**JESH: Journal of Social, Economics, and Humanities**
Vol. 4 No. 1, April 2026
E-ISSN: 2988-4934
DOI: 10.30595/jesh.v4i1.464

# Comparison of The Effectiveness of Biometric Security Technology, Encryption, Ai Fraud Detection Preventing Fraud on Online Loan Applications

**Arinda Manar Rizqiani**
Universitas Muhammadiyah Purwokerto, Purwokerto, Indonesia

**Article Info**

***Article history:***

Received March 19, 2026
Revised March 24, 2026
Accepted March 28, 2026

***Keywords:***

Fintech, Online lending, Digital security, Fraud prevention, AI fraud detection

**ABSTRACT**

The rapid growth of online lending services (*peer to peer lending*) in Indonesia as part of the *financial technology* (fintech) ecosystem has increased financial inclusion, but at the same time accompanied by a high risk of digital fraud and the rise of illegal platforms. The characteristics of fully digital services, minimal face-to-face interaction, and reliance on remote verification make online loan applications very vulnerable to various forms of fraud, such as identity theft, account abuse, *synthetic identity*, and *loan stacking*. This study aims to assess and compare the effectiveness of biometric security technology, encryption, and AI fraud detection in preventing fraud in online loan applications. The research method used is *a literature review* with a comparative descriptive approach to scientific articles, regulatory reports, and relevant fintech industry publications. The results of the study show that there is no single security technology that is completely effective when applied alone. Biometric technology has proven to be effective in the early stages of authentication to prevent identity misuse, encryption serves as a security foundation in protecting data confidentiality and integrity, while AI fraud detection demonstrates the most comprehensive effectiveness in detecting and preventing complex and dynamic fraud patterns. This study concludes that a *multi-layer security* approach that combines biometrics, encryption, and AI fraud detection is the most optimal strategy to minimize fraud risk, maintain operational efficiency, improve user comfort, and strengthen the trust and sustainability of the online lending industry in Indonesia.



***Corresponding Author:***
Arianda Manar Rizqiani,
Universitas Muhammadiyah Purwokerto
Email:

## 1. INTRODUCTION

The development of digital technology has encouraged the rapid growth of the *financial technology industry* in Indonesia, especially in online lending services (Jameaba, 2022). According

to the International Trade Administration (2025), the number of fintech players in Indonesia reached nearly 300 companies, supported by the number of internet users in Indonesia continues to show a significant increase in line with the acceleration of national digital transformation. Data from the Indonesian Internet Service Providers Association (APJII) notes that in 2025 the number of internet users in Indonesia will reach around 229.43 million people, or equivalent to 80.66% of the total population, an increase from around 221.56 million users (79.5%) in 2024.

Technology is developing in all aspects, one of which is in loan services that were previously conventional, now have innovated with online lending technology. Data from the Financial Services Authority (OJK) shows that the outstanding value of online loan financing continues to increase significantly, reaching around IDR 77.02 trillion at the end of December 2024, an increase of around 29.14% on an annual basis compared to the previous year, this shows the increasing role of lending services in Indonesia's digital financial ecosystem. Another OJK report noted that in February 2025, *outstanding* P2P lending financing increased by around 31% (yoy) to around IDR 80.07 trillion, indicating rapid expansion amid growing demand for digital credit.

This phenomenon is in line with the increasing trend of national financial inclusion. The adoption of *fintech* services is also driven by smartphone penetration and wider internet access, which according to industry research is projected to reach tens of millions of users in Indonesia and is one of the main drivers of online loan growth (Rebecca, 2025). Meanwhile, statistical reports show that the productive age group of 19-34 years dominates the use of online lending services, this reflects that segments of society that are adaptive to digital technology are the largest contributors to online credit demand (Sindi, 2025).

Financial digitalization allows the process of applying for and disbursing loans to be done quickly, easily, and without geographical restrictions. This condition is in line with efforts to increase national financial inclusion, where people who previously had difficulty accessing conventional banking services can now obtain access to credit through digital applications. Ease of access, speed of service, and penetration of smartphone use are the main factors that accelerate the adoption of online loans in various levels of society (Firdaus, S. E., & Baidhowi, B, 2025).

