A Comparative Study of Machine Learning Methods in Financial Fraud Detection

*Zishan Liu

Beijing University of Technology, Beijing, 100124, China
*Email:1280538273@qq.com

Abstract. Financial fraud detection has become increasingly crucial with the rise of digital finance, where fraudulent activities are growing more sophisticated and concealed. This paper provides a comparative analysis of various machine learning methods applied to financial fraud detection, evaluating their effectiveness in different scenarios. Supervised learning techniques such as Logistic Regression, Decision Trees, Random Forests, and Support Vector Machines (SVM) are examined for their performance, model complexity, and interpretability. Unsupervised methods like K-Means and DBSCAN are also considered, focusing on their ability to identify fraud patterns in unstructured data. Deep learning models, including Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Graph Neural Networks (GNN), are evaluated for their capacity to handle large-scale, complex datasets but also face challenges related to data requirements and computational costs. The paper highlights the strengths and limitations of each approach, offering insights into their practical applications and areas for future research in enhancing fraud detection models' adaptability, interpretability, and efficiency.

Keywords: Financial Fraud Detection； Machine Learning； Supervised Learning; Unsupervised Learning; Deep Learning

1 INTRODUCTION

Financial fraud is a common form of economic crime. With the proliferation of digital finance, fraudulent activities have become more concealed and complex. To effectively detect and prevent financial fraud, financial institutions are increasingly adopting advanced machine learning technologies[1]. This paper aims to compare the application effectiveness of several common machine learning methods in financial fraud detection, providing references for researchers and practitioners.

2 BACKGROUND AND CHALLENGES OF FINANCIAL FRAUD

Financial fraud includes various forms such as credit card fraud, loan fraud, and insurance fraud. As technology advances, fraudulent tactics are constantly evolving,

A. Bhunia et al. (eds.), *Proceedings of the 2024 2nd International Conference on Finance, Trade and Business Management (FTBM 2024)*, Advances in Economics, Business and Management Research 304,
https://doi.org/10.2991/978-94-6463-546-1_44

posing challenges to traditional rule-based methods. Machine learning technologies, by learning and analyzing large amounts of historical data, can timely identify potential fraudulent activities, offering greater flexibility and adaptability[2].

2.1 Characteristics of Financial Fraud

Concealment: Fraudsters often use complex techniques to hide their activities, making detection difficult.

Diversity: Fraud takes many forms, including identity theft, document forgery, and fraudulent transactions.

High Real-time Requirements: Financial transactions usually require real-time processing, demanding that detection models respond quickly.

2.2 Challenges in Financial Fraud Detection

Financial fraud detection faces numerous challenges, including large and complex data volumes. Financial systems generate massive amounts of transaction data daily, encompassing both structured and unstructured information[3], which increases the difficulty of data processing and analysis. Additionally, the proportion of fraudulent activities in financial transactions is usually very low, leading to highly imbalanced datasets, making it difficult for detection models to accurately identify the few instances of fraud. Furthermore, as fraudulent methods continue to evolve, models need strong generalization capabilities to cope with the dynamic nature of fraud and maintain the effectiveness of detection.

3 APPLICATION OF MACHINE LEARNING IN FINANCIAL FRAUD DETECTION

As financial transactions become increasingly digitized, financial fraud has grown more complex and covert. Traditional rule-based methods struggle to keep pace with these emerging fraudulent techniques. Machine learning technology, with its robust data processing and predictive capabilities, has found widespread application in the field of financial fraud detection. Below is a detailed introduction to several common machine learning methods and their applications in financial fraud detection[4].

3.1 Supervised Learning

Supervised learning is one of the most common techniques in the field of machine learning. It involves training models using labeled datasets to learn the mapping between input data and target labels, which can then be applied to predict new data. In financial fraud detection, supervised learning methods can effectively identify known fraud patterns and make predictions based on historical data. Commonly used supervised learning algorithms include Logistic Regression, Decision Trees, Random Forests, and Support Vector Machines (SVM)[5].

Logistic Regression. Logistic Regression is a linear model widely used for binary classification problems. It learns the linear relationship between input features and the target variable, using a Sigmoid function to map the output to a range of [0,1], thus predicting whether a transaction is fraudulent. Logistic Regression is relatively simple, easy to implement and interpret, making it particularly suitable for scenarios requiring quick results. Its computational efficiency makes it ideal for real-time fraud detection. However, due to its linear assumption, Logistic Regression has limited performance when dealing with complex non-linear data. When there are intricate interactions or non-linear relationships between data features, the model may struggle to capture these, leading to suboptimal detection performance[6].

