JOURNAL OF LEGAL AND SOCIAL CHANGES
Scientia Plus Corp
P-ISSN: 00000
E-ISSN: 00000

AI Integration in Financial Institutions: Implications for Transparency and Data Security

Ihsan Risqi Satria Winahyu[1*], Muhammad Daffa Putra Zaman[2], Eka Imam Utomo[3], Muhammad Happy Marcelino[4], Dani Reza Aprilian[5]

[12345] Faculty Of Law and Political Science, Muhammadiyah University Surakarta, Sukuharjo, Central Java, 57169, Indonesia
*c100230112@student.ums.ac.id

Article

Keywords: Financial Instituions, Artificial Intelligence, Banking.

Article History
Received: 17/12/2025
Reviewed: 20/12/2025
Accepted: 29/01/2026
Published: 31/01/2026

Abstract

This study was conducted to determine the effectiveness of fraud detection in the banking and financial technology (fintech) sectors. With the presence of a new innovation such as Artificial Intelligence (AI), it is expected to be able to analyze the impact of integration on the operational transparency of financial institutions and identify potential risks and challenges of data security due to the use of AI, as well as to develop recommendations for governance and regulatory strategies that support the ethical and safe implementation of AI. This method uses a normative juridical approach with a descriptive-analytical nature to examine the protection of personal data in the use of artificial intelligence (AI) for fraud detection in the banking and fintech sectors. The normative approach is a review of the legal and ethical aspects of customer data protection. AI integration can increase efficiency and accuracy in financial processes, including detecting fraud and risk management. The application of AI can create potential vulnerabilities to data security due to the use of big data and automated algorithms. The transparency of this AI system is still a focus of challenges because many algorithms are still black box (not easy to understand). Stricter regulations and data security standards are needed so that the application of AI does not harm customers. The purpose of this research is to inform policymakers' considerations in formulating AI regulations in the financial sector, and to provide financial institutions with insights into strengthening their technology transparency and security systems. This research provides a novel approach, presenting an integrated analysis of AI technology, transparency, and customer data security within the context of Indonesian financial institutions. Combining legal and technological approaches provides an ethical perspective on AI

implementation, which has previously focused solely on technical aspects.

INTRODUCTION

The development of digital technology over the past five years has had a significant impact on the banking and financial technology (fintech) sectors. One key innovation is the use of Artificial Intelligence (AI), which can rapidly process large amounts of data, thereby improving operational efficiency, providing more personalized services, and strengthening transaction security systems. AI integration is considered a strategic factor capable of driving digital transformation in the financial industry, particularly in addressing the increasingly complex dynamics of online transactions (Putra & Andriani, 2019).

In the context of digital financial services, one of the most prominent applications of AI is fraud detection. The rapid growth of electronic transactions has not only increased customer convenience but also opened up opportunities for cybercriminals to commit fraud, data theft, and transaction manipulation. AI, through machine learning and deep learning, can analyze transaction patterns, identify anomalies, and provide early warnings of suspicious activity. This technology offers advantages over traditional methods, which are often slow and not adaptive to new fraud patterns (Santoso & Hidayat, 2020; Wulandari et al., 2022).

However, the adoption of AI in fraud detection poses several challenges closely related to algorithm transparency and data security. First, in terms of transparency, AI algorithms are often viewed as black boxes because it is difficult to explain the reasoning behind their decisions. This raises ethical and regulatory questions: how can banks or fintech providers explain to customers why certain transactions are deemed risky or declined? Without transparency, public trust in digital financial institutions can erode (Hidayat & Supriyanto, 2021). Second, in terms of security, the use of AI requires access to big data, which includes sensitive information such as personal identity, transaction history, and consumer behavior. This vast amount of data is highly vulnerable to leaks, theft, and misuse, both by internal and external parties. Therefore, the implementation of AI must be balanced with a multi-layered security system, ranging from encryption and multi-factor authentication to compliance with data protection regulations (Handayani et al., 2023).

Recent research in Indonesia demonstrates the importance of striking a balance between technological innovation and regulatory aspects. Wulandari et al. (2022)

emphasize that AI has been proven to improve the accuracy of fraud detection, but policies that guarantee explainability to prevent system bias are still needed. Meanwhile, Handayani et al. (2023) highlight the urgency of implementing strict cybersecurity standards, as cyberattacks against digital banks are increasing. This aligns with global findings that the main challenge to AI adoption in the financial sector is maintaining the technology's trustworthiness, namely the reliability of the systems used.