However, behind this significant growth, online lending applications also face a high risk of *fraud* and the problem of illegal entities. The Financial Services Authority (OJK) recorded tens of thousands of public complaints related to illegal loans throughout 2025, as of August 2025 there were more than 11,600 complaint reports related to illegal online loans received by regulators. Even during the January-October 2025 period, the total number of complaints from illegal financial entities reached more than 20,000 cases, with the majority related to online loans. In the previous period, throughout 2024 there were around 15,162 complaints specifically for illegal online loans (Fadlilah, 2025).

The series of complaints from Ndubuisi (2024) reflects the high frequency of problems experienced by users, such as *identity theft*, unauthorized collection, misuse of personal data, and various forms of manipulation and transaction fraud. Data from the Indonesia Anti Scam Center (IASC) formed by the Financial Services Authority (OJK) together with the Task Force for the Eradication of Illegal Financial Activities (Satgas PASTI) shows that since its launch on November 22, 2024 to November 11, 2025, IASC has received more than 343,000 reports of financial fraud, including various modes of digital fraud against the Indonesian people. The total number of accounts reported related to the scam stands at more than 563,000, with more than 106,000 accounts having been blocked in an effort to handle cases. In the same period, the total report of the loss of public funds due to fraud or *scam* reached around IDR 7.8 trillion based on data collected by the PASTI Task Force (Saputra, 2025).

In addition, previous data developments also indicate that IASC received hundreds of thousands of other financial fraud reports throughout the 20242025, from November 2024 to October 2025 alone, more than 323,000 *scam* reports were recorded with total reported losses of around IDR 7.5 trillion (PPATK, 2025). These data show how serious and widespread the threat of digital financial fraud is in Indonesia, which involves various modes including identity abuse, fake transactions, and online financial service fraud.

The characteristics of online loan services that are fully digital, minimal face-to-face, and rely on remote verification make them easy targets for cybercriminals, including illegal platform operators who continue to emerge despite the continued blocking efforts by regulators. Data from the Financial Services Authority (OJK) shows that throughout 2025, the Task Force for the Eradication of Illegal Financial Activities (Satgas PASTI) has identified and closed thousands of illegal online lending entities. From January to September 30, 2025, the OJK managed to close 1,556 illegal online lending entities and 274 illegal investment offers that have the potential to harm the public on various digital sites and applications (Estherina, 2025). In the same period, the monitoring system also detected tens of thousands of phone numbers connected to illegal activities related to online billing and lending. In different periods, the OJK also noted that from 2017 to early 2025, a total of more than 12,000 illegal financial entities were stopped, of which around 10,197 were illegal online lending entities operating without official licenses (Saputra, 2025).

The phenomenon of this illegal platform not only causes direct financial losses to users, but also erodes public trust in the *fintech lending industry* as a whole. The Indonesian Joint Funding Fintech Association (AFPI) even estimates that the scale of illegal financing far exceeds that of officially registered online loans, with an estimated outstanding figure of illegal financing reaching between Rp 230 trillion to Rp 260 trillion, compared to around Rp 80 trillion for legal platforms in mid-2025 (Isaac, 2025). The high cases of fraud and illegal platform operations not only cause financial losses to fintech companies and users, but also threaten the stability and reputation of the fintech industry as a whole. This far-reaching impact suggests that without more effective digital security and regulatory mechanisms, online lending services are vulnerable to exploitation by criminal actors who take advantage of digital verification loopholes and internet anonymity.

In this context, digital security is a crucial factor in maintaining user trust in online loan applications. Trust is the main foundation in digital financial services, without a reliable security system, users will be hesitant to hand over personal data or make financial transactions. Based on international reports on fintech, data security is one of the most important factors that users consider before using digital financial services, with the majority of respondents considering data protection as a key requirement for their involvement in fintech services. This data shows that strong security is directly related to the level of consumer usage and loyalty to digital financial services (Bodorin & Ciobanu, 2026).

FinTechs process and store sensitive information such as personal data, transaction history, and financial details of users, so that the security vulnerabilities of the system directly contribute to the increased risk of financial fraud, identity theft, and transaction manipulation (Oladinni, A., & Odumuwagun, 2025). The fintech sector has a higher level of exposure to cyberattacks than traditional financial institutions, so weaknesses in authentication and data protection mechanisms are key factors in the occurrence of digital fraud (Ali et al., 2024).