Decision Tree. A Decision Tree is a classification model based on a tree structure that divides data into different categories through a series of decision conditions. In financial fraud detection, a Decision Tree model can classify transactions based on the different values of features, thereby determining whether a transaction is fraudulent[7]. The structure of a Decision Tree is intuitive and easy to understand and explain. It can handle non-linear relationships and does not require data preprocessing (e.g., normalization or standardization). Additionally, Decision Trees can handle various types of data (numerical and categorical). However, Decision Tree models are prone to overfitting, meaning they may perform well on training data but lack generalization ability on new data. To address this issue, pruning techniques or combining with other models (e.g., Random Forests) are usually needed to improve the robustness of the model.

Random Forest. Random Forest is an ensemble learning method that improves the predictive power and stability of the model by constructing a collection of multiple decision trees[8]. Each tree is independently trained on different subsets of samples, and the final prediction is the vote or average of the predictions from each tree. Random Forest performs well in handling high-dimensional and imbalanced datasets, as it aggregates the results of multiple models, reducing the risk of overfitting in individual models. Its robustness and predictive accuracy make it suitable for large-scale datasets in financial fraud detection. However, because Random Forest consists of multiple decision trees, the model has high computational complexity, leading to longer training and prediction times. Additionally, due to its ensemble nature, Random Forest's interpretability is lower, making it difficult to intuitively understand the impact of individual features on the prediction results.

Support Vector Machine (SVM). Support Vector Machine (SVM) is a powerful binary classification model that finds a hyperplane that maximizes the margin between different classes of data points[9]. SVM is particularly suitable for handling small sample sizes and high-dimensional data, performing well in high-dimensional spaces, and handling complex non-linear relationships. By using kernel functions (such as Gaussian kernels, polynomial kernels), SVM can map non-linear data to higher-dimensional spaces for linear classification. Despite this, SVM is sensitive to outliers, and when dealing with large datasets, the computational complexity is high, resulting in long training times. Moreover, the choice of kernel function and parameter tuning significantly impacts the model's performance, requiring certain expertise and fine-tuning.

3.2 Unsupervised Learning

Unsupervised learning is suitable for situations where data labels are lacking or unknown, by analyzing the inherent structure or patterns of the data to identify anomalies. In financial fraud detection, unsupervised learning methods can be used to discover new fraud patterns or identify anomalous transactions[10]. Commonly used unsupervised learning methods include K-Means clustering, Density-Based Spatial Clustering of Applications with Noise (DBSCAN), and Principal Component Analysis (PCA).

K-Means Clustering. K-Means is a centroid-based clustering algorithm that assigns data points to a predefined number of k clusters, minimizing the distance between data points within a cluster. This method is often used to find natural distribution patterns in data, making it particularly suitable for processing large-scale datasets. K-Means is simple and computationally efficient, helping to uncover potential fraud patterns in transaction data. However, K-Means is sensitive to the selection of initial centroids and may lead to local optima. Additionally, its performance is poor in handling non-convex clusters or noisy data, and the choice of k value needs to be predefined, usually determined through experimentation.

Density-Based Spatial Clustering of Applications with Noise (DBSCAN). DBSCAN is a density-based clustering algorithm that forms clusters by identifying regions of high density and labeling data points in low-density regions as noise. DBSCAN can effectively handle noisy data and irregularly shaped clusters, making it a robust clustering method. Unlike K-Means, DBSCAN can automatically identify the number of clusters without the need for a predefined number, and it is more effective in dealing with noisy data. However, the parameter selection (such as ε and MinPts) significantly influences clustering results, and its performance is less stable in high-dimensional data. Additionally, this algorithm has lower computational efficiency when processing large datasets, which may require longer running times.

Principal Component Analysis (PCA). Principal Component Analysis (PCA) is a commonly used dimensionality reduction technique that extracts the principal components of data through linear transformations, retaining the main information, thus simplifying the data structure and highlighting anomalous patterns. In financial fraud detection, PCA can reduce the dimensionality of the data, remove redundant information, and improve the computational efficiency of the model. It helps to discover the global structure of the data and reveal anomalies within the data. However, PCA can only capture linear relationships in the data, which may result in the loss of some useful non-linear information. Furthermore, due to the statistical nature of PCA's dimensionality reduction process, the physical meaning of the principal components is not easily understood, leading to poorer interpretability.

3.3 Deep Learning

Deep learning is a class of machine learning methods based on neural networks that extract features from large, complex datasets through multi-layer neural networks' non-linear mappings. Deep learning performs well in handling large-scale data and complex tasks, such as financial fraud detection. Common deep learning methods include Deep Neural Networks (DNN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN).

