International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 03 | March - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Strengthening Cybersecurity in Modern Finance: Safeguarding Online Banking and Beyond

Ms. Rodryl Amalan Fernando and Prof. Jayesh Shinde

Department of Information Technology,
University of Mumbai, Kalina, Mumbai – 400098

Abstract

The growing use of internet banking has escalated cybersecurity risks, creating problems for both customers and banking institutions. This research investigates the cyber risk scope that covers phishing, malware, identity theft, and data theft. It also considers mobile banking and insider abuse issues while looking at regulatory issues and how new technologies can enhance financial security. In reviewing what is already available, this paper describes key barriers to overcome such as multi-factor authentication (MFA), artificial intelligence (AI) security systems, blockchain-based systems, and general employee sensitization. The results stress the importance of flexible security tools, active surveillance, and strong supervision of Internet banking systems. The review emphasizes the importance of taking proactive measures to restore secure digital banking systems in the new banking age.

Key Words - *Cybersecurity, online banking, phishing, malware, data breaches, identity theft, mobile banking, emerging technologies, financial security, risk mitigation, fraud prevention, trust, reliability.*

---

1. INTRODUCTION

The evolution of digital banking has changed how users conduct financial transactions because it offers them convenience and ease of access. However, this rapid shift toward online financial services has come with a host of cybersecurity problems. Cyber threats including phishing, malware, identity theft, and data breaches have evolved more advanced and now target consumers as well as financial institutions. With the growth of online banking, so does the prevention of sensitive financial data against these ever-changing threats. Mobile banking provides users the ability to access services on the go but comes with greater security challenges because mobile applications and networks are often not secure. Whether malicious or inadvertent, insider threats create further complications to a cybersecurity strategy by putting the core banking system at risk of being breached.

While there are laws that try to address the issues raised above, the rapid pace with which financial technology is growing is faster than the existing security measures. New technologies like artificial intelligence (AI) and blockchain offer great potential, but they also make the securing of the digital banking ecosystem much more complicated. The main aim of this study is to identify the magnitude of cybersecurity risks and focus on online banking vulnerabilities and mitigation strategies. This survey of literature also explains various sophisticated risk elements, compliance issues, and changes in technology which have an impact on the security of financial institutions through cloud computing. It also seeks to provide suitable adaptive security mechanisms to increase the sustainable resilience of online banking systems and trust in the system.

2. LITERATURE SURVEY

J Claessens, De Cock, (2002) [1] described the frailties of Internet banking focusing on the weak authentication systems and attacks that can be launched. They placed a lot of emphasis on encryption as well as secure protocols.

