Proceedings of CONF-SEML 2025 Symposium: Machine Learning Theory and Applications
DOI: 10.54254/2755-2721/2025.TJ23322

Research on Fraudulent Transaction Detection

Chuqiao Cheng

Queen Mary School Hainan, Beijing University of Posts and Telecommunications, Lingshui Li Autonomous County, China
2023213790@bupt.cn

Abstract: With the rapid development of global e-commerce and online payments, the number and complexity of fraudulent transactions have increased significantly, bringing serious economic losses and a crisis of trust to financial institutions and consumers. This paper systematically reviews the characteristics, detection methods and research progress of fraudulent transactions. Firstly, the characteristics of fraudulent transactions are analyzed from the aspects of time, place, transaction mode and technical means. Secondly, the advantages and disadvantages of traditional detection methods (such as rule-based and statistical analysis) and emerging technologies (such as machine learning and deep learning) and their application effects are reviewed. Finally, the limitations of current research in data imbalance, model complexity and multi-type fraud detection are discussed, and future research directions are proposed, including data enhancement techniques, integrated learning frameworks and privacy protection strategies. The research of this paper aims to provide theoretical support and practical guidance for the academic and industrial circles, and promote the further development of the financial security field.

Keywords: Fraudulent transaction detection, Machine learning, Deep learning, Data imbalance, Privacy protection, Financial security.

1. Introduction

With the rapid development of e-commerce and online payments worldwide, the number and complexity of financial transactions has increased significantly. However, this convenience also brings new challenges, not least the proliferation of fraudulent transactions. Fraudulent transaction refers to the transaction behavior of obtaining others' property or information through illegal means, which usually involves various forms such as credit card fraud, online payment fraud, and identity theft [1]. According to an Interpol report, the global economic losses caused by fraudulent transactions reach billions of dollars every year, and this figure continues to grow [2]. Fraudulent transactions not only cause huge economic losses to financial institutions, but also seriously affect the trust of consumers and the stability of the financial system.

The complexity of fraudulent transactions lies in their diversity and concealment. With the continuous diversification of fraud in the financial field and the improvement of technical content, traditional supervision and prevention methods have gradually exposed their limitations [3]. For example, credit card fraud usually involves stealing someone else's credit card information to make an illegal transaction, while online payment fraud may be carried out through fake transactions, phishing websites, etc. In addition, the timing and location of fraudulent transactions are also highly

DOI: 10.54254/2755-2721/2025.TJ23322

uncertain, often occurring in specific high-risk time periods or regions, further increasing the difficulty of detection.

In order to meet this challenge, a variety of fraudulent transaction detection methods have been proposed by academia and industry. Traditional detection methods are mainly based on rules and statistical analysis, which are suitable for simple fraud detection. However, with the continuous escalation of fraud methods, the limitations of traditional methods are gradually becoming apparent. In recent years, the rapid development of machine learning and deep learning technologies has provided new solutions for fraudulent transaction detection. For example, a more common fraud detection technology based on supervised methods is an artificial neural network (ANN), which can handle massive data and has good performance [4]. However, the existing research still faces problems such as data imbalance, high model complexity, and insufficient detection of multiple types of fraud.

This paper will review the detection of fraudulent transactions from three main perspectives: the characteristics of fraudulent transactions, detection methods (including traditional methods and emerging methods), existing limitations and future prospects. First, this article will analyze the characteristics of fraudulent transactions such as time, location, frequency, and account in detail to help readers better understand the basic patterns of fraudulent behavior. Secondly, this paper systematically reviews the existing fraud detection methods, including rule-based detection, machine learning and deep learning methods, and summarizes the advantages and disadvantages of each method and its performance in practical applications. Finally, this paper will explore the limitations of existing research and propose future research directions, such as data enhancement techniques, integrated learning frameworks, and multi-type fraud detection.

The research significance of this paper is to provide theoretical support and practical guidance for the future research of fraudulent transaction detection. Through the summary of the existing research, this paper can not only help the academic community better understand the status quo and challenges of fraudulent transaction detection, but also provide practical technical reference for the industry to promote the further development of the financial security field. In addition, the research results of this paper can provide a basis for policy makers to make more effective anti-fraud policies and regulations.