In this context, research from Devaraj (2024) shows that the application of digital security technology has a significant effect on reducing fraud rates. The study of Yusop et al (2025) found

that the use of biometric authentication, such as fingerprinting and facial recognition, effectively reduces fraud based on credential theft and fake accounts because biometric characteristics are difficult to forge and cannot be shared like passwords. Research shows that the application of *end-to-end* data encryption is able to reduce the risk of data misuse and transaction manipulation by ensuring the confidentiality and integrity of information, even when there is an interception attempt by unauthorized parties (Prosper, 2025). Thus, biometrics and encryption not only serve as a technical security mechanism, but also play a direct role in breaking the initial chain of financial fraud in fintech services.

AI fraud detection has also been seen as one of the most effective solutions in detecting suspicious transaction behavior. AI-based systems can learn user behavior patterns and distinguish normal activity from potentially fraudulent activity, so it can flag or block suspicious transactions before losses occur. The use of AI in fraud detection is also reported to be able to significantly reduce certain fraud cases, especially those that are automated or repetitive (Bello et al., 2023).

However, each digital security technology has different characteristics, advantages, and limitations in dealing with different types of fraud on online loan services. Biometric technology has proven to be effective in protecting user authentication processes and preventing unauthorized access, but it still faces challenges in the case of *deepfake-based fraud* and artificial intelligence-based identity engineering (Siryeh et al., 2025). On the other hand, robust encryption technologies are able to protect the confidentiality and integrity of user data and financial transactions, but their implementation requires complex system architecture and strict cryptographic key management so as not to create new security loopholes (Olaiya et al., 2024).

Artificial *intelligence* (AI) technology in *fraud detection* offers more adaptive analysis capabilities to complex and dynamic fraud patterns (Ahmad, 2023). AI can identify transaction anomalies and suspicious user behavior, but its effectiveness is highly dependent on the availability of large, quality, and representative datasets (Kumar, 2024).

Without adequate data, AI models risk producing high levels of *false positives* or *false negatives* and can disrupt the user experience and reduce trust in the system (Habbal et al., 2024).

This condition shows that no single technology is able to provide comprehensive protection against the entire spectrum of digital fraud. Therefore, a deep understanding of the strengths and limitations of each technology is essential for online loan service providers in designing effective security strategies.

In addition to technology and regulatory aspects, the level of digital literacy and financial literacy of users also plays a crucial role in the effectiveness of fraud prevention in online lending services. Reports show that most victims of digital fraud come from a group of users who have limited understanding of data security, the risks of sharing personal information, and the ability to distinguish between legal and illegal online lending platforms. This low literacy is often taken advantage of by fraudsters through social engineering techniques that are difficult to detect with technology alone.

This research is important to be conducted in the midst of the rapid growth of online lending services that have not been fully balanced with a comprehensive understanding of the relative effectiveness of various digital security technologies. In the midst of increasing fraud threats and user data protection demands, a study is needed that is able to provide a comparative picture of the most effective and relevant security technologies to be applied to online lending applications. The results of this research are expected to contribute to strengthening the fintech security system, improving user literacy, and maintaining the trust and sustainability of the online lending industry in Indonesia.

**Research Problems**

As fraud threats in online lending services increase, various digital security technologies have been developed and implemented by fintech providers to protect systems as well as user data. Technologies such as biometrics are used to strengthen authentication and prevent identity abuse, encryption is applied to maintain the confidentiality and integrity of user data, while AI fraud detection is utilized to automatically detect suspicious transaction patterns. This diversity of technology shows the seriousness of the fintech industry in responding to increasingly complex security risks. However, academic research that discusses the effectiveness of security technology is still fragmented. Some studies focus more on the technical aspects of biometrics in user authentication, while others focus on the power of encryption to protect data, or on AI's ability to detect fraud predictively. This partial approach has led to a lack of a comprehensive picture of the comparison of the effectiveness of security technologies in the context of comprehensive fraud prevention.

There have not been many systematic studies to compare the effectiveness of biometric, encryption, and AI fraud detection technologies directly within one analytical framework, while each technology has different goals, mechanisms, and limitations, so its effectiveness in preventing fraud depends on the context of its application. In the absence of a comparative study, fintech developers and regulators have the potential to face difficulties in determining which security technology is the most appropriate or what combination of technologies is most optimal to implement.

