Article

Not peer-reviewed version

AI-Based Financial Transaction Monitoring and Fraud Prevention with Behaviour Prediction

Jiahao Xu *, Tianyi Yang , Shikai Zhuang , Huixiang Li , Wenran Lu

Posted Date: 16 July 2024

doi: 10.20944/preprints202407.1107.v1

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

Article

AI-Based Financial Transaction Monitoring and Fraud Prevention with Behaviour Prediction

Jiahao Xu [1,*] and Tianyi Yang [2],Shikai Zhuang [3],Huixiang Li [4] and Wenran Lu [5]

[1] Computer Science, Fudan University, ShangHai, China
[2] Financial Risk Management,University of Connecticut,Stamford CT,USA
[3] Electrical Engineering, University of Washington, Seattle,WA, USA
[4] Information Studies, Trine University, AZ, USA
[5] Electrical Engineering, University of Texas at Austin, Austin, TX, USA
* Correspondence: 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. The results demonstrate deep learning models' strong feature extraction capability and adaptability, highlighting their potential to surpass traditional methods. 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 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." [1,2]Financial institutions shall establish a sound transaction monitoring system to identify transactions that may involve money laundering or other upstream crimes by analyzing 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. Through suspicious transaction monitoring, it can effectively detect and prevent the flow of illegal funds and play a role in safeguarding the security and stability of the financial system, combating criminal activities and maintaining social fairness and justice. 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 transaction monitoring and identification from the common difficulties faced by financial institutions at present.

 doi:10.20944/preprints202407.1107.v1

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; Preventing 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. The most essential risks of traditional finance are credit risk and high leverage risk, which arise from people's limited rationality and opportunism tendency. [5]Therefore, the most fundamental aspect of traditional financial regulation is to reduce and correct people's limited rationality and opportunism in order to minimize financial uncertainty. The traditional financial threshold is high, especially the quality of investors and consumers involved in high-risk business is relatively high, and the more important content of supervision is to protect the interests of the largest number of depositors through the prevention of credit risks. [6]To a large extent, the emergence of traditional financial supervision is due to the theory of financial fragility. In reality, the objects of traditional financial supervision are real various financial institutions, which have already possessed a huge scale and system after years of development. The function of these financial institutions as economic intermediaries or capital intermediaries is very powerful. Therefore, the traditional financial regulation has been based on the functional regulation theory from the very beginning, focusing on correcting opportunism and paying attention to the supervision of legal institutions and risk supervision. 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 [7], 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. The Internet financial risk is also a credit risk in essence, especially for the business with financial leverage transactions, which is widely involved in traditional finance. If we pursue this source of risk, compared with traditional financial risks, these financial products and models have a short time and change quickly, and there is no fixed routine and ready-made rules to restrict and supervise.

However, in reality, the huge capital supply and demand market is quite attractive to subjects without formal financial licenses, so there is a profit-seeking behavior to circumvent regulation, which increases the information cost and transaction cost of the financial market, increases the

 doi:10.20944/preprints202407.1107.v1

uncertainty, and then increases the risk. [8]From the perspective of matching risk and return, the regulator should focus on not "preventing failure", but providing a better environment and more transparent disclosure rules, so that the risk-return of Internet financial investment can be more easily identified by investors, and the supervision should focus on making Internet finance transparent and legalized, and incorporated into the formal regulatory system to eliminate the mismatch between risk and return. Therefore, Internet financial regulation should pay more attention to the education and protection of financial consumers and investors. [9]The "twin peaks" theory, which represents the new international financial regulation theory, emphasizes equal emphasis on risk regulation and consumer protection. Therefore, Internet financial regulation should be based on this theory from the beginning, focusing on correcting limited rationality, focusing on natural person supervision, developing supervision, and exerting the positive role of Internet finance on the real economy through supervision. Furthermore, Traditional financial regulation indirectly serves economic development by preventing risks, while Internet financial regulation is more direct in promoting the development of the real economy.

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. On the basis of 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. The regulatory rules focus on strict requirements on financial industry capital, such as the Basel Agreement stipulates that the capital adequacy ratio of banks shall not be less than 8% and the core capital adequacy ratio shall not be less than 4%[10]. In addition, with the development of the financial industry, the Basel Agreement has been continuously revised, and the capital adequacy standard has been continuously improved. Basel II includes operational risk measurement into risk capital, and proposes basic index method and internal rating method, both of which are based on quantitative indicators and a large amount of internal data. Basel III also put forward specific ratio requirements for loan-to-deposit ratio and loan-to-loan ratio, and also increased new liquidity regulatory indicators such as net stable financing ratio and liquidity coverage ratio.

