Analysis of the Impact of Financial Technology on Fraud Behavior

Boyang Chen[1], Fangfei Liu[2] and Ziye Zhang[3*]

[1] School of Accounting, Southwestern University of Finance and Economics, Chengdu, Sichuan, China
[2] School of Finance, Southwestern University of Finance and Economics, Chengdu, Sichuan, China
[3] SILC BUSINESS SCHOOL, Shanghai University, Shanghai, China

*zzy23901111@shu.edu.cn

Abstract. With the rapid development of financial technology (FinTech), the financial system has enhanced transaction efficiency and convenience, while also bringing more complex risk challenges, especially the continuous evolution and increasing concealment of financial fraud methods. Traditional manual review and risk control methods are gradually revealing their limitations in dealing with these new types of fraud, failing to meet the demands of the modern financial environment. This study, through a comprehensive review of relevant literature, examines the application of technologies such as artificial intelligence (AI), machine learning (ML), and blockchain in financial fraud detection. It is found that these technologies significantly improve the accuracy, efficiency, and model interpretability of fraud detection, and have a positive impact on the security of enterprises and individuals. However, the research also indicates that these technologies still face challenges in data quality, real-time performance, and adaptability. Moreover, although the development of FinTech has provided fraudsters with new means of committing crimes, the ability to combat fraud can be effectively enhanced through technological innovation and institutional improvement. In the future, it is necessary to strengthen international cooperation and information sharing to build a global anti-fraud network, ensuring the healthy development of FinTech.

Keywords: Financial Technology, Fraud Behavior, Artificial Intelligence, Machine Learning.

1 Introduction

With the rapid development of financial technology (FinTech), the digital transformation of the financial sector has accelerated, bringing numerous conveniences to people's lives and economic activities. However, this transformation has also given rise to a series of new risks and challenges, among which financial fraud has become particularly prominent. In recent years, various types of financial fraud cases have occurred

© The Author(s) 2025
B. Siuta-Tokarska et al. (eds.), *Proceedings of the 2025 3rd International Academic Conference on Management Innovation and Economic Development (MIED 2025)*, Advances in Economics, Business and Management Research 348,
https://doi.org/10.2991/978-94-6463-835-6_19

frequently, not only causing significant economic losses to investors but also severely undermining the stability and trust foundation of the financial market. Internet financial fraud, which exploits the portability and anonymity of e-commerce platforms and the information asymmetry between enterprises and their internal and external environments, has led to increasingly complex and evolving fraud methods. Traditional manual review and simple risk control measures are no longer sufficient to address such intricate and dynamic fraud patterns. Against this backdrop, how to effectively prevent and combat financial fraud and safeguard financial security has become an urgent issue that needs to be resolved.

The academic community has long paid attention to the issue of financial fraud. Early research mainly focused on the causes of fraudulent behavior, such as motives, opportunities, and excuses, as well as improvements to traditional auditing and risk control methods. However, with the emergence of emerging technologies such as big data and artificial intelligence, an increasing number of studies have begun to explore how to leverage these advanced technologies to enhance the efficiency and accuracy of financial fraud detection and prevention. In the e-commerce field, the development of a new fraud management system (FMS) can effectively address these challenges, reduce fraud losses, increase bank authorization rates, and boost revenue [1]. Regarding corporate financial fraud, digital finance has been shown to significantly inhibit such behavior. The breadth of coverage and depth of usage of digital finance both have inhibitory effects on financial fraud. This effect is mediated through the alleviation of financing constraints, reduction of corporate leverage, and decrease in agency costs [2]. In the context of cryptocurrency exchange fraud detection, large language models (LLMs) can significantly adjust their assessments to identify red flags of fraudulent behavior after information updates, although their initial assessments tend to be conservative [3, 4]. Given these findings, the core idea of this paper is to provide a comprehensive review of the various FinTech technologies applied in the field of financial fraud detection in recent years, analyze their current applications, strengths, and limitations, and explore future development trends.

