Cybersecurity as the Foundation for the Development of Mobile Financial Applications: A Literature Study on Cybercrime and Its Mitigation

Shabrun Jamil[1]✉, Chandra Purna Irawan[2], Deliysa[3]
(1) Universitas Mahasaraswati Denpasar, Bali
(2) Universitas Tanjungpura
(3) Universitas Widya Mataram

✉ Shabrun Jamil
shabrunjamil65@gmail.com

Abstract

This study examines the importance of cybersecurity in mobile financial applications, particularly in the face of rising cybercrime threats. The aim of this research is to provide deeper insights into the significance of cybersecurity in mobile financial apps and to develop approaches that financial companies can adopt to protect their users' data and information. The research employs a qualitative descriptive method using a systematic literature review (SLR) approach. Meta-synthesis analysis is applied to synthesize data from 26 journal articles published between 2019 and 2024. The findings reveal that cybercrime in the financial and FinTech industries is driven by internal factors such as weak security systems, lack of system updates, limited human resource competencies, and careless user behavior. External factors include malware attacks, unclear regulations, and the use of advanced technology. To counter these, it is necessary to implement technologies such as firewalls and blockchain, strong risk management, enhanced network infrastructure, the establishment of cybersecurity teams, the development of clear regulations, and user education to raise awareness and improve cybersecurity. Therefore, the implementation of a comprehensive cybersecurity strategy is crucial in maintaining the integrity and trust of users in mobile financial applications

Keyword: cybercrime, cybersecurity, fintech, mitigation, mobile bankin

INTODUCTION

In the contemporary digital era, when information technology penetrates nearly every facet of daily life, mobile financial applications have transformed the way individuals and organizations manage and access their finances. Through the convenience of smartphones, users can now conduct financial transactions, make payments, transfer funds, or even monitor investments without the need for face-to-face interaction at traditional banking offices. This digitalization of financial services has not only enhanced efficiency but also expanded financial inclusion, allowing people from diverse social and economic backgrounds to participate in formal financial systems. However, the very same technological accessibility that drives convenience has also brought forth a series of new and complex risks that challenge the foundations of data protection and cybersecurity. As digital transformation accelerates, the security of mobile financial applications becomes a matter of growing urgency, particularly given their direct connection to personal, financial, and institutional data.

Despite its significant advantages, technology's pervasive nature also introduces vulnerabilities that must be addressed with caution. The exponential increase in digital interconnectivity has given rise to sophisticated threats such as identity theft, ransomware, data breaches, and large-scale cyberattacks targeting financial institutions. According to Raodia (2019), these risks have created deep anxiety within organizations responsible for safeguarding sensitive consumer information. Financial institutions, in particular, face a dual challenge: on one hand, they are expected to innovate and expand digital access; on the other, they must ensure that such innovations do not compromise data integrity and confidentiality. The attack on Bank Syariah Indonesia (BSI) in May 2023 exemplifies the magnitude of this issue, where ransomware disrupted banking operations for several days and led to the theft of personal data belonging to millions of users. The incident underscored that cybersecurity is not merely a technical necessity but an essential pillar of trust in the modern financial ecosystem.

DOI: https://doi.org/10.62238/emis.v1i1.292, 1(1), 2023, Pages 23-30

The historical evolution of financial technology reflects an ongoing interplay between innovation and security. As highlighted by Professor Douglas W. Arner from the University of Hong Kong, the development of Fintech can be categorized into four distinct phases—from Financial Technology 1.0, which relied heavily on telecommunication systems, to the ongoing 3.5 era marked by mobile-based digital transformation and consumer-driven innovation (Widiyati & Erliana, 2024). The emergence of Fintech has revolutionized access to financial products and services, enabling personalized and efficient solutions for customers. Yet, this progress is accompanied by the parallel evolution of cyber threats that exploit vulnerabilities in both systems and human behavior. Modern financial institutions, including Islamic banking sectors, are now compelled to pursue digital innovation while simultaneously reinforcing cyber resilience. Thus, cybersecurity has become inseparable from the strategic and operational framework of the financial industry.