2. Relatively simple and fixed regulatory measures. 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. In the approval of access, the examination and review of senior executives, businesses and institutions is carried out. In terms of on-site inspection methods, in traditional financial transactions, it takes a relatively long time to collect information, negotiate transactions, sign contracts and supervise the performance of contracts, resulting in large transaction costs. For the consideration of cost and income, a single transaction generally has a considerable amount of underlying capital, and banking institutions can realize economies of scale by using fine management. [11]On-site inspection can effectively identify this micro-behavior and conduct a certain compliance review, and effectively track down similar large funds. In terms of off-site supervision methods, the regulatory authorities have established a data submission system with financial institutions, formulated a relatively complete statement and data system, standardized and unified the statements of traditional financial institutions and regulatory authorities, and established a strict data docking audit system. Through the use of off-site information

 doi:10.20944/preprints202407.1107.v1

system can be more convenient to realize the business information disclosure and risk warning, and this system is more and more transparent and advanced. 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. With the globalization and digitization of financial business, this amount of data continues to increase. Processing and analyzing such a huge amount of data requires powerful computing power and advanced data processing techniques.

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 actually 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 [13]. 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. In the end, Interpol intervened and coordinated with police and financial institutions in many countries to successfully crack the case.

 doi:10.20944/preprints202407.1107.v1

In conclusion, the traditional financial transaction monitoring system is faced with large and complex data volume, high false alarm rate, monitoring system response speed and real-time problems, and cross-institutional and cross-border coordination problems. [12]These challenges not only increase the operating costs and regulatory burden of financial institutions, but also make some suspicious transactions that actually exist may be overlooked. In order 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 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 a sufficient amount of data and identifying patterns and biases in order to detect and prevent illegal behaviour.

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. The common disadvantage of both false positives and false negatives is that they rely on pre-defined rules that may not cover all possibilities, but cannot be modified due to their number. There is therefore a need for more intelligent and flexible fraud detection methods.

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. [14]However, ensuring that data sources are reliable and timely is critical to improving the outcomes of legacy systems. Generating high quality data is not easy, which is particularly important for organisations working with legacy systems and mixed data sources.

However, with the advent of artificial intelligence and machine learning technologies, financial services organisations have an opportunity to overcome these challenges. Artificial intelligence and machine learning techniques can help process large amounts of data quickly and in real time, identify subtle patterns that may indicate fraud, and adapt to new fraud strategies. Artificial intelligence and machine learning technologies use predictive modelling, natural language processing and anomaly detection techniques to help organisations 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. [15]This includes automated anomaly detection, behavioural analysis and natural language processing that can identify and evaluate trends and activities that may be indicators of fraud. 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. By quickly processing large amounts of data, it can accurately identify subtle fraud patterns that can cause financial damage and maintain consumer confidence. In addition, AI technology can be used in the broad area of transaction verification, monitoring transactions and their myriad distinguishing features, and can also identify many of the signature

 doi:10.20944/preprints202407.1107.v1

characteristics used for identity theft using behavioural biometrics. Clearly, artificial intelligence in fraud detection is a highly effective tool for maintaining transaction security and preventing fraud losses.

The use of artificial intelligence and machine learning algorithms can revolutionise the way organisations in different industries identify and prevent fraud.

1. Predictive modelling

Artificial intelligence and machine learning algorithms can analyse historical data to predict the likelihood of future fraudulent activity. By identifying patterns and anomalies in data, predictive models can proactively identify potential fraud before it occurs, enabling organisations to take preventative action.

2. Anomaly detection

Artificial intelligence and machine learning techniques are good at identifying unusual patterns of behaviour that could indicate fraud. For example, a sudden change in customer behaviour, such as a large purchase from a new location, can be flagged as an indicator of potential fraud for further investigation and mitigation.

3. Natural Language Processing (NLP)[16]

NLP is another key area where artificial intelligence and machine learning play an important role in fraud detection. By analysing written communications such as emails and chat logs, these technologies can identify suspicious behaviour such as unusual language use or requests, helping to identify fraudulent activity at an early stage.

4. Machine Vision

Machine vision is a technology that uses computer vision to analyse images and video, which can be used to detect fraudulent activity such as counterfeit goods or to identify people in surveillance footage. This visual analysis capability enhances fraud detection in a variety of settings.

5. Keep learning

AI algorithms can be continuously trained with new data to improve their accuracy and effectiveness over time. This continuous learning approach ensures that fraud detection systems are always aware of the latest fraud trends and patterns, improving their overall effectiveness in identifying and preventing fraudulent activity.