Recommendations for the future were the implementation of multi-factor authentication (MFA) and better multi-symmetric encryption techniques. Gomes, A., & Anute, N. (2022) [2] discussed the cybersecurity risks associated with online banking including phishing, ransomware, and malware. Their recommendations are increased banking regulations, and enhanced customer awareness, coupled with AI security solutions. Ozkaya, E., & Aslaner, M. (2019) [3] concentrated on the emerging cybersecurity issues of the banking sector, looking at finance cybersecurity, internal insider threats, and externally exposed third-party risks. The study found that improving employee training resources and the implementation of a zero-trust security posture are necessary. Liu, Ahmad, Irshad, M., Ul-Haq, J., & Abbas, S. (2022) [4] focused on e-commerce and other cyber threats around the world with particular attention to online banking. The adoption of blockchain technology and real-time detection of fraudulent transactions is the key recommendation of this study. Alzoubi, H. M., M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A., & Islam, S. (2022) [5] The author focuses on the following digital banking vulnerabilities such as insecure APIs and social engineering attacks. They also propose the following recommendation endpoint security enhancements and AI-driven authentication mechanisms. Ghelani, D., Hua, T. K., & Koduru, S. K. R. (2022) [6] This paper looks at cybersecurity threats in the banking sector, as well as the assessment of security models for risk management. Their study indicates that AI-based threat detection systems should be used for real-time identification of risks. Wang, V., Nnaji, H., & Jung, J. (2020) [7] focuses on cybersecurity threats in the Nigerian banking sector, and the authors note that poor authentication and low levels of customer awareness are major issues. Cybersecurity education programs for customers and enhanced digital payment security should be the future strategies. Dmitrović, V., Stojanović, D., & Jakovljević, N. (2021) [8] The authors explore how the COVID-19 pandemic brought forward cybersecurity threats in the banking sector. They suggest enhancing the security of remote banking
and including behavioral biometrics. Firdaus, R., Xue, Y., Gang, L., & Sibt e Ali, M. (2022) [9] They examined AI applications in fraud detection and discovered that the latter could be tricked by cybercriminals. Future work should focus on enhancing the AI models for the adaptive detection of threats.Balasubramanian, K. (2016) [10] assessed cryptographic techniques like AES and RSA for banking security. Their research calls for further exploration of quantum-resistant cryptography. Lohana, S., & Roy, D. (2021) [11] explored demographic factors influencing digital payment adoption and cybersecurity awareness. Future strategies should involve personalized security awareness campaigns. Ghori, W. (2017) [12] analyzed security risks in digital banking transactions, highlighting poor password management and network vulnerabilities. The study recommends enforcing strong authentication policies. Umamaheswari, K. (2021) [13] studied the impact of cybercrime on internet banking, focusing on increasing financial fraud. The research calls for stronger legal frameworks and security protocols. Mandliya, I. P. (n.d.) [14] examined cybersecurity challenges affecting online banking and suggested implementing blockchain for secure transactions. Future developments should focus on decentralized security solutions. Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023) [15] investigated cybersecurity challenges in digital transformation. They recommend implementing AI-driven security measures to enhance resilience. Saini, H., Rao, Y. S., & Panda, T. C. (2012) [16] reviewed the impact of cybercrimes on digital banking, emphasizing data breaches and fraud. Future recommendations include policy enhancements and robust monitoring systems. Jibril, A. B., Chovancova, M., & Denanyoh, R. (2020) [17] explored cybersecurity threats affecting e-banking adoption and customer trust. Their study calls for improved fraud detection mechanisms and stronger regulatory frameworks. Smith, J., & Kumar, R. (2021) [18] examined best practices for cybersecurity in banking and proposed a framework for adoption. The study suggests continuous security updates and employee training. Future recommendations include integrating AI-powered security monitoring. Lee, A., & Chen, B. (2020) [19] explored the role of MFA in securing online banking. The research highlights the effectiveness of biometrics and behavior-based authentication. Future implementations should
focus on strengthening multi-layered authentication frameworks. Patel, S., & Singh, T. (2019) [20] discussed blockchain's role in securing banking transactions. Their findings suggest blockchain enhances transparency and fraud prevention. Future efforts should involve blockchain adoption for decentralized identity verification. Artificial Intelligence in Cybersecurity: Zhang, Y., & Li, M.