The context of online lending applications as a high-risk fintech sector is still relatively rarely used as the main focus in digital security comparative research. Some digital security studies are still general or focus on the conventional banking, e-commerce, or digital payment system sectors, which have different risk characteristics than online loans, while online loans have a higher level of vulnerability to fraud due to remote verification processes, fast transactions, and large-scale use of personal data. Based on these conditions, it can be concluded that there is a significant research gap (*gap phenomenon)* related to the need for a systematic study that compares the effectiveness of biometric security technologies, encryption, and AI fraud detection specifically in the context of online loan applications. This gap underlies the importance of this research, to provide a comprehensive and literature-based understanding of the most effective security technologies in preventing fraud and supporting the trust and sustainability of the online lending industry.

## Research Objectives

### General Purpose

The general purpose of this study is to assess and compare the effectiveness of various digital security technologies commonly used in the fintech industry, especially in online lending applications, in an effort to prevent digital fraud, as well as to provide information and education to the public who will make online loans to better understand the level of security of services, risks that may be faced, and how to protect their personal and financial data. This research focuses on three main technologies, namely biometric technology, data encryption, and AI fraud detection, in order to obtain a comprehensive overview of the roles, strengths, and limitations of each technology in the context of high-risk fintech.

### Special Purpose

1. Analyze the role and working mechanism of biometric technology in preventing identity misuse and unauthorized access to online loan applications.

2. Assess the effectiveness of data encryption technology in protecting users' personal data and transactions from the risk of data leakage, theft, and manipulation.
3. Evaluate the ability of AI fraud detection technology to automatically detect and prevent various fraud patterns in online loan services.
4. Compare the effectiveness of biometric technology, encryption, and AI fraud detection comprehensively in the context of online loan applications that have a high level of fraud risk.
5. Identify potential combinations of optimal digital security technologies to improve system protection while maintaining user efficiency and convenience.

**Research Benefits**

**Theoretical Benefits**

1. Adding and enriching the scientific literature in the field of digital security and fintech fraud prevention, especially in the online lending sector.
2. Provide a comparative perspective on biometric security, encryption, and AI fraud detection technologies that have been studied more partially or separately.
3. It becomes a conceptual and academic reference for further research that discusses the security of digital financial systems, especially those focusing on high-risk fintech services.

**Practical Benefits**

1. Providing strategic insight for fintech developers in designing and implementing an effective and efficient online loan application security system.
2. Assist regulators and policymakers in drafting science-based fintech digital security policies, guidelines, and standards.
3. Assist in determining the most optimal combination of security technologies according to the characteristics of fraud risk in online loan services.
4. Supporting increased user trust and convenience, through the application of security technology that is able to protect personal data and transactions without reducing the ease of use of the application.

**Literature Review**

Fintech is the use of digital technology to improve the efficiency and automation of financial services, including financing and risk management (Rahman & Fasa, 2024). One form that is growing rapidly is online lending (P2P lending) which is driven by easy access to credit, minimal requirements, and the use of digital data, and in Indonesia is strengthened by increasing financial inclusion and internet penetration (Rustan, 2025). However, the characteristics of being fully digital and dependent on automated systems make online lending a high-risk financial service with vulnerability to cybersecurity threats and digital fraud (Arifin, 2025). Fraud in Online Loans

Fraud in online lending is a major challenge for the fintech industry which is increasing along with the complexity of digital transactions (Caseba & Dewayanto, 2024). Common forms of fraud include the idea of*identity theft, account takeover, synthetic identity fraud,* and *loan stacking* that take advantage of digital verification loopholes and internet anonymity so that they are difficult to detect (Lestari, 2025). The impact is not only in the form of financial losses, but also loss of user trust as well as increased legal and reputational risks that can threaten the sustainability of the fintech business (Kusuma et al., 2025).

To mitigate the risk of fraud, online lending applications apply digital security technologies such as biometrics, encryption, and AI fraud detection. Biometrics are effective in user authentication

because they use biological characteristics that are difficult to counterfeit (Jannah et al., 2024), while encryption acts as the foundation of information security by protecting the confidentiality and integrity of data even though it does not directly prevent fraud (Salsabila, 2025). AI fraud detection complements both technologies with the ability to detect fraud patterns automatically, especially in complex frauds such as *loan stacking* and *synthetic identity* (Prayoga & Voutama, 2024)

## 2. METHOD

### Types of Research

This study uses *the literature review method* with a comparative descriptive approach. This method was chosen because the research focuses on the analysis and comparison of concepts, working mechanisms, and the effectiveness of various digital security technologies, namely biometrics, encryption, and AI fraud detection in preventing fraud in online loan applications. The literature review is considered very relevant because it allows researchers to gain a comprehensive understanding based on empirical and conceptual findings from previous research without having to access sensitive and limited primary data in the fintech industry, especially related to user data and financial transactions.