2. Characteristics and identification of fraudulent transactions

Fraudulent transactions have significant characteristics in the financial field, which are not only reflected in the time, place and frequency of transactions, but also reflected in many aspects such as account behavior, transaction mode and technical means. First of all, from the perspective of time, fraudulent transactions usually occur in specific time periods, such as holidays or nights [5]. These periods tend to be low periods of normal trading activity, and fraudsters use this feature to avoid detection by monitoring systems. In addition, the rapid change of transaction time is also one of the significant characteristics of fraudulent transactions, such as a large number of transactions within a few minutes or hours, which is significantly different from the transaction pattern of normal consumers [6].

Secondly, from the location dimension, fraudulent transactions may be concentrated in certain high-risk areas, or occur in different countries or cities over a short period of time, especially places that do not match the cardholder's usual residence. This unusual change in geographical location often goes hand in hand with the behavior pattern of the fraudster. In addition, the anomaly of IP address is also one of the important indicators to identify fraudulent transactions. Transactions taking place at a different IP address than the cardholder normally does, especially from high-risk areas, often indicate potential fraud. Differences in technology and talent pools between different countries and regions also add complexity to the problem of financial fraud. [6] Technologically advanced

DOI: 10.54254/2755-2721/2025.TJ23322

regions are better able to prevent fraud, while regions with less talent are more difficult to cope, which undoubtedly increases the difficulty of combating financial fraud across regions.

From the perspective of transaction patterns, fraudulent transactions are usually manifested as abnormal consumption amounts or frequent small transactions. An unusually high amount of consumption, especially if it does not match the cardholder's historical transaction amount, is often a significant sign of fraudulent transactions [7]. Frequent small transactions may be a way for fraudsters to test whether the card is valid, gradually increasing the amount to evade detection systems. In addition, duplicate transactions and transactions using false information are also common patterns of fraudulent transactions. Repeated transactions of the same merchants or goods do not conform to normal consumption patterns, and the use of false personal information for transactions is a common means for fraudsters to circumvent detection systems.

Finally, from a technical point of view, fraudulent transactions often involve transactions using unfamiliar or new devices, such as different mobile phones, computers, or public devices. This behavior is significantly different from the device usage habits of normal consumers, so it can be an important basis for identifying fraudulent transactions. To sum up, the characteristics of fraudulent transactions are not only reflected in the time, place and frequency, but also in the transaction mode, account behavior and technical means. Through comprehensive analysis of these characteristics, people can effectively identify and prevent the occurrence of fraudulent transactions.

3. Detection and prevention strategies for fraudulent transactions

3.1. Detection of fraudulent credit card transactions

Credit card fraud is one of the most common types of fraudulent transactions and usually involves stealing someone else's credit card information to make an illegal transaction. In order to effectively detect credit card fraud, researchers have proposed a variety of methods. The rule-based detection method is one of the earliest widely used technologies to identify abnormal transactions by setting a series of rules (such as transaction amount threshold, transaction location limit, etc.) [8]. However, this approach is limited in the face of complex and variable fraud methods. In recent years, machine learning methods have gradually become mainstream, such as decision trees and random forest algorithms, which can automatically learn the characteristics of fraudulent behavior by analyzing historical transaction data [9]. Studies have shown that random forest has a high accuracy and recall rate in credit card fraud detection, but its computational complexity is high, which may affect the efficiency of real-time detection [10].

3.2. Online transaction fraud detection

Online transaction fraud usually involves fake transactions, phishing websites and other means, and its detection methods are different from traditional credit card fraud. The detection method based on behavior analysis identifies abnormal behaviors by analyzing users' trading habits (such as login device, transaction time, purchase preference, etc.) [11]. In addition, deep learning models (such as LSTM and CNN) perform well in processing time series data and complex patterns, and can effectively capture the dynamic characteristics of fraud behavior [12]. For example, the LSTM model performs well in processing high-frequency trading data over a short period of time, but its training process requires a lot of computational resources. Overall, fraud detection methods for online transactions require a trade-off between accuracy and real-time performance.