1.2 Formulation of the Problem

1. What are the regulations regarding fraud detection?
2. What is the role of Artificial Intelligence (AI) in detecting transaction fraud?

1.3 Previous Research

The integration of artificial intelligence (AI) into the financial sector has become a subject of increasing research interest in recent years. Previous studies have paved the way for understanding the impacts, opportunities, and challenges of this digital transformation. To map the foundation for this research, the literature review will be grouped into three main themes: studies supporting the potential of AI, studies addressing challenges, and studies offering framework solutions.

A. Research on the Potential and Benefits of AI in Finance A substantial body of literature has confirmed the strategic value of AI. A study by Chen et al. (2021) emphasized the role of AI in transforming risk management and fraud detection, where machine learning algorithms demonstrated significantly higher accuracy than traditional methods. This study successfully illustrated how AI could save financial institutions billions of dollars by preventing fraud. On the other hand, research by Dhar & Stein (2017) discussed the application of AI in customer service through chatbots and virtual assistants, which have been shown to increase customer satisfaction while reducing operational costs. However, both studies focused more on efficiency and economic aspects without exploring the ethical and data security implications in depth.
B. The Role of Artificial Intelligence in Detecting Financial Fraud AI in the ACL Analytic program can accelerate the audit process, prevent and detect financial statement fraud, and analyze large amounts of data more quickly and accurately than conventional methods. This study found a user-centered explanation for a financial fraud detection model using explainable artificial intelligence (XAI) methods. By integrating a group predictor model with an explainable framework based on the Shapley principle, the researcher developed a method for detecting financial fraud that is both precise and explainable. This study shows that the explainable framework can provide both local and global explanations, meeting the needs of various external

stakeholders. This study did not find the root cause of fraud; instead, it found the root cause of ML predictions with desirable theoretical characteristics. Accounting experts can then observe these explanations for further analysis.

C. Zhou et al. (2023) This study found a user-centered explanation for a financial fraud detection model using explainable artificial intelligence (XAI) methods. The researchers developed a precise and explainable financial fraud detection method by combining a group predictive model with an explainable framework based on Shapley values. This study demonstrated that the explainable framework can provide both local and global explanations, meeting the needs of various external stakeholders. This study did not find the root cause of fraud; instead, it found the root cause of ML predictions with desirable theoretical characteristics. Accounting experts can then observe these explanations for further analysis.

METHOD

This research uses a normative-juridical approach with a descriptive-analytical nature to examine personal data protection in the use of artificial intelligence (AI) for fraud detection in the banking and fintech sectors. The scope of the research includes a review of national laws and regulations, such as the Personal Data Protection Law, the Banking Law, the ITE Law, and regulations from the Financial Services Authority (OJK) and Bank Indonesia (BI), as well as international legal instruments such as the GDPR, OECD guidelines, and relevant global AI regulations. The research data consists of primary legal materials (laws, regulations, authority guidelines), secondary legal materials (academic literature, law journals, industry reports, and authoritative studies on AI and data protection), and tertiary legal materials (legal dictionaries, encyclopedias, and regulatory indexes).

RESULTS AND DISCUSSION

2.1 Fraud Detection Regulations in the Indonesian

Legal System Fraud detection regulations in Indonesia do not exist within a single, specific regulation but are spread across various regulations governing the financial, information technology, and data protection sectors. The goal is to ensure that all activities related to electronic systems, financial transactions, and data management are conducted securely, transparently, and free from potential fraud. In the Indonesian legal system, fraud detection encompasses many important aspects regulated by various regulations, particularly in the financial and healthcare sectors. Financial Services Authority (OJK) Regulation Number 12 of 2024 establishes an Anti-Fraud Strategy for Financial Services Institutions, consisting of four main pillars: prevention, detection, investigation and reporting, sanctions, and monitoring and evaluation. Financial services institutions must implement a fraud detection system. They must also enhance the knowledge of relevant internal and external parties and establish a dedicated unit to implement the anti-fraud strategy in accordance with the complexity of the business. In the Indonesian legal system, fraud detection encompasses many important aspects regulated by various regulations, particularly in the financial and healthcare sectors.