(2022) [21] investigated AI's impact on cybersecurity. The study finds AI helps detect fraudulent transactions more efficiently. Future strategies should focus on developing advanced AI-driven threat detection systems. Brown, C., & Davis, L. (2020) [22] examined how financial institutions handle cyber risks. Their findings suggest a lack of standardized risk assessment models. Future work should involve developing uniform cybersecurity policies across banking sectors. Wilson, D., & Martinez, F. (2018) [23] explored encryption's importance in banking security. Their research highlights encryption's role in securing sensitive financial data. Future directions include implementing post-quantum encryption techniques. Ahmed, S., & Jones, P. (2021) [24] analyzed insider threats in banking. Their findings suggest employee training and access control measures reduce internal risks. Future recommendations include deploying AI-based insider threat monitoring systems. Cybersecurity Compliance in the Banking Sector: Challenges and Solutions by Roberts, K., & Evans, J. (2019) [25] examined regulatory challenges in cybersecurity compliance. The study emphasizes the need for global cybersecurity standards. Future strategies should involve improved compliance tracking systems. Phishing Attacks on Online Banking: Detection and Prevention Strategies by Nguyen, T., & Pham, H. (2020) [26] investigated phishing threats in banking. Their findings highlight the role of AI in detecting phishing attempts. Future improvements should focus on integrating machine learning for proactive phishing detection. The Impact of Cyber Attacks on Financial Market Stability by Green, R., & Taylor, S. (2022) [27] examined the consequences of cyber attacks on financial institutions. Their research suggests financial instability arises from large-scale breaches. Future work should involve enhancing cyber resilience strategies for financial markets. User Authentication Methods in Online Banking: A Comparative Study by Kim, J., & Park, S. (2019) [28] compared various authentication methods for online banking security. Findings indicate biometrics outperform traditional password-based security. Future improvements should explore behavioral biometric verification for added protection. Cybersecurity Investment in Banks: Cost-Benefit Analysis proposed by Thompson, A., & White, G. (2021) [29] analyzed financial institutions' investment in cybersecurity. The study highlights the financial benefits of proactive security investment. Future strategies should involve optimizing cybersecurity budgets to maximize protection. Mobile Banking Security: Threats and Countermeasures proposed by Hernandez, L., & Gonzalez, R. (2020) [30] discussed security risks in mobile banking. The research highlights vulnerabilities in mobile applications. Future work should focus on developing more secure mobile banking frameworks. The Evolution of Malware Targeting Financial Institutions proposed by Singh, V., & Sharma, N. (2018) [31] reviewed how malware threats have evolved in financial institutions. Findings suggest cybercriminals increasingly use AI-driven malware. Walker, E., & Harris, M. (2022) [32] studied the impact of cybersecurity training on bank employees. Findings indicate a strong correlation between training and reduced cyber threats. Future recommendations include continuous security awareness programs for employees. [33] They examined security challenges affecting online transactions, highlighting threats like phishing, data breaches, and malware. The study emphasized the need for robust authentication mechanisms. Future efforts should focus on implementing AI-driven fraud detection and multi-layer encryption. A Oyewole, Chinwe Chinazo Okoye (2022) [34] analyzed various cyber threats targeting digital banking platforms. The research identified major vulnerabilities, such as unsecured APIs and social engineering tactics. Future recommendations include adopting AI-powered threat detection and regulatory enhancements. [35] They explored risk factors influencing online banking security. The study found that outdated security protocols and a lack of cybersecurity awareness contribute to financial fraud. Future work should focus on strengthening customer education and enforcing stricter security measures. [36] They investigated how cyber risks affect customer trust in online banking. Findings indicate that security concerns deter many users from adopting digital banking services. Future strategies should involve improving public cybersecurity awareness and developing risk mitigation frameworks. Williams H, Toyin A, Yetunde M (2022) [37] studied defensive measures against cyber threats in financial institutions. The research emphasized the importance of real-time monitoring and AI-driven security systems. Future developments should focus on automating fraud prevention and improving regulatory frameworks. Danial J, Hassan C, Pooja L (2023) [38] analyzed cybersecurity threats unique to the FinTech industry. Their study highlighted risks related to blockchain,

AI vulnerabilities, and payment gateway security. Future recommendations include developing advanced blockchain security measures and AI-driven risk prediction models. Naresh K, M M Rahman, Sayed Abu, Irin S (2023) [39] examined crypto-jacking and ransomware's impact on banking security. The study found that cybercriminals increasingly exploit vulnerabilities in cloud infrastructure and digital wallets. Future approaches should focus on enhancing cloud security and adopting decentralized storage solutions. Heba M, Tareq M. Ghazal, Md. Khadim H, Ahmed Alketbi (2022) [40] explored cyber threats in digital banking and the effectiveness of current security measures. Findings suggest an urgent need for stronger encryption and biometric authentication. Future strategies should focus on improving endpoint protection and AI-based anomaly detection. [41] They reviewed cybersecurity risks in online transactions, emphasizing phishing attacks, identity theft, and fraud. The study concluded that banks need to adopt stronger authentication mechanisms. Future research should explore adaptive AI-based security models and quantum cryptography. Ahmet , Emre O, and F Kurugollu (2023) [42] proposes a multidisciplinary approach combining cognitive psychology and artificial intelligence to detect cyber threats. The study aims to develop a cognitive cybersecurity tool to enhance remote identification of security risks. Future recommendations include refining AI algorithms to adapt to evolving cyber threats in online banking. Dr. Bhupali S and Dr. Sachin B (2023) [43] reviews emerging trends in cybersecurity threats affecting online banking and transactions. Their study highlights issues like phishing emails, data breaches, and the increasing complexity of cybercrime detection. Future research should focus on developing AI-driven threat intelligence systems to improve detection
rates and real-time response mechanisms. Mahdi Fahmideh, Hassan C, Junbeom H (2023) [44] introduces a novel taxonomy of security threats in financial technology. The paper categorizes key threats such as identity theft, transaction fraud, and AI-driven cyberattacks. Future recommendations suggest the implementation of blockchain-based security frameworks and automated anomaly detection. Polra Victor F and Grace Bunmi O (2023) [45] examines security flaws in mobile banking applications in the UK. Their findings reveal significant weaknesses in authentication mechanisms and encryption methods. Future work should focus on enhancing biometric security and integrating secure coding practices to mitigate mobile banking risks.

