Proceedings of the 3rd International Conference on Management Research and Economic Development
DOI: 10.54254/2754-1169/177/2025.22230

Research on Fraudulent Transaction Detection Technology

Linwei Li

Bachelor of Science, University of Sydney, Sydney, Australia
lili0884@uni.sydney.edu.au

Abstract: With the popularization of digital payment and the rapid development of financial technology, the problem of fraudulent transactions has become increasingly serious, bringing huge economic losses and trust crises to individuals, enterprises and society. This paper systematically discusses the definition, types, characteristics and influence of fraudulent transactions, and deeply analyzes the current mainstream fraudulent transaction detection techniques, including machine learning, generative adversarial network (GAN) and graph neural network (GNN) methods. It is found that although these technologies show high accuracy and robustness in the detection of fraudulent transactions, they still face limitations such as data imbalance, poor model interpretation, and insufficient public data sets. In order to solve these problems, this paper puts forward some improvement measures such as combining multiple models, data enhancement technology, federated learning and model visualization, and looks forward to the future development direction, such as reinforcement learning, blockchain technology and multi-modal data fusion application. This paper aims to provide a systematic reference for researchers and industry practitioners to promote the development of more efficient and intelligent fraud detection technologies, thereby improving financial security and reducing fraud risks.

Keywords: Fraudulent Transaction Detection, Types of fraudulent transactions, Detection technology.

1. Introduction

In the digital age, with the rapid development of e-commerce, mobile payment and financial technology, transaction methods have become more convenient and diversified. However, this convenience also provides more opportunities for fraudulent transactions. Fraudulent transactions not only bring huge economic losses to individuals and enterprises but also pose a serious threat to the social and economic order and trust system [1,2]. According to the literature [3], in 2020, the global losses of fraudulent transactions in digital credit payments increased by 35% compared with 2018 and are still on the rise. The forms of fraudulent transactions are diverse and the methods are complex, from traditional credit card theft to advanced cyber attacks using artificial intelligence technology, and the technical methods of fraudsters are constantly upgrading. Fraudulent transaction refers to the behavior that the criminal suspects cheat or defraud the victims through various improper means in the process of transaction, so that they make consumption decisions without knowledge or incomplete information, resulting in damage to their economic interests. This behavior not only damages the interests of consumers, but also may have a serious impact on the reputation of enterprises and social

DOI: 10.54254/2754-1169/177/2025.22230

and economic order. Fraudulent transactions take various forms, including but not limited to false transactions, identity theft, credit card fraud, etc [4,5].

This paper will start with the types, characteristics and influences of fraudulent transactions, deeply discuss the current mainstream fraudulent transaction detection technology, analyze its limitations, and put forward the corresponding improvement measures. Through a detailed analysis of machine learning, generative adversarial networks (Gans), graph neural networks (GNN) and other technologies, this article aims to provide readers with a comprehensive overview of fraudulent transaction detection technologies and a look at the future direction.

2. Types of Fraudulent Transactions

Fraudulent transactions can be classified based on different characteristics, including transaction patterns, geographical anomalies, and abnormal account behaviors [6].

2.1. Pattern-Based Fraudulent Transactions

This type of fraud involves exploiting payment system vulnerabilities or manipulating transaction mechanisms for illicit gains. Common scenarios include the misuse of lost or stolen credit cards, arbitrage fraud that takes advantage of quick payment loopholes, and unauthorized access to dynamic passwords obtained through phishing, data breaches, or social engineering attacks. These fraudulent activities often occur rapidly to maximize financial gain before detection systems can intervene.

2.2. Geographical Anomalies in Transactions

Fraudulent transactions often show inconsistencies in geographical patterns compared to a user's normal behavior. For example, a cardholder may typically conduct transactions in a specific city, but fraudulent transactions appear in a distant location or even across borders. These discrepancies may indicate unauthorized access or account takeovers, especially when combined with other suspicious factors such as high-value purchases or unusual transaction frequency.

2.3. Abnormal Account Behaviors

Unusual account activities can also be strong indicators of fraudulent transactions. Criminals may attempt to modify personal information, such as addresses or phone numbers, to bypass security checks. They may frequently switch login devices or use anonymous networks to obscure their identity. Additionally, an excessive number of transactions within a short period or repeated failed login attempts can signal potential fraud attempts.

3. Fraudulent Transaction Detection Technology

Research systems based on machine learning mainly build fraud detection models or behavioral analysis models by analyzing large amounts of data, and improve the recognition ability of models by learning such features [7]. The decision tree is a common algorithm of system learning, and the application of this model needs to find a suitable database. In literature [8], card_transdata is used to analyze the first five data by using different analysis methods, and it is concluded that the prediction of the system hybrid model is the best and has strong processing and prediction ability.