DOI: 10.54254/2755-2721/2025.TJ23322

3.3. Detection method

Traditional fraud detection methods are mainly based on rules and statistical analysis, and are suitable for simple fraud detection. Rule-based detection methods identify abnormal transactions through predefined rule sets (such as transaction amount ceiling, transaction location limit, etc.), which has the advantage of being easy to implement and explain, but difficult to deal with complex and changeable fraud methods [13]. Statistical analysis methods identify outliers by analyzing the distribution characteristics of transaction data (such as mean, variance, etc.), but their ability to deal with nonlinear relationships is limited [14]. With the continuous upgrading of fraud methods, the limitations of traditional methods are increasingly prominent, and it is difficult to meet the needs of modern fraud detection.

The emerging methods are mainly based on machine learning and deep learning techniques and are able to deal with complex fraud. Random forest and support vector machine (SVM) are commonly used machine learning methods, which can identify fraudulent behavior by analyzing a large amount of feature data [15]. Neural network models (such as CNN and LSTM) perform well in processing high-dimensional data and time series data, and can capture the deep characteristics of fraud [16]. These emerging methods have significant advantages in accuracy and robustness, but their implementation complexity and computational cost are high, which may affect their popularization in practical applications.

To sum up, fraud detection methods have evolved from traditional rules and statistical analysis to modern machine learning and deep learning techniques, gradually improving the accuracy and adaptability of detection. However, different methods have advantages and disadvantages in practical applications, and future research needs to further optimize the algorithm performance and explore the detection strategy of multi-method fusion.

4. Existing limitations and future prospects

Although remarkable progress has been made in the research and application of fraudulent transaction detection, there are still many limitations. These limitations are mainly reflected in the three aspects of data, model and concept, and also provide a clear direction for future research.

4.1. Data limitations and future prospects

One of the major data issues facing fraud detection today is data imbalance. Due to the relatively low proportion of fraud samples in the whole data set, the model tends to favor normal transactions in the training process, resulting in insufficient ability to detect fraud. In addition, data privacy issues are becoming more prominent. When it comes to fraud detection, big data technologies need to collect and analyze users' account information, which has sparked controversy about privacy protection. On the one hand, the adequate collection of data helps to improve the accuracy of detection, thus ensuring financial security; On the other hand, misuse or disclosure of data may violate personal privacy and even raise legal and ethical issues.

To solve the problem of data imbalance, more fraud samples can be generated by data enhancement technology or generative adversarial network (GAN) in the future, so as to improve the training effect of the model. In view of data privacy issues, the application of privacy computing technologies (such as federated learning and differential privacy) can make full use of data value on the premise of protecting user privacy [17]. In addition, the industry should improve relevant laws and regulations to ensure the rational use of data, and strengthen the professional ethics of practitioners to balance the relationship between data utilization and privacy protection.

DOI: 10.54254/2755-2721/2025.TJ23322

4.2. Model limitations and future prospects

The existing fraud detection models have two main defects: First, the traditional rule model is difficult to adapt to the dynamic change of fraud patterns, while the machine learning model can process complex data but has high computational cost; Secondly, the existing research mainly focus on the modeling of single fraud type, and lack the joint detection mechanism for multiple types of fraud. For example, rule-based systems are unable to identify new forms of fraud, while deep learning models applied in isolation are not accurate enough to detect fraud across types.

The improvement direction can be developed from three aspects. First is to build an ensemble learning framework to integrate the advantages of traditional models such as random forest and time series models such as LSTM; Second is to develop a dynamic weight allocation mechanism to automatically adjust model combination strategies according to fraud characteristics; Third is to establish an online learning system to continuously optimize model parameters through real-time data flow to improve the response speed to new fraud patterns.

4.3. Conceptual limitations and future prospects

There are two limitations in industry cognition: excessive pursuit of model optimization and neglect of business logic integration at the technical level, and lack of unified data usage norms at the ethical level. At the same time, the existing system is not interpretable enough, resulting in about one-third of user complaints related to algorithmic transparency issues.

Future development needs to build a multi-dimensional governance system. First is At the technical level, integrating interpretable AI tools such as SHAP value visualization; Second is At the institutional level, promoting the implementation of algorithmic audit regulations and establishing a model deviation accountability mechanism; Third is At the ethical level, "responsible AI" evaluation standards should be formulated, fairness indicators should be incorporated into the system acceptance system, and technological innovation and risk management should be balanced through regulatory sandboxes and other mechanisms.

