Proceedings of the 6th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/87/20241541

Integrating a machine learning-driven fraud detection system based on a risk management framework

Lingfeng Guo[1,6], Runze Song[2], Jiang Wu[3], Zeqiu Xu[4], Fanyi Zhao[5]

[1]Business Analytics, Trine University, AZ, USA
[2]Information System & Technology Data Analytics, California State University, CA, USA
[3]Computer Science, University of Southern California, Los Angeles, CA, USA
[4]Information Networking, Carnegie Mellon University, PA, USA
[5]Computer Science, Stevens Institute of Technology, NJ, USA

[6]glf9871@gmail.com

Abstract. This article explores the application of machine learning techniques, specifically focusing on ensemble methods like Random Forests, for detecting fraudulent activities in digital financial transactions. Highlighting the evolution from traditional statistical approaches to modern machine learning models, it underscores the effectiveness of Random Forests in handling the inherent challenges of imbalanced datasets typical in fraud detection scenarios. Using a Kaggle dataset of credit card transactions, the study optimizes Random Forest parameters through rigorous parameter tuning, achieving significant improvements in model performance metrics such as Area Under the Curve (AUC). The findings underscore the critical role of machine learning in enhancing fraud detection capabilities, emphasizing the ongoing evolution and future potential of these methodologies in financial risk management.

Keywords: Fraud Detection, Machine Learning, Random Forest, Financial Risk Management

1. Introduction

The risk management system is a broad and complex topic involving a body of knowledge covering many aspects. Its construction process is not uniform but according to different business structures for "targeted" shape from the perspective of industry division, standard credit card industry, cash loan industry, third-party payment/transaction industry, auto finance industry, and financial leasing industry. From the perspective of the division of the end audience, it can be divided into B end (to B) and C end (to C). With the continuous improvement of national policy supervision, especially in the financial industry, the importance of risk compliance has increased sharply.[1]Therefore, the construction of the risk management sub-system can be divided into risk prevention and control and risk compliance.

The division from different angles is to focus better, but it does not mean that these are independent, divided states.

Anti-fraud risk management covers customer credit and money applications for Internet revolving credit products. Among them, the leading fraud prevention in the credit application process includes non-personal applications, false information, gang fraud, etc. The prominent fraud cases to be prevented in the application of funds include account theft, account cracking, and dragging the library into the

DOI: 10.54254/2755-2721/87/20241541

library. In this complex risk management environment, machine learning-driven fraud detection systems have become a powerful tool that can provide effective fraud prevention and control at all process stages and improve financial institutions' overall risk management capabilities.

2. Related work

2.1. Traditional Fraud Detection Methods

Many foreign scholars studied fraud detection relatively early, starting in the late 1980s, and gradually developed various fraud detection methods. [2-3]In the late 1980s, researchers presented a fraud detection case study using simple statistical techniques, one of the first attempts. This was followed by another study for fraud detection using regression analysis methods, further advancing the field. For credit card fraud detection in the late 1990s, a study applied distributed data mining technology to credit card fraud detection, significantly improving detection efficiency. This method marks an essential advancement in credit card fraud detection.

In the 21st century, credit card fraud detection methods based on cost-sensitive learning have been proposed.[4]This method defines a performance measure that reflects the cost of a classifier within a specific operating range and directly optimizes this performance measure through evolutionary programming to train a classifier suitable for real-world credit card fraud detection. This innovation has achieved remarkable results in improving the practical application effect of the classifier. In addition, a credit card fraud detection method based on the Hidden Markov model (HMM) is also proposed. In this approach, the researchers simulated the sequence of operations that process credit card transactions using HMM. HMM is trained on the expected behavior of the cardholder. If HMM does not accept a credit card transaction received with a high enough probability, it is considered fraud. This method uses serial pattern recognition technology to provide a new perspective and method for credit card fraud detection.

