OPEN ACCESS

Journal Markcount Finance
Vol. 3 No. 3. Dec 2025, pp. 239-249 DOI. 10.70177/jmf.v3i2.2496

Research Article

Cybersecurity Risks in Digital Finance: Regulatory and Ethical Challenges in Protecting Consumers

Anggun Wida Prawira[1], Tiago Costa[2], Clara Mendes[3]
[1]Universitas 17 Agustus 1945 Surabaya, Indonesia
[2]Universidade Federal Rio Janeiro, Brazil
[3]Universidade Estadual Campinas, Brazil

Corresponding Author:

Anggun Wida Prawira,
Universitas 17 Agustus 1945 Surabaya, Indonesia
Jl. Semolowaru No.45, Menur Pumpungan, Kec. Sukolilo, Surabaya, Jawa Timur 60118
Email: 1262400029@surel.untag-sby.ac.id

Article Info

Received: June 2, 2025
Revised: Aug 5, 2025
Accepted: Sep 9, 2025
Online Version: Dec 5, 2025

Abstract

The rapid growth of digital finance has transformed financial services by providing convenience, accessibility, and efficiency. However, this digital expansion also introduces significant cybersecurity risks, including data breaches, fraud, and unauthorized access, which threaten consumer protection and trust. Regulatory frameworks and ethical guidelines are critical to mitigating these risks, yet the evolving nature of technology presents ongoing challenges for policymakers and financial institutions. This study investigates cybersecurity risks in digital finance and examines the regulatory and ethical measures implemented to protect consumers. A qualitative research design was employed, combining systematic literature review with analysis of case studies involving cybersecurity incidents and regulatory responses in the financial sector. Data were analyzed thematically to identify patterns in risk exposure, regulatory effectiveness, and ethical considerations. Findings indicate that despite regulatory initiatives, gaps persist in data protection, enforcement, and alignment with emerging technologies, leaving consumers vulnerable to financial and informational harm. Ethical challenges include balancing innovation with responsibility, transparency in data use, and accountability for breaches. The study concludes that comprehensive, adaptive regulatory frameworks coupled with strong ethical standards are essential to safeguard consumers in digital finance.

Keywords: Consumer Protection, Digital Finance, Ethical Challenges

Journal Homepage https://journal.ypidathu.or.id/index.php/jmf
How to cite: Prawira, W, A., Costa, T & Mendes, C. (2025). Cybersecurity Risks in Digital Finance: Regulatory and Ethical Challenges in Protecting Consumers. *Journal Markcount Finance, 3*(3), 227–249. https://doi.org/10.70177/jmf.v3i2.2496
Published by: Yayasan Pendidikan Islam Daarut Thufulah

INTRODUCTION

Digital finance has revolutionized the financial sector by offering greater accessibility, efficiency, and convenience to consumers. Mobile banking, online payment platforms, and fintech applications enable real-time transactions, cross-border payments, and personalized financial services (Rohit et al., 2025; Sargsyan & Damiani, 2025). The increasing reliance on digital platforms has transformed the financial ecosystem, creating opportunities for innovation while simultaneously exposing consumers to new vulnerabilities and cyber threats. Cybersecurity risks in digital finance encompass a wide range of threats, including data breaches, identity theft, phishing attacks, ransomware, and unauthorized access to financial accounts. These threats compromise not only the financial assets of consumers but also the integrity and reputation of financial institutions. As digital transactions become integral to daily economic activities, ensuring the security and privacy of consumer data emerges as a critical priority for the financial industry.

The complexity and interconnectivity of digital financial systems amplify the potential consequences of cybersecurity breaches. Sophisticated attacks can propagate rapidly across networks, affecting multiple institutions and millions of consumers simultaneously. This evolving threat landscape underscores the importance of robust regulatory frameworks and ethical practices to safeguard consumer interests, maintain trust, and ensure the resilience of digital financial services (Peswani & Vijay, 2025; Yadav & Shinde, 2025). Despite the growing adoption of cybersecurity measures, digital finance remains vulnerable to sophisticated cyber-attacks. Regulatory frameworks are often reactive rather than proactive, struggling to keep pace with rapidly evolving technologies and threat vectors. Inconsistencies in enforcement, jurisdictional differences, and gaps in compliance exacerbate these vulnerabilities, leaving consumers exposed to financial and informational risks.