Cybersecurity, in essence, represents an integrated set of tools, processes, and policies designed to safeguard information infrastructure, digital networks, and user data from unauthorized access and malicious attacks. It ensures the confidentiality, integrity, and availability of information across cyberspace—three foundational principles often referred to as the “CIA triad.” According to Ardiyanti (2019) and Septasari (2023), cybersecurity encompasses not only technological safeguards but also organizational strategies, governance mechanisms, and awareness programs that collectively reduce the likelihood of data breaches. It extends beyond merely defending against external attacks; it involves building a culture of digital security where individuals and organizations proactively manage and anticipate risks. In financial applications, this means employing strong encryption, multi-factor authentication, and regular system audits to protect sensitive financial information such as account details, transaction records, and credit data.

Parallel to cybersecurity, the phenomenon of cybercrime has evolved into one of the most pressing global challenges in the digital economy. Gregory (2005) defines cybercrime as criminal activity that exploits computer networks and Internet connectivity to conduct unlawful acts. These crimes include hacking, phishing, identity theft, malware distribution, and ransomware operations—all of which can lead to severe financial and reputational losses. Suhaemin and Muslih (2023) emphasize that cybercrime encompasses both newly emerged crimes targeting information systems and traditional crimes that have migrated into cyberspace. This convergence of technology and criminality has given rise to the interdisciplinary field of cybercriminology, which combines elements of criminology, sociology, psychology, computer science, and digital forensics to analyze the motives, methods, and impacts of cyber-offenses. Within the financial sector, cybercrime not only disrupts transactions but also erodes the public’s trust in digital banking platforms.

Among the various forms of cyber threats, malware and ransomware represent the most damaging and persistent. Malware—short for malicious software—is designed to infiltrate systems, corrupt data, and exploit vulnerabilities for illicit purposes (Ilhamdi & Kunang, 2021). Common variants include spyware, viruses, worms, trojans, and browser hijackers, each functioning to either steal, damage, or encrypt information. Ransomware, in particular, has emerged as one of the most devastating forms of attack. As Fitria (2023) and Hartono (2023) explain, ransomware encrypts user data, rendering it inaccessible until a ransom—often paid in cryptocurrency—is transferred to the attackers. The process typically begins with phishing emails or compromised websites, followed by system infiltration and data encryption. Victims are then confronted with extortion messages demanding payment in exchange for decryption keys. Beyond financial loss, such attacks paralyze institutional operations, compromise consumer data, and jeopardize the overall stability of financial ecosystems. Consequently, understanding and implementing robust cybersecurity strategies is no longer optional—it is an imperative for ensuring digital trust and protecting the integrity of financial technology systems.

RESEARCH METHOD

The research method employed in this study is a qualitative descriptive method using a systematic literature review (SLR) approach. This method is conducted systematically to identify literature from various indexed research journals through three main stages: planning, implementation, and reporting of the literature review (Suwarno et al., 2022). The SLR approach emphasizes clear statements regarding the research objectives, materials, and methods, as well as provides conclusions based on the proper development of methodology. The systematic literature review was conducted on 26 journal articles on cybersecurity published between 2019 and 2024, consisting of 15 international journals, 9 national journals, and 2 theses. The selected journals were qualified based on their relevance to cybercrime threats and anticipatory cybersecurity measures.

The meta-synthesis analysis technique was applied in this study to synthesize or summarize findings from qualitative descriptive research. The main purpose of meta-synthesis is to draw conclusions from various research findings through a more precise and in-depth analytical process (Kitchenham & Brereton, 2013). The initial step in meta-synthesis involves formulating research questions, followed by searching for relevant journal articles. The collected journals are then screened to ensure their relevance to the research topic. Subsequently, the data obtained from these journals are analyzed, and a quality control process is conducted on the findings. The meta-synthesis process concludes with the preparation of the final report.