Financial Services Authority (OJK) Regulation Number 12 of 2024 establishes an Anti-Fraud Strategy for Financial Services Institutions, which consists of four main pillars: prevention, detection, investigation and reporting, sanctions, and monitoring and evaluation. FSIs must implement a fraud detection system. They must also enhance the knowledge of relevant internal and external parties and establish a dedicated unit to implement the anti-fraud strategy according to the complexity of the business. Corruption, asset misappropriation, financial statement fraud, and other violations in accordance with applicable law are examples of regulated fraud types. Minister of Health Regulation Number 16 of 2019 regulates the health sector, particularly the National Health Insurance program, regarding fraud detection and handling.

This regulation regulates fraud prevention and reporting mechanisms in the national social security management system, as well as the authority to impose administrative sanctions on fraud perpetrators, such as warnings and fines. These sanctions are intended to deter individuals and reduce fraud in health insurance management and services. In general, the Indonesian legal system requires mechanisms to prevent fraud, such as internal and external audits, a whistleblowing system, and investigations conducted in accordance with procedures. Investigation results must include recommendations for sanctions and procedural improvements to prevent recurrence of fraud. Furthermore, fraud control guidelines refer to laws related to good governance and the eradication of corruption. Therefore, fraud detection in the Indonesian legal

system is carried out systematically, combining prevention, detection through audits and investigations, reporting, sanctions, and repeated evaluations. This is particularly true for the financial services and healthcare sectors, where there is a strong legal basis and dedicated oversight units within the relevant institutions.

One of the main legal foundations is Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which emphasizes the obligation of electronic system operators to maintain data reliability, security, and integrity. These provisions form the basis for the implementation of a digital surveillance system capable of detecting suspicious activity in electronic networks. Furthermore, Law No. 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU) and OJK Regulation No. 12/POJK.01/2017 concerning the Anti-Money Laundering and Prevention of Terrorism Financing Program also regulate the implementation of a transaction monitoring and customer identity verification system (Know Your Customer). These instruments are essentially the initial implementation of a fraud detection system in the banking sector.

In the government sector, Government Regulation Number 60 of 2008 concerning the Government Internal Control System (SPIP) also emphasizes the importance of preventing and detecting irregularities in the implementation of public activities. This system requires a supervisory mechanism capable of providing early detection of corrupt acts or misappropriation of funds. Furthermore, POJK Number 13/POJK.03/2020 concerning the Use of Information Technology by Commercial Banks stipulates that financial institutions are required to integrate fraud risk management with modern information technology. This means that digital-based supervision is a legal obligation for financial institutions in Indonesia. From these regulations, it is clear that fraud control and detection in Indonesia encompass two important aspects:

A. Prevention through internal supervision, information technology systems, and regulatory compliance; and

B. Repressive action against fraudsters who violate criminal and administrative laws.

In other words, national regulations provide a sufficient legal basis for developing a digital-based fraud detection system that is adaptive to technological changes.

2.2 The Role of Artificial Intelligence (AI) in Fraud Detection Systems

Advances in Artificial Intelligence (AI) have revolutionized fraud prevention and detection methods across various sectors. AI possesses advanced analytical

capabilities for processing large amounts of data, identifying unusual behavioral patterns, and providing early warnings of fraud. In banking and finance, AI is utilized to perform predictive analysis and anomaly detection on customer transaction behavior. This system is capable of rapidly recognizing changes in transaction patterns, such as unusually large transactions or sudden activity from different locations. This allows potential fraud to be identified before it results in significant losses.

In other sectors, such as insurance, e-commerce, and public services, AI is also used to detect identity fraud, data manipulation, and claims misappropriation. Facial recognition, voice verification, and machine learning technologies enable systems to distinguish between legitimate users and fraudsters with high accuracy. However, the use of AI poses challenges, particularly related to personal data protection. AI requires large volumes of data to learn and adapt, increasing the risk of privacy breaches. Therefore, the application of AI in fraud detection must be in line with legal and ethical principles of data protection, so that innovation does not lead to violations of individual human rights.