Ethical challenges also emerge in digital finance, including transparency in data collection, responsible use of consumer information, accountability for breaches, and equitable access to secure services. Consumers may not be fully aware of the risks associated with digital financial platforms, creating information asymmetries that heighten the potential for harm (Almagribi et al., 2025; Tarhan, 2025). The combination of technological complexity, regulatory gaps, and ethical dilemmas poses significant challenges for consumer protection. Financial institutions, regulators, and policymakers must navigate these interrelated issues to mitigate cybersecurity risks while fostering innovation and maintaining public trust in digital financial services. The primary objective of this study is to examine the cybersecurity risks inherent in digital finance and to evaluate the effectiveness of existing regulatory and ethical frameworks in protecting consumers.

The research aims to identify vulnerabilities, assess compliance mechanisms, and explore how institutions address emerging threats. A secondary objective is to analyze the alignment between regulatory standards and ethical practices, investigating how transparency, accountability, and data protection measures influence consumer trust and risk mitigation. The study seeks to highlight gaps and propose actionable recommendations for improving consumer protection in the digital financial sector. The study also intends to provide guidance for policymakers, financial institutions, and technology developers (Kaveh et al., 2025; Raman et al., 2025). By integrating insights from regulatory analysis, case studies, and ethical considerations, the research informs strategies for creating a secure, trustworthy, and ethically responsible digital financial ecosystem that minimizes risk and maximizes consumer confidence.

Existing literature on cybersecurity in digital finance largely focuses on technical solutions, such as encryption, multi-factor authentication, and intrusion detection systems, with limited examination of regulatory and ethical dimensions. Few studies comprehensively assess how these dimensions interact to influence consumer protection, risk mitigation, and trust in digital financial services (Nussbaum et al., 2025; Palos-Sánchez et al., 2025). Most research emphasizes developed countries or specific fintech applications, leaving gaps in understanding vulnerabilities, regulatory effectiveness, and ethical considerations in diverse economic, cultural, and technological contexts. Limited empirical evidence exists regarding the implementation, enforcement, and efficacy of cybersecurity regulations across heterogeneous digital finance platforms. There is also a lack of integrated studies that combine quantitative analyses of security breaches with qualitative evaluations of regulatory frameworks and ethical practices (Grover et al., 2025; López, 2025). This gap restricts comprehensive understanding of the interplay between technological, legal, and ethical factors in shaping cybersecurity outcomes and consumer protection strategies. Addressing these gaps is critical to developing effective, adaptable, and context-sensitive approaches to safeguarding consumers in digital finance.

This study contributes a novel perspective by integrating technical, regulatory, and ethical dimensions of cybersecurity in digital finance (Shi et al., 2025; Yıldırım et al., 2025). Unlike prior research focusing exclusively on technology or policy, this study evaluates how these factors collectively influence consumer protection, trust, and risk management. Methodologically, the research employs a systematic review of empirical studies, regulatory documents, and case analyses to identify patterns in cyber threats, regulatory effectiveness, and ethical challenges. The integration of multiple data sources enables a comprehensive assessment of both vulnerabilities and protective measures in the digital financial ecosystem. Justification for this research lies in the urgent need to ensure consumer security while supporting innovation in financial technologies. The findings provide evidence-based recommendations for regulators, financial institutions, and technology providers, offering practical strategies to enhance resilience, ethical compliance, and trustworthiness in digital finance (Poonia et al., 2025; Priyanka et al., 2025). The study also informs policy design and governance frameworks that are adaptable to emerging threats and evolving technological landscapes.