Deep Neural Networks (DNN). Deep Neural Networks (DNN) are neural network models composed of multiple layers of perceptrons that extract deep features from input data through layer-by-layer non-linear transformations. DNN can handle large-scale, complex feature data and perform well in recognizing complex patterns and relationships, especially in automatically extracting high-level features without the need for manual feature engineering. Despite this, DNN models require a long training time and high computational resources, and due to their multi-layer non-linear structure, they are prone to overfitting, especially when the training data is insufficient. Additionally, DNN's interpretability is poor, making it difficult to understand its internal workings, which may pose challenges in risk management and compliance in some financial applications.

Convolutional Neural Networks (CNN). Convolutional Neural Networks (CNN) were initially used for image processing by extracting local features through convolution operations. However, CNN has also been successfully applied to financial data detection, capturing local patterns in transaction data to identify anomalies. CNN can effectively extract spatial features from data, performing well in pattern recognition, particularly suitable for processing sequentially arranged data, such as time series or continuous transaction records. Nevertheless, although CNN performs well in image data, it may not be as effective as specialized sequence models (such as RNN) when processing time series data. Additionally, CNN's structural complexity is high, and its training and inference speed is slow, which may become a bottleneck in real-time fraud detection.

Recurrent Neural Networks (RNN). Recurrent Neural Networks (RNN) are neural network models particularly suited for processing time series data, incorporating recurrent connections into the network to remember and process dynamic changes in sequential data. RNN can capture dependencies in time series data, making it suitable for real-time fraud detection in financial transactions, by remembering previous inputs, RNN performs well in handling continuous transaction records. However, RNN is prone to gradient vanishing or exploding problems, affecting the training of long sequences. To address this, modified RNN variants, such as Long Short-Term Memory Networks (LSTM) and Gated Recurrent Units (GRU), have partially solved this issue, but these models still require long training times and have high computational complexity.

3.4 Graph Neural Networks (GNN)

Graph Neural Networks (GNN) are neural network models designed to process graph-structured data by learning relationships and connections between nodes, making them particularly suitable for handling data in complex network structures, such as gang fraud detection in social networks. GNN can capture both node features and graph structure information simultaneously, enhancing the learning of relationships and patterns in complex networks, and can handle heterogeneous and dynamic graph data, making it applicable for identifying anomalous behavior and gang fraud in social networks. However, GNN models have high computational complexity, with long training times and high hardware requirements. Moreover, because GNN models learn by aggregating information from neighboring nodes, their internal mechanisms are complex, resulting in low interpretability, which may pose challenges in practical applications.

4 COMPARISON AND DISCUSSION OF MACHINE LEARNING METHODS

In financial fraud detection, different machine learning methods have their own advantages and disadvantages in terms of model performance, complexity, interpretability, data requirements, and computational cost. The following section provides a detailed comparison and discussion of the machine learning methods mentioned in this paper.

4.1 Model Performance

In financial fraud detection, model performance is evaluated using metrics like accuracy, recall, F1 score, and AUC. Supervised learning methods include Logistic Regression, Decision Trees, Random Forests, and SVM. Logistic Regression is effective for binary classification with clear feature differences but struggles with complex non-linear data. Decision Trees handle non-linear features well and are easy to interpret but can overfit and are sensitive to noise. Random Forests enhance robustness by aggregating multiple Decision Trees, improving generalization but increasing complexity and resource requirements. SVM is effective with high-dimensional data and small samples, capturing non-linear relationships through kernel functions, but is sensitive to outliers and computationally intensive with large datasets.

Unsupervised learning methods like K-Means and DBSCAN are used to identify patterns in transaction data. K-Means is effective for finding clusters but is sensitive to initial values and struggles with non-convex clusters. DBSCAN handles noise and outliers well, detecting clusters with complex shapes, but its performance is sensitive to parameter choices and less stable in high-dimensional data.

Deep learning methods include DNN, CNN, RNN, and GNN. DNNs excel at extracting deep features from large-scale data but require substantial labeled data and are prone to overfitting. CNNs are effective for spatial data patterns and have been adapted for financial data, though they may be less effective for time series data compared to RNNs. RNNs are suited for time series data and real-time fraud detection but face challenges with gradient vanishing in long sequences, partially mitigated by LSTM. GNNs are effective for graph-structured data, capturing complex relationships in networks, but are computationally expensive and closely tied to the graph structure, limiting their applicability to non-graph data.

4.2 Model Complexity and Interpretability

Logistic Regression and Decision Trees are both simple and interpretable, with Logistic Regression providing clear feature contributions, though limited by its linear assumptions. Decision Trees are intuitive and handle non-linear features well but are prone to overfitting, requiring pruning for better generalization.

