. *United International Journal for Research and Technology*, *2*(08), pp.1-8.

[48] Walton, S., Wheeler, P., Zhang, Y., & Zhao, X. (2020). An integrative review and analysis of cybersecurity research: current state and future directions. Journal of Information Systems, 35(1), 155-186. https://doi.org/10.2308/isys-19-033

[49] Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: effect mechanisms, human vulnerabilities and attack methods. Ieee Access, 9, 11895-11910. https://doi.org/10.1109/access.2021.3051633

[50] Wang, Z., Zhu, H., Liu, P., & Sun, L. (2021). Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. Cybersecurity, 4(1). https://doi.org/10.1186/s42400-021-00094-6

[51] Yang, Y. and Motter, A. (2017). Cascading failures as continuous phase-space transitions. Physical Review Letters, 119(24). https://doi.org/10.1103/physrevlett.119.248302

[52] Zakaria, W., Abdollah, M., Othman, M., & Ariffin, A. (2017). The rise of ransomware.. https://doi.org/10.1145/3178212.3178224