Proceedings of the 2nd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/77/2024MA0068

AI-based financial transaction monitoring and fraud prevention with behaviour prediction

Jiahao Xu[1a,*], Tianyi Yang[1b], Shikai Zhuang[2], Huixiang Li[3], Wenran Lu[4]

[1a]Master of Science in Financial Engineering, University of Southern California, CA,USA
[1b]Financial Risk Management, University of Connecticut, Stamford CT, USA
[2]Electrical Engineering, University of Washington,Seattle,WA,USA
[3]Information Studies, Trine University, AZ, USA
[4]Electrical Engineering, University of Texas at Austin, Austin, TX,USA

*Corresponding author E-mail: lizengyi.zy@bytedance.com

Abstract. In this study, we explored the application of deep learning techniques for credit card fraud detection, aiming to improve the performance and reliability of anomaly detection methods in financial transactions. We first utilized the Isolation Forest algorithm, achieving a detection accuracy of 26% for the top 1000 transactions. Subsequently, we experimented with the Autoencoder algorithm, an unsupervised deep neural network model, which enhanced the detection accuracy to 33.6% in the best case, despite some fluctuations. However, the high imbalance in the dataset, with only 0.17% of transactions being fraudulent, poses a significant challenge. This study underscores the necessity for further experimentation and optimization of network structures and hyperparameters to achieve more stable and efficient fraud detection. The findings provide valuable insights and reference points for future research in the field of financial fraud detection using deep learning methodologies.

Keywords: Deep Learning, Fraud Detection, Autoencoder, Financial Transactions

1. Introduction

Article 11 of the Measures for the Administration of Large Transactions and Suspicious Transaction Reports by Financial Institutions provides that "If a financial institution finds or has reasonable grounds to suspect that a customer, the customer's funds or other assets, the customer's transactions or attempted transactions are related to criminal activities such as money laundering or terrorist financing, it shall file a suspicious transaction report, regardless of the number of funds involved or the value of the assets involved". [1] Financial institutions shall establish a sound transaction monitoring system to identify transactions that may involve money laundering or other upstream crimes through the analysis of customer information and transaction information, and conduct further due diligence. If there are reasonable grounds for suspicion or the suspicion cannot be ruled out, the suspicious transaction report shall be reported to the China Anti-Money Laundering Monitoring and Analysis Centre and relevant departments [2]. Based on the prediction of transaction fraud based on financial market monitoring, this paper discusses some suggestions to improve the effectiveness, timeliness, and integrity of suspicious

DOI: 10.54254/2755-2721/77/2024MA0068

transaction monitoring and identification from the common difficulties faced by financial institutions at present.

2. Related work

2.1. Traditional transaction monitoring system

The objective of financial supervision is not only the criterion for evaluating the quality of financial supervision but also the basis for regulators to take supervisory actions and the premise for realizing effective financial supervision. [3] The goals of financial supervision can be divided into general goals and specific goals. The objectives of financial regulation are threefold: to maintain financial security, stability, and good financial order; to prevent monopolies in the financial sector to maintain financial efficiency; Protecting the interests of investors and depositors. [4] Supervision is to take into account the three goals of safety, efficiency, and depositors' interests, and adjust the focus of supervision goals accordingly with the changes in economic and financial situations. In this regard, the emphasis of Internet financial regulation is different from that of traditional financial regulation.

(1) Traditional financial regulation is based on functional regulation theory

Traditional and Internet financial regulation, as institutional arrangements, fundamentally aim to correct financial market failures caused by risks, reduce these risks, and improve financial efficiency. Both regulations aim to reduce transaction costs caused by economic uncertainty to the greatest extent. From the perspective of risk prevention, supervision must first focus on tracing the source of risk, so as to form the theoretical basis of supervision. [5] With the development of regulatory economics, there are still differences between functional supervision and institutional supervision in the academic circle, and traditional financial supervision is showing an increasingly diversified theoretical tendency. However, with traditional financial institutions still existing and thriving today, I think functional supervision theory is still the main theoretical principle that traditional financial supervision should follow.