RESULTS AND DISCUSSION

Results of Journal Classification Based on Year of Publication

The mapping results based on the year of publication of journals discussing cybercrime and cybersecurity issues are presented in the figure below. It can be observed that the number of articles addressing this topic peaked in 2023, with a total of eight publications. In contrast, in other years, the number of published articles averaged between two and five per year. This indicates a significant rise in research interest in 2023, which was likely influenced by the rapid development of financial technology (fintech) that began in 2019, as reported by OJK.go.id. Public interest in cybersecurity research reached its highest level in 2023. During the period from 2019 to 2023, society was still in the process of adapting to and understanding the utilization of fintech advancements. However, these developments revealed complex patterns and various potential threats. Consequently, in 2023, many researchers became increasingly interested in exploring issues related to cybercrime and cybersecurity to address the challenges emerging from advancements in financial technology.

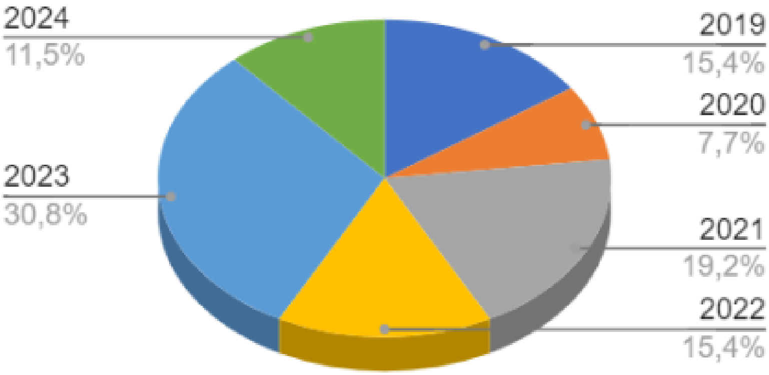

Figure 1. Journal Classification Results Based on Year of Publication.

Results of Journal Classification Based on Type of Journal

The mapping results based on the Publisher Accreditation Level that discuss topics related to cybercrime and cybersecurity can be seen in the diagram below. Indonesian scholars are currently making significant efforts to increase the number of research outputs in the form of scientific articles published both nationally and internationally. Accessible scientific articles are highly important, as the level of cybersecurity and awareness of cybercrime can be influenced by the quality of such publications.

Currently, the accreditation levels of journals in Indonesia are categorized into Sinta 1, 2, 3, 4, 5, and 6. Based on the mapping results, the majority of articles discussing cybercrime and cybersecurity were published in international journals (53.8%), followed by non-accredited national journals (19.2%), and Sinta 4 journals (11.5%). Publications in Sinta 5 journals accounted for 3.8%, while theses represented 7.7%, and Scopus-indexed international journals made up 3.8%.These percentages indicate a growing attention and research interest in the field of cybersecurity and cybercrime, supported by strong government initiatives to encourage publications at the global level.

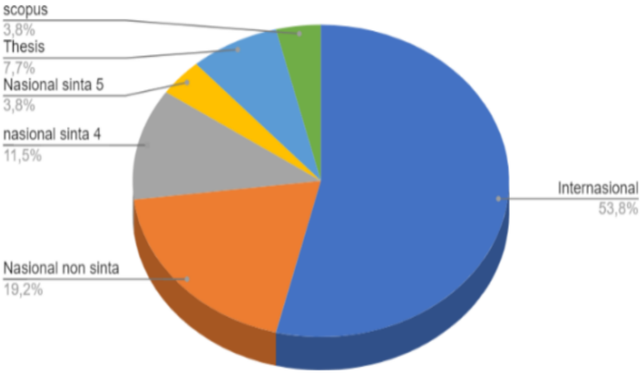

Figure 2. Results of Journal Classification Based on Type of Journal

Results of Journal Classification Based on Research Issues

Based on the classification results of 26 journals over a five-year research period (2019–2024), the researchers identified two main issues to be discussed in this study. Several journals addressed more than one issue as determined by the researchers. This is detailed in the table below. Therefore, the total number of journal entries based on research issues is 33, while the total number of journals mapped is 26. The issues highlighted in the articles are as follows:

Table 1. Results of Journal Classification Based on Research Issues

No	*Isu Research*	Amount
1	Factors Causing Cybercrime	19
2	*Cybersecurity to Mitigate the Risks of Cybercrime*	14
	Total	33

