International Journal of Science Academic Research
Vol. 06, Issue 05, pp.9997-10000, May, 2025
Available online at http://www.scienceijsar.com

ISSN: 2582-6425

Research Article

SECURITY CHALLENGES IN DIGITAL BANKING: A SYSTEMATIC LITERATURE REVIEW

[1, *]Mesud Mohammed and [2]Dr. Gurudutta P. Japee

[1]School of Commerce, Gujarat University, India
[2]Department of Advanced Business Studies, School of Commerce, Gujarat University, India

Received 24th March 2025; **Accepted** 27th April 2025; **Published online** 30th May 2025

Abstract

The rise of digital banking has radically changed how banking services are accessed and delivered, with increased reach, efficacy, and client convenience. But this digital transformation has also brought with it a set of sophisticated security issues that present significant risks for consumers and for financial organizations as well. This systematic review provides an insight into the ever transforming threat scenario with digital banking along with the key threats, which include Phishing, Identity Theft (ID Theft), Malware and SIM swap fraud. A leitmotif of the literature is the greater sophistication of the cyber-threat and the increased sense of insecurity among users, with the asphyxiating effect these have on trust as well as on the take-up of digital technologies. According to the review, institutions are struggling to secure increasingly connected systems, in particular the interbank payment infrastructures, which are being targeted on an almost daily basis by cyber adversaries. In turn, banks have implemented technological barriers, such as multi-factor authorization, real-time fraud detection, and cyber incident response labs. However, these measures work provided they are updated continuously in response to new threats. Concluding remarks This overview has emphasized the importance of a number of 'lines of defense' consisting of technological change, user learning, regulatory compliance and a proactive management of e-security risk. Future research can also examine the potential impact of advanced technologies such as AI, blockchain and behavioral biometrics in enhancing Cybersecurity systems to make digital banking ecosystems more sustainable and resilient.

Keywords: Digital banking, Cybersecurity, Payment systems security, Financialfraud, Risk management.

INTRODUCTION

The Information technology revolution has massively changed the banking industry, moving it from traditional banks into active online and mobile platforms (Asmar & Tuqan, 2024). It is a transformation that redefines how banking business is being made, using technologies that improve organizational performance and adjusting to the current context and demands of the digital age (Porfírio *et al.,* 2023; Shanti *et al.,* 2023). The rise of digital banking is pushed by its comparative advantage that customers can make payments, check balances and purchase financial products from wherever they are (Cele & Kwenda, 2024). The term digital banking, online banking, internet banking or virtual banking refers to the digital or Internet-based provision of banking services to the customers via digital channels, including websites, mobile apps, and other interfaces (Asmar & Tuqan, 2024). Large international banks are focusing on digital transformation to compete for customers and lower costs (Liu, 2021). Digital banking does not come without its challenges least of which remains security (Gr, 1992). While digital banking represents a major change in the interaction between customers and banks as well as in how quickly services are provided, the issue of security in online banking is still complex and many customers are hesitant to use online banking services for security reasons, (Mahmadi *et al.,* 2016). In the digital arena…, banks and their clients are vulnerable to a myriad of security risks, including classical fraud and advanced forms of cybercrime (Khando, *et al.,* 2022). With the growing number of services available in the digital banks, the vulnerability to cybersecurity threats, such as phishing, malware, and identity theft also increases drastically, exposing financial institutions and their clients to a potential risk (Bueno *et al.,* 2024). There are perceived advantages of online banking which resolve around the benefits associated with provision of services whilst still at home or at work, together with the lower associated costs of providing these services (Mehana & Pireva, 2020). Secure digital banks are integral to preserving consumer confidence, safeguarding financial information, and maintaining the integrity of the financial system. With the growing digitalization of banking, banks are struggling to address the ever-present need to secure transactions and provide consumers with a trusted experience. Digital banking growth is also counteracted by the threat of cybercrime, such as malware, phishing and identity theft, which could result in substantial financial losses as well damage consumers' confident (Chu & Zhan, 2024).