3. Personal Data Protection in the Use of AI for Fraud Detection

In the context of national law, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) serves as the primary legal umbrella governing the collection, storage, and processing of personal data, including by AI-based systems. This law emphasizes that all data control must have a valid legal basis, uphold the principle of transparency, and respect the rights of data subjects. AI used to detect fraud often processes sensitive personal data such as identity, financial information, and even user location. Therefore, data controllers must:

a. Obtain valid consent from data owners or have a clear legal basis for processing;

b. Implement the principles of purpose limitation and data minimization, using only relevant information;

c. Ensure data security through encryption systems, access control, and cybersecurity audits;

d. Provide data subjects with the right to access, correct, or delete their data when necessary.

In addition to legal compliance, ethical aspects are also crucial in the implementation of AI. AI systems must be free from algorithmic bias that could lead to false detections or discrimination against certain groups. Therefore, every

system requires human oversight and regular audits to ensure its accuracy and fairness. The principles of Privacy by Design and Privacy by Default are also key guidelines. This means that personal data protection must be considered from the design stage of an AI system, not only after the system is operational. This ensures comprehensive user security and privacy without hindering fraud detection functions.

4. Synergy between Fraud Detection and Personal Data Protection

The relationship between fraud detection systems and personal data protection is complementary. These two concepts are inseparable because successful fraud detection relies heavily on the availability of valid data, while public trust in digital systems is crucially determined by guaranteed privacy protection. The ideal approach is to implement a Risk-Based Approach (RBA), where personal data processing is carried out proportionally according to the level of risk. The greater the potential for fraud, the more extensive data analysis can be conducted, while still remaining within legal oversight and the principle of accountability.

Furthermore, collaboration between institutions such as the Financial Services Authority (OJK), the Ministry of Communication and Information Technology (Kominfo), and the National Cyber and Crypto Agency (BSSN) is crucial to ensure the implementation of responsible technology governance (AI governance). The implementation of ethical standards such as algorithm transparency, data protection compliance, and cybersecurity resilience must be mandatory in every AI system. This approach also aligns with international principles, particularly the European Union's General Data Protection Regulation (GDPR), which emphasizes the importance of protecting privacy rights without stifling digital innovation. With this step, Indonesia is moving towards a legal system that balances technological needs with the protection of human rights in the digital realm.

5. Legal, Ethical, and Social Implications

The use of AI to detect fraud has broad legal, ethical, and social implications. Legally, misuse or failure of an AI system that results in data leakage can give rise to criminal or administrative liability in accordance with Articles 57–63 of the Privacy and Data Protection Law. Conversely, algorithmic inaccuracy that results in individuals being falsely accused of fraud can lead to violations of privacy rights and defamation. From an ethical perspective, AI must be operated based on the principles of fairness, transparency, and non-discrimination. The algorithms used must be accountable (explainable AI), so that the resulting decisions are not unilateral and do not create social bias.

Meanwhile, from a social perspective, the accurate and transparent implementation of AI can actually increase public trust in financial institutions and the government. People will feel safer conducting transactions if they know that the system used can detect fraud without violating their privacy. Conversely, if AI systems are implemented without oversight and adequate data protection, this can create resistance and distrust towards digital transformation.

CONCLUSION

Overall, the Indonesian legal system's fraud detection regulations are fundamentally well-founded, despite being scattered across various regulations. The government emphasizes that fraud prevention and enforcement are not solely the responsibility of a single institution, but are a shared responsibility across the financial, healthcare, government, and electronic system providers sectors. Through various legal instruments, such as the Financial Services Authority Regulation (POJK), the ITE Law, the Money Laundering Law (TPPU), and the SPIP (Information and Transaction Reports), the government is pushing for stricter, more transparent, and technology-based oversight to detect irregularities early. Technological developments, particularly Artificial Intelligence (AI), are further strengthening the system's ability to detect fraud. AI can read transaction patterns, recognize unusual behavior, and automatically provide early warnings. This technology has proven effective in minimizing the risk of fraud in the banking, healthcare, insurance, e-commerce, and public service sectors. However, despite these advantages, the use of AI must still address personal data protection and ethical issues. Without clear controls, the use of large amounts of data can create new risks. Therefore, the integration of AI-based fraud detection and national regulations needs to go hand in hand. Indonesia already has an adequate legal basis, but the challenge ahead is how to ensure the oversight system remains adaptive to technological developments, without neglecting the protection of individual rights. Prevention, detection, investigation, and evaluation efforts must be continuously strengthened to ensure Indonesia's digital ecosystem is increasingly secure, accountable, and free from fraudulent practices.

