Proceedings of ICFTBA 2024 Workshop: Finance in the Age of Environmental Risks and Sustainability
DOI: 10.54254/2754-1169/98/2024OX0125

An Investigation of Machine Learning Applications in the Financial Fraud Detection

Yuge Han[1,a,*]

[1]*Finance, East China Normal University, Changfeng Xincun Street, Putuo District, China*
a. 10204700464@stu.ecnu.edu.cn
**corresponding author*

Abstract: Financial fraud presents itself in various forms, and it often involves intricate financial transaction networks, making it challenging to detect the perpetrators and identify the characteristics of the fraud. In recent years, machine learning has gained widespread application within the financial sector. Therefore, various financial fraud detection models have been developed based on diverse machine learning methodologies. In the method part, this paper provides an overview of the machine learning process and then discusses the application of machine learning models in various financial fraud scenarios. Financial fraud in the insurance field has been further refined into automobile and medical insurance fraud. In automobile insurance fraud detection, some studies applied implicit Naive Bayes Model to analyze observable features and estimate hidden variables, and some studies used resampler to solve data imbalance and adopted 7 kinds of machine learning models for analysis. In health insurance fraud detection, many studies train medical data with multiple models, including AdaBoost, Logistic Regression and Support Vector Machine. In credit card fraud detection, studies use five algorithms, including random forest and decision tree et al., and some construct a model combining Decision Tree (DT) and Logistic Regression (LR). In bank fraud detection, some studies introduce Value-at-Risk to combine it with machine learning algorithms, and some studies propose a decentralized model training method based on federated learning. In the discussion section, this paper addresses the current limitations of the research, such as poor interpretability, uneven distribution of data sets, and issues related to customer privacy, and proposes corresponding solutions.

Keywords: Machine learning, fraud detection, finance

1. Introduction

Financial fraud is a method of using illegal and fraudulent means to obtain economic benefits, and it can occur in different fields e.g. banking, healthcare and insurance. Fraud in various sectors exhibits distinct characteristics. For instance, within the banking industry, financial fraud may manifest as anomalous credit card transactions or irregularities in bank account activity. The financial fraud within the insurance industry is evidenced by fraudulent activities in the automobile insurance sector and the collusion of multiple parties within the medical industry to deceive the insurance fund. There is also the practice of money laundering, in which criminals transfer large amounts of illegal funds to undisclosed locations and utilize existing financial services to integrate them into legitimate funds.

DOI: 10.54254/2754-1169/98/2024OX0125

A documentary on Netflix in 2023 recreated the story of Madoff, the mastermind of the largest Ponzi scheme of all time, who with his accomplices stole more than $19 billion from more than 40,000 investors by forging brokerage accounts [1]. Therefore, the detection of financial fraud in advance is crucial due to its significant impact on society and the economy. However, most traditional methods are manual, which is time-consuming, expensive, inaccurate, and unrealistic. Nowadays, with the progress of Artificial Intelligence (AI) methods, machine learning has been used to detect fraudulent activities and continue to evolve.

AI is a branch of computer science that focuses on developing intelligent machines capable of performing tasks that typically require human intelligence. Machine learning is dedicated to creating algorithms and models that enable computers to learn from data and make predictions and decisions. At present, there are many models of machine learning, including neural network, Support Vector Machine (SVM), decision tree etc.

AI is currently being utilized across a wide range of sectors, such as healthcare, manufacturing, transportation, agriculture, and more. Within these domains, AI technology plays a crucial role in data analysis, prediction, optimization, and other applications, delivering significant value to businesses and organizations. For instance, deep learning and machine learning methods are used to perform image and data analysis to classify and track objects such as trains, maintenance equipment, pedestrians, or obstacles [2]. AI is also being used in finance, many studies have discovered the potential of the Long Short-Term Memory (LSTM) networks and used it to predict stock prices [3]. Moreover, some researchers model the investment process as an allocation strategy for a Markov decision process and use risk decomposition techniques and deep reinforcement learning agent models to calculate variance and efficiently update portfolios [4]. In addition, numerous researchers also employ machine learning techniques to conduct in-depth studies on the detection of financial fraud. Aldosari came up with the GRFO-KNN model and used it for credit card fraud detection to classify data as fraudulent or legitimate [5]. Pan et al. proposed an unsupervised method for identifying auto insurance fraud, which is based on dynamic heterogeneous network representation learning. This method utilizes the maximum mutual information coefficient to detect events with a high probability of fraud in the auto insurance process [6]. Based on the recent rapid progress of this field, it is necessary to conduct a comprehensive review of these research findings.

The structure of this review is as follows: the first section serves as the introduction, while the second part provides a specific overview of the research. This section delves into recent advancements in machine learning applications for financial fraud detection. The third segment consists of a discussion that examines the limitations of current achievements and anticipates future research directions. Lastly, the fourth part offers a comprehensive summary of the entire paper.