(2) Internet financial regulation is based on the new regulatory theory

Because our country has been in the financial repression environment for a long time, Internet finance has carried out more aggressive regulatory arbitrage than traditional finance. Its development, for a long time the traditional financial system is too large [6], small and micro enterprises financing difficulties and lack of investment channels, an "extra-legal" supplement, in essence can even be said to be the development and extension of private finance with high-tech means. The essence of Internet finance is still a financial contractual relationship or a lending contractual relationship. Financial development and financial risk cannot be separated or opposed but should be reflected in the matching of returns and risks.

2.2. Traditional finance relies on mature traditional regulatory standards and means

Along with the deepening of the reform of financial institutions and financial markets, China's financial supervision has tended to mature. Based on fully studying the development of the domestic financial industry and reasonably drawing lessons from the experience of financial supervision in developed countries, the three committees have formed relatively mature supervision methods and rules.

1. Relatively clear regulatory quantitative standards. Since traditional financial transactions mainly rely on the medium of financial institutions for financing and other aspects, transaction behaviors are more dependent on paper texts for regulation and operation. As a medium of financial transactions, financial institutions can collect their trading behavior and financial data information relatively easily, which provides conditions for regulators to study information and make decisions.

2. Relatively simple and fixed regulatory measures. [7] The three major regulatory means of traditional financial regulation are market access, on-site inspection and off-site supervision based on regulatory rules. In terms of market access methods, due to the leverage role of the financial industry, combined with the existence of systemic risks and systemically important financial institutions, traditional financial supervision has a naturally high threshold in terms of market access, and the formal entry and exit mechanisms are very strict.

DOI: 10.54254/2755-2721/77/2024MA0068

For example, after the traditional 1104 reporting system, the CBRC has developed the EAST on-site inspection system based on bank business data in recent years, which is more closely connected with the internal system of the bank, and the authenticity of the obtained data is stronger. In terms of punishment, the regulatory authorities can adopt traditional mandatory measures such as fines, suspension of access, and restriction of dividend distribution.

2.3. Common problems and challenges of traditional financial transaction supervision

(1) Large and complex data

Every day, financial institutions process large amounts of transaction data from a wide range of sources and complex structures, including but not limited to customer information, transaction records, account activity, etc. [8] For example, a large bank processes millions of transactions every day, and this transaction data includes details such as transaction amount, time, location, counterparty, and so on. To monitor these transactions, banks need to store and process huge amounts of data and identify suspicious activity in a short period of time. This poses a huge challenge to existing [12]IT infrastructure and data processing capabilities.

(2) High false alarm rate

Existing transaction monitoring systems often rely on preset rules and thresholds, which are set based on historical data and experience. However, the diversity and complexity of financial transactions make it challenging for these rules to cover all anomalies, resulting in many false positives. False alerts not only waste resources but can also cause actual suspicious transactions to go unnoticed. For example, in one month, a financial institution's transaction monitoring system generated thousands of suspicious transaction alerts. However, after a manual review, it was found that less than 1% of these alerts were those that required further investigation. The other 99 percent are false alarms that cost a lot of manpower and time.

(3) The response speed and real-time performance of the monitoring system

In order to effectively prevent financial crimes, transaction monitoring systems need to have real-time analysis and response capabilities [9]. However, traditional monitoring systems are often slow to respond, making it difficult to detect and block suspicious transactions in a timely manner. Real-time monitoring requires the system to be able to analyze and judge at the moment of transaction, which puts higher requirements on technology and algorithms. For example, in a real-time transaction monitoring test, a bank's system took an average of 10 minutes to assess and respond to the risk of each transaction. This means that during those 10 minutes, potentially suspicious transactions may have been completed, leaving room for criminals to operate.

