

The Relationship Between Cybersecurity and Public Trust in Digital Services Based on Fintech Lending Applications

**Harry Sudhana¹, Dhian Tyas Untari¹, Ahmad Syarif¹, Nyayu Maya Ardini¹
Muhammad Firman Maulana¹, Pandri Zulfikar^{6*}**

¹ Magister Ilmu Hukum; Syekh-Yusuf Islamic University, Tangerang - Banten;

*Correspondence e-mail : Pandri.zulfikar@unis.ac.id

Abstract

The rapid growth of fintech lending applications has significantly transformed access to financial services, especially in developing countries. These platforms provide fast, convenient, and accessible financial solutions; however, they also raise critical concerns regarding cybersecurity and data protection. This study aims to analyze the relationship between cybersecurity and public trust in digital lending applications through a qualitative literature review. Cybersecurity is a key determinant of trust, as users must share sensitive personal and financial information when accessing digital lending services. Empirical studies indicate that data breaches, unauthorized access, and misuse of personal data significantly reduce consumer trust. Conversely, strong cybersecurity mechanisms such as encryption, authentication systems, and regulatory compliance enhance trust and encourage adoption. This paper finds that cybersecurity is not only a technical requirement but also a strategic factor in building sustainable trust relationships between users and fintech providers. Strengthening cybersecurity frameworks, improving regulatory enforcement, and increasing digital literacy are essential to fostering trust in digital lending ecosystems. The study contributes to the understanding of how cybersecurity influences trust and provides insights for policymakers and fintech providers in developing secure and reliable digital financial services.

Keywords: *Cybersecurity, Fintech Lending, Digital Trust, Data Protection, User Behavior*

INTRODUCTION

The advancement of digital technology has significantly transformed financial services through the emergence of financial technology (fintech), particularly lending applications. Fintech lending platforms enable individuals to access loans quickly and efficiently through mobile applications without traditional banking procedures. This innovation has improved financial inclusion and expanded access to credit, especially in developing economies. However, the rapid growth of fintech lending has also introduced new challenges, particularly in the area of cybersecurity and data privacy.

Fintech lending applications require users to provide sensitive personal information, including identification data, financial records, and contact details. This data-intensive nature makes fintech platforms highly vulnerable to cyber threats such as data breaches, identity theft, phishing attacks, and malware. Cybersecurity risks have become a major concern for users, as these threats can lead to financial loss and misuse of personal data. According to Handayani (2023), fintech lending services are increasingly exposed to cybersecurity threats, particularly related to personal data protection, requiring robust legal and technological safeguards.

The issue of data misuse is particularly critical in fintech lending applications. Cases of unauthorized data access and illegal data sharing have been widely reported, raising concerns about user privacy. Rahmawati et al. (2024) highlight that personal data misuse in fintech lending includes unauthorized disclosure and exploitation of user information, which can lead to legal consequences and reduced consumer confidence.

Public trust is a crucial factor in determining the adoption and sustainability of fintech lending services. Trust is defined as the willingness of users to rely on a system despite potential risks. In digital environments, trust is strongly influenced by perceived security and data protection mechanisms. When users perceive a system as secure, they are more likely to trust and use it. Conversely, security breaches can significantly reduce trust and discourage users from engaging with digital services.

Empirical evidence supports the relationship between cybersecurity and trust. Widiana and Kusuma (2025) found that data breaches and misuse of personal data significantly reduce consumer trust in online lending services. Meanwhile, Efryanto (2024) demonstrates that security plays a significant role in influencing users' decisions to adopt fintech lending applications. In addition, the presence of illegal fintech platforms further complicates the trust issue. Suryono et al. (2021) report that many illegal fintech applications operate without proper regulation, increasing the risk of fraud and reducing public confidence in digital lending services.

Given these challenges, cybersecurity has become a fundamental requirement for building trust in fintech lending applications. This paper aims to analyze the relationship between cybersecurity and public trust by reviewing relevant theoretical and empirical studies. It seeks to provide insights into how cybersecurity influences trust and how fintech providers can enhance trust through improved security measures.