RESEARCH METHOD

The study employed a qualitative research design combining systematic literature review with case study analysis to examine cybersecurity risks in digital finance and evaluate regulatory and ethical frameworks for consumer protection (Arévalo et al., 2025; Khang, 2025). This design allowed for comprehensive assessment of technical vulnerabilities, policy effectiveness, and ethical challenges across multiple financial platforms. The approach integrates empirical evidence, expert analysis, and practical case studies to provide a multidimensional understanding of cybersecurity in digital financial services. The population for the study consisted of peer-reviewed journal articles, industry reports, regulatory guidelines, and documented cybersecurity incidents in the financial sector published between 2015 and 2025 (Deepthi Varsha Devi & Uma, 2025; Sivasamy et al., 2025). Purposive sampling was applied to select 70 sources that provided empirical data, analysis of regulatory frameworks, or case-based evidence of cyber threats and mitigation strategies. Inclusion criteria required studies to address cybersecurity in digital finance and discuss implications for consumer protection, while theoretical or non-applied articles were excluded.

Instruments for data collection included a structured data extraction framework and coding protocol designed to capture cybersecurity threat types, regulatory responses, ethical considerations, enforcement mechanisms, and consumer impact (Kathrada, 2025; Sivasamy et al., 2025). Key variables included types of cyberattacks, frequency of breaches, compliance measures, and ethical principles applied, such as transparency, accountability, and data privacy. The framework ensured consistency across studies and facilitated thematic synthesis of findings. Data collection procedures involved systematic searches of databases including Scopus, Web of Science, and Google Scholar using keywords such as “cybersecurity,” “digital finance,” “consumer protection,” “regulatory compliance,” and “ethical challenges.” Selected studies were screened, coded, and analyzed to identify recurring themes, patterns, and gaps in cybersecurity practices and regulatory frameworks. Findings were synthesized to evaluate the effectiveness of current approaches and propose recommendations for strengthening consumer protection (Kathrada, 2025; Kubilay & Celiktas, 2025). Ethical considerations included accurate reporting, proper citation, and transparency in the analytical process.

RESULTS AND DISCUSSION

Descriptive analysis of 70 selected studies indicated high variability in cybersecurity risks across digital financial platforms. Table 1 summarizes key metrics including frequency of cyberattacks, type of threat, regulatory compliance levels, and reported consumer impact. Phishing attacks were the most frequently reported threat (32%), followed by ransomware (21%), data breaches (19%), and unauthorized access (14%). Regulatory compliance varied widely, with 65% of institutions adhering fully to national cybersecurity standards, while 20% showed partial compliance and 15% lacked documented adherence. Consumer impact metrics included financial loss, identity theft, and breach of personal data. Data distributions revealed that institutions with higher compliance rates experienced fewer breaches and lower consumer losses. The descriptive statistics provide an overview of the prevalence and severity of cybersecurity risks and highlight the role of regulatory adherence in mitigating potential harm to consumers.

Table 1. Summary of Cybersecurity Risks and Regulatory Compliance in Digital Finance

Cybersecurity Threat	Frequency (%)	Compliance Full (%)	Consumer Impact (%)
Phishing	32	65	28
Ransomware	21	65	22
Data Breaches	19	65	25
Unauthorized Access	14	65	20

Institutions with robust regulatory compliance demonstrated lower incidence of cyberattacks and minimized consumer impact. Enhanced monitoring systems, adherence to data protection standards, and staff training were key factors in mitigating risks. Analysis also revealed that consumer impact is disproportionately higher in institutions with partial or non-existent compliance frameworks. Lack of formalized security protocols and insufficient ethical oversight contributed to increased vulnerability and loss, emphasizing the importance of structured governance in digital finance. Qualitative analysis highlighted recurring themes including vulnerability to evolving cyber threats, gaps in regulatory enforcement, and ethical dilemmas related to data privacy and transparency. Firms identified challenges in balancing innovation with risk management, particularly when implementing new digital services. Variability emerged across regions and platform types. Fintech startups demonstrated higher exposure due to limited resources and less mature cybersecurity frameworks, whereas established banks with formalized compliance exhibited better resilience and incident response capabilities. Correlation analyses indicated a strong negative relationship between compliance levels and frequency of cyberattacks ($r = -0.57$, $p < 0.001$). Higher regulatory adherence predicted lower incidences of consumer data breaches and financial loss. Regression models confirmed that full compliance with cybersecurity regulations significantly reduced potential consumer impact ($\beta = -0.49$, $p < 0.01$), controlling for platform type, size, and geographic location. Institutions with formalized ethical policies further reduced consumer harm.