In recent years, more studies have compared various data mining techniques to credit card fraud detection. One study used three models: random forest, support vector machine, and logistic regression, and the results showed that random forest performed best in this process. [5]In addition, the new method based on a cost-sensitive decision tree has better performance indicators such as accuracy and actual positive rate on a given set of problems than the existing known methods. The method also defines a cost-sensitive measure for credit card fraud detection. These traditional and emerging methods have laid a solid foundation for fraud detection research and driven the continuous evolution and application of the technology.

2.2. Application of Machine Learning in Fraud Detection

Because ML algorithms can learn from historical fraud patterns and identify them in future transactions, fraud detection using machine learning becomes possible. Machine learning algorithms are more efficient than humans regarding information processing speed. In addition, machine learning algorithms can detect complex fraud features that humans cannot.

1. Work faster.[6]A rules-based fraud prevention system means creating precise written rules that "tell" the algorithm which types of operations look normal and should be allowed and which shouldn't because they look suspicious. However, writing rules takes a lot of time. Moreover, manual interactions in e-commerce are so dynamic that things can change significantly in days. Here, machine learning fraud detection methods will come in handy to learn new patterns.
2. Scale. ML methods show better performance as the data sets, they fit grow - meaning that the more samples of fraudulent operations they accept, the better their ability to identify fraud. The principle only applies to rules-based systems if they never evolve independently. In addition, data science teams should be aware of the risks of rapid model scaling. If the model does not detect fraud and incorrectly flags it, this will lead to underreporting in the future.
3. Efficiency. Machines can take over the repetitive work of routine tasks and human fraud analysis, and experts will be able to spend their time making more advanced decisions.

DOI: 10.54254/2755-2721/87/20241541

The recent emergence of cards with chips (EMV cards)[7] has helped reduce card fraud in Europe but not in the United States, where the elimination process for magnetic stripe cards has been prolonged.

Furthermore, fraud models can be solved by supervised and unsupervised machine learning algorithms. A traditional classification algorithm is used. In the second case, we can use anomaly detection techniques. The use of neural networks is also effective, but it requires a lot of training data, with two types of data points in equal numbers: abnormal and normal. However, in the case of fraud detection, there is always a lack of balanced data sets.

2.3. Risk Management Framework

Under the influence of big data, the financial risk may become the ignition point of the financial crisis at any time, and the impact and consequences of the financial crisis are tremendous, far from the specific measures that financial institutions can solve alone. [8]Therefore, the financial industry must implement measures at the early stage of financial risks to avoid financial crises. In their work, those working in the financial industry must ensure the security of funds in each transaction and consider its potential to create financial risks. The relevant personnel of financial enterprises need to keenly perceive financial risks, control the overall development situation when dealing with financial business, and effectively avoid financial risks.

Risk management measures mainly include four aspects. First of all, enterprise risk analysis is conducted, transaction data in financial business is analyzed, data security is ensured, and an in-depth analysis of ACH transaction data is conducted. Second, the staff needs to analyze business contacts and fraud by identifying credit card holder information and verifying portrait, fingerprint, or personal information to ensure that there is no fraud. [9-10]Third, cross-account reference analysis should be carried out, the scope of financial business expanded, and comprehensive analysis should be conducted through ACH transaction data. Finally, statistics and analysis of network risks are carried out so counterparties can fully grasp the potential risks. The comprehensive application of these measures can effectively improve the risk management capabilities of financial institutions and prevent financial risks from evolving into financial crises.

2.4. Conclusion and Transition to Methodology

Traditional fraud detection methods have laid the groundwork for current practices by employing statistical techniques, regression analysis, and data mining methods, achieving significant advancements in fraud detection efficiency. The development of cost-sensitive learning and the application of Hidden Markov Models (HMM) have further enhanced the detection of fraudulent activities. These methods, along with new approaches like the artificial immune system and feature engineering, have progressively improved fraud detection systems.

Machine learning (ML) [11]has revolutionized fraud detection by offering rapid, scalable, and efficient solutions unlike rules-based systems, which require manual updates, ML algorithms can learn and adapt from historical data, identifying complex fraud patterns that are challenging for humans to detect. The application of ML in fraud detection ranges from supervised and unsupervised learning algorithms to neural networks, although challenges such as imbalanced datasets remain.