This paper focuses on the technological applications, model construction, data processing, and practical effectiveness in financial fraud detection. Through a thorough review and analysis of a large number of relevant studies, this paper finds that although artificial intelligence and data mining technologies have shown great potential in financial fraud detection, they still face many challenges in practice, such as data quality, model interpretability, real-time performance, and adaptability. Moreover, different types of financial fraud exhibit variations in data characteristics and behavioral patterns, necessitating the targeted selection and optimization of detection models. Compared with existing research, this paper provides a more comprehensive and systematic perspective on the application of FinTech technologies in financial fraud detection. It not only summarizes the characteristics and application scenarios of various technologies but also explores the synergistic effects between different technologies and potential future directions, offering valuable references and insights for future research. Additionally, this paper analyzes the existing problems and challenges in current research, providing ideas and suggestions for further optimizing the financial fraud detection technology system.

2 Fraud Detection in the FinTech Sector

With the rapid development of FinTech, its applications in financial services have become increasingly widespread. However, FinTech also faces numerous security and privacy issues, such as cyber-attacks, data breaches, and fraudulent activities. These issues not only affect user trust but also pose threats to the stability and security of financial services. It is crucial to enhance the accuracy of fraud detection and the security of systems through technological means.

In fraud detection, certain characteristics may indicate the presence of fraudulent behavior. First is the lack of transparency, where companies are unwilling or unable to provide detailed information. Second is abnormal trading behavior, where transaction data do not align with market trends or involve insider trading. Third is the conflict of interest, where companies have complex relationships with related parties and may prioritize or solely consider their own interests. Fourth is the overly consistent returns, such as financial products claiming to be risk-free or offering consistent returns in highly volatile markets. Fifth is market manipulation, where certain individuals mislead investors by manipulating trading prices or volumes. Sixth is financial reporting issues, where financial data do not match market behavior or lack detailed reporting. Finally, there is the absence of independent auditing, where companies lack transparent financial audits and custody practices. These characteristics are repeatedly mentioned in multiple rating systems and models, indicating that they are key indicators in fraud detection [3].

In recent years, deep learning methods, such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN), have been employed to process time-series data and image data in order to identify the spatiotemporal features of fraudulent behavior [5]. Anomaly detection methods identify outliers by clustering data points into different groups and recognizing data points that do not belong to any normal cluster [4]. Additionally, fraudulent activities can be detected by constructing transaction networks and analyzing the relationships between nodes [5]. Ensemble methods enhance the accuracy of fraud detection by leveraging the strengths of multiple models. For example, AdaBoost improves classification performance by weighting multiple weak classifiers [4]. These approaches are capable of effectively handling the complexity and uncertainty of data, thereby improving the accuracy and reliability of fraud detection.

Stojanović and Božić proposed a cloud-based fraud detection system architecture, conducting a systematic risk assessment and formal verification to analyze the vulnerabilities of FinTech systems against cyber-attacks. They employed the PRISM model checker to probabilistically model attack scenarios and assess the system's risk exposure levels [5]. Pi et al. utilized fuzzy models and the Analytic Hierarchy Process (AHP) to quantify FinTech risks. By constructing fuzzy judgment matrices and a comprehensive evaluation model, they identified key risk factors such as technological risk, ethical risk, and legal risk, and proposed targeted risk mitigation measures [6]. Mirza et al. applied two algorithms—Random Forest (RF) and AdaBoost—for fraud detection. The RF model, which constructs multiple decision trees and aggregates their votes to enhance classification accuracy, achieved a True Positive Rate (TPR) of 0.9956 and a True Negative Rate (TNR) of 0.9673[4]. AdaBoost, which combines multiple weak

classifiers to improve performance, slightly outperformed RF with TPR and TNR values close to 1.0. They also used Information Value (IV) analysis to evaluate the predictive power of each feature, finding that Competitive Advantage was the most influential feature with a high IV value. In contrast, Sales Volume had a low IV value, indicating its minimal contribution to fraud detection.

Through formal modeling and big data analytics, the risk assessment and early warning systems in the FinTech domain are continuously being refined. The fraud detection system proposed by Stojanović and Božić in a cloud environment can real-time assess the system's risk exposure and generate early warning signals through a model checker [5]. In addition to technical solutions, researchers have also proposed recommendations for improving legal and regulatory frameworks. Pi et al., through their fuzzy model analysis, highlighted the impact of legal risks and regulatory vacuums on FinTech security and suggested specific measures for strengthening legislation and regulation [6].