The generative adversarial network model can be divided into two types, generative model and discriminant model. The role of the generative model is to generate false data and the discriminant model is to accept the false data and mix the false data with the true data and classify the true and false data. In the literature [9], they used the credit card transaction data of European cardholders in September 2013 to judge the performance of the model by adopting common indicators. Through

DOI: 10.54254/2754-1169/177/2025.22230

experiments and performance comparison, the mixed model data of this system are all higher than 0.9 and higher than other systems, which indicates that this system model has strong data processing and prediction ability.

Graph neural network is a kind of deep learning model that can take advantage of the interactions in graph structure. By adding sampling and node weights, the model pays more attention to the weights of a small number of samples. The data set used in the literature [10] is the Bank transaction fraud detection (BTFD-GNN) from Yulin Bank Transaction fraud detection Project in Guangxi and uses a graph neural network. Before starting the experiment, data should be selected to select the average AUC (the average for all users). Compared with other models, although BTFD-GNN has a slightly lower recall index, its overall performance is better than other detection methods.

4. Existing Limitations of Fraudulent Transaction Monitoring

4.1. Fraudsters Disguise Themselves

Fraudsters may disguise their actions by transacting with real users, thus masking the characteristics of fraud. This makes it difficult for fraudulent transaction detection models to identify genuine fraud, especially when the fraudsters are using advanced technical means. For example, they may simulate the transaction patterns of real users, hide their real IP addresses using virtual private networks (VPNs), or even use artificial intelligence technology to generate realistic fake transaction data.

In addition, fraudsters may also use "social engineering" to gain users' trust and further conceal their fraud. For example, they may impersonate bank customer service or merchants to induce users to provide sensitive information such as bank card numbers, passwords, or dynamic verification codes.

4.2. Data Imbalance

In real life, the number of fraudulent transactions is often far less than the number of normal transactions [6]. This data imbalance makes it difficult for the fraud detection model to identify a few fraudulent transactions from a large number of normal transactions, resulting in poor detection results. The unbalanced of data distribution makes the fraud transaction detection model tend to be biased towards most classes (i.e. normal transactions) in the training process, which leads to the lack of recognition ability for a few classes (i.e. fraudulent transactions). For example, in a data set containing 1 million transactions, only a few hundred may be fraudulent transactions, and this extremely unbalanced data distribution will cause the model to ignore the characteristics of fraudulent transactions during the training process, leading to poor detection results.

4.3. Few Public Data Sets

Due to the sensitivity and privacy of transaction data, banks and financial institutions generally do not disclose their transaction data [6]. This makes it difficult for researchers to obtain enough data to train and test fraudulent transaction detection models, thus limiting the development of research. In addition, the lack of public data sets also limits the comparability and reproducibility of different studies, making it difficult to generalize research results in practical applications. For example, many existing studies can only rely on a small number of publicly available data sets, which are often small in size and have limited features that do not provide a full picture of fraudulent transactions in the real world.

4.4. Data is not Visible

Fraudulent transaction detection models are often complex and difficult to explain the decision-making process. This makes it difficult for users to understand how the model arrived at its

DOI: 10.54254/2754-1169/177/2025.22230

conclusions, reducing trust in the model. For example, a fraudulent transaction detection model based on a deep neural network may determine whether a transaction is fraudulent in a few milliseconds, but its judgment basis and decision-making process are difficult to show users in an intuitive way. This lack of visibility not only reduces the user's trust in the model, but also may lead to the model being questioned and rejected in practical applications. In addition, the invisibility of data also reduces the transparency and interpretability of the model, which further limits its popularization in practical applications.

5. Problem-Solving Strategies

5.1. Use More Models or Combine Multiple Models

In order to improve the accuracy of fraudulent transaction detection, a hybrid model can be constructed by combining the characteristics of various models. For example, machine learning models and deep learning models can be combined to take advantage of the interpretability of machine learning models and the efficiency of deep learning models, thereby improving the detection ability of fraudulent transactions. However the decision-making process is often complex and difficult to explain. By combining machine learning models and deep learning models, the advantages of both can be fully leveraged. For example, you can use a deep learning model to extract features from high-dimensional data, and then input the extracted features into a machine learning model for classification. This method can not only improve the prediction accuracy of the model, but also preserve the interpretability of the model to a certain extent.

5.2. Visualize the Process

In order to improve the user's trust in the fraudulent transaction detection model, the decision-making process of the model can be displayed by visualization technology. The advantage of visualization technology is its ability to show complex model decision processes in an intuitive way, thereby increasing user trust in the model. For example, visualization tools such as heat maps and decision trees can be used to show how the model extracts features from input data and makes decisions. Decision trees can clearly show the decision path of the model and help users understand how the model extracts features from the input data and makes classification decisions. This not only improves the transparency of the model, but also helps users better understand the decision-making process of the model.