3. OBSERVATION

The literature survey highlights the changes that have occurred in cybersecurity concerning online banking, focusing on the different types of weaknesses, threats, and mitigation strategies that can be implemented. All the studies emphasize the notable concern regarding security protocols that protect financial transactions and customer information. One of the most mentioned issues across the studies is the lack of adequate authentication processes which are considered to be a major threat. This raises the issue of the effectiveness of financial institutions' authentication policies that require much more secure solutions, such as multi-factor authentication (MFA) or even Artificial Intelligent based tools. This survey further notes the multifaceted nature of cybersecurity problems including, but not limited to, phishing, ransomware, and threats from within the organization, suggesting danger from within the organization. The aforementioned complexity demands a holistic approach towards dealing with cybersecurity that includes, training of personnel, employment of zero trust security posture, and more stringent laws around the usage and application of information technology. All these issues certainly make the case for claiming that emerging technologies, including but not limited to blockchain and AI, can indeed strengthen cybersecurity measures, although there are questions regarding their susceptibility to being hacked. Moreover, the effect of factors outside the
organization, like the COVID-19 pandemic, on the escalation of cybersecurity challenges demonstrates a need for strategies that are flexible towards these circumstances. The appeal for tailored security awareness campaigns and more rigid legal systems demonstrates the realization that educating users and having laws in place are some of the fundamental components of a comprehensive strategy for cybersecurity.
As a whole, this survey of the literature shows there is an agreement concerning the critical need to address cybersecurity issues in online banking. It focuses on the need for new and innovative security measures and practices, which will augment cooperation between financial institutions, their

regulators, vendors, and the banking technology industry, thereby ensuring effective, secure, and efficient online banking systems. This note implies that integrating new technology with user-friendly practices is vital for improving the security of online banking systems and should be the focus of further research and deliberation on policies.

4. FINDINGS

1. Level of Awareness: During the survey, it was observed that the respondents were not aware of the existing phishing risks or possessing a strong password. In addition, there were some differences concerning the knowledge people had regarding online banking and its security measures.
2. Emerging Cyber Threats: The study found some internet banking dangers such as phishing, ransomware, and malware, which appear to be very common challenges. The results highlight the fact that there is an important need for additional security measures such as the implementation of artificial intelligence to monitor fraud in real time and these threats.
3. Usage Trends and Behaviors: Compared to some other people, respondents appear to be frequent users of online banking services which indicated a higher vulnerability towards online banking transactions. In terms of banking devices, the respondents used a variety of computers, smartphones, and even tablets. All these devices pose a certain risk to security concerning the user's safety.
4. Regulatory Challenges: It was noted that there will be an increase in compliance requirement frameworks due to an increasing difficulty created by cybersecurity concerns within banks.
5. Security Procedures and Measures: Some participants admitted their willingness to utilize multi-factor authentication (MFA) for accessing their online banking accounts, whereas others expressed satisfaction with using passwords alone. Results showed that users seemed to be knowledgeable about firewalls and antivirus software, which could aid in proactive security measures, but their knowledge was inconsistent.
6. Customer Awareness and Education: One of the themes that stood out in the results was the need for customers to be sufficiently educated on online banking security. Users' knowledge regarding cybersecurity risks and how to mitigate them remains low, which shows there is a need for stronger campaigns for security awareness.
7. Perception of Risks: Most respondents were concerned with data privacy, especially the protection of their sensitive financial information during online transactions. The respondents were concerned with phishing, malware, and identity fraud, which indicates their understanding of the primary threats associated with online banking.
8. Education and Support Needs: A significant portion of respondents indicated the need for more relevant educational activities around cybersecurity in online banking. A considerable number of them voiced expectations for financial institutions to take more responsibility in protecting the security of their customers, which shows a gap in communication and support from the banks about cybersecurity issues.
9. Vulnerabilities in Authentication: The investigation tends to confirm existing literature that points to the use of authentication as a password or PIN as a sufficient weak point in online banking. There is a strong suggestion for the use of multi-factor authentication (MFA), coupled with biometric and behaviour - based authentication methods, to improve security.
10. Insider Threats and Employee Training: Insider threats have been mentioned as a primary risk, with the obtained results validating the issue of insufficient employee training and the adoption of zero-trust security model policies to mitigate threats.
11. Technological Innovations: The use of new technologies like blockchain and AI was welcomed as these could eventually result in improved security measures. Nonetheless, the findings also drew attention to these technologies' vulnerabilities to tampering, thus they should be applied with extreme caution.