Internal Factors Contributing to Cybercrime Attacks

Another critical factor lies in the insufficient implementation and maintenance of security systems. Many organizations fail to enforce regular updates or adopt systematic patching protocols for their software and applications, which leaves them open to exploitation. Cyberattackers often exploit known vulnerabilities in unpatched systems, making preventive maintenance an indispensable element of cybersecurity. When institutions neglect periodic system audits or fail to upgrade their infrastructure in line with technological evolution, they inadvertently create gateways for malicious actors. According to Kunnas (2022), weak internal security management within mobile banking platforms not only jeopardizes operational stability but also undermines the credibility and long-term reputation of the institution. In the financial sector, where trust serves as the foundation of all transactions, such oversights can have devastating consequences.

Human capital and organizational competence also play an equally decisive role in shaping cybersecurity resilience. The accelerating pace of digital transformation requires that personnel, particularly those in internal control and audit divisions, possess both technical proficiency and adaptive capacity to recognize evolving forms of cyber threats. However, Una and Prabowo (2022) observe that many financial institutions continue to rely on staff whose expertise is rooted in traditional audit mechanisms, leaving them ill-equipped to address contemporary cybersecurity risks. The problem is compounded by high employee turnover and managerial unfamiliarity with information systems, both of which diminish institutional vigilance. As Ng and Kwok (2019) note, such gaps not only weaken preventive mechanisms but also heighten the risk of internal fraud, making the fintech ecosystem increasingly vulnerable to both human error and intentional exploitation. Equally significant is the influence of user behavior in shaping the cybersecurity landscape. Even the most advanced systems can be rendered ineffective when users engage in unsafe online practices. Simple yet dangerous habits—such as clicking suspicious links, downloading unverified attachments, or using weak and repetitive passwords—serve as primary entry points for hackers. Fitria (2023) and Ouytsel (2021) point out that human negligence remains one of the most exploited weaknesses in cyberattacks. Furthermore, the practice of password sharing, often done under the guise of trust or convenience, exposes users to further risk. In digital ecosystems where personal and financial data are deeply interconnected, a single lapse in user judgment can compromise entire networks of information.

Institutional weaknesses are also reflected in the absence of comprehensive internal policies and procedures. Emerging fintech organizations, in particular, often prioritize rapid growth and innovation over the formulation of rigorous internal control systems. Rawindaran et al. (2023) explain that the lack of structured governance frameworks not only leaves these institutions vulnerable to external threats but also increases the likelihood of insider misconduct. Senior employees with access to confidential information may exploit systemic loopholes for personal gain—through theft, data sabotage, or inadvertent disclosure of sensitive material. Without clear accountability mechanisms, even minor oversights can escalate into significant breaches that jeopardize customer trust and institutional integrity.

Another pressing concern is the growing reliance on third-party collaborations. As financial institutions increasingly partner with external service providers—such as technology vendors, cloud storage companies, or payment gateway operators—they expose themselves to additional layers of risk. Yohanes and Perajaka (2021) argue that these partnerships, while beneficial for innovation and efficiency, often lack uniformity in their security standards. Discrepancies between the cybersecurity protocols of primary institutions and their partners can create exploitable gaps within interconnected systems. Hackers frequently take advantage of these inconsistencies to infiltrate networks through less secure third-party channels, underscoring the need for continuous monitoring, strict contractual obligations, and transparent communication between collaborating entities. Lastly, the lack of systematic evaluation and effective communication further undermines the resilience of financial institutions against cyber threats. Maulana and Nasrulloh (2024) assert that the absence of robust feedback mechanisms to assess customer perceptions, policy effectiveness, and incident responses leads to stagnation in cybersecurity improvement. When institutions fail to communicate transparently with users regarding security incidents or preventive measures, trust deteriorates. Moreover, the inability to evaluate strategic interventions objectively prevents organizations from refining their defense systems. Therefore, continuous assessment, open dialogue, and adaptive communication are essential to bridging the gap between institutional readiness and user awareness in an increasingly volatile cyber environment.