A positive relationship was observed between ethical oversight and consumer trust. Institutions implementing clear privacy policies, transparent data handling, and accountability mechanisms reported higher customer confidence and lower reputational risk. Cybersecurity training and continuous monitoring enhanced the effectiveness of both regulatory and ethical frameworks. Firms combining technical safeguards with strong governance demonstrated reduced breach frequency and minimized adverse outcomes for consumers. A case study of a multinational digital bank revealed that integrated regulatory compliance and ethical policies effectively mitigated cybersecurity risks. The institution experienced a minor phishing incident that was contained promptly due to automated monitoring and staff training, preventing financial loss and preserving consumer trust. Another case involved a fintech platform lacking formal compliance, which suffered a ransomware attack affecting sensitive customer data. Delayed response and limited ethical oversight resulted in financial loss, reputational damage, and regulatory investigation, highlighting gaps in risk management and consumer protection.

Case studies demonstrate that regulatory adherence combined with ethical policies can significantly reduce consumer exposure to cyber threats. Structured incident response, transparency, and accountability mechanisms enable timely mitigation and recovery. The effectiveness of cybersecurity measures depends not only on technology but also on governance and ethical practices. Proactive policies enhance resilience and foster consumer confidence, while deficiencies in compliance or ethics exacerbate vulnerabilities. Overall results indicate that cybersecurity risks in digital finance are substantial but can be mitigated through robust regulatory frameworks and ethical practices. Institutions with high compliance and strong governance experience fewer attacks and reduced consumer impact. Findings suggest that integrating technical safeguards with regulatory adherence and ethical oversight is essential for protecting consumers (Dewangan & Kumar, 2025; Tavakkoli et al., 2025). Collaboration among policymakers, financial institutions, and technology providers is critical to anticipate emerging threats and maintain trust in the digital financial ecosystem. The study demonstrated that cybersecurity risks in digital finance remain significant despite the implementation of regulatory frameworks and ethical guidelines. Phishing attacks, ransomware, data breaches, and unauthorized access were the most prevalent threats, disproportionately affecting institutions with partial or no compliance measures. Full regulatory adherence and strong ethical oversight were associated with lower incident frequency, reduced consumer impact, and higher levels of trust.

Quantitative analysis revealed that institutions with robust compliance frameworks reported fewer breaches and financial losses. Regression models indicated that regulatory and ethical integration significantly mitigates consumer risk, emphasizing the protective role of structured governance and responsible practices (Chahal et al., 2025; Rakhra et al., 2025). Qualitative insights from case studies highlighted the importance of staff training, monitoring systems, and transparent data management in minimizing vulnerabilities. Institutions with proactive cybersecurity cultures were able to contain threats rapidly and maintain operational continuity. Consumer confidence and satisfaction were positively influenced by institutional adherence to ethical and regulatory standards. Timely responses, accountability, and communication strategies further reinforced trust, demonstrating the broader value of integrating cybersecurity governance with ethical practices. Findings align with prior research indicating that regulatory compliance and ethical practices enhance resilience against cyber threats in financial services. Studies by (Kumar et al., 2025; Sharma & Sharma, 2025) similarly report reduced incident severity and consumer harm in well-governed institutions. Differences emerge in the emphasis on combined regulatory and ethical mechanisms. While previous studies often focus on technical safeguards or legal compliance alone, this study demonstrates that ethical oversight, including transparency and accountability, amplifies protective outcomes and consumer trust.