THEORETICAL REVIEW

Cybersecurity in Fintech Lending

Cybersecurity refers to the protection of systems, networks, and data from digital attacks. In fintech lending applications, cybersecurity is critical due to the sensitive nature of financial and personal data. Fintech platforms are prime targets for cybercriminals because they handle valuable information and financial transactions. Cyber threats in fintech include phishing, malware, data breaches, and identity theft. These threats can compromise system integrity and lead to significant financial and reputational damage. Research indicates that fintech platforms must implement advanced security measures such as encryption, multi-factor authentication, and intrusion detection systems to mitigate these risks (Javaheri et al., 2023).

Moreover, cybersecurity is not solely a technical issue; it also involves governance and regulatory frameworks. Handayani (2023) emphasizes that legal protection and regulatory compliance are essential components of cybersecurity in fintech lending.

Concept of Trust in Digital Lending Services

Trust is a fundamental concept in digital financial services, reflecting users' confidence in the reliability and security of a system. In fintech lending, trust is particularly important due to the involvement of financial transactions and personal data. Trust is influenced by several factors, including perceived security, privacy protection, service quality, and transparency. Nangin et al. (2019) found that perceived security significantly influences trust in fintech applications.

Additionally, structural assurance, such as regulatory compliance and system reliability, plays a critical role in building trust. Pratama (2021) highlights that system integrity and ease of use are important determinants of trust in fintech lending platforms. Trust is also shaped by user experience and knowledge. Users with higher digital literacy are more likely to trust fintech applications, as they understand security mechanisms and risks.

Relationship Between Cybersecurity and Trust

The relationship between cybersecurity and trust is direct and interdependent. Cybersecurity serves as a foundation for trust, as users rely on secure systems to protect their data and transactions. When users perceive a system as secure, their trust increases, leading to higher adoption rates. Conversely, cybersecurity risks negatively affect trust. Putri et al. (2021) found that security risks have a negative impact on trust in fintech services.

Similarly, data breaches and cybercrime incidents reduce user confidence and discourage the use of digital lending applications. Widiana and Kusuma (2025) emphasize that data leakage significantly decreases consumer trust. The Technology Acceptance Model (TAM) explains this relationship by suggesting that perceived usefulness and ease of use influence adoption, while perceived risk and security affect trust. Primadasa et al. (2021) demonstrate that trust significantly influences users' intention to use fintech applications.

Regulatory and Institutional Perspective

Regulation plays a crucial role in strengthening cybersecurity and trust. Strong regulatory frameworks ensure data protection, prevent fraud, and enhance accountability. In Indonesia, the Personal Data Protection Law provides a legal framework for protecting user data and increasing trust in digital services. Muin and Suhra (2024) emphasize that inadequate regulation can lead to data misuse and privacy violations, which undermine trust in fintech lending services.

METHOD

This study uses a qualitative literature review approach to examine the relationship between cybersecurity and public trust in fintech lending applications. Data were collected from peer-reviewed journal articles published between 2019 and 2025. The selection criteria included relevance to cybersecurity, fintech lending, and digital trust, as well as methodological rigor. The analysis was conducted using thematic analysis to identify key patterns and relationships. This approach allows for a comprehensive understanding of how cybersecurity influences trust and provides a conceptual foundation for future empirical research.

DISCUSSION

The relationship between cybersecurity and public trust in fintech lending applications is increasingly recognized as a critical determinant of digital financial sustainability. The findings from this study demonstrate that cybersecurity is not merely a technical requirement but a strategic factor that directly shapes user trust, adoption

behavior, and long-term engagement with digital lending platforms. In fintech ecosystems, where sensitive personal and financial data are continuously processed, the perception of security becomes a central component influencing trust formation.

One of the most prominent findings in the literature is that fintech platforms are inherently vulnerable to cyber threats due to their data-centric nature. Cyber threats such as phishing, malware, data breaches, and identity theft are prevalent in mobile-based financial services, making cybersecurity a crucial concern for both providers and users. Studies indicate that fintech systems are highly attractive targets for cybercriminals because of the financial value and sensitive data they manage (Javaheri et al., 2023). These risks are further exacerbated by the continuous evolution of cyber threats, which require adaptive and sophisticated security strategies.

The presence of cybersecurity threats significantly affects user trust. When users perceive high levels of risk, their willingness to use fintech lending applications declines. This aligns with risk theory, which suggests that trust is inversely related to perceived risk. Empirical findings confirm that perceived security plays a mediating role between fintech usage and trust. Dewatmoko et al. (2024) found that security perception significantly influences trust in financial transactions, highlighting the importance of secure systems in shaping user confidence. Similarly, Nangin et al. (2019) demonstrate that security is a key determinant of trust and adoption in fintech services.