5.3. Model Interpretation

To improve the interpretability of the model, interpretable machine learning models such as decision trees, logistic regression, etc., can be used. These models can not only provide high prediction accuracy, but also explain their decision-making process, thus increasing user trust in the model. For example, the decision tree model recursively divides a data set into smaller subsets, ultimately generating a tree-like structure. Each node represents a feature, each branch represents a decision rule, and the leaf node represents the final classification result. With the decision tree, the user can clearly see how the model extracts features from the input data and makes classification decisions. With feature weights, users can understand the contribution of each feature to model decisions.

DOI: 10.54254/2754-1169/177/2025.22230

6. Future Development Direction

6.1. User Behavior Analysis

User behavior analysis is a method to identify abnormal behavior by analyzing the historical behavior patterns of users. In fraud transaction detection, abnormal transaction behavior can be identified by analyzing the user's trading habits, login device, geographical location and other information. For example, if a user normally makes a transaction at one location and suddenly makes a large transaction at another location, the system can flag it as a suspicious transaction. However, it is also important to note that the user's behavior patterns may change over time, such as when the user moves, changes devices, or changes spending habits. Second, fraudsters may try to evade detection by mimicking the user's behavior patterns.

6.2. Multi-modal Data Fusion

Fraudulent transactions often involve multiple data types, such as transaction data, geolocation data, device information, etc. By fusing multi-modal data, transaction behavior can be analyzed more comprehensively, thus improving the detection ability of fraudulent transactions. For example, it is possible to combine transaction data with geolocation data to identify unusual transaction behavior. The advantage of multimodal data fusion is that it can analyze transaction behavior from multiple dimensions, thus improving the accuracy of detection. For example, if the system detects a large transaction, the amount of the transaction alone cannot tell whether it is a fraudulent transaction. But when combined with other data, such as the transaction location (inconsistent with the user's usual location), login device (new device), IP address (high-risk area), etc., the system can more accurately assess the risk of the transaction.

7. Conclusion

Fraudulent transactions are a complex and fluid issue, and as technology advances, so do fraudsters' tactics. To effectively deal with fraudulent transactions, companies and research institutions need to continuously improve and optimize fraudulent transaction detection technologies. By combining a variety of models, using data enhancement technology, and improving the interpretation and transparency of models, the accuracy and robustness of fraudulent transaction detection can be effectively improved, so as to protect the interests of consumers and enterprises and maintain the economic order of society. In the future, with the development of reinforcement learning, blockchain technology, multi-modal data fusion and other technologies, fraud transaction detection will become more intelligent and efficient, providing a more solid guarantee for the economic security of society.

References

[1] *Edge, M. E., & Sampaio, P. R. F. (2009). A survey of signature based methods for financial fraud detection. computers & security, 28(6), 381-394.*

[2] *Al-Hashedi, K. G., & Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review, 40, 100402.*

[3] *Bansal, A., & Garg, H. (2021). An efficient technique for fraudulent detection in credit card dataset: A comprehen sive study. IOP Conference Series: Materials Science and Engineering, 1116(1), 012181. https://doi.org/10.1088/ 1757-899X/1116/1/012181*

[4] *Albashrawi, M. (2016). Detecting financial fraud using data mining techniques: A decade review from 2004 to 2015. Journal of Data Science, 14(3), 553-569.Chaudhary, K., Yadav, J., & Mallick, B. (2012). A review of fraud detection techniques: Credit card. International Journal of Computer Applications, 45(1), 39-44.*

[5] *Chaudhary, K., Yadav, J., & Mallick, B. (2012). A review of fraud detection techniques: Credit card. International Journal of Computer Applications, 45(1), 39-44.*

DOI: 10.54254/2754-1169/177/2025.22230

[6] Liu Hualing, Cao Shijie, Xu Junyi & Chen Shanghui. (2023). Research progress on anti-fraud in digital credit transactions. Computer Science and Exploration (10), 2300-2324.

[7] Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., ... & Saif, A. (2022). Financial fraud detection based on machine learning: a systematic literature review. Applied Sciences, 12(19), 9637.

[8] Liu Xiaoqun, Li Ning & He Guangwei. (2024). Intelligent analysis of transaction fraud based on machine learning. Wireless Internet Technology (23), 35-38.

[9] Liu Yong-Ling. (2024). Credit card transaction fraud detection based on generative adduction network. Modern Commerce Industry, 45 (17), 266-268. (in Chinese) doi:10.19311/j.cnki.1672-3198.2024.17.090.

[10] Qin Zhong-Piao, Zhou Yatong & Li Zhe. (2024). Graph neural network-based fraud detection method for bank transactions. Computer Science, 51 (S2), 921-928.