5. Conclusion

Fraudulent transactions have become a significant concern across various industries, particularly in the financial and digital sectors. As digital transactions grow in frequency and complexity, the detection and prevention of fraud have gained increasing importance. Addressing this issue requires a comprehensive approach that combines multiple technologies, methodologies, and interdisciplinary perspectives.

This review has examined fraudulent transaction detection from several key angles, including the characteristics and identification of fraudulent activities, as well as the various detection and prevention strategies currently in use. The significance of this review lies in its ability to synthesize the most relevant research, offering insights into the ongoing challenges faced by the field and potential future directions. As fraudulent activities continue to evolve, it is essential for the development of more sophisticated and adaptive detection systems. This review serves as a foundation for further research and collaboration among industry professionals, researchers, and policymakers to address the challenges of fraud detection in an increasingly digital world.

References

[1] *Xu, K. (2022). Research on the Innovative Development of Motor Vehicle Insurance in the Digital Economy Era [Master's thesis, Guangxi University].*

[2] *Al-Zyoud, H., Wang, E. Z., Ali, S., & others. (2024). Can supervisor reminders help prevent fraud in the mutual funds sector. Journal of Financial Crime, 32(2).*

DOI: 10.54254/2755-2721/2025.TJ23322

[3] *Wang, J., Zhao, S., & Bai, T. (2003). Research on Securities Market Violations and Crimes in Western Regions. Pan Deng, (03), 91–95.*

[4] *Cheng, D., Zou, Y., Xiang, S., & others. (2025). Graph neural networks for financial fraud detection: A review. Frontiers of Computer Science, 19(9), 1–15.*

[5] *Bintay, R. R., & Joan, T. D. (2024). The risk of fraudulent letter of credit transactions in Bangladesh: A growing threat to Bangladesh's economy. Journal of Financial Crime, 31(5), 1174–1189.*

[6] *Sanzbas, D., Rosal, C. D., Alonso, S. L. N., & others. (2021). Cryptocurrencies and Fraudulent Transactions: Risks, Practices, and Legislation for Their Prevention in Europe and Spain. Laws, 10.*

[7] *Sun, X. Q., Shen, H. W., Cheng, X. Q., & others. (2012). Degree-Strength Correlation Reveals Anomalous Trading Behavior. PLOS ONE, 7.*

[8] *Manohar, V. G., Bhattacharjee, B., & Pratap, M. (2021). Preventing misuse of discount promotions in e-commerce websites: An application of rule-based systems. International Journal of Services Operations and Informatics, 11(1), 54–74.*

[9] *Dong, S. (2024). Research on Fraud Detection Algorithms Based on Graph Neural Networks and Knowledge Reasoning [Master's thesis, Beijing University of Posts and Telecommunications].*

[10] *Verma, P., & Tyagi, P. (2022). Credit Card Fraud Detection using Selective Class Sampling and Random Forest Classifier. ECS Transactions, (1), 107.*

[11] *Yan, Y. (2016). Analysis and Prevention of Operators' Fraudulent Behavior in Online Transactions. Global Market Information Herald, (33), 1.*

[12] *Ding, W. (2025). Research on Credit Card Transaction Fraud Detection Based on Deep Learning Technology [Master's thesis, Shanghai Jiao Tong University].*

[13] *Shi, X., & Li, X. (2024). Comparative Study on Detecting Online Fraud Apps Based on Four Machine Learning Algorithms. Information Technology and Informatization, (4), 183–187.*

[14] *Yuan, C. (2024). New Ideas for Measurement Management in Fair Trade Markets under the New Situation of Market Supervision. Quality and Market, (07), 39–41.*

[15] *Wang, W., Lu, Z., Zhang, J., & others. (2022). Design of Methodology System for Telephone Fraud Behavior Using Random Forest Data Mining Technology. China New Communications, 24(13), 122–124.*

[16] *Xiao, W. (2025). Research on Telecom Fraud Identification Based on BP Neural Network [Master's thesis, Central China Normal University].*

[17] *Chen, D., & Wu, Y. (2024). Research on the Use of Communication Big Data and AI Artificial Intelligence Technology to Construct Telecom Fraud Prevention Behavior Portrait. Intelligent Decision Technologies: An International Journal, (3), 18.*