(4)Cross-institutional and cross-border coordination issues

Financial crime often cuts across multiple institutions and countries, so transaction monitoring requires coordination and cooperation across institutions and borders. However, legal, regulatory requirements and technical standards vary across agencies and countries, making information sharing and collaboration more difficult. In addition, data privacy and security concerns have also become barriers to cross-border cooperation.

For example, in an international money laundering case, multiple banks and multiple countries are involved. Although each bank has its own surveillance system, the lack of effective cross-border cooperation and information sharing has allowed criminals to take advantage of regulatory differences in different countries to successfully launder money.[10] These challenges not only increase the operating costs and regulatory burden of financial institutions, but also make some suspicious transactions that exist may be overlooked. To solve these problems and improve the effectiveness and efficiency of financial transaction monitoring, the application of artificial intelligence (AI) and behavior prediction technology has become a viable solution.

3. Application of AI Fraudulent Behaviour Prediction

In a world where transactions and interactions take place almost entirely online, the threat of fraud is paramount. As more and more financial transactions take place in the digital space, controls should be

DOI: 10.54254/2755-2721/77/2024MA0068

in place to ensure security. Artificial intelligence has proven to be an effective tool in the fight against fraud. Its function is based on learning from enough data and identifying patterns and biases in order to detect and prevent illegal behaviors.

3.1. Traditional fraud detection methods

Traditional rule-based fraud detection methods are very ineffective in today's financial transaction environment. False positives and missed positives are the main reasons for this. Fraud detection through false positives is inaccurate, resulting in transactions being delayed before confirmation and requiring further investigation, causing inconvenience without providing any benefit. Under-reporting, on the other hand, is even more damaging, as financial institutions fail to prevent fraudulent activity, resulting in financial loss and reputational damage.

Second, data quality can negatively impact the performance of traditional fraud detection systems. Incomplete, incorrect or outdated data can compromise a system's ability to adequately identify fraud patterns. Because of the volume and variety of data collected today, it is difficult to obtain high-quality data that can be properly interpreted. Artificial intelligence and machine learning technologies use predictive modelling, natural language processing and anomaly detection techniques to help organizations improve the accuracy and efficiency of fraud detection.

3.2. Fraud detection with AI

Artificial intelligence plays an important role in fraud detection, using complex algorithms to analyse activity, identify anomalies and spot fraud in large data sets. AI systems learn from past experience, which in practice means they get better at predicting and identifying fraud over time by adapting to new technologies used by fraudsters. AI fraud detection works by observing operations, taking an average of normal operations, and refining judgments to distinguish between correct and fraudulent operations in real time. Clearly, artificial intelligence in fraud detection is a highly effective tool for maintaining transaction security and preventing fraud losses.

3.3. Using artificial intelligence and machine learning algorithms in fraud detection

In fraud detection, specific machine learning algorithms play a crucial role in identifying and preventing fraudulent activity. Here is an explanation of some of the key algorithms commonly used in fraud detection:

1. Logistic regression

Logistic regression is a fundamental algorithm in fraud detection and is particularly useful when the outcomes are categorical, such as determining whether a transaction is fraudulent or not. By fitting the data to a logical function, it can estimate the probabilities of different outcomes, providing insight into the likelihood of fraud based on specific parameters and historical data. Its simplicity and interpretability make it a valuable tool for analyzing transaction data and identifying potentially fraudulent activity.

2. Decision Tree

Decision trees are multifunctional algorithms that excel at creating interpretable rules based on transaction characteristics. In fraud detection, decision trees are used to segment or classify data to predict the likelihood of fraud based on transaction characteristics such as amount, location and frequency. Their intuitiveness allows the creation of rule-based systems that can effectively identify suspicious transactions and flag them for further investigation.

3. Random Forest

Random forests represent an advance in fraud detection by using ensemble learning to improve accuracy and mitigate overfitting. By combining multiple decision trees, random forests aggregate predictions, resulting in more powerful and accurate fraud detection capabilities. Its ability to handle large data sets and complex patterns makes it particularly effective at identifying fraudulent activity in different trading environments, helping to improve risk mitigation strategies in the financial industry.