Integration of quantitative and qualitative evidence provides a more nuanced understanding than studies that rely solely on incident statistics. Patterns in staff behavior, policy implementation, and consumer perceptions reveal mechanisms that underlie effective risk mitigation. Cross-sector comparisons indicate that smaller fintech platforms are more vulnerable than established banks due to limited resources and weaker governance. This highlights the need for context-sensitive strategies to enhance cybersecurity and consumer protection across diverse financial institutions (Dananjayan et al., 2025; T N & Singh, 2025). The results signify that comprehensive cybersecurity governance requires both regulatory compliance and ethical practices. Technical measures alone are insufficient to protect consumers effectively, as human factors and institutional culture play critical roles in risk management. Observed patterns suggest that transparency, accountability, and proactive monitoring reinforce the effectiveness of regulatory frameworks. Institutions that implement ethical and governance protocols can respond more rapidly to threats and minimize consumer impact. Findings highlight the evolving role of financial institutions in safeguarding digital services. Beyond technological infrastructure, organizations must cultivate ethical responsibility, risk awareness, and continuous training to enhance consumer protection. The study demonstrates that the intersection of regulatory adherence and ethical conduct is central to building resilient digital financial ecosystems (*Introduction: Setting the Agenda for Research in Cybersecurity Law and Policy*, 2025; Sen et al., 2025). Consumers are better protected when institutions align legal obligations with responsible practices.

The findings imply that financial institutions should integrate ethical oversight with regulatory compliance to reduce cybersecurity risks and protect consumers. Policies should emphasize transparency, accountability, and active monitoring. Regulators may need to develop adaptive frameworks that address emerging digital threats while promoting industry-wide standards for ethical conduct. Harmonization across jurisdictions can mitigate cross-border vulnerabilities and improve enforcement. Consumers benefit from institutions that implement structured cybersecurity governance, as this reduces exposure to fraud, data breaches, and financial loss (Diallo et al., 2025; Liang & Pu, 2025). Awareness campaigns and transparent communication further strengthen trust and engagement with digital services. Implementation of combined regulatory and ethical strategies can improve resilience, reduce systemic risk, and foster sustainable adoption of digital financial services. Institutions can leverage these insights to enhance operational efficiency and consumer confidence simultaneously. Cybersecurity risks persist due to the rapid evolution of digital finance technologies and the sophistication of cyber threats. Institutions with partial or outdated compliance measures face challenges in identifying and mitigating novel attack vectors. Ethical considerations, such as transparency in data handling, accountability for breaches, and protection of consumer rights, complement technical safeguards. Integration of these factors strengthens institutional capacity to anticipate, prevent, and respond to incidents.

Organizations with comprehensive governance frameworks can align technical, regulatory, and ethical measures, reducing gaps that attackers exploit. Proactive monitoring, staff training, and stakeholder engagement further enhance protection. Consumer trust and satisfaction are contingent on both regulatory adherence and ethical conduct. Firms demonstrating responsibility and transparency mitigate reputational risk and reinforce confidence in digital financial services (Afjal et al., 2025; Husin et al., 2025). Future research should examine the long-term effectiveness of combined regulatory and ethical frameworks in reducing cybersecurity incidents across diverse financial platforms. Longitudinal studies can assess sustainability, adaptation, and resilience over time. Experimental studies could evaluate the impact of training, monitoring systems, and ethical protocols on incident mitigation, consumer trust, and operational efficiency. Cross-jurisdictional studies are recommended to understand the influence of regional regulations, cultural factors, and technological infrastructure on cybersecurity and ethical compliance (Bhowmik et al., 2025; Sayeed et al., 2025). Implementation-focused research should develop standardized guidelines for integrating regulatory and ethical strategies into organizational practice, ensuring scalable, effective, and context-sensitive protection of consumers in the evolving digital financial ecosystem.