Given the continuous evolution of fraud detection methods and the critical role of risk management, the next section will explore the methodology for developing a machine learning-driven fraud detection model. This model aims to address the complexities and dynamic nature of fraudulent activities, leveraging advanced ML techniques to enhance the accuracy and efficiency of fraud prevention in financial institutions.

3. Methodology

In digital financial payments, accurately predicting user payment behavior is crucial to help financial institutions better understand user needs, manage risks, and optimize services. Ensemble learning is not a single machine learning algorithm; it integrates multiple base learners (i.e., weak learners), eventually forming a strong learner. [12]These base learners should have a degree of predictive accuracy and

DOI: 10.54254/2755-2721/87/20241541

diversity; that is, they differ in the learning process. Decision trees and neural networks are commonly used as base learners.

3.1. Model discussion

Decision trees are a standard machine learning method that can generate 3-5 layers of decision trees based on selected specific variables to generate anti-fraud rules. A decision tree can decompose the complex decision process into a series of simple steps, making the decision process more intuitive and easier to understand. In the anti-fraud field, decision trees can be used to identify fraud, for example, to determine whether a transaction is authentic based on the user's behavior, transaction history, and other characteristics.

1. Random forest is an ensemble learning method that makes predictions by generating many decision trees and taking the average of their outputs. [13-14]This approach can generate hundreds or thousands of trees, allowing for more non-human-controlled combinations of variables and entry threshold possibilities. This means that random forests can deal with complex fraud more flexibly and with higher recognition accuracy.

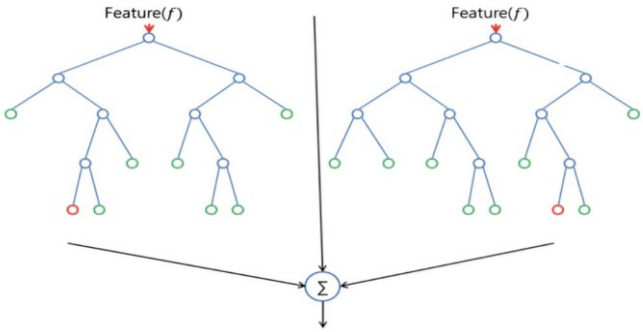

Figure 1. Decision tree random forest model

2. In the anti-fraud field, the number of samples is usually tiny, and the fraud risk of each sample is different. In this case, traditional machine learning methods may not accurately identify fraud due to insufficient data volume. Therefore, it is recommended that ensemble learning methods such as random forest be used to improve the accuracy of recognition.

3.2. Data set

The dataset used in this study is from a Kaggle challenge focused on predicting fraudulent activities in credit card transactions. The "Credit Card Fraud Detection" dataset records transactions made by European credit cardholders in September 2013. It contains a total of 284,807 transactions, of which 492 are fraudulent.

This study aims to explore and compare the performance of three commonly used machine learning models: XGBoost, decision tree, and random forest on financial digital payment datasets. Therefore, by comparing the classification prediction performance of these three models on financial digital payment datasets, we aim to determine which model is most suitable for digital payment behavior prediction.

This dataset is commonly used in machine learning research for fraud detection due to its imbalance between every day and fraudulent transactions, making it challenging yet representative of real-world scenarios.

Table 1. Dataset Description

Feature Column	Description
PCA Component 1	Description of PCA component 1
PCA Component 2	Description of PCA component 2

DOI: 10.54254/2755-2721/87/20241541

Table 1. (continued).

...	...
PCA Component 29	Description of PCA component 29
Class	Target variable indicating fraudulent (1) or normal (0) transaction

3.2.1.1. Notes

- **Purpose**: The dataset aims to study and predict fraudulent credit card transactions to enhance the security of payment systems and user trust.
- **Features**: The transformed dataset contains 29 principal component columns derived from PCA, representing linearly independent components of the original data.
- **Feature Examples**: These components may encapsulate various transaction-related factors such as transaction amount, time, location, and other transaction details.