4. Neural Networks

DOI: 10.54254/2755-2721/77/2024MA0068

Neural networks, inspired by the structure of the human brain, are powerful algorithms capable of learning complex patterns and relationships in data. In fraud detection, neural networks excel at efficiently processing large amounts of transactional data to detect anomalies, classify transactions and identify fraud patterns. Overall, the integration of AI into fraud detection represents a significant step forward in securing digital transactions and increasing trust in online interactions. Through ongoing research and collaboration between industry stakeholders, AI will continue to play a key role in enhancing security and fostering trust in the digital ecosystem.

4. Methodology

In recent years, deep learning has shown great potential in anomaly detection. In particular, deep learning methods excel when it comes to practical problems such as credit card fraud detection. By using deep learning algorithms, we are able to identify unusual transactions more effectively, helping financial institutions to reduce potential losses.

4.1. Experimental design

In our study, we used a common credit card fraud dataset to evaluate the performance of different algorithms. First, we used the Isolation Forest algorithm, and the results show that the detection accuracy of top1000 can reach 26%. Although this result is satisfactory, we hope to explore more advanced deep learning methods in the hope of achieving better performance. Next, we tried the Autoencoder algorithm, which is an unsupervised learning deep neural network model suitable for anomaly detection tasks. After several experiments, we found that Autoencoder was able to improve the detection accuracy of the top1000 to 33.6% in the best case.

The experimental part of this study will describe in detail the dataset, model structure, experimental process, and result analysis we adopted to provide a valuable reference for future research.

4.2. Data processing

The data showed that only 0.17% of transactions were fraudulent. The data is very skewed. Let's run our model without balancing first, and if we don't get good accuracy then we can find a way to balance this data set. But first, let's run the model without adjustment and only adjust the data if necessary.

4.3. Plot correlation matrix

Correlation matrices graphically give us an idea of how features relate to each other and can help us predict which features are most relevant to the prediction.

In the heat map we can clearly see that most features are not correlated with other features, but there are some features that are positively or negatively correlated with each other. For example, V2 and V5 are strongly negatively correlated with a feature called Amount. We also see some correlation with V20 and Amount. This gives us a deeper understanding of the data we have.

DOI: 10.54254/2755-2721/77/2024MA0068

4.4. Experimental result

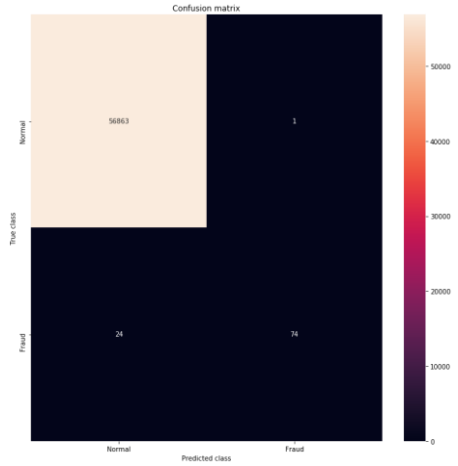

Figure 1. Model diagram of training results

Through this experiment, we have a deeper understanding of the application of deep learning in financial fraud detection. The results of the experiment show that while traditional isolated forest algorithms have performed satisfactorily in credit card fraud detection, achieving a top1000 detection accuracy of 26%, deep learning methods, especially Autoencoder algorithms, show greater potential. In the best case, Autoencoder's top1000 detection accuracy improved to 33.6%, despite some fluctuations in its results.

4.5. Experimental discussion

The advantages of deep learning methods in financial fraud detection are mainly reflected in the following aspects:

1. Strong feature extraction ability: Deep learning models can automatically extract complex features from data without manually designing features. This makes the model more adaptable in the face of high-dimensional, non-linear and complex data.