Cybersecurity to Mitigate the Risks of Cybercrime

The foundation of a resilient cybersecurity framework in financial technology lies in a combination of technical infrastructure, institutional readiness, and human awareness. Protection against both internal and external threats must begin with the implementation of robust preventive technologies such as firewalls and blockchain systems. Firewalls act as the first line of defense, preventing unauthorized access and filtering harmful traffic that may infiltrate servers. The role of a firewall extends beyond mere blockage—it enforces the principle of least privilege by ensuring that every access attempt is authenticated and monitored. According to Meidiandra et al. (2023), an effective firewall strategy involves multiple layers of control, including precise configuration, strict access management, regular updates, and ongoing monitoring to detect anomalies. Blockchain technology, on the other hand, represents a structural innovation that enhances data integrity and transparency. By distributing identical copies of the ledger across a decentralized network, blockchain minimizes the risk of unauthorized modification or deletion of information, thereby ensuring accountability and resilience. Javaid et al. (2022) and Mohamed (2023) argue that blockchain has redefined transactional trust by embedding the core cybersecurity principles of confidentiality, integrity, and availability into the architecture of financial operations.

Beyond technological reinforcement, effective cybersecurity also requires a comprehensive risk management framework supported by internal governance. Digital innovation must always be accompanied by disciplined oversight, clear standard operating procedures, and layered data protection strategies. Kurniawan and Solihin (2022) highlight that multi-layered storage systems and regular data backups can significantly mitigate losses resulting from cyberattacks. Likewise, the introduction of Three-Factor Authentication (3FA) strengthens the reliability of digital access by combining three distinct verification layers—knowledge (passwords or PINs), possession (devices or tokens), and inherence (biometric identifiers such as fingerprints or facial recognition). This multifactor approach does not merely secure user access; it fundamentally reshapes the interaction between human behavior and digital security. When implemented consistently, risk management and multi-layer authentication systems form a defense architecture that is adaptive, predictive, and preventive in facing evolving cyber threats.

Equally important is the development of strong network infrastructure and competent human resources to operate and maintain it. No technology can be fully secure without adequately trained professionals who understand both its potential and vulnerabilities. Financial institutions must continuously invest in employee upskilling through targeted cybersecurity training that matches evolving threat landscapes. Rawindaran et al. (2023) emphasize that employees function as both the guardians and potential weak links of organizational security. Therefore, continuous learning and institutional discipline are crucial in cultivating cyber resilience. Parallel to this, network modernization—such as transitioning from open gateways to single, monitored gateways—enhances visibility and allows real-time response to anomalies (Maulana & Nasrulloh, 2024). Establishing a dedicated cybersecurity team further strengthens institutional preparedness. This team serves as the operational nerve center, responsible for identifying vulnerabilities, managing threats, and coordinating emergency responses. Their role extends into policy-making, ensuring compliance with legal frameworks, and integrating security protocols with national and international standards (Riskiyadi et al., 2021).

Finally, the human element—users themselves—remains the most unpredictable yet essential component of cybersecurity. No matter how sophisticated a system becomes, it can still be compromised by negligent user behavior or lack of awareness. Therefore, user education is not a supplementary initiative but a strategic necessity. By cultivating cybersecurity literacy, users can function as active participants in protecting their data rather than passive consumers of technology. Awareness campaigns, training modules, and preventive guidelines—such as installing antivirus software, using strong and unique passwords, verifying URLs, and avoiding suspicious email attachments—are critical measures in reducing exposure to threats (Abdulrahaman et al., 2019; Fitria, 2023). As Kurniawan and Solihin (2022) emphasize, a secure fintech ecosystem can only be achieved when technological protection, institutional policy, and human responsibility operate synergistically. Thus, the future of cybersecurity depends not only on advanced algorithms or infrastructures but also on the collective discipline of every actor within the digital financial ecosystem.