By presenting the dataset characteristics in this tabular format, readers can easily grasp the structure and purpose of the data used in your study. This approach clarifies the use of PCA for dimensionality reduction and emphasizes the focus on predicting fraudulent transactions to improve financial system security and user confidence.

3.2.1.2. Prediction model

Random forest is a very representative Bagging integration algorithm, which is strengthened based on Bagging. All its base learners are CART decision trees. The traditional decision tree selects the optimal attribute in the attribute set of the current node (assuming d attributes) when selecting partition attributes. However, in the decision tree of random forest, now the attribute set of each node randomly selects a subset of some k attributes, and then selects an optimal feature in the subset to make the left and right subtree division of the decision tree:

$$k = \log_2 d \tag{1}$$

In sci-kit-learn, the classification class of Random Forest is Random Forest Classifier and the regression class is RandomForestRegressor. Parameters for parameter adaptation include two parts. The first part is the parameters of the Bagging framework. The second part is the parameters of the CART decision tree.

This study focuses on optimizing the Random Forest (RF) model parameters for predicting fraudulent credit card transactions using the Kaggle dataset. The dataset comprises 284,807 transactions from September 2013, with a significant class imbalance—492 fraudulent cases and the remaining normal transactions. To address this imbalance, an under-sampling strategy was employed to balance the dataset for training. The primary objective was to enhance model performance by tuning key parameters such as estimators, adept, and min_samples_split.

3.3. Experimental design

Initially, the RF model was trained using default parameters, achieving an initial out-of-bag (OOB) score and test AUC of 0.924 and 0.967, respectively. Subsequently, parameter optimization began with a grid search approach. First, estimators were optimized, resulting in the selection of 50 trees for improved performance. Next, adept was tuned to 6, followed by min_samples_split set to 5, yielding further improvements in AUC to 0.978 and 0.982, respectively. Integrating these optimized parameters into the final RF model significantly enhanced its predictive capabilities. The refined RF model with estimators=50, adept=6, and min_samples_split=5 achieved an OOB score of 0.933 and a test AUC of 0.978, demonstrating notable improvements over the default settings.

DOI: 10.54254/2755-2721/87/20241541

3.4. Experimental result

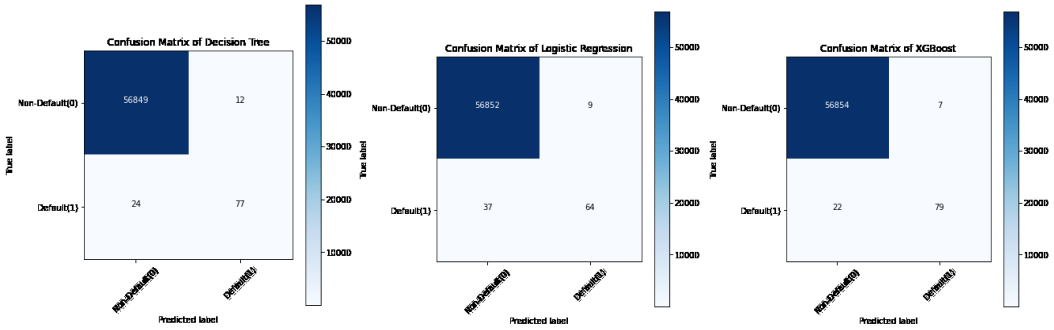

Figure 2. Fraud detection training results of three models

Discussion: Take the confusion matrix of the XGBoost model as an example.

- The first line is the transaction with an actual fraud value of 0 in the test set. It can be calculated that 56,861 of the fraud values are 0. Of the 56,861 non-fraudulent transactions, the classifier correctly predicted 56,854 of them to be 0 and predicted 7 of them to be 1. This means that for 56,854 non-fraudulent transactions, the actual churn value in the test set was 0, which the classifier also correctly predicted. We can say that our model has classified non-fraudulent transactions and that the transactions are good.
- The second line. There were 101 transactions with a fraud value of 1. The classifier correctly predicted 79 of them as one and incorrectly predicted 22 of them as 0. The wrong predicted value can be considered an error in the model.