ACKNOWLEDGMENTS

Despite being dispersed among numerous rules, the fraud detection laws of the Indonesian legal system are essentially sound. The government highlights that the financial, healthcare, government, and electronic system providers sectors all have responsibility for preventing and enforcing fraud. The government is advocating for more stringent, transparent, and technology-based oversight to identify irregularities early through a number of legal tools, including the Financial Services Authority Regulation (POJK), the ITE Law, the Money Laundering Law (TPPU), and the SPIP (Information and Transaction Reports).

REFERENCES

Books

Iswanaji, chaidir, et al. *Perkembangan Industri Halal & Penguatan Lembaga Keuangan Syariah*. Indramayu, Penerbit Adab, 2024

Wibowo, Agus. *REGULASI APLIKASI AI (*Artificial *Intelligence)*. Semarang, Yayasan prima agus Teknik, 2025

.

Jurnal

Abdul Hadi & Bima Guntara. (2022). *PEMBAHARUAN HUKUM NASIONAL DALAM UPAYA PERLINDUNGAN DATA PRIBADI DI ERA DISTRUPSI KECERDASAN BUATAN (ARTIFICIAL INTELLIGENCE).* Jurnal Hukum Mimbar Justitia, Vol. 8 No. 1: 233-253.

Achmad Kholiq. (2025). *IMPLIKASI ETIKA DAN HUKUM DALAM TATA KELOLA IMPLEMENTASI AI (ARTIFICIAL INTELLIGENCE) DI SEKTOR KEUANGAN DALAM PERSPEKTIF HUKUM EKONOMI SYARIAH.* Syirkatuna, Vol. 13 No. 1: 1 – 14

Angel Sri Monika Sijabat, Grace Stela Zane Simamora & Leoni Geraldin Br. Simamora. (2025). Peran Kecerdasan Buatan dalam Inovasi Bisnis: Studi Kasus Penerapan AI di Sektor Keuangan dan E-Commerce. No.2, 109-115.

Anggi Putri & Dian Anita Nuswantara. (2025). Artificial Intelligence and Data Mining in Detecting Financial Statement Fraud: A Systematic Literature Review. Journal of Accounting Science, ISSN 2548-3501

An Suci Azzahra. (2025). The Use of Artificial Intelligence (AI) in Fraud Detection by Government Auditors: A Systematic Literature Review. International conference proceedings, Vol.1: 1-15

Arri, H. S. (2022). Real-Time Credit Card Fraud Detection Using Machine Learning. Interantional Journal of Scientific Research in Engineering and Management. https://doi.org/10.55041/ijsrem12659

Asri Juana Seran & Desi Ismah Anggraini. (2025*). Analisis Penggunaan AI dalam Deteksi Kecurangan Laporan Keuangan*. Vol. 03, Hal. 2288-2294

Baker, H. K., Purda, L., & Saadi, S. (2020). Corporate fraud exposed: An overview. Corporate Fraud Exposed: A Comprehensive and Holistic Approach, 3–18. https://doi.org/10.1108/978-1-78973-417-120201002

B. Narsimha et al. (2022). Cyber Defense in the Age of Artificial Intelligence and Machine Learning for Financial Fraud Detection Application. International Journal of Electrical and Electronics Research. Vol.10 (2): 87-92

Chenoori, R. K., & Kavuri, R. (2022). Online Transaction Fraud Detection Using Efficient
Dimensionality Reduction and Machine Learning Techniques. Revue D Intelligence
Artificielle. https://doi.org/10.18280/ria.360415

D.N.Bindu, B.Divya Datta, & A.Bhanu Srikar Reddy. (2023). Credit Card Fraud Detection Using LSTM. International Journal of Scientific Research in Engineering and Management. Vol.7 (3): 2582-3930