### Data Sources

The data sources in this study are secondary data obtained from various trusted references, including articles in national and international scientific journals that discuss fintech, digital security, and fraud prevention. The research also uses official reports published by the government, financial regulators, and the fintech industry, such as supervisory authority reports, fintech association publications, and annual reports of related institutions. The use of these sources aims to ensure the accuracy, credibility, and relevance of the data to the context of online loans in Indonesia.

### Data Collection and Data Analysis Process

The process of collecting and analyzing data is carried out systematically through literature studies by browsing articles and scientific documents from databases such as Google Scholar, Scopus, and national journal portals using keywords related to fintech, online lending, fraud, biometrics, encryption, and AI *fraud detection*. The articles obtained were then selected based on topic suitability, publication period, context relevance, and methodology quality, then the data was analyzed in depth to identify the roles, advantages, and limitations of each digital security technology, as well as compare the effectiveness of biometrics, encryption, and AI *fraud detection* in preventing various types of fraud on online loan applications, thereby resulting in synthesis and comparative conclusions relevant to the context of high-risk fintech.

## 3. RESULTS AND DISCUSSION

### Results Analysis

Based on the results of a literature review of various previous studies, it can be concluded that there is no single digital security technology that is completely the most effective independently in preventing fraud in online loan applications. Each technology, such as biometrics, encryption, and AI fraud detection has a different level of effectiveness depending on the type of fraud faced and the stage of the online loan service process. Biometric technology has proven to be effective in preventing fraud in the early stages, especially related to *identity theft* and unauthorized access,

because it increases the accuracy of user authentication through unique and difficult to replicate biological characteristics, thereby reducing *the false acceptance* rate and cutting off the initial path of fraud based on credential theft (Shaheed et al., 2024). Encryption plays a fundamental role in maintaining the confidentiality and integrity of user data and financial transactions, both during storage and transmission, by reducing the risk of data leakage and manipulation even if fraud is not directly detected (Zhang & Lin, 2024). Meanwhile, *artificial intelligence* (AI) technology in *fraud detection* shows the highest effectiveness in identifying complex and dynamic fraud patterns, such as *loan stacking* and *synthetic identity fraud*, through the ability to analyze large-scale data and adapt to new patterns, making it the most comprehensive component in digital fraud prevention (Bello et al., 2023).

## Discussion

### Effectiveness of Technology Based on Scale of Use

In the context of small-scale online loan applications, the application of biometric technology and basic encryption is considered quite effective and efficient. At this stage, the main focus is on preventing unauthorized access and protecting user data with relatively affordable implementation costs. The use of AI fraud detection at this scale is still limited because it requires larger data infrastructure and computing resources (Thomas & Santoso, 2025). At medium scale, a combination of biometrics, encryption, and AI fraud detection is starting to become a necessity. AI is used to monitor transaction patterns and user behavior more systematically, while biometrics and encryption remain a fundamental layer of security (Ogunwobi, 2025). This combination allows for a significant reduction in fraud risk without sacrificing service speed (Ogunmokun et al., 2022). In large-scale online lending applications with high transaction volumes and wide risk exposure, the application of machine learning-based AI fraud detection is crucial (Njoku et al., 2024). At this scale, biometrics serve as an initial authentication gateway, encryption ensures data security throughout the transaction cycle, and AI acts as a continuous monitoring system capable of detecting and responding to threats (Shetiya, 2024).

### Optimal Combination of Security Technologies

This discussion emphasizes that the *layered security* approach is the most optimal strategy in the context of online lending. The combination of biometrics for identity authentication, encryption for data protection, and AI fraud detection for dynamic fraud detection and prevention is able to create a security system that balances the level of protection and operational efficiency (Aziza & Wardhani, 2025). This combinatorial approach not only improves system security, but also supports process efficiency by reducing manual intervention and user convenience, as authentication and fraud monitoring can be done automatically without hindering the user experience. Ultimately, an effective and efficient security system contributes directly to increased user trust, which is a key factor for the sustainability and reputation of online lending apps amid increasingly fierce fintech industry competition.