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 analysing 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

 doi:10.20944/preprints202407.1107.v1

in different trading environments, helping to improve risk mitigation strategies in the financial industry.

4. Neural Networks

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. Their ability to adapt and detect sophisticated fraud schemes makes them an indispensable tool in the ongoing fight against financial fraud, enabling organisations to stay ahead of emerging threats and protect their assets.

Overall, the integration of AI into fraud detection represents a significant step forward in securing digital transactions and increasing trust in online interactions. By harnessing the power of machine learning and data analytics, AI systems can constantly adapt to evolving fraud techniques and stay one step ahead of malicious actors. As AI technology continues to mature, we can expect fraud detection to become more accurate and efficient, further strengthening security measures across industries. However, addressing ethical issues and ensuring transparency in AI-driven fraud detection systems is critical to maintaining trust and accountability. 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. However, this result is subject to large fluctuations, and sometimes the detection accuracy can drop to around 25%.

Nevertheless, these experimental results show that the application of the autoencoder in credit card fraud detection has great potential. In order to further improve the stability and performance of the model, we need to conduct more experiments to explore and optimise more suitable network structures and hyperparameter settings. Through continuous experimentation and adjustment, we expect to find a more stable and efficient deep learning model that can better meet the challenge of anomaly detection.

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.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 16 July 2024 doi:10.20944/preprints202407.1107.v1

4.2. Data Processing

```
(284807, 31)
                Time            V1  ...         Amount          Class
count  284807.000000  2.848070e+05  ...  284807.000000  284807.000000
mean    94813.859575  3.919560e-15  ...      88.349619       0.001727
std     47488.145955  1.958696e+00  ...     250.120109       0.041527
min         0.000000 -5.640751e+01  ...       0.000000       0.000000
25%     54201.500000 -9.203734e-01  ...       5.600000       0.000000
50%     84692.000000  1.810880e-02  ...      22.000000       0.000000
75%    139320.500000  1.315642e+00  ...      77.165000       0.000000
max    172792.000000  2.454930e+00  ...   25691.160000       1.000000

[8 rows x 31 columns]
```

```
0.0017304750013189597
Fraud Cases: 492
Valid Transactions: 284315
```

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.

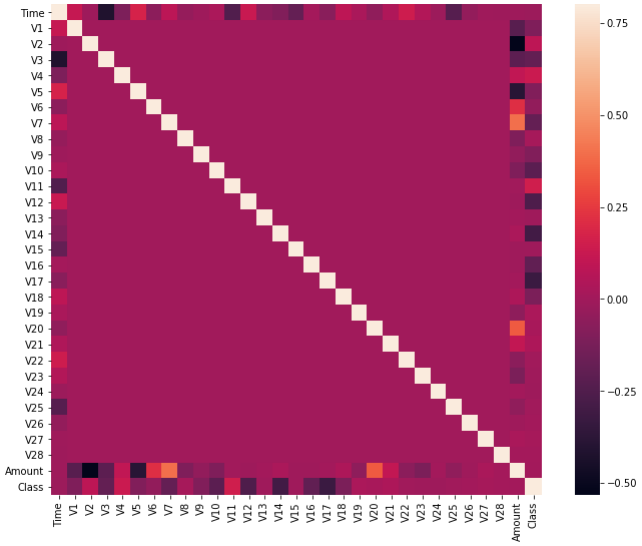

Figure 1. Results of training matrix.

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:10.20944/preprints202407.1107.v1

4.4. Experimental Result

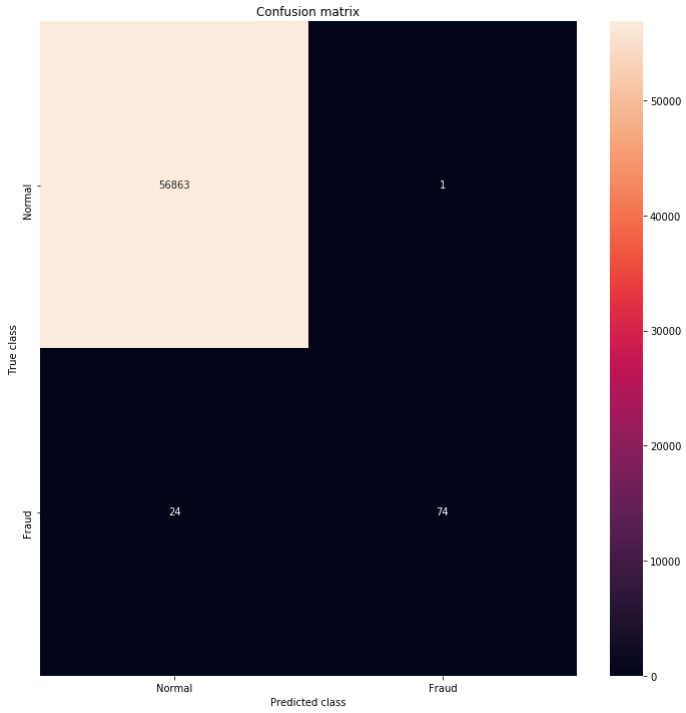

Figure 2. Model diagram of training results.