3 Impact of Fintech Fraud Detection on Businesses

With the widespread adoption of digital technologies and the popularization of online transactions, advances in financial technology offer new opportunities to enhance corporate fraud monitoring and prevention. The use of artificial intelligence by businesses for fraud prevention is a rich, diverse and evolving application of technology that enables them to significantly improve their information processing capabilities. Through in-depth analysis of transactional and financial data, enterprises can mine valuable information to provide an accurate basis for fraud prevention, prompting enterprises to rely more on data to identify potential fraud anomalies, and then effectively prevent fraud. Concurrently, enterprises can also use artificial intelligence to analyze market conditions, policy changes and other external factors to predict and prevent possible fraud risks in advance.

The progression of artificial intelligence can significantly mitigate the financing constraints of enterprises, thereby reducing the incentive for management to engage in fraudulent behavior due to performance pressure. Through accurate risk assessment and credit scoring models, AI can help financial institutions more accurately assess the credit status of enterprises, thereby providing them with more reasonable financing support. This not only helps alleviate the financial pressure on enterprises, but also reduces the possibility of enterprises engaging in fraudulent behavior due to a shortage of funds at the source. In addition, through in-depth analysis of enterprise operation data, industry chain-related data, as well as data on the network behavior of managers and employees, AI can unearth key information hidden therein and assist in determining the authenticity of an enterprise's financial statements [2]. Digital financial institutions can use this data to compare with annual reports, such as financial statements issued by companies, to detect potential financial fraud risks in a timely manner.

Big Data Analytics Capability (BDAC) is also able to process and analyze massive amounts of data using advanced AI analytics to generate key insights to support decision-making [7]. AI-based fraud detection operates on similar principles; For instance through machine learning algorithms, AI can learn normal trading patterns and financial

data characteristics to build appropriate models. Once there is a new data input, the algorithm will automatically compare it with the learned patterns and features, and if it is found that there are abnormalities in the data, such as the transaction amount, time, frequency, etc., which do not match the normal pattern, or unreasonable fluctuations in the financial data, the AI will be able to issue an early warning in time, indicating the potential existence of fraudulent behavior.

4 Impact of Fintech Fraud Detection on Individual Users

In the context of the rapid evolution of financial technology, the trading system, as the core link of financial activities, is gradually being endowed with more intelligent functions. The implementation of these technologies not only bolsters the security and efficiency of transactions, but also has a profound impact on the trading experience of individual users.

AI-driven transaction monitoring has significantly enhanced the security of individual user transactions. By analyzing massive amounts of transaction data in real time, AI-driven transaction monitoring systems can quickly identify potential fraud. For instance, machine learning algorithms can learn and analyze historical transaction data to build models that can distinguish between normal and fraudulent transactions. These models are designed to recognize abnormal patterns in characteristics such as transaction amount, transaction time, and transaction location, and then issue timely alerts [8]. This intelligent transaction monitoring not only improves the accuracy of fraud detection, but also greatly reduces the response time, enabling financial institutions to take measures before fraud causes significant losses, reducing the property losses of individual users due to fraud. For example, fintech platforms can effectively identify phishing attacks by analyzing user behavioral patterns and scanning suspicious email content in combination with natural language processing (NLP) technology [9].

In practical applications, fintech companies can effectively identify and prevent fraud through the adoption of advanced AI technologies. Thakor (2020) in “Fintech and Banking” emphasizes that fintech has driven innovation in fraud detection by reducing the cost of information validation and increasing data economies of scale innovation.[8] For example, some fintech platforms utilize machine learning algorithms to model user behavior, and by analyzing users' transaction habits and patterns, identify abnormal transactions and take timely measures [10]. The application of this technology not only improves the efficiency of fraud detection, but also reduces the false alarm rate, thereby enhancing the user experience.

Big data-based trading risk assessment provides individual users with more accurate and personalized services. By integrating massive data from diverse channels, including users' transaction history, credit records, behavioral habits, etc., the trading system is able to construct more comprehensive and accurate risk assessment models. These models can assess the risk level of each transaction in real time and take appropriate measures according to the level of risk, such as requiring additional identity verification, temporarily freezing transactions, etc[6]. For example, by tracking user behavior over a long period of time, the system can identify a user's normal transaction patterns,

and when an abnormality occurs (such as a sudden increase in the transaction amount or an off-site operation), it is determined to be a high-risk transaction and is further reviewed. This big data-based assessment method not only reduces the risk of fraud, but also improves the transaction approval rate and reduces the decline in user experience caused by misjudgments[9].