***Corresponding Author: Mesud Mohammed,**
School of Commerce, Gujarat University, India.

LITERATURE REVIEW

There are a number of security threats that digital banking applications need to deal with, such as the threat related to data breach and unauthorized access, which could cause sensitive customer's information leakage that may lead to disruption of banking operations (Windasari *et al.,* 2022). Strong verification approaches like multi-factor authentication are crucial to mitigating these threats by verifying the identity of a user before giving access to an account (Adeyinka *et al.,* 2020). The digital banking arena is also challenged by several types of fraudulent activities, such as phishing attacks unleashed by the criminals in the form of messages or emails with fraudulent websites designed to deceive the users so that they provide critical information such as credit card numbers and PINs (Ama *et al.,* 2024). Banking sector has given a priority on enhancing the security features of cyber protection,

and there are plenty of systems designed to observe / content/credit etc. for cyber fraud (Btoush *et al.,* 2023. The spread of digital banking has also opened new channels for fraud, such as SIM swapping fraud, skimming/ website cloning, smishing/ vishing (Ama et al., 2024).Banks and other financial companies are spending more on new technologies as well as on security to shield themselves against cyber-attacks and the resulting financial losses and data breaches. With increasing complexities and interdependencies in digital banking systems, such systems have become interesting targets for cyber criminals who are constantly evolving techniques to find new vulnerabilities and bypass security measures. The Bank needs a new system of information security, which would foreclose attacks and would have control administrative management, monitoring and build-in system of immediate response to the incidents (Kondratyeva et al. 2021). Risks to payment and banking services from cyber-attacks has become a global issue, thereby requiring financial institutions to embrace risk in their business practices (Haruna *et al.,* 2022). On a global scale, digital payments have brought billions of people into the formal financial system yet schemes of illicit finance have quickly adapted to leverage that fast-moving system (Kurshan *et al.,* 2021). The financial industry is highly dependent on technology for providing customer service, and running day-to-day operations makes it more susceptible to various cyber threats (Abbas & Arif, 2023).

Interbank payments systems are a dangerous target for cybercriminals due to the increasing links between payment systems and between the payment system and information technology – the digitalization of financial services (Fazio & Zuffranieri, 2018). With the growing attacks amongst bank establishments and other economic misappropriation of their systems, there is an urgent need for protection of bank payment systems (Oyewole *et al.,* 2024). Attacks on payment systems and payment service providers is increasingly common worldwide, with individuals, entities, and physical attacks (Acharya, 2018). The issue of securities is becoming increasingly important for banks and for their customers (Kondratyeva *et al.,* 2021). With a potential for concerted attacks on national information and telecommunication infrastructures, financial systems are believed to be 3 times more prone to cyber-attacks than other sectors and the digital transition has profoundly transformed the banking sector with the resulting operational risks and greater systems interdependencies, illustrating the importance of resilience in payment systems (Khiaonarong *et al.,* 2021). The growing power shutoffs, cyber events and natural disasters have potential to result in major disruption. The advent of digital banking also poses significant security challenges and requires an overall effective risk control framework (Seetharaman & Raj, 2009).

The trust is also a crucial issue, since if the security conditions are not satisfied in these payments systems then customers will refrain from using online activities (Al-Qawasmi, 2020). Monetary transactions are greatly simplified and money becomes much less vulnerable in the hands of its owner such e-payments are the toast of the day than cash (currency) system (Masihuddin *et al.,* 2017). The security of electronic payment is often more challenging than the current security issue on the web (Hassan *et al.,* 2020). The growth on electronic payments presents its inherent risks and the development of solid risk mitigation factors is crucial (Putrevu & Mertzanis, 2023). Significant payment system disruptions have highlighted a case for greater resilience of payment systems (Khiaonarong et al., 2021). The use of technology in banking services, is a function of performance of the bank more optimal, can perform various activities quickly and accurately with an impact on productivity (Fatonah *et al.,* 2018).

METHODOLOGY

Systematic literature review was used to explore digital banking security threats. The narrative synthesis provided a solid and rigorous process for accessing, appraising and synthesizing cumulative knowledge in this area. Articles are selected for inclusion here, based on the depth of the articles, their covering the current issues and the contribution to the field.