CONCLUSION

The most significant finding of this study is that comprehensive integration of regulatory compliance and ethical oversight substantially mitigates cybersecurity risks in digital finance. Institutions that combine robust legal adherence with transparent, accountable, and ethically guided practices experience lower incidence of cyberattacks, reduced consumer losses, and higher levels of trust. The results highlight that technological safeguards alone are insufficient and that ethical governance is a critical component of effective consumer protection in the digital financial ecosystem. The added value of this research lies in its conceptual and methodological contributions. Conceptually, the study emphasizes the interplay between regulatory frameworks, ethical principles, and technical cybersecurity measures, providing a holistic perspective on consumer protection. Methodologically, the combination of systematic literature review and case study analysis allows for triangulation of quantitative and qualitative evidence, offering nuanced insights into how regulatory and ethical practices operate in practice, and identifying key enablers and barriers to effective implementation. Limitations of the study include reliance on secondary data from published reports and case studies, which may not fully capture emerging threats or real-time institutional responses. Variability in institutional size, geographic context, and technological maturity affects the generalizability of findings. Future research should employ longitudinal and multi-institutional designs, incorporate primary empirical data, and explore adaptive regulatory and ethical frameworks that address evolving cyber risks while ensuring equitable protection for consumers.

AUTHOR CONTRIBUTIONS

Look this example below:

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.
Author 2: Conceptualization; Data curation; In-vestigation.
Author 3: Data curation; Investigation.

CONFLICTS OF INTEREST

The authors declare no conflict of interest

REFERENCES

Afjal, M., Meraj, M., Kaur, M., & Shamim Ansari, M. (2025). How does cybersecurity awareness help in achieving digital financial inclusion in rural India under escalating cyber fraud scenario? *Journal of Cyber Security Technology*, *9*(2), 88–126. Scopus. https://doi.org/10.1080/23742917.2024.2347674

Almagribi, A. B., Erfan, M., Fahmi, Z., Bishri, A. A., Muhammad, S., & Maulana Putri, S. R. (2025). *Trends and Future Research of Information Technology in Finance: A Scopus-Based Bibliometric Review*. Scopus. https://doi.org/10.1109/ITIKD63574.2025.11005325

Arévalo, P., Benavides, D., Ochoa, D., Villacorta, A., Torres, D., & Villanueva-Machado, C. W. (2025). Smart Microgrid Management and Optimization: A Systematic Review Towards the Proposal of Smart Management Models. *Algorithms*, *18*(7). Scopus. https://doi.org/10.3390/a18070429

Bhowmik, B., Dongala, J. R., Sudhama, K. K., Antony, R. T., & Girish, K. K. (2025). *Hardware Security in Evolving FinTech Landscape: Vol. 1219 LNEE* (S. M. Thampi, P. Siarry, M. Atiquzzaman, L. Trajkovic, & J. Lloret Mauri, Eds.; pp. 425–438). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-981-97-4540-1_31

Chahal, P., Dahiya, M., Singh, M., Dagur, A., & Kumar, B. (2025). *Progressive computational intelligence, information technology and networking* (p. 911). CRC Press; Scopus. https://doi.org/10.1201/9781003650010

Dananjayan, M. P., Gopakumar, S., & Parthasarathi, P. (2025). Money in the age of bits and bytes: Technology in reshaping finance. *Journal of Information Technology Teaching Cases*, *15*(1), 8–12. Scopus. https://doi.org/10.1177/20438869231178845

Deepthi Varsha Devi, M., & Uma, K. (2025). Role of promoting green banking towards sustainable development. *International Journal of Accounting and Economics Studies*, *12*(1), 163–170. Scopus. https://doi.org/10.14419/a40nqv21

Dewangan, S., & Kumar, S. (2025). *Frontiers of innovation: Unveiling the future opportunities in Fintech* (pp. 153–165). Emerald Publishing; Scopus. https://doi.org/10.1108/978-1-83753-750-120251008

Diallo, A., Samhi, J., Bissyandé, T. F., & Klein, J. (2025). (In)Security of mobile apps in developing countries: A systematic literature review. *Empirical Software Engineering*, *30*(5). Scopus. https://doi.org/10.1007/s10664-025-10689-z

Grover, V., Agnihotri, A., Balusamy, B., Gite, S., & Arockiam, D. (2025). *The AI Revolution in Digital Financial Inclusion: Bridging Socioeconomic Gaps: Vol. 1075 LNNS* (V. Goar, M. Kuri, R. Kumar, & T. Senjyu, Eds.; pp. 391–405). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-981-97-6106-7_24