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.

Overall, this study validates the potential of deep learning in financial fraud detection and provides a valuable reference for subsequent research. We believe that through continuous experimentation and optimization, deep learning models will be able to identify financial fraud more

 doi:10.20944/preprints202407.1107.v1

stably and efficiently, thereby helping financial institutions reduce potential losses and improve security.

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 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. First, the application of deep learning will greatly improve the accuracy and effectiveness of financial fraud detection. Deep learning algorithms, such as autoencoders and neural networks, are capable of processing complex non-linear data to extract valuable features. Through continuous optimisation, these algorithms will have higher detection accuracy and real-time capability to detect anomalous behaviour more effectively and reduce the false positive rate. 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.

AI technology can therefore help financial institutions to share information and data more efficiently and promote international cooperation. Through harmonised technical standards and data interfaces, AI will facilitate the exchange of information across borders, thereby enhancing the overall capacity of global financial regulation.

References

1. Shi, Y., Yuan, J., Yang, P., Wang, Y., & Chen, Z. Implementing Intelligent Predictive Models for Patient Disease Risk in Cloud Data Warehousing.
2. Zhan, T., Shi, C., Shi, Y., Li, H., & Lin, Y. (2024). Optimization Techniques for Sentiment Analysis Based on LLM (GPT-3). arXiv preprint arXiv:2405.09770.
3. Lin, Y., Li, A., Li, H., Shi, Y., & Zhan, X. (2024). GPU-Optimized Image Processing and Generation Based on Deep Learning and Computer Vision. *Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023*, *5*(1), 39-49.
4. Chen, Zhou, et al. "Application of Cloud-Driven Intelligent Medical Imaging Analysis in Disease Detection." Journal of Theory and Practice of Engineering Science 4.05 (2024): 64-71.
5. Wang, B., Lei, H., Shui, Z., Chen, Z., & Yang, P. (2024). Current State of Autonomous Driving Applications Based on Distributed Perception and Decision-Making.
6. Jiang, W., Qian, K., Fan, C., Ding, W., & Li, Z. (2024). Applications of generative AI-based financial robot advisors as investment consultants. Applied and Computational Engineering, 67, 28-33.
7. Yang, J., Qin, H., Por, L. Y., Shaikh, Z. A., Alfarraj, O., Tolba, A., ... & Thwin, M. (2024). Optimizing diabetic retinopathy detection with inception-V4 and dynamic version of snow leopard optimization algorithm. Biomedical Signal Processing and Control, 96, 106501.
8. Fan, C., Li, Z., Ding, W., Zhou, H., & Qian, K. Integrating Artificial Intelligence with SLAM Technology for Robotic Navigation and Localization in Unknown Environments.
9. Guo, L., Li, Z., Qian, K., Ding, W., & Chen, Z. (2024). Bank Credit Risk Early Warning Model Based on Machine Learning Decision Trees. *Journal of Economic Theory and Business Management*, *1*(3), 24-30.
10. Li, Zihan, et al. "Robot Navigation and Map Construction Based on SLAM Technology." (2024).
11. Fan, C., Ding, W., Qian, K., Tan, H., & Li, Z. (2024). Cueing Flight Object Trajectory and Safety Prediction Based on SLAM Technology. Journal of Theory and Practice of Engineering Science, 4(05),