CONCLUSION

Cybercrime attacks in the financial and fintech industries are driven by internal factors such as weak security systems, insufficient system updates, limited human resource competence, and careless user behavior. External factors include malware attacks, unclear regulations, and the use of advanced technologies. To address these issues, the implementation of technologies such as firewalls and blockchain, strong risk management, improved network infrastructure, the establishment of cybersecurity teams, development of clear regulations, and user education to raise awareness and enhance cybersecurity are essential.This study has a limited focus on secondary data from existing literature and does not include primary data, such as interviews or investigative reports, and therefore does not cover all critical aspects of cybersecurity in mobile financial applications. Future research is expected to utilize additional data sources, such as interviews with key informants, and focus on evaluating the effectiveness of cybersecurity strategies in the financial technology sector.

REFERENCES

Abdulrahaman, M. D., Alhassan, J. K., Ojeniyi, J. A., & Abdulhamid, S. M. (2019). Security Risk Analysis and Management in mobile wallet transaction: A Case study of Pagatech Nigeria Limited. International Journal of Computer Network and Information Security, 10(12), 21–33. https://doi.org/10.5815/ijcnis.2018.12.03

Al-Harrasi, A., Shaikh, A. K., & Al-Badi, A. (2021). Towards protecting organisations' data by preventing data theft by malicious insiders. International Journal of Organizational Analysis, 31(3), 875–888.

Ardiyanti, H. (2019). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. Jurnal Politica, 5(1), 95–110.

Assifa, B. A. (2023). Perlindungan Hukum Terhadap Nasabah Bank Syariah Indonesia dari serangan Cybercrime. Universitas Islam Negeri Syarif Hidayatullah Jakarta.

Demirkan, S., Demirkan, I., & McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, 7(2), 189–208. https://doi.org/10.1080/23270012.2020.1731721

Fitria, K. M. (2023). Analisis Serangan Malware Dalam Perbankan Dan Perencanaan Solusi Keamanan. Jurnal Informatika Dan Teknik Elektro Terapan, 11(3). https://doi.org/10.23960/jitet.v11i3.3312

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. Bincang Sains Dan Teknologi, 2(02), 55–62. https://doi.org/10.56741/bst.v2i02.353

Ilhamdi, Y., & Kunang, Y. N. (2021). Analisis Malware Pada Sistem Operasi Windows Menggunakan Teknik Forensik. Bina Darma Conference on Computer Science, 3, 256–264.

Islam, M. S. (2019). Systematic Literature Review: Security Challenges of Mobile Banking and Payments System. International Journal of U- and e-Service, Science and Technology, 7(6), 107–116. https://doi.org/10.14257/ijunesst.2014.7.6.10

Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 2(3), 100073. https://doi.org/10.1016/j.tbench.2022.100073

Kitchenham, B., & Brereton, P. (2013). A systematic review of systematic review process research in software engineering. In Information and Software Technology (Vol. 55, Issue 12).
https://doi.org/10.1016/j.infsof.2013.07.010

Kumari, R., Jasojit, T., Kumari, R., Jasojit, T., Keuangan, K., & Penulis, U. (2017). Jurnal Regulasi dan Kepatuhan Keuangan.

Kunnas, J. (2022). EMPLOYEE ATTITUDES TOWARDS INFORMATION Identifying archetypes using machine learning Bachelor ' s Thesis Juho Kunnas Aalto University School of Business Information and Service Management. Aalto University School of Business Information and Service Management.

Kurniawan, F. A., & Solihin, K. (2022). Penguatan Manajemen Risiko Lembaga Keuangan Syariah Non-Bank dalam Menghadapi Ancaman Cyber Security. JIOSE: Journal of Indonesian Sharia Economics, 1(1), 1–20. https://doi.org/10.35878/jiose.v1i1.360

Laidlaw. (2021). Privacy and Cybersecurity in Digital Trade: The Challenge of Cross Border Data Flows. SSRN Electronic, 10(1), 1–81.

Maulana, B. R., & Nasrulloh, N. (2024). Analisis Strategi Pemulihan Citra Bank Syariah Indonesia Pasca Dugaan Serangan Siber. Ekonomi Syariah Dan Bisnis Perbankan, 8(1), 76–91.

Meidiandra, M. K., Sari, Y. P., & Sutabri, T. (2023). Mendesain Cyber Security Core Banking System untuk Keamanan Menggunakan Firewall Pada PT. Bank Syariah Indonesia Tbk. Syntax Idea, 5(7), 843–848.