2. Strong adaptability: Deep learning models can better adapt to different data distributions and abnormal patterns by adjusting network structure and hyperparameters, thus improving detection accuracy.

3. High potential performance: Although the results of Autoencoder are volatile, further experiments and optimization are expected to find a more stable and efficient network structure, thus stably improving the detection performance.

During the experiment, we also found a significant bias in the dataset, with only 0.17% of transactions being fraudulent. We ran the model without balancing the data. If the detection accuracy is not ideal in this case, then we can consider balancing the data set. Through correlation matrix analysis, we understand the relationship between different features, which helps us understand which features are most important for prediction.

5. Conclusion

In conclusion, this study demonstrates the significant potential of deep learning methods, particularly the Autoencoder algorithm, in the detection of financial fraud. Our experiments reveal that while traditional algorithms like the Isolation Forest can achieve satisfactory results, deep learning techniques offer superior feature extraction capabilities and adaptability to complex data patterns. Despite some fluctuations in performance, the Autoencoder achieved a top detection accuracy of 33.6%, indicating its promise for further optimization. This research underscores the importance of continuous experimentation and improvement in deep learning models to enhance the stability and efficiency of

DOI: 10.54254/2755-2721/77/2024MA0068

fraud detection systems, ultimately aiding financial institutions in mitigating risks and safeguarding their operations.

Looking ahead, the application of artificial intelligence (AI) in financial transaction monitoring and behaviour prediction has broad prospects and will greatly enhance the safety, stability and efficiency of the financial system in the future. Traditional financial transaction monitoring systems are often slow to respond, and advanced AI technology will change this. The financial regulatory system of the future will be able to perform real-time analysis and judgement at the moment a transaction occurs, quickly identifying and blocking suspicious transactions. This will not only significantly reduce the success rate of fraud, but also improve the security and stability of the entire financial system.

References

[1] Mozaffari, S., Al-Jarrah, O. Y., Dianati, M., Jennings, P., & Mouzakitis, A. (2020). Deep learning-based vehicle behavior prediction for autonomous driving applications: A review. IEEE Transactions on Intelligent Transportation Systems, 23(1), 33-47.

[2] Choudhury, M., Li, G., Li, J., Zhao, K., Dong, M., & Harfoush, K. (2021, September). Power Efficiency in Communication Networks with Power-Proportional Devices. In 2021 IEEE Symposium on Computers and Communications (ISCC) (pp. 1-6). IEEE.

[3] Xiao, Jing Jian. "Applying behavior theories to financial behavior." Handbook of consumer finance research. New York, NY: Springer New York, 2008. 69-81.

[4] Perry, V. G., & Morris, M. D. (2005). Who is in control? The role of self-perception, knowledge, and income in explaining consumer financial behavior. Journal of consumer affairs, 39(2), 299-313.

[5] Hirsh Leifer, D. (2015). Behavioral finance. Annual Review of Financial Economics, 7, 133-159.

[6] Huo, Mingda, et al. "JPX Tokyo Stock Exchange Prediction with LightGBM." Proceedings of the 2nd International Conference on Bigdata Blockchain and Economy Management, ICBBEM 2023, May 19–21, 2023, Hangzhou, China. 2023.

[7] Srivastava, S., Huang, C., Fan, W., & Yao, Z. (2023). Instance Needs More Care: Rewriting Prompts for Instances Yields Better Zero-Shot Performance. arXiv preprint arXiv:2310.02107.

[8] Bao, Wenqing, et al. "The Challenges and Opportunities of Financial Technology Innovation to Bank Financing Business and Risk Management." Financial Engineering and Risk Management 7.2 (2024): 82-88.

[9] Merton, R. C., & Bodie, Z. (2006). Design of financial systems: towards a synthesis of function and structure. In The world of risk management (pp. 1-27).

[10] Ngai, Eric WT, et al. "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of the literature." Decision support systems 50.3 (2011): 559-569.