Therefore, when comparing the confusion matrix of all models, the K-Nearest Neighbors model does an excellent job of classifying fraudulent transactions from non-fraudulent transactions, followed by the XGBoost model.This summary encapsulates the study's key outcomes, emphasizing the impact of parameter tuning on improving the RF model's ability to detect fraudulent transactions in financial digital payment systems.

4. Conclusion

With the rapid development of financial technology and the digital transformation of financial services, applying machine learning in financial risk management is particularly important and necessary. Especially in identifying and preventing fraudulent activities, traditional statistical methods have been unable to meet the increasingly complex fraud detection needs.

In addition, as regulatory requirements and consumer expectations rise, financial institutions are increasingly focused on risk management and security. Machine learning can help institutions respond quickly to potential fraud in real-time transactions and optimize overall risk management strategies through a data-driven approach. As a result, foreseeable future developments in the financial sector include more efficient risk prediction and management through enhanced learning and real-time data processing technologies, as well as the use of emerging technologies such as blockchain and secure computing to ensure the security and trust of financial information. The application of machine learning in financial risk management is promising, but continuous innovation and progress are needed to meet the changing financial environment and technological challenges. Through interdisciplinary collaboration and technological innovation, we can expect more significant progress and achievements in fraud detection and risk management in the future.

References

[1] Power, Michael. "The risk management of everything." The Journal of Risk Finance 5.3 (2004): 58-65.

DOI: 10.54254/2755-2721/87/20241541

[2] Ahmed, Ammar, Berman Kayis, and Sataporn Amornsawadwatana. "A review of techniques for risk management in projects." Benchmarking: an international journal 14.1 (2007): 22-36.
[3] Hopkin, P. (2018). Fundamentals of risk management: understanding, evaluating and implementing effective risk management. Kogan Page Publishers
[4] Rasmussen, J. (1997). Risk management in a dynamic society: a modeling problem. Safety Science, 27(2-3), 183-213.
[5] Abdallah, Aisha, Mohd Aizaini Maarof, and Anazida Zainal. "Fraud detection system: A survey." Journal of Network and Computer Applications 68 (2016): 90-113.
[6] Ogwueleka, F. N. (2011). Data mining application in credit card fraud detection system. Journal of Engineering Science and Technology, 6(3), 311-322.
[7] Song, Jintong, et al. "LSTM-Based Deep Learning Model for Financial Market Stock Price Prediction." Journal of Economic Theory and Business Management 1.2 (2024): 43-50.
[8] Cheng, Qishuo, et al. "Monetary Policy and Wealth Growth: AI-Enhanced Analysis of Dual Equilibrium in Product and Money Markets within Central and Commercial Banking." Journal of Computer Technology and Applied Mathematics 1.1 (2024): 85-92.
[9] Li, Huixiang, et al. "AI Face Recognition and Processing Technology Based on GPU Computing." Journal of Theory and Practice of Engineering Science 4.05 (2024): 9-16.
[10] Qin, Lichen, et al. "Machine Learning-Driven Digital Identity Verification for Fraud Prevention in Digital Payment Technologies." (2024).
[11] 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.
[12] Lakshmi, S. V. S. S., & Kavilla, S. D. (2018). Machine learning for credit card fraud detection system. International Journal of Applied Engineering Research, 13(24), 16819-16824.
[13] Qian, K., Fan, C., Li, Z., Zhou, H., & Ding, W. (2024). Implementation of Artificial Intelligence in Investment Decision-making in the Chinese A-share Market. Journal of Economic Theory and Business Management, 1(2), 36-42.
[14] Qi, Y., Wang, X., Li, H., & Tian, J. (2024). Leveraging Federated Learning and Edge Computing for Recommendation Systems within Cloud Computing Networks. arXiv preprint arXiv:2403.03165.