Mohamed, A. O. Y. (2023). Intelligent Blockchain-Based Secure Framework for Transaction in Mobile Electronic Payment System. International Journal of Interactive Mobile Technologies, 17(4), 37–46. https://doi.org/10.3991/ijim.v17i04.37671

Ng, A., & Kwok, B. K. B. (2019). Emergence of Fintech and cybersecurity in a global financial centre. Journal of Financial Regulation and Compliance, 25(4), 422–434. https://doi.org/10.1108/jfrc-01-2017-0013

Ouytsel, J. Van. (2021). The prevalence and motivations for password sharing practices and intrusive behaviors among early adolescents' best friendships – A mixed-methods study. Telematics and Informatics, 63(101668).

Raodia, R. (2019). Pengaruh Perkembangan Teknologi Terhadap Terjadinya Kejahatan Mayantara (Cybercrime). Jurisprudentie : Jurusan Ilmu Hukum Fakultas Syariah Dan Hukum, 6(2), 39. https://doi.org/10.24252/jurisprudentie.v6i2.11399

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2023). Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. International Journal of Information Management Data Insights, 3(2), 100191. https://doi.org/10.1016/j.jjimei.2023.100191

Restika, R., & Sonita, E. (2023). Tantangan Keamanan Siber Dalam Manajemen Likuiditas Bank Syariah : Menjaga Stabilitas Keuangan Di Era Digital. Krigan: Journal of Management and Sharia Business, 1(2), 25. https://doi.org/10.30983/krigan.v1i2.7929

Riskiyadi, M., Anggono, A., & Tarjo. (2021). Cybercrime dan Cybersecurity pada Fintech: Sebuah Tinjauan Pustaka Sistematis. Jurnal Manajemen Dan Organisasi, 12(3), 239–251. https://doi.org/10.29244/jmo.v12i3.33528

Septasari, D. (2023). The Cyber Security and The Challenge of Society 5.0 Era in Indonesia. Aisyah Journal Of Informatics and Electrical Engineering (A.J.I.E.E), 5(2), 227–233. https://doi.org/10.30604/jti.v5i2.231

Suhaemin, A., & Muslih. (2023). Karakteristik Cybercrime di Indonesia. EduLaw : Journal of Islamic Law and Yurisprudance, 5(2), 15–26.

Sumadi, M. I. T. B. N., Putra, R., & Firmansyah, A. (2022). Peran Perkembangan Teknologi Pada Profesi Akuntan Dalam Menghadapi Industri 4.0 Dan Society 5.0. Journal of Law, Administration, and Social Science, 2(1), 56–68. https://doi.org/10.54957/jolas.v2i1.162

Suwarno, R., Cahyono, D., & Maharani, A. (2022). Systematic Literature Review: Faktor Keunggulan Bank Syariah Di Indonesia. Jurnal Peneliti Ekonomi, 1(6), 40–54.

Una, B. K., & Prabowo, H. Y. (2022). Fintech lending fraud prevention strategy: A case study. Journal of Contemporary Accounting, 4(1), 37–52.

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. Journal Computers & Security, 147(104051).

Wang, Y. (2023). Application of Big Data Technology in Mobile Payment Security. Journal of Research in Social Science and Humanities, 2(12), 18–23. https://doi.org/10.56397/jrssh.2023.12.04

Widiyati, D., & Erliana. (2024). Pengaruh Literasi Keuangan, Perlindungan Data, dan Cybersecurity terhadap Penggunaan Financial Technology. JURNAL AKUNTANSI DAN EKONOMI AKREDITASI NOMOR, 9(1), 130–141. https://doi.org/10.29407/jae.v9i1.21945

Yang, T. (2020). Mobile Payment Security in the Context of Big Data: Certificateless Public Key Cryptography. International Journal of Network Security, 22(4), 621–626.

Yohanes, N., & Perajaka, M. A. (2021). Penerapan Model Manajemen Risiko Teknologi Digital di Lembaga Perbankan Berkaca pada Cetak Biru Transformasi Digital Perbankan Indonesia. Jurnal Manajemen Risiko, 2(2), 59–74.