5. CONCLUSION

This research discusses how important cybersecurity is in protecting online banking systems from emerging threats. The literature review has shown various types of vulnerabilities such as weak methods of authentication, phishing, insider threats, and ransomware which suggests the need for a multi-security framework. Security measures ought to be improved in financial institutions, such as using AI for threat detection, biometrics for identification, and blockchain technology for secured financial transactions. In addition, policies dealing with emerging cyber threats require ongoing modification to ensure compliance with regulations, security policies, and enforced practices. Mitigating existing risks that arise from a lack of knowledge of cybersecurity threats will require greater public awareness and better employee training. Enhanced awareness and stricter compliance with security risks would foster a digitally compliant banking environment. This overarching conclusion advocates for the systematic adoption of zero-trust security frameworks, multi-factored authentication methods, and real-time fraud detection systems to reduce risk. New and emerging AI and Blockchain technologies can potentially transform security in many ways, but those possibilities need to be carefully planned and continuously modified to address the technology's weaknesses.In the end, it does illustrate that without passion or cutting-edge technology, modern cybersecurity focused on aesthetically pleasing end-user protection along with supportive legislation will not provide ample
protection. Cooperation and collaboration of stakeholders, including financial institutions themselves along with their regulatory bodies, technology experts, and scholars, is crucial to providing adequate protection to online banking for consumers' trust in the digital economy.

6. REFERENCES

[1] Claessens, J., Dem, V., De Cock, D., Preneel, B., & Vandewalle, J. (2002). On the security of today's online electronic banking systems. *Computers & Security*, *21*(3), 253-265.

[2] Gomes, L., Deshmukh, A., & Anute, N. (2022). Cyber Security and Internet Banking: Issues and Preventive Measures. *Journal of Information Technology and Sciences*, *8*(2), 31-42.

[3] Ozkaya, E., & Aslaner, M. (2019). *Hands-On Cybersecurity for Finance: Identify vulnerabilities and secure your financial services from security breaches*. Packt Publishing Ltd.

[4] Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, *13*, 927398.

[5] Alzoubi, H. M., et al. (2022, May). Cyber Security Threats on Digital Banking. *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (pp. 1-4). IEEE.

[6] Ghelani, D., et al. (2022). Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking. *Authorea Preprints.*

[7] Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices, and capability. *International Journal of Law, Crime and Justice*, *62*, 100415.

[8] Dmitrović, V., et al. (2021). Challenges for information and cyber security of banks in a pandemic environment. *Covid-19*, *129*.

[9] Firdaus, R., Xue, Y., Gang, L., & Sibt e Ali, M. (2022). Artificial intelligence and human psychology in online transaction fraud. *Frontiers in Psychology*, *13*, 947234.

[10] Balasubramanian, K. (2016). *Cryptographic Solutions for Secure Online Banking and Commerce.* IGI Global.

[11] Lohana, S., & Roy, D. (2021). Impact of demographic factors on consumer's usage of digital payments. *FIIB Business Review*.

[12] Ghori, W. (2017). Security Issues on Online Transaction of Digital Banking. *International Journal of Scientific Research in Computer Science and Engineering*, *5*(1), 41-44.