The application of blockchain technology has brought about a qualitative leap in the security and transparency of individual user transactions. Blockchain technology, with its decentralized and untamperable nature, ensures that the details of each transaction are authentic and untamperable. This not only helps prevent fraud from occurring, but also provides a reliable basis for the resolution of transaction disputes [6]. For example, in cross-border payment, blockchain technology can realize instant clearing and settlement of transactions, greatly shortening the transaction time and reducing the transaction cost, as well as minimizing the risk of fraud caused by numerous intermediate links [11]. Additionally, the smart contract feature on the blockchain automatically enforces the terms of the contract, further improving the efficiency and security of the transaction [6]. For individual users, this means that their transactions are more transparent and efficient, reducing losses due to transaction disputes or intermediary issues.

The increased real-time and adaptability of trading systems allows for a smoother and more reliable trading experience for individual users. To cope with the fast-changing market environment and constantly renovating fraudulent means, the trading system must have a high degree of real-time and adaptability. Through the implementation of advanced technological architecture and algorithms, trading systems are able to process and analyze transaction data in real time, ensuring that potential risks are detected and dealt with at the earliest opportunity [6]. Simultaneously, the trading system needs to be continuously updated and refined to adapt to new fraud patterns and business needs. Thakor mentioned that fintech companies can improve their ability to adapt to and identify new types of fraud by continuously optimizing the parameters of risk assessment models through algorithms [8]. For individual users, this means that their transactions are more efficient and reliable, reducing the risk of transaction failure or risk due to system delays or lack of adaptability.

In conclusion, the application of these technologies not only reduces the risk of fraud, but also improves the passage rate and transparency of transactions, enabling individual users to conduct transactions with greater peace of mind and convenience. As fintech continues to evolve, in the future, fintech is expected to integrate blockchain and the Internet of Things (IoT) more broadly to further optimize real-time data collection and analysis capabilities [11], the application of these technologies will provide individual users with more secure, efficient and convenient financial services.

5 Limitations and Future Perspectives of Fintech Technology in Anti-Fraud Behavior

The burgeoning development of financial technology (FinTech) has raised new fraud risks and security challenges while enhancing the efficiency of financial services and user experience. With the widespread use of technologies such as digital payments,

online lending and blockchain, forms of fraud have become more sophisticated and insidious. For example, Brogi and Lagasio point out that the rapid expansion of the FinTech industry has led to the frequent occurrence of unethical behaviors such as market manipulation, data breaches, and improper lending, which not only undermines consumer trust, but also poses a threat to the stability of financial markets[12]. Moreover, Ali et al. underscore that traditional fraud detection methods are often inefficient and unable to cope with the increasing sophistication of fraud tactics, prompting researchers to turn to advanced techniques such as machine learning to improve the precision and timeliness of fraud detection[13].

The adoption of fintech technology also confronts numerous hurdles. Griffin et al. investigated the performance of fintech lenders in the U.S. Small Business Paycheck Protection Program (PPP) and discovered a substantial prevalence of potential fraud in loans originated by fintech lenders [10]. In the process of rapid business expansion, these lenders might have neglected to scrutinize loan applications, resulting in a large number of ineligible businesses receiving loans. The anonymity and convenience of fintechs may also facilitate fraud. In addition, lagging regulatory frameworks make it difficult for fintech companies to prevent fraud, and existing laws and regulations often fail to adapt to the rapidly changing technological environment in a timely manner [14].

Prospectively, the fintech industry must strike a balance between technological innovation and risk management. Researchers and practitioners ought to strengthen their studies on emerging technologies, especially how to utilize artificial intelligence and big data analytics to enhance fraud detection capabilities while ensuring the security and privacy of user data. In addition, the establishment of a sound regulatory mechanism to address the new challenges posed by technology will be key to ensuring the sustainable development of FinTech [14]. Through multi-party cooperation, the fintech industry can achieve better coordination between innovation and security and promote the healthy development of the industry.