Random Forests and SVMs offer robustness and effective handling of complex data but come with interpretability challenges. Random Forests aggregate multiple Decision Trees, increasing complexity and reducing direct interpretability, while feature importance analysis offers some insights. SVMs have interpretable decision boundaries in linear cases, but the use of kernel functions for non-linear data complicates interpretation.

Deep learning methods excel in fraud detection but struggle with interpretability. DNNs are powerful but function as "black boxes," with tools like LIME and SHAP offering limited explanations. CNNs provide some interpretability through filters and feature maps, but this is limited for time series data. RNNs, especially LSTM and GRU models, handle sequence data well but are complex and difficult to interpret due to state transitions and memory units. GNNs capture complex graph patterns, but their internal mechanisms are hard to explain, and interpretability in this area is still under development.

4.3 Data Requirements and Computational Costs

Logistic Regression and Decision Trees have low data requirements and are suitable for environments with limited data, as they can train on smaller datasets and converge quickly. In contrast, Random Forests require large datasets to fully utilize ensemble learning, especially for high-dimensional data. SVM performs well with small samples, but as data and feature dimensions increase, so do its data needs. Deep learning models like DNN, CNN, and RNN require substantial labeled data to avoid overfitting and learn complex patterns, with performance declining when data is insufficient. GNNs require not only node features but also the relationships between nodes, with more complex graph structures demanding higher data quality and quantity.

In terms of computational costs, Logistic Regression and Decision Trees are low-cost, suitable for real-time applications and resource-limited environments. Logistic Regression is fast to compute, and Decision Trees manage computational load by controlling tree depth. Random Forests, with multiple Decision Trees, have higher training and prediction costs. SVM has high computational complexity with large datasets, especially when using kernel functions, leading to longer training times. Deep learning models like DNN, CNN, and RNN have high computational costs, particularly during training, requiring significant resources and time. GNNs have significantly higher computational costs with increased graph complexity, requiring high-performance computing resources for training and inference.

5 FUTURE RESEARCH DIRECTIONS

There are still many unresolved issues with machine learning methods in financial fraud detection, including how to enhance model interpretability, address constantly evolving fraud patterns, and improve model efficiency in real-time detection. Future research can combine technologies such as heterogeneous data fusion, multi-modal learning, and federated learning to further improve the accuracy and adaptability of fraud detection.

6 CONCLUSION

This paper compares and analyzes the application of several major machine learning methods in financial fraud detection. Different methods have their own advantages in handling data complexity, model interpretability, and computational resource requirements. In the future, as machine learning technology advances and data in the financial field continues to accumulate, machine learning-based financial fraud detection methods will become more intelligent and efficient.

REFERENCE

1. Liu Hualing, Xu Junyi, Cao Shijie, et al. Research Progress on Digital Financial Fraud Detection in Social Relationship Networks [J]. Journal of Zhejiang University (Science Edition), 2024, 51 (01): 41-54.
2. Wan Qichang. Research on Fraud Detection Models in Fraudster Camouflage Based on Graph Machine Learning [D]. Huazhong University of Science and Technology, 2023.
3. Liu Xiaofei. Research and Application of Knowledge Graph in Financial System Anti-Fraud [D]. University of International Business and Economics, 2023.
4. Li Zhiming. Fraud Detection in the Financial Field Based on Quantum Machine Learning Algorithms [D]. University of Electronic Science and Technology of China, 2023.
5. Hu Xinxin. Research on Key Technologies for Telecom Network Fraud Detection Based on Graph Machine Learning [D]. Strategic Support Force Information Engineering University, 2023.

6. Ning Pengxiang. Research on Financial Fraud Detection Methods Based on Graph Neural Networks [D]. Donghua University, 2023.
7. Zhang Yiyang, Qian Yurong, Tao Wenbin, et al. A Survey on Attribute Graph Anomaly Detection Based on Deep Learning [J]. Computer Engineering and Applications, 2022, 58 (19): 1-13.
8. Meng Meng. Research on Feature Engineering Methods for Internet Financial Fraud Prediction [J]. Technology and Market, 2022, 29 (10): 60-62.
9. Liu Hualing, Liu Yaxin, Xu Junyi, et al. Research Progress on the Application of Graph Anomaly Detection in Financial Anti-Fraud [J]. Computer Engineering and Applications, 2022, 58 (22): 41-53.
10. Lü Fang, Tang Fenghe, Huang Junheng, et al. Research on Financial Fraud Account Detection for Imbalanced Datasets [J]. Computer Engineering, 2021, 47 (06): 312-320.