Search Strategy

A systematic literature search was performed to find related research publications from Scoups, Web of Science and IEEE Xplore. The keywords used for the search include "Digital banking," "Cybersecurity," "Payment systems security," "Financial fraud," and "Risk management". The search strategy was planned to be wide ranging and include articles on technical, managerial and policy aspects of security in digital banking.

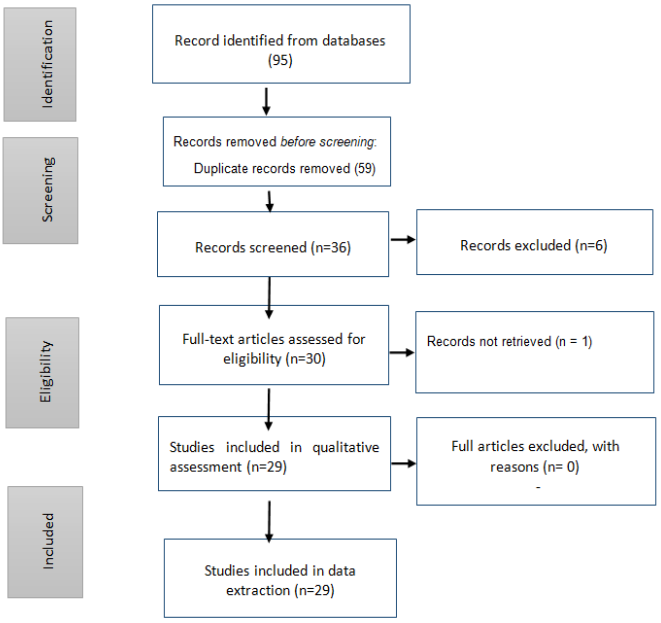
Inclusion Criteria

The eligibility criteria were an article published in a peer-reviewed journal, article related to security challenges in the digital banking, and article which presents empirical evidence, theoretical model or a case study in context of security in digital banking.

Exclusion Criteria

The exclusion criteria were articles which were not written in English; those that covered general cyber security rather than the security challenges of the digital banking; and articles that made limited scholarly.

PRISMA flow Diagram



RESULTS AND DISCUSSION

- ✓ The literature review on digital banking security challenges demonstrates a landscape of complex and dynamic threats driven by explosive technological innovation and adoption of digital financial channels. Digital banking has democratized the ability to access and use financial services bank in the day, but it's also opened the door to substantial security risks for both financial institutions and the consumers they serve.
- ✓ A common finding in the reviewed documents is that of cyber threats i.e. phishing, identity theft, malware and SIM swap. These risks are increased further by the increasing sophistication of cyber-crime and the explosion of digital services. Growth in phishing and social engineering—as well as other techniques—has led to a substantial rise in financial fraud, which has eroded user trust and held back the transition to digital banking.
- ✓ Customer insecurity on a customer view remains a significant barrier to the expansion of cyber banking. Most of the clients are put off by security concerns of their banking and personal information.
- ✓ This vulnerability is exacerbated by the lack of sufficient awareness about digital security among the users, making them an easy target for cyber fraud.
- ✓ At the institutional level, banks are struggling to keep their interconnected digital systems specifically their interbank payment systems — safe, as they have increasingly become the preferred target of cyberattacks since they are key to moving money around the world.
- ✓ The nature and magnitude of these systems requires a strong monitoring and incident response mechanism in place in real time.
- ✓ Despite these barriers, literature also directs our attention towards the steps that financial institutions take towards combating cyber threats, which consist of such activities as investment in multi-factor authentication systems, fraud management systems or dedicated cybersecurity operation centers. These steps are great, but they have to be updated all the time to keep up with rapidly developing threats.
- ✓ Although digital banking brings transformative advantages, but it can only succeed by addressing its multi-layered security challenges. A proactive, multilayered, cooperative strategy across technology innovation, user education and regulation is required not only to boost resistance against the cyber threats, but also to bring long-term trust in digital financial ecosystem.