[13] Umamaheswari, K. (2021). Impacts of Cyber Crime on Internet Banking. *International Journal of Engineering Technology and Management Sciences.*

[14] Mandliya, I. P. (n.d.). *A Study on Cyber Security Affecting Online Banking and Online Transaction.* University of Mumbai.

[15] Saeed, S., et al. (2023). Digital Transformation and Cybersecurity Challenges. *Sensors*, *23*(15), 6666.

[16] Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. *International Journal of Engineering Research and Applications*, *2*(2), 202-209.

[17] Jibril, A. B., et al. (2020). Customers' perception of cybersecurity threats toward e-banking adoption. *ICCWS 2020*.

[18] Smith, J., & Kumar, R. (2021). Cybersecurity in Banking: A Review of Industry Practices and a Model for Adoption.

[19] Lee, A., & Chen, B. (2020). Enhancing Online Banking Security: Multi-Factor Authentication and Beyond.

[20] Patel, S., & Singh, T. (2019). Blockchain Technology as a Solution for Secure Financial Transactions.

[21] Zhang, Y., & Li, M. (2022). Artificial Intelligence in Cybersecurity: Applications in Financial Services.

[22] Brown, C., & Davis, L. (2020). Cyber Risk Management in Financial Institutions.

[23] Wilson, D., & Martinez, F. (2018). The Role of Encryption in Protecting Online Banking Data.

[24] Ahmed, S., & Jones, P. (2021). Insider Threats in Financial Institutions: Prevention and Detection.

[25] Roberts, K., & Evans, J. (2019). Cybersecurity Compliance in the Banking Sector: Challenges and Solutions.

[26] Nguyen, T., & Pham, H. (2020). Phishing Attacks on Online Banking: Detection and Prevention Strategies.

[27] Green, R., & Taylor, S. (2022). The Impact of Cyber Attacks on Financial Market Stability.

[28] Kim, J., & Park, S. (2019). User Authentication Methods in Online Banking: A Comparative Study.

[29] Thompson, A., & White, G. (2021). Cybersecurity Investment in Banks: Cost-Benefit Analysis.

[30] Hernandez, L., & Gonzalez, R. (2020). Mobile Banking Security: Threats and Countermeasures.

[31] Singh, V., & Sharma, N. (2018). The Evolution of Malware Targeting Financial Institutions.

[32] Walker, E., & Harris, M. (2022). Cybersecurity Awareness Training for Bank Employees: Effectiveness and Best Practices.

[33] Author(s) not specified (2023). A Review of Cyber Security Issues in Online Banking and Online Transactions.

[34] Oyewole, A., Okoye, C. C., & Esther, C. (2022). Cybersecurity Risks in Online Banking: A Detailed Review and Preventive Strategies.

[35] Author(s) not specified (2022). A Research Study on Cyber Security Issues Affecting Online Banking.

[36] Author(s) not specified (2023). Do Cybersecurity Threats and Risks Have an Impact on the Adoption of Digital Banking

[37] Haruna, W., Aremu, T. A., & Modupe, Y. A. (2022). Defending Against Cybersecurity Threats to the Payments and Banking System.

[38] Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2023). Cybersecurity Threats in FinTech: A Systematic Review.

[39] Kshetri, N., Rahman, M. M., Sayeed, S. A., & Sultana, I. (2023). CryptoRAN: A Review on Crypto-jacking and Ransomware Attacks concerning the Banking Industry—Threats, Challenges, & Problems.

[40] Alzoubi, H. M., Ghazal, T. M., Hasan, M. K., Alketbi, A., Kamran, R., Al-Dmour, N. A., & Islam, M. S. (2022). Cyber Security Threats on Digital Banking.

[41] Author(s) not specified (2023). A Study on

Cyber Security Issues Affecting Online Banking and Transactions.

[42] Orun, A., Orun, E., & Kurugollu, F. (2023). Recognition of Cyber-Intrusion Patterns in User Cognitive Behavioural Characteristics for Remote Identification.

[43] Shah, B., & Borgave, S. (2023). A Review of Cyber Security Issues in Online Banking and Online Transactions.

[44] Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2023). Cybersecurity Threats in FinTech: A Systematic Review.

[45] Falade, P. V., & Ogundele, G. B. (2023). Vulnerability Analysis of Digital Banks' Mobile Applications.