Another important aspect is the role of data protection in building trust. Fintech lending applications require extensive user data, including personal identification and financial information. Any misuse or unauthorized access to this data can severely damage user trust. Research shows that data breaches not only lead to financial loss but also result in long-term reputational damage for fintech providers (Riskiyadi et al., 2021). This highlights the importance of implementing strong data governance frameworks to ensure user privacy and security.

In addition to technical security measures, regulatory frameworks play a crucial role in strengthening trust. Effective regulation ensures accountability, transparency, and compliance with data protection standards. Studies emphasize that weak regulatory environments contribute to increased cybercrime and reduced trust in fintech services (Mustapha et al., 2023). Regulatory support not only enhances security but also provides structural assurance to users, which is essential for trust formation.

Furthermore, emerging technologies such as artificial intelligence (AI) and blockchain have been identified as key enablers of cybersecurity in fintech. These technologies enhance fraud detection, identity verification, and transaction security. A systematic review by Gindre and Ibarra (2024) shows that AI and blockchain significantly

improve fintech security by optimizing processes such as Know Your Customer (KYC) and fraud prevention. However, these technologies also introduce new challenges, including scalability and regulatory adaptation, which must be addressed to maintain user trust.

Another critical factor influencing trust is user awareness and digital literacy. Users with higher levels of cybersecurity awareness are more likely to trust fintech applications because they understand the risks and protective measures involved. Bharathiar and Sumathy (2024) found that self-efficacy and awareness significantly enhance cybersecurity understanding and contribute to trust formation. This suggests that trust is not solely dependent on system security but also on user knowledge and experience.

The discussion also reveals that trust in fintech lending is multidimensional, involving cognitive, emotional, and behavioral components. Cognitive trust is based on rational evaluation of security features, while emotional trust is influenced by user experience and perceived reliability. Behavioral trust is reflected in the actual use of fintech applications. The interaction of these dimensions highlights the complexity of trust in digital environments.

Moreover, the integration of advanced technologies in fintech ecosystems introduces both opportunities and risks. Kamuangu (2025) highlights that the convergence of cybersecurity, fintech, and artificial intelligence creates new challenges in risk detection and data governance, requiring innovative approaches to maintain trust. This indicates that cybersecurity strategies must evolve alongside technological advancements to address emerging threats.

The role of user experience is also significant in shaping trust. Even with strong cybersecurity measures, poor user experience can reduce trust and discourage adoption. Fintech providers must balance security and usability to ensure that security measures do not hinder user convenience. This balance is critical in maintaining user engagement and satisfaction. Another key finding is the importance of transparency in building trust. Users need clear information about how their data is collected, stored, and used. Transparent communication reduces uncertainty and enhances trust. Fintech companies that provide clear privacy policies and security assurances are more likely to gain user confidence.

Additionally, trust is influenced by social and institutional factors. Social influence, such as recommendations from peers, can enhance trust in fintech applications. Institutional trust, on the other hand, is shaped by the reputation of fintech providers and the effectiveness of regulatory frameworks. Studies show that trust in technology is a significant factor influencing adoption in high-risk environments (Chen et al., 2025). Despite the importance of cybersecurity, challenges remain in its implementation. Many fintech companies face limitations in resources, expertise, and infrastructure, which can hinder the

effectiveness of cybersecurity measures. Furthermore, the rapid pace of technological change makes it difficult to maintain up-to-date security systems.

In conclusion, the discussion highlights that cybersecurity is a fundamental determinant of public trust in fintech lending applications. Strong cybersecurity measures enhance trust by reducing perceived risks, protecting user data, and ensuring system reliability. However, trust is influenced by multiple factors, including regulation, user awareness, service quality, and transparency. Therefore, a holistic approach that integrates technological, organizational, and social factors is essential for building and maintaining trust in digital lending services.

CONCLUSION

This study highlights that cybersecurity is a fundamental pillar in building and sustaining public trust in fintech lending applications. Strong security systems, including data protection, encryption, and authentication mechanisms, reduce perceived risks and enhance user confidence in digital financial services. Conversely, cybersecurity threats such as data breaches, fraud, and misuse of personal information significantly weaken trust and hinder user adoption. Trust in fintech lending is not only shaped by technical security but also influenced by regulatory frameworks, transparency, and user awareness. Therefore, fintech providers must adopt a comprehensive approach that integrates advanced cybersecurity technologies, effective governance, and continuous user education. Strengthening these aspects is essential to ensure sustainable trust, promote wider adoption, and support the long-term development of secure digital lending ecosystems.