Husin, M. M., Aziz, S., Sajjad, S., & Talib, J. (2025). *Harnessing the Power of Digital Finance: The Malaysian SME Perspective* (pp. 433–457). IGI Global; Scopus. https://doi.org/10.4018/979-8-3373-1112-8.ch016

Introduction: Setting the agenda for research in cybersecurity law and policy. (2025). 1–3. Scopus. https://doi.org/10.4337/9781803929194.00006

Kathrada, M. (2025). *Robot Field Development Teams: Harnessing Multi-Agent Artificial Intelligence Systems in Petroleum Engineering*. Scopus. https://doi.org/10.2118/225325-MS

Kaveh, F., Delshad, M. M., & Pourghader Chobar, A. P. (2025). *Transformation of SME Financing Models Using Disruptive Technologies* (pp. 239–252). IGI Global; Scopus. https://doi.org/10.4018/979-8-3693-4369-2.ch015

Khang, A. (2025). *Shaping cutting-edge technologies and applications for digital banking and financial services* (p. 458). Taylor and Francis; Scopus. https://doi.org/10.4324/9781003501947

Kubilay, B., & Celiktas, B. (2025). Relationships Among Organizational-Level Maturities in Artificial Intelligence, Cybersecurity, and Digital Transformation: A Survey-Based Analysis. *IEEE Access*, *13*, 88399–88411. Scopus. https://doi.org/10.1109/ACCESS.2025.3571537

Kumar, R., Sharma, A., Tripathi, V., Devi, P., & Singh, N. (2025). *Power of Fintech in the Financial Inclusion*. 40–44. Scopus. https://doi.org/10.1109/IC363308.2025.10956819

Liang, J., & Pu, L. (2025). Integrating Big Data and AI for Network Security in 6G to Enhance University Financial Management. *Internet Technology Letters*, *8*(5). Scopus. https://doi.org/10.1002/itl2.70106

López, P. (2025). The National Security Framework as a Cybersecurity Reference for Information Cryptosystems. In *Law, Governance and Technology Series* (Vol. 71, pp. 125–144). Springer Nature; Scopus. https://doi.org/10.1007/978-3-031-74889-9_6

Nussbaum, B. H., Cornell, K. A., & Huang, L. (2025). *The Perfect Victim? Family Offices as Targets for Cybercriminals: Vol. 15532 LNCS* (K. Adi, S. Bourdeau, C. Durand, V. Viet Triem Tong, A. Dulipovici, Y. Kermarrec, & J. Garcia-Alfaro, Eds.; pp. 3–17). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-87499-4_1

Palos-Sánchez, P. R., Chang-Tam, R. J., & Folgado-Fernández, J. A. (2025). The role of Neobanks and FinTech in sustainable finance and technology. The customer/user perspective for entrepreneurs. *Sustainable Technology and Entrepreneurship*, *4*(3). Scopus. https://doi.org/10.1016/j.stae.2025.100109

Peswani, R., & Vijay, P. (2025). *Understanding the Influence of Demographics and Stream of Education on Cybercrime Awareness Among Students in Rajasthan, India*. 213–218. Scopus. https://doi.org/10.1109/ICCMSO67468.2025.00045

Poonia, R. C., Upreti, K., & Khan, M. S. (2025). *Smart Cyber-Physical Systems: Innovations and Real-World Implications* (p. 363). CRC Press; Scopus. https://doi.org/10.1201/9781003542513

Priyanka, K., Ray, S., & Surendran, J. K. (2025). *Strengthening Cybersecurity in India's FinTech: E-Governance and Financial Literacy Against Digital Fraud: Vol. 1384 LNNS* (A. Joshi, R. Ragel, M. Mahmud, & S. Kartik, Eds.; pp. 401–410). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-981-96-5751-3_34

Rakhra, M., Kanday, R., Aggarwal, G., Ather, D., Kler, R., & Jairath, K. (2025). *Quantum Cryptography: Enhancing Secure Communication in the Era of Quantum Computing*. 1395–1398. Scopus. https://doi.org/10.1109/NETCRYPT65877.2025.11102170