2. Method

2.1. Process of Machine Learning

The complete machine learning process can be roughly divided into the following five parts:

Data collection and preprocessing: In this step, data is collected from various sources and undergoes cleaning, transformation, and feature engineering.

Model selection and training: The appropriate machine learning model such as decision tree and neural network is chosen according to specific requirements and trained using pre-processed and engineered features.

Model evaluation and tuning: After training, the model is evaluated using metrics such as accuracy, recall, F1 values, Receiver Operating Characteristic (ROC) curves, and Area Under Curve (AUC) before being fine-tuned.

DOI: 10.54254/2754-1169/98/2024OX0125

Model deployment: Once evaluated and tuned, the model is deployed into a real environment through integration into applications or building API interfaces for batch or stream inference.

Model monitoring and maintenance: Post-deployment actions include monitoring performance, updating the model as needed to fix errors or improve its functionality.

The process is depicted by a flow chart as shown in Figure 1 below.

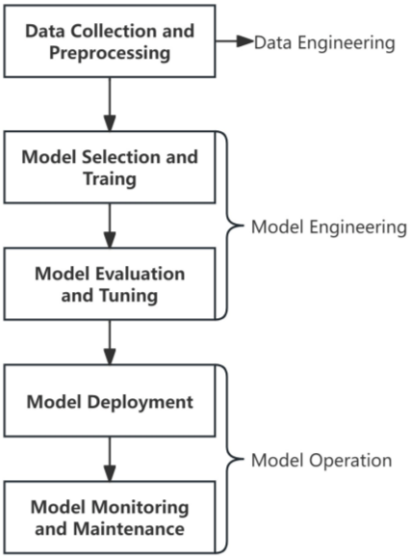

Figure 1: The general workflow of machine learning algorithms (Photo/Picture credit: Original).

2.2. Insurance Fraud Detection

Insurance fraud refers to the act of filing a false insurance claim with the intention of obtaining an illegitimate financial gain, commonly seen in the realms of auto and medical insurance.

2.2.1. Motor Insurance Fraud Detection

Preetham et al. selected the Auto Insurance Claims dataset which includes information about customers, policies, events, and claim amounts, and performed data cleaning, handled missing values, as well as applying feature scaling techniques such as Min-Max scaling for feature normalization [7]. Subsequently, they partitioned the data set into three groups: test, validation, and training. They utilized the Hidden Naive Bayes (HNB) model for analyzing observable features and estimating hidden variables, employed classification labels to denote the legitimacy or suspicion of claims, and furnished fraud scores to offer a quantitative assessment of fraud likelihood [8]. Aiemsuwan et al. obtained three datasets related to auto insurance from the Kaggle website: Car Insurance Fraud [9], Fraudulent Claim on Cars Physical Damage [10], and Auto Insurance Fraud [11] and addressed the data imbalance through resampling techniques and reverse elimination feature selection methods [12]. They employed seven machine learning models, including Random Forest (RF), Logistic Regression (LR), Decision Tree (DT), Naive Bayes (NB), XGBoost (XGB), K Nearest Neighbors (K-NN) and Support Vector Machine (SVM), and utilized scikit-learn during the model training phase.

2.2.2. Healthcare Insurance Fraud Detection

In health insurance, machine learning is also being applied to fraud detection. Chirchi et al. integrated inpatient, outpatient, and beneficiary details data and conducted a series of pre-processing tasks including data cleaning, standardization, and feature engineering et al. [13]. They utilized

DOI: 10.54254/2754-1169/98/2024OX0125

comprehensive healthcare data to train five models, including AdaBoost (ADA), Gradient Boosting Classifier (GBC), LR, SVM and XGB and incorporated the Synthetic Minority Over-sampling Technique (SMOTE) technique to enhance the model's sensitivity towards the small percentage of fraudulent events, thereby establishing a robust and sensitive detection system. Zhou et al. proposed an innovative approach to delineate the spatiotemporal relationship between patients by establishing a shared access network among them and employing the Louvain method for detecting suspicious groups from the shared access network, combined with graphical visualization analysis for fraud monitoring [14].

2.3. Credit Card Fraud Detection

Credit card fraud refers to the unauthorized acquisition of a cardholder's primary credentials, which are then utilized through text or phone communication in a manner that the fraudster disagrees with.

Sreekala et al. choose a credit card transaction dataset from Kaggle, initially applying the elbow method to determine the optimal number of clusters [15]. Then, they utilized K-means in unsupervised learning to train five classification algorithms (RF, DT, K-NN, SVM, and NB) using cluster assignment as pseudo-labels. This integration ensured a comprehensive understanding of fraud patterns. Jemai et al. preprocessed simulated credit card transaction data from the EU cardholder dataset and the Sparkov simulator, and applied three classifiers using Naive Bayes, Random Forest, and XGBoost algorithms for classification [16]. DINGARI JAHNAVI et al. opted for the Kaggle website to access the dataset, implemented a robust hybrid model combining DT and LR, utilized K-Fold cross-validation method, and sequentially applied DT and LR techniques for model evaluation on the segmented dataset. Leveraging the interpretability of LR and the capability of DT to discern intricate decision boundaries, this amalgamated model has the potential to enhance overall fraud detection performance [17].