### Research Recommendations


**Figure 1. Research Recommendations**

Based on the results of the analysis and discussion, the author recommends the implementation of a layered digital security strategy as the most effective approach in preventing fraud in online loan applications. This recommendation is aimed mainly at online loan service providers as system managers, regulators and policymakers such as the Financial Services Authority (OJK) in formulating digital security standards, as well as system developers and technology providers in designing secure and adaptive application architectures.

The author recommends that developers of online lending applications make biometric technology as an initial authentication standard, especially in the user registration and login process. The implementation of biometrics can significantly reduce the risk of identity theft and the use of fake accounts, while also increasing user convenience by reducing reliance on conventional passwords. Data encryption needs to be applied comprehensively across the entire data management cycle, both when it is stored and transmitted. The authors recommend the use of standardized and proven encryption algorithms to ensure the protection of users' personal data and financial transactions. This step is important not only to prevent data leaks, but also to meet the demands of compliance with data protection regulations and increase public trust in online lending platforms.

For platforms with medium to large transaction volumes, it is recommended to implement AI fraud detection based on *adaptive machine learning* and supported by human evaluation to minimize detection errors. Regulators and policymakers need to push for minimum security standards that include biometrics, encryption, and AI proportionately at the scale of fintech providers through adaptive and risk-based regulation. The next research is suggested to develop empirical studies based on primary data and explore the integration of new technologies, such as blockchain and *zero trust architecture* to strengthen fintech security in a sustainable manner.

## 4. CONCLUSION

This study compared the effectiveness of biometric security, encryption, and AI fraud detection technologies in preventing fraud in online lending applications through a literature review, and found that no single technology is completely effective when applied alone. Biometrics are effective in preventing identity-based fraud and unauthorized access in the early stages, encryption plays an important role in protecting the confidentiality and integrity of data even if it does not detect fraud directly, while AI fraud detection is the most comprehensive in detecting and preventing complex fraud patterns. Therefore, a multi-layered security approach that combines these three technologies

is considered the most optimal strategy to minimize fraud risk, maintain user efficiency and convenience, and increase trust and sustainability of the online lending industry in Indonesia.

This research has limitations, because it only focuses on technological factors that include biometric technology, encryption, and *artificial intelligence* (AI). Further research is suggested to add other factors in the digital technology industry that could potentially contribute to the prevention of online fraud. In addition, this study only examines the context of online lending services, so that future research can expand the scope to other digital behavioral contexts, such as online buying and selling transactions and other digital services.

## 5. REFERENCES

Arifin, S. (2025). Challenges and Opportunities Faced by Banks in Facing the Digital Financial Era. Persya: Journal of Sharia Banking, 3(1), 27-33.

Indonesian Internet Service Providers Association. (2025). *APJII Internet Survey 2025*. APJII survey. https://survei.apjii.or.id/

Ahmad, A. S. (2023). Application of big data and artificial intelligence in strengthening fraud analytics and cybersecurity resilience in global financial markets. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, *7*(12), 11-23.

Ali, G., Mijwil, M. M., Buruga, B. A., & Abotaleb, M. (2024). A comprehensive review on cybersecurity issues and their mitigation measures in FinTech. *Iraqi Journal for Computer Science and Mathematics*, *5*(3), 12.

Aziza, N., & Wardhani, D. F. (2025). Mobile Banking Application Security Evaluation: Threats, Protection and Case Studies on Digital Banking Systems. Scientific Journal of Information Technology and Robotics, 7(1), 11–22.

Bello, O. A., Ogundipe, A., Mohammed, D., Adebola, F., & Alonge, O. A. (2023). AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities. European Journal of Computer Science and Information Technology, 11(6), 84–102.

Bello, O. A., Ogundipe, A., Mohammed, D., Adebola, F., & Alonge, O. A. (2023). AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities. European Journal of Computer Science and Information Technology, 11(6), 84–102.

Bodorin, B. E., & Ciobanu, E. (2026). AI, security, and trust in the digital wallet: Evidence from current Romanian FinTech users. International Journal of Financial Studies, 14(1), 1. https://doi.org/10.3390/ijfs14010001

Caseba, F. L., & Dewayanto, T. (2024). The application of artificial intelligence, big data, and blockchain in fintech payments to computer fraud risk: A systematic literature review. Diponegoro Journal of Accounting, 13(3).

Devaraj, S. M. (2024). Next-Generation Fraud Detection: A Technical Analysis of AI Implementation in Financial Services Security. *International Journal for Multidisciplinary Research (IJFMR), 6*(6).

Estherina, I. (2025, October 12). Indonesia's OJK shuts down 1,556 illegal loan apps and 284 investment scams.

Asia-Pacific Solidarity Network. https://www.asi A-Pacific C-solidarity.net/news/202 5-1 0-12/IndonesiaSOJKshut S-Dow N-155 6-Long L-Loa N-App S- AN, D-28, 4-

Investmen, T-scams.htm L

Fadlilah, R. (2025). Online Loans in Financial Services Authority Regulation Number 40 of 2024 concerning Information Technology-Based Joint Funding Services from the Perspective of Maqāṣid Sharīʿah (Doctoral dissertation, IAIN Ponorogo).

Firdaus, S. E., & Baidhowi, B. (2025). Digitalization of Banking and MSME Access: Legal Opportunities and Challenges. Academic Journal of Economics and Management, 2(2), 109–113.

Habbal, A., Ali, M. K., & Abuzaraida, M. A. (2024). Artificial Intelligence Trust, risk and security management (AI trism): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*, *240*, 122442.

International Trade Administration. (2025, November 17). *Indonesia — Financial Services (Financial Technology)*. U.S. Department of Commerce. https://www.trade.gov/country-commercia l-guides/indonesiaafinancialservice s-financia l-technolog y

Isaac, J. (2025, 12 August). Association raises alarm over massive circulation of illegal online loans. Indonesia Business Post. https://indonesiabusinesspost.com/4974/market S-an D-finance/associationraise s-alar m-ove r-massiv e-circulatio n-o f-illega l-onlin eloans

Jannah, M., Hidayat, M. F., Agustiyyani, M., Buana, P. W., & Purwani, F. (2024). Implementation of Biometric Authentication to Improve Security and Privacy of Digital Wallet Users. Journal of Scientech Research and Development, 6(2), 531–539.

Jameaba, M. S. (2022). Digitalization, Emerging Technologies, and Financial Stability: Challenges and Opportunities for the Indonesian Banking Industry and Beyond. *DOI: https://doi. org/10.32388/CSTTYQ, 2*.

Kusuma, A. C., Lois, A., Thessaloniki, L., Darosyifa, T., & Evelin, A. (2025). Legal Implications for the Stability of the Digital Finance Industry and Post-Case Supervision of PT Investree Radhika Jaya. Causa: Journal of Law and Citizenship, 16(1), 1151–1160.

Kumar, P. (2024). AI-Powered Fraud Prevention in Digital Payment Ecosystems: Leveraging Machine Learning for Real-Time Anomaly Detection and Risk Mitigation. *Journal of Information Systems Engineering and Management*, *9*(4).

Lestari, R. A., & Lestari, N. M. (2025). Fraud in the Implementation of Sharia Bank Financing Cards: Challenges and Construction of Legal Protection for Customers. Istikhlaf: Journal of Sharia Economics, Banking and Management, 7(1), 44–66.

Njoku, D. O., Iwuchukwu, V. C., Jibiri, J. E., Ikwuazom, C. T., Ofoegbu, C. I., & Nwokoma, F. O. (2024). Machine learning approach for fraud detection system in financial institution: A web base application. Machine Learning, 20(4), 01–12.

Ndubuisi, A. F. (2024). The intersection of false projections, identity manipulation, and emerging financial cybercrime threats. *INTERNATIONAL JOURNAL OF RESEARCH*, *5*(12), 5529-5546.

Ogunmokun, A. S., Balogun, E. D., & Ogunsola, K. O. (2022). A strategic fraud risk mitigation framework for corporate finance cost optimization and loss prevention.

International Journal of Multidisciplinary Research and Growth Evaluation, 3(1), 783–790.

Olaiya, O. P., Adesoga, T. O., Adebayo, A. A., Sotomi, F. M., Adigun, O. A., & Ezeliora, P. M. (2024). Encryption techniques for financial data security in fintech applications. *International Journal of Science and Research Archive*, *12*(1), 2942-2949.

Ogunwobi, E. (2025). Advancing Financial Security Using Behavioral Biometrics and AI-Driven Authentication. International Journal of Research Publication and Reviews, 6(3), 720–727.