Erni Wiriani, Jauharil Maknuni, Esti Alemia Puspita, Masitah Masitah. (2025*).* *Peran Artificial Intelligence dalam Mitigasi Risiko Transaksi Mobile Banking: Tinjauan Governansi dan Etika Data.* No.1: 103-111

Ervian Ridho Mawlidy, Rieswandha Dio Primasatya & Like Lorensa. (2024). *KEMAMPUAN ARTIFICIAL INTELLIGENCE TERHADAP PENDETEKSIAN FRAUD: STUDI LITERATUR.* Jurnal akuntansi dan keuangan, 7, 89-104

Grace Leroy Sinaga, Muhammad Rizky Harahap, Agoestina Mappadang. (2025) Tata Kelola Perusahaan Literatur Komprehensif Tentang Pencegahan Dan Deteksi Penipuan Akuntansi. Jurnal Akuntansi dan Manajemen Vol 23, No 1, 1-10

Lummatul Mahya et al. (2023). INTELLIGENT AUTOMATION OF FRAUD DETECTION AND INVESTIGATION:A BIBLIOMETRIC ANALYSIS APPROACH. Jurnal Reviu Akuntansi dan Keuangan, Vol. 13(3): 588-613

Mohanty, B., Aashima, & Mishra, S. (2023). *Role of artificial intelligence in financial fraud detection*. Academy of Marketing Studies Journal, 27(4), 1–15.

Muhammad Ray Syahronny & Totok Dewayanto. (2024). PENERAPAN TEKNOLOGI ARTIFICIAL INTELLIGENCE DAN BLOCKCHAIN DALAM MENDETEKSI FRAUD PADA PROSES AUDIT:

SYSTEMATIC LITERATURE REVIEW.DIPONEGORO JOURNAL OF ACCOUNTING, Vol.13(3): 1-14

Mukherjee, U., Thakkar, V., Dutta, S., Mukherjee, U., & Bandyopadhyay, S. K. (2021). Emerging Approach for Detection of Financial Frauds Using Machine Learning. Asian Journal of Research in Computer Science. https://doi.org/10.9734/ajrcos/2021/v11i330263

Nurul Ilahi, I Nyoman Budiono. (2024*). PENERAPAN ARTIFICIAL INTELLIGENCE SEBAGAI INOVASI DI ERA DISRUPSI DALAM MENGURANGI RESIKO KEUANGAN*. Jurnal Manajemen dan Keungan Syariah,

Putri Indah Sari Setiawan & Mukhtaruddin. (2024). *IMPLEMENTASI SISTEM PEMBAYARAN REAL-TIME BERTENAGA AI.* Integrative Perspectives of Social and Science Journal, 3064-4011

Rahman, M. M., & Saha, T., "Artificial Intelligence in Financial Services: Opportunities andChallenges," Journal of Banking and Financial Technology 5, no. 1 (2021): 115

Septiriana, R., Rheno Widianto, S., & Darma, P. E. (2024). *Application of artificial intelligence in the prevention of fraud in financial statements.* Jurnal Ekonomi, 13.

Serly Maharani & Moiling Sari. (2025). *Transformasi Digital dalam Layanan PerbankanMenyongsong Era Baru Keuangan Digital.* Jurnal Bisnis dan Manajemen, No.1, 135-150

Silvia Anggraini & Muharom Fatihaturrizqi. (2025*). Konvergensi Teknologi Blockchain danArtificial Intelligence Untuk Meningkatkan Kepercayaan Pelanggan Di Sektor Fintech*. Nomor 1: 1-13

Suci Nurlayli Alimatu Sholiqah, Retno Ayu Widyastuti, & Tri Ratnawati. (2023). Peran Artificial Intelligence Untuk Mendeteksi Fraud Dalam Audit: Sebuah Studi Literatur. JURNAL RISET EKONOMI DAN AKUNTANSI. Vol. 1(4): 226-238

Wulandari, D., Prasetyo, R., & Nugraha, F. (2022). "Analisis Implementasi Deep Learning untuk Deteksi Penipuan pada Transaksi Keuangan Digital." Jurnal Teknologi Informasi dan Komputer, 8(1), 12–25.

Zhou, Y., Li, H., Xiao, Z., & Qiu, J. (2023). *A User-centered explainable artificial intelligence approach for financial fraud detection*. Finance Research Letters, 58, 1-