6 Conclusion

This paper comprehensively discusses the current status, advantages and limitations of the application of financial technology (FinTech) technology in financial fraud detection, while also forecasting future development trends. By combing through a large amount of related literature, this paper finds that artificial intelligence, machine learning, blockchain and other technologies have significant advantages in improving the accuracy, efficiency and model interpretability of fraud detection. Meanwhile, FinTech still faces numerous challenges in fraud detection. Data quality, real-time and adaptability issues limit the performance of the model, while different types of fraud vary in data characteristics and behavioral patterns, requiring targeted selection and optimization of the detection model. Additionally, the anonymity and accessibility of fintech may also facilitate fraud, which is further exacerbated by lagging regulatory frameworks.

Looking forward, the fintech industry is impelled to strike a balance between technological innovation and risk management. Researchers and practitioners should

strengthen their studies on emerging technologies, especially how to utilize artificial intelligence and big data analytics to enhance fraud detection capabilities while ensuring the security and privacy of user data. In addition, the establishment of a sound regulatory mechanism to cope with the new challenges posed by technology will be key to ensuring the sustainable development of fintech. Through multi-party cooperation, the fintech industry can achieve better coordination between innovation and security and promote the healthy development of the industry.

By conducting a comprehensive analysis of the current status and challenges of the application of financial technology technologies in fraud detection, this paper provides valuable references and insights for subsequent research. This paper not only summarizes the characteristics and application scenarios of various types of technologies, but also explores the synergies between different technologies and possible future development directions, providing ideas and suggestions for optimizing the financial fraud detection technology system. With the continuous advancement of financial technology, the research results in this paper will contribute to promoting the positive role of financial technology in safeguarding financial security and promoting economic development.

Authors Contribution

All the authors contributed equally and their names were listed in alphabetical order.

References

1. Nanduri, J., Jia, Y., Oka, A., Beaver, J., Liu, Y.: Microsoft uses machine learning and optimization to reduce e-commerce fraud. INFORMS J. Appl. Anal. 50, 64–79 (2020).
2. Sun, G., Li, T., Ai, Y., Li, Q.: Digital finance and corporate financial fraud. Int. Rev. Financ. Anal. (2023).
3. Gregory, G., Vito, L.: ChatGPT: A canary in the coal mine or a parrot in the echo chamber? Detecting fraud with LLM: The case of FTX. Finance Res. Lett. (2024).
4. Mirza, N., Elhoseny, M., Umar, M., Metawa, N.: Safeguarding FinTech innovations with machine learning: Comparative assessment of various approaches. Res. Int. Bus. Financ. (2023).
5. Stojanović, B., Bozic, J.: Robust financial fraud alerting system based in the cloud environment. Sensors 22 (2022).
6. Pi, T., Hu, H., Lu, J., Chen, X.: The analysis of FinTech risks in China: Based on fuzzy models. Mathematics (2022).
7. Yu, W., Wong, C.Y., Chavez, R., Jacobs, M.A.: Integrating big data analytics into supply chain finance: The roles of information processing and data-driven culture. Int. J. Prod. Econ. (2021).
8. Stojanović, B., Jordan, E., Hofer-Schmitz, K., Božić, J., Runevic, J., Nahrgang, K., Badii, A., Weber, A., Sundaram, M.: Follow the trail: Machine learning for fraud detection in FinTech applications. Sensors 21(5), 1594 (2021).
9. Bello, O.A., Olufemi, K.: Artificial intelligence in fraud prevention: Exploring techniques and applications, challenges and opportunities. Comput. Sci. IT Res. J. (2024).

10. Griffin, J.M., Kruger, S., Mahajan, P.: Did FinTech lenders facilitate PPP fraud? Regul. Financ. Inst. eJ. (2021).
11. Karpoff, J.M.: The future of financial fraud. J. Corp. Financ. 66, 101694 (2020).
12. Brogi, M., Lagasio, V.: New but naughty. The evolution of misconduct in FinTech. Int. Rev. Financ. Anal. (2024).
13. Ali, A., Abd Razak, S., Othman, S.H., Eisa, T.A., Al-Dhaqm, A., Nasser, M., Elhassan, T.A., Elshafie, H.Y., Saif, A.: Financial fraud detection based on machine learning: A systematic literature review. Appl. Sci. (2022).
14. Kun, E.: Challenges in regulating cloud service providers in EU financial regulation: From operational to systemic risks, and examining challenges of the new oversight regime for critical cloud service providers under the Digital Operational Resilience Act. Comput. Law Secur. Rev. 52, 105931 (2024).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.