REFERENCES

- Alpcan, T., Levi, A., & Savas, E. (2011). Digital trust models. *Lecture Notes in Computer Science*, 7037.
- Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. *MIS Quarterly*, 37(2), 471–482.
- Bharathiar, J. T., & Sumathy, M. (2024). Cybersecurity awareness and fintech trust. *Formosa Journal of Computer and Information Science*, 3(1).
- Chen, X., Liu, Y., & Wang, Z. (2025). Cyber risk and fintech adoption. *Journal of Behavioral and Experimental Finance*, 100687.
- Darman, D. (2019). Fintech lending characteristics. *Jurnal Manajemen Teknologi*, 18(2).
- Dewatmoko, S., Prasetyo, B., & Nugroho, A. (2024). Security perception and trust. *Management Studies and Entrepreneurship Journal*, 4(6).

- Efryanto. (2024). Security and e-service quality in fintech lending. Account: Jurnal Akuntansi, Keuangan dan Perbankan, 11(1), 2208–2221.
- Fu, J., & Mishra, M. (2023). Fintech risks and trust. The British Accounting Review, 55(4).
- Gill, M. A., Rahman, A., & Khan, S. (2023). Cybersecurity evolution in fintech. Journal of Computing & Biomedical Informatics, 5(1).
- Gindre, F., & Ibarra, G. (2024). AI and blockchain in fintech security. Journal of Computer Science and Technology, 26(4).
- Handayani, A. (2023). Cybersecurity threats in fintech lending. Jurist-Diction, 6(4).
- Hughes, L., Dwivedi, Y. K., Rana, N. P., & Williams, M. D. (2023). Cybersecurity in digital systems. International Journal of Information Management, 68.
- Javaheri, D., Hosseini, S., & Rezaei, M. (2023). Cybersecurity threats in fintech. Expert Systems with Applications, 241, 122697.
- Kamuangu, P. (2025). Cybersecurity and fintech convergence. Global Business Review, 43(4).
- Liang, W., Zhang, R., & Liu, Y. (2024). Blockchain privacy. ACM Computing Surveys, 56(12).
- Moore, T., & Pym, D. (2015). Cybersecurity research. Journal of Cybersecurity, 1(1). ISSN: 2057-2085.
- Muin, I., & Suhra, A. (2024). Data protection in fintech. Restorative Journal, 1(2).
- Muthukannan, P., Tan, B., Gozman, D., & Johnson, L. (2020). Fintech ecosystem research. Technological Forecasting and Social Change, 161.
- Mustapha, I., Abdullahi, M., & Bello, A. (2023). Cybersecurity in fintech mobile apps. International Journal of Interactive Mobile Technologies, 17(22). ISSN: 1865-7923.
- Nangin, M. A., Barus, B., & Sumarwan, U. (2019). Security and trust in fintech adoption. Journal of Consumer Sciences, 5(2), 124–138.
- Pietrzak, P., & Takala, J. (2021). Digital trust framework. Forum Scientiae Oeconomia, 9(1).
- Pratama, J. (2021). Trust in P2P lending. Jurnal Sisfokom, 10(1).
- Primadasa, Y., Gunawan, A., & Santoso, H. (2021). TAM and trust in fintech. CogITo Smart Journal, 7(2).
- Putri, M. Z., Sutarso, Y., & Hiqmah, F. (2021). Security risk and trust. Journal of Business & Banking, 11(1). ISSN: 2088-7841.
- Rahmawati, E., Putra, A., & Lestari, D. (2024). Personal data misuse in fintech lending. Airlangga Development Journal, 8(1).
- Riskiyadi, M., Santoso, B., & Wibowo, A. (2021). Cybercrime and fintech. Jurnal Manajemen dan Organisasi, 12(3). ISSN: 2088-7096.
- Suryono, R. R., Budi, I., & Purwandari, B. (2021). Fintech ecosystem issues in Indonesia. Heliyon, 7(4). ISSN: 2405-8440.



Zhang, Y., & Xu, H. (2022). Blockchain security systems. Security and Communication Networks, 2022(1).