 doi:10.20944/preprints202407.1107.v1

12. Ding, W., Tan, H., Zhou, H., Li, Z., & Fan, C. Immediate Traffic Flow Monitoring and Management Based on Multimodal Data in Cloud Computing.
13. Zhou, C., Zhao, Y., Liu, S., Zhao, Y., Li, X., & Cheng, C. (2024). Research on Driver Facial Fatigue Detection Based on Yolov8 Model.
14. Xin, Q., Xu, Z., Guo, L., Zhao, F., & Wu, B. (2024). IoT Traffic Classification and Anomaly Detection Method based on Deep Autoencoders.
15. Yang, T., Li, A., Xu, J., Su, G., & Wang, J. (2024). Deep Learning Model-Driven Financial Risk Prediction and Analysis.
16. Zhou, C., Zhao, Y., Zou, Y., Cao, J., Fan, W., Zhao, Y., & Cheng, C. (2024). Predict Click-Through Rates with Deep Interest Network Model in E-commerce Advertising. arXiv preprint arXiv:2406.10239.
17. He, Z., Shen, X., Zhou, Y., & Wang, Y. (2024, January). Application of K-means clustering based on artificial intelligence in gene statistics of biological information engineering. In Proceedings of the 2024 4th International Conference on Bioinformatics and Intelligent Computing (pp. 468-473).
18. Gong, Y., Zhu, M., Huo, S., Xiang, Y., & Yu, H. (2024, March). Utilizing Deep Learning for Enhancing Network Resilience in Finance. In 2024 7th International Conference on Advanced Algorithms and Control Engineering (ICAACE) (pp. 987-991). IEEE.
19. Zhou, C., Zhao, Y., Cao, J., Shen, Y., Gao, J., Cui, X., ... & Liu, H. (2024). Optimizing search advertising strategies: Integrating reinforcement learning with generalized second-price auctions for enhanced ad ranking and bidding. arXiv preprint arXiv:2405.13381.
20. Tian, J., Li, H., Qi, Y., Wang, X., & Feng, Y. (2024). Intelligent medical detection and diagnosis assisted by deep learning. Applied and Computational Engineering, 64, 121-126.
21. Yang, P., Chen, Z., Su, G., Lei, H., & Wang, B. (2024). Enhancing traffic flow monitoring with machine learning integration on cloud data warehousing. Applied and Computational Engineering, 67, 15-21.
22. Restrepo, D., Wu, C., Cajas, S. A., Nakayama, L. F., Celi, L. A. G., & Lopez, D. M. (2024). Multimodal Deep Learning for Low-Resource Settings: A Vector Embedding Alignment Approach for Healthcare Applications. medRxiv, 2024-06.
23. Cajas, S. A., Restrepo, D., Moukheiber, D., Kuo, K. T., Wu, C., Chicangana, D. S. G., ... & Celi, L. A. A multi-modal satellite imagery dataset for public health analysis in colombia.
24. hang H, Diao S, Yang Y, Zhong J, Yan Y. Multi-scale image recognition strategy based on convolutional neural network. Journal of Computing and Electronic Information Management. 2024 Apr 30;12(3):107-13.
25. Zhou, Y., Zhan, T., Wu, Y., Song, B., & Shi, C. (2024). RNA Secondary Structure Prediction Using Transformer-Based Deep Learning Models. *arXiv preprint arXiv:2405.06655*.
26. Liu, B., Cai, G., Ling, Z., Qian, J., & Zhang, Q. (2024). Precise Positioning and Prediction System for Autonomous Driving Based on Generative Artificial Intelligence. Applied and Computational Engineering, 64, 42-49.
27. Cui, Z., Lin, L., Zong, Y., Chen, Y., & Wang, S. (2024). Precision Gene Editing Using Deep Learning: A Case Study of the CRISPR-Cas9 Editor. Applied and Computational Engineering, 64, 134-141.
28. Rosner, B., Tamimi, R. M., Kraft, P., Gao, C., Mu, Y., Scott, C., ... & Colditz, G. A. (2021). Simplified breast risk tool integrating questionnaire risk factors, mammographic density, and polygenic risk score: development and validation. Cancer Epidemiology, Biomarkers & Prevention, 30(4), 600-60.
29. Wang, B., He, Y., Shui, Z., Xin, Q., & Lei, H. (2024). Predictive Optimization of DDoS Attack Mitigation in Distributed Systems using Machine Learning. Applied and Computational Engineering, 64, 95-100.
30. Zhan, X., Ling, Z., Xu, Z., Guo, L., & Zhuang, S. (2024). Driving Efficiency and Risk Management in Finance through AI and RPA. Unique Endeavor in Business & Social Sciences, 3(1), 189-197.
31. Xu, Z., Guo, L., Zhou, S., Song, R., & Niu, K. (2024). Enterprise Supply Chain Risk Management and Decision Support Driven by Large Language Models. Applied Science and Engineering Journal for Advanced Research, 3(4), 1-7.
32. Song, R., Wang, Z., Guo, L., Zhao, F., & Xu, Z. (2024). Deep Belief Networks (DBN) for Financial Time Series Analysis and Market Trends Prediction.