Raman, R., Mandal, S., Jebbor, A., Papadopoulos, T., & Nedungadi, P. (2025). Transforming business management practices through metaverse technologies: A Machine Learning approach. *International Journal of Information Management Data Insights*, *5*(1). Scopus. https://doi.org/10.1016/j.jjimei.2025.100335

Rohit, D., Shah, K., Patel, S., Parmar, N., Patel, M., Patel, D., Patel, Y., Patel, A., Sharma, S., Nayak, A., & Patel, C. (2025). *Unveiling Cryptocurrency Fraud: Leveraging Graph Attention Networks for Enhanced Detection in Bitcoin Transactions: Vol. 1383 LNNS* (A. Joshi, R. Ragel, M. Mahmud, & S. Kartik, Eds.; pp. 91–104). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-981-96-5754-4_9

Sargsyan, G., & Damiani, E. (2025). *Using Legends into AI-Based Business Decision Making: Embedding Ethics, Cybersecurity and Resilience*. 498–503. Scopus. https://doi.org/10.1109/CSR64739.2025.11130036

Sayeed, S. A., Rahman, M. M., Alam, S., & Kshetri, N. (2025). *FSCsec: Collaboration in Financial Sector Cybersecurity—Exploring the Impact of Resource Sharing on IT Security*. Scopus. https://doi.org/10.1109/ISDFS65363.2025.11012024

Sen, A. C., Kumar, P., Dave, M. J., Parmar, H. R., Kalra, A., & Goyal, M. (2025). *Machine Learning-Driven Anomaly Detection in Blockchain Transactions for High-Security Digital Banking: Vol. 2382 CCIS* (J. Singh, S. B. Goyal, M. Kumar, & R. Mittal, Eds.; pp. 143–157). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-86069-0_12

Sharma, A., & Sharma, N. (2025). *Opening the vault for securing the communication: An introduction to cryptography* (pp. 1–13). CRC Press; Scopus. https://doi.org/10.1201/9781003508632-1

Shi, J., Firmansyah, E. A., Wang, Y., & Xu, W. (2025). Technological innovation and regulatory harmonization in Islamic finance: A systematic review and machine learning analysis (2000–2023). *Journal of Islamic Accounting and Business Research*. Scopus. https://doi.org/10.1108/JIABR-01-2025-0026

Sivasamy, S., Gangrade, M., & Manjulalayam, R. M. (2025). *Role of Cloud Computing and Data Security in Financial Services*. 394–399. Scopus. https://doi.org/10.1109/ICCMSO67468.2025.00075

T N, T. N., & Singh, A. D. (2025). *Navigating Cybersecurity Challenges in the Frontier of Innovative Fintech Solutions: Vol. 1319 LNNS* (M. S. Kaiser, J. Xie, & V. S. Rathore, Eds.; pp. 215–229). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-981-96-4145-1_17

Tarhan, K. (2025). Türkiye’s Cybersecurity, Critical Infrastructure, and National Resilience in a Technopolar World Order. *Insight Turkey*, *27*(2), 149–172. Scopus. https://doi.org/10.25253/99.2025272.10

Tavakkoli, N., Çetin, O., Ekmekcioglu, E., & Savaş, E. (2025). From frontlines to online: Examining target preferences in the Russia–Ukraine conflict. *International Journal of Information Security*, *24*(1). Scopus. https://doi.org/10.1007/s10207-025-00981-w

Yadav, R., & Shinde, A. N. (2025). *Unlocking potential: The synergy of blockchain, AI, and Deepfake technology in transforming business decision-making and enhancing network security* (pp. 1–46). Nova Science Publishers Inc.; Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-105008361179&partnerID=40&md5=3331a98aafea9ab5a153bfc499cd57ef

Yıldırım, D. Ç., Yildirim, S., & Kandpal, V. (2025). *Sustainable digitalization strategies in business and healthcare* (p. 439). IGI Global; Scopus. https://doi.org/10.4018/979-8-3373-5087-5