Conclusion

- ✓ Despite the fact that digital banking technology has been widely adopted, concern about user privacy and transaction security has played a role in the fact that we do not fully use the tools available to us. Although the banks have taken substantial steps in investing in protective technologies from multi-factor authentication, to fraud detection systems, to cyber incident response centers these investments need to be continually refreshed in response to the ever-increasing sophistication of the threats.
- ✓ The review recaps the need for a comprehensive strategy towards digital banking security, which comprises advanced technical measures, strong regulatory requirements, and holistic cybersecurity awareness among users. Cybersecurity should be added to the strategic plans of financial institutions, creating security-first cultures which combine innovation with risk management.
- ✓ To summarise, securing digital banking is not just a technical necessity, but also a precondition for maintaining the trust of customers and the continued good health of digital financial ecosystems. Further, we need to investigate new and emerging technologies like artificial intelligence, behavioral biometrics or blockchain as potential enablers to develop more secure and adaptive digital banking infrastructures.

Recommendation and Further Research Direction

- ✓ Reliable security posture must be maintained through strict imposition of strict processes, tighter compliance to applicable regulations and continuous conformance with best practices across the industry all of which synchronously protect the perpetual confidentiality, integrity, accessibility of financial information.
- ✓ It also necessary to focuses on the importance of using the integrated approach while tackling security issues in the digital banking industry using a multi-dimension approach which involves the use of technology and regulations and proactive risk managements.
- ✓ There is a need for more research on Compliance with regulatory environment,government and the industry in digital banking security and Investigate on the role of emerging technologies, like AI, blockchain and behavioral biometrics, adoption in digital banking security frameworks to improve threat detection, user authentications and fraud prevention.

REFERENCES

Abbas, T., & Arif, K. (2023). End-Users' Perception Of Cybercrimes Towards E-Banking Adoption And Retention. *Journal of Independent Studies and Research - Computing,* 21(1). https://doi.org/10.31645/jisrc.23.21.1.10

Acharya, S. (2018). Implication of International Law in Electronic Commerce and Cyber Crime: An Experience of Nepal. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3273915

Adeyinka, A., Taiwo, A., & Akintola, O. (2020). Effect of Computerization on Banks' Performance in Quoted Nigerian Banking Sector. *Research Journal of Finance and Accounting.* https://doi.org/10.7176/rjfa/11-16-17

Al-Qawasmi, K. (2020). Proposed E-payment Process Model to Enhance Quality of Service through Maintaining the Trust of Availability. *International Journal of Emerging Trends in Engineering Research,* 8(6), 2296. https://doi.org/10.30534/ijeter/2020/16862020

Ama, G. A. N., Onwubiko, C. O., & Nwankwo, H. A. (2024). Cybersecurity Challenge in Nigeria Deposit Money Banks. *Journal of Information Security,* 15(4), 494. https://doi.org/10.4236/jis.2024.154028

Asmar, M., & Tuqan, A. (2024a). Integrating Machine Learning for Sustaining Cybersecurity in Digital Banks. https://doi.org/10.2139/ssrn.4686248

Btoush, E., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning [Review of A systematic review of literature on credit card cyber fraud detection using machine and deep learning]. *Peer J Computer Science,* 9. PeerJ, Inc. https://doi.org/10.7717/peerj-cs.1278

Bueno, L. A., Sigahi, T. F. A. C., Rampasso, I. S., Filho, W. L., & Anholon, R. (2024). Impacts of digitization on operational efficiency in the banking sector: Thematic analysis and research agenda proposal. *International Journal of Information Management Data Insights*, 4(1), 100230. https://doi.org/10.1016/j.jjimei.2024.100230

Cele, N. N., & Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime.* https://doi.org/10.1108/jfc-10-2023-0263

Chu, H., & Zhan, X. (2024). The Impact of Digital Banking Services on Customer Satisfaction. *Frontiers in Business Economics and Management,* 15(3), 356. https://doi.org/10.54097/5qaf7d23

Fatonah, S., Yulandari, A., & Wibowo, F. W. (2018). A Review of E-Payment System in E-Commerce [Review of A Review of E-Payment System in E-Commerce]. *Journal of Physics Conference Series,* 1140, 12033. IOP Publishing. https://doi.org/10.1088/1742-6596/1140/1/012033

Fazio, A., & Zuffranieri, F. (2018). Interbank Payment System Architecture from a Cyber Security Perspective. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3123094

Gr, G. (1992). One moment, please. PubMed, 82(1), 37. https://pubmed.ncbi.nlm.nih.gov/1499783

Haruna, W., Aremu, T. A., & Modupe, Y. A. (2022). Defending against cybersecurity threats to the payments and banking system. arXiv (Cornell University). https://doi.org/ 10.48550/arxiv.2212.12307

Hassan, M. A., Shukur, Z., Hasan, M. K., & Al-Khaleefa, A. S. (2020). A Review on Electronic Payments Security [Review of A Review on Electronic Payments Security]. Symmetry, 12(8), 1344. *Multidisciplinary Digital Publishing Institute.* https://doi.org/10.3390/sym12081344

Khando, K., Islam, M. S., & Gao, S. (2022). The Emerging Technologies of Digital Payments and Associated Challenges: A Systematic Literature Review. Future Internet, 15(1), 21. https://doi.org/10.3390/fi15010021

Khiaonarong, T., Leinonen, H., & Rizaldy, R. (2021). Operational Resilience in Digital Payments: Experiences and Issues. IMF Working Paper, 2021(288), 1. https://doi.org/10.5089/9781616355913.001

Kondratyeva, M. N., Svirina, D. D., & Tsvetkov, A. I. (2021). The role of information technologies in ensuring banking security. IOP Conference Series Materials Science and Engineering, 1047(1), 12069. https://doi.org/10.1088/1757-899x/1047/1/012069

Kurshan, E., Shen, H., & Yu, H. (2021). Financial Crime & Fraud Detection Using Graph Computing: Application Considerations & Outlook. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2103.01854

Liu, E. (2021). Stay Competitive in the Digital Age: The Future of Banks. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3852774

Mahmadi, F., Zaaba, Z. F., & Osman, A. M. (2016). Computer Security Issues in Online Banking: An Assessment from the Context of Usable Security. *IOP Conference Series Materials Science and Engineering*, 160, 12107. https://doi.org/10.1088/1757-899x/160/1/012107

Masihuddin, M., Khan, B. U. I., Mattoo, M. M. U. I., & Olanrewaju, R. F. (2017). A Survey on E-Payment Systems: Elements, Adoption, Architecture, Challenges and Security Concepts. *Indian Journal of Science and Technology,* 10(20), 1. https://doi.org/10.17485/ijst/2017/v10i20/113930

Mehana, A., & Pireva, K. (2020). Fraud Detection using Data-Driven approach. arXiv (Cornell University). https://doi.org/10.48550/arxiv.2009.06365

Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio [Review of Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio]. *World Journal of Advanced Research and Reviews*, 21(3), 625. GSC Online Press. https://doi.org/10.30574/wjarr.2024.21.3.0707

Porfírio, J., Felício, J. A., & Carrilho, T. (2023). Factors affecting digital transformation in banking. *Journal of Business Research,* 171, 114393. https://doi.org/10.1016/j.jbusres.2023.114393

Putrevu, J., & Mertzanis, C. (2023). The adoption of digital payments in emerging economies: challenges and policy responses. *Digital Policy Regulation and Governance*, 26(5), 476. https://doi.org/10.1108/dprg-06-2023-0077

Seetharaman, A., & Raj, J. R. (2009). Evolution, Development and Growth of Electronic Money. *International Journal of E-Adoption,* 1(1), 76. https://doi.org/10.4018/jea.2009010106

Shanti, R., Siregar, H., Zulbainarni, N., & Tony, T. (2023). Role of Digital Transformation on Digital Business Model Banks. Sustainability, 15(23), 16293. https://doi.org/10.3390/su152316293

Windasari, N. A., Kusumawati, N., Larasati, N., & Amelia, R. P. (2022). Digital-only banking experience: Insights from gen Y and gen Z. Journal of Innovation & Knowledge, 7(2), 100170. https://doi.org/10.1016/j.jik.2022.100170

****