Financial Services Authority. (2025, February 25). Financing institutions, venture capital, fintech P2P lending and micro finance industry update December 2024. OJK International InformationHub.https://institute.ojk.go.id/iru/dataandstatistics/detaildataandstatistics/13379/FinancinG-Institution S-Ventur E-capita L-Fintec H-P2 P-Lendin G-An DMICROfinanc E-Industr Y-updat E-DecembeR-202 4

Oladinni, A., & Odumuwagun, O. O. (2025). Enhancing cybersecurity in fintech: Safeguarding financial data against evolving threats and vulnerabilities. *International Journal of Computer Applications Technology and Research*, *14*(1), 62-78.

Prayoga, A. H., & Voutama, A. (2024). Development of the Bank Account Fraud Detection application using the XGBOOST algorithm. JATI (Student Journal of Informatics Engineering), 8(3), 2916–2922.

Prosper, J. (2025). Next-Gen Data Protection in Digital Transformation: A Sector-Wise Review of Encryption, Database Security, and API Threat Mitigation.

Financial Transaction Reporting and Analysis Center [PPATK]. (2025, December 3). Queen Máxima visits Indonesia as UNSGSA, emphasizes fight against "scams". PPATK. https://www.ppatk.go.id/news/read/1578/ratumximSão Pauloi-Indonesiaa-São Pauloi-S.S.a-tekankan-Wari-scam.html

Rahmah, A. T., & Fasa, M. I. (2024). The Influence of Digital Transformation and Financial Technology (Fintech) Development on Islamic Banking Service Innovation. Journal of Academic Media, 2(10).

Rebecca. (2025). Indonesia Digital Lending & P2P Platforms Market (Report No.6209380). Ken Research / Research and Markets. https://www.researchandmarkets.com/reports/6209380/indonesia-DigitaLlendin G-An D-P2 P-Platform S-Marke T

Rustan, D. M. (2025). The Role of Financial Technology (FinTech) in Increasing Financial Inclusion in Indonesia. Collaborative Journal of Science, 8(1), 928–936.

Salsabila, N. (2025). Analysis of Accounting Information System (SIA) Control of Data Security and Accounting Information. Edutik: Journal of Information and Communication Technology Education, 5(4), 1004–1012.

Siryeh, F. A., Alrammahi, H., & Abdu İbrahim, A. (2025). Tamper Detection in Multimodal Biometric Templates Using Fragile Watermarking and Artificial Intelligence. *Computers, Materials & Continua*, *84*(3).

Saputra, F. (2025, March 14). Samir: The existence of illegal loans has a negative impact Industry Fintech lending Cash. https://keuangan.kontan.co.id/news/sami r-existence n-

pinjo l-ilegalberdampa k-negati f-terhada p-industr i-fintec h-lendin g

Saputra, F. (2025, November 18). Task Force Definite: Losses due to fraud reach Rp 7,8 trillions per 11 November 2025.Cash.https://keuangan.kontan.co.id/news/satga S-Past I-Loss N-Akiba TPenipuNCAPA I-R P-7 8-Triliu N-PE R-1 1-Novembe R-2025

Shaheed, K., Szczuko, P., Kumar, M., Qureshi, I., Abbas, Q., & Ullah, I. (2024). Deep learning techniques for biometric security: A systematic review of presentation attack detection systems. Engineering Applications of Artificial Intelligence, 129, 107569.

Shethiya, A. S. (2024). AI-Enhanced Biometric Authentication: Improving Network Security with Deep Learning. Nexus Journal Academy, 3(1).

Sindi. (2025, June 11). Pinjol users in Indonesia are dominated by the age of 19 to 34 years. Medan.Mediakeuangan.id. https://medan.mediakeuangan.id/detail/296564/penggun A-Pinjo LD I-Dominas I-USI A-1 9-hing G-3 4-Tahu N

Thomas, S. T., & Santoso, E. H. (2025). Machines That Think, Data That Tells: The Artificial Intelligence Revolution in the World. Global Creative Media.

Yusop, M. I. M., Kamarudin, N. H., Suhaimi, N. H. S., & Hasan, M. K. (2025). Advancing passwordless authentication: A systematic review of methods, challenges, and future directions for secure user identity. *IEEE Access*.

Zhang, W., & Lin, H. (2024). Evaluating the Role of Encryption Standards in Supporting Long-Term Information Assurance in Data Storage and Transmission. Journal of Computational Intelligence, Machine Reasoning, and Decision-Making, 9(9), 1–25.