2.4. Bank Account Fraud

In recent years, the surge in online banking users has raised concerns over the substantial losses incurred by banks and other financial institutions due to New Bank Account (NBA) fraud. NBA refers to the act of opening an account at a bank or other financial institution to commit fraud.

Usman et al. selected the Bank Account Fraud (BAF) dataset and extracted relevant features from the dataset in terms of demographic, behavioral, risk management, and transaction perspectives [18]. They introduced Value-at-Risk (VaR) and used it as a risk measure to treat fraud instances as the worst-case scenario. They used its adjustable confidence level to adjust the skewness of fraud and modeled the skewness of fraud. They combined VaR with machine learning algorithms, such as Binary Logistic Regression (BLR), NB, and K-NN, to form an improved fraud detection model. Awosika et al. proposed a decentralized model training approach based on Federated Learning (FL) that ensures data privacy by locally training the model on the device and sharing only aggregated updates [19]. They developed a Deep Neural Network (DNN) model specifically tailored to detect patterns associated with fraudulent activity across federal databases, ensuring high accuracy. They also mentioned the use of Explainable AI (XAI) in financial fraud detection, such as Autoencoders and Restricted Boltzmann Machines (RBM), which can provide explanations and greater transparency into model decisions.

DOI: 10.54254/2754-1169/98/2024OX0125

3. Discussion

3.1. Limitations and Challenges

Although significant progress has been made in this field, current research still has some limitations. In terms of the methods surveyed in this paper, Usman's experiment did not take into account the time window [18], and the models selected by Jemai, such as XGBoost, were found to be overfitting to the real data set [16].

In the transition from traditional machine learning to deep learning, there exist several challenges within the field. The primary issue lies in the black box perception of deep neural networks, where the interpretability of the model is limited [20]. Deep learning models often derive meaning from outcomes without understanding the underlying reasons or processes that led to those outcomes. This lack of transparency leads to irreproducible results and makes it difficult to identify the cause of prediction errors. Simultaneously, the lack of interpretability in such models may lead to skepticism among domain experts, particularly those in specialized fields like healthcare, to be unconvinced by the model's predictions.

Secondly, large datasets are essential for training machines in deep learning. However, there are instances where the data may be unavailable due to small or unevenly distributed datasets, or real-time data that cannot be updated promptly due to its dynamic nature, and the distribution of data may vary simultaneously [21]. The uneven distribution of data can result in a decline in the predictive performance of the model, and when a specific dataset is used for initial model training, its performance may not generalize well to new datasets.

Last but not least, some of the initial achievements of machine learning and deep learning in various application domains were primarily associated with large-scale centralized data collection, whether within a single data center or through cloud services [22]. However, the centralized gathering of data in a cloud service can significantly infringe upon privacy and subject the clients of the cloud service to substantial legal liabilities in case of a data breach. This is particularly pertinent in relation to healthcare information, voice recordings, home surveillance footage, financial transactions, and other sensitive data. Centralized data collection often leads to a "loss of control" post-upload.

3.2. Future Prospects

In view of the above existing limitations, some potential solutions can be considered.

Researchers have developed a variety of methods to improve the interpretability of large machine learning models, especially deep learning models. These methods are designed to shed light on the decision-making processes of models, helping researchers and users understand how models generate outputs from input data. For example, Locally Interpretable Model-Sensitive Analysis (LIME) approximates the behavior of a model near a specific input by creating a simplified local model, such as linear regression. And Shapley Additive Explanations (SHAP) game theory-based methods for quantifying the contribution of each input feature, such as a word in text, to a specific prediction of a GPT model. This helps reveal key factors in the model's decision-making process.

Transfer learning can be used to reduce distribution differences. Through distribution alignment, the direct difference between the data distribution of the target domain and the data distribution of the source domain is reduced, so that the model can be seamlessly transferred. And the Synthetic Minority Oversampling Technique (SMOTE) has emerged as a robust and widely embraced solution to the challenge of data imbalance.

In terms of privacy, Federated Learning (FL) is a distributed machine learning framework that utilizes secure encryption technology to enable decentralized participants to collaborate on model training without exposing their private data to other participants, thus ensuring privacy protection.

DOI: 10.54254/2754-1169/98/2024OX0125

4. Conclusion

This article offers a comprehensive review of the most recent developments in utilizing machine learning for fraud detection. In the process of the review, it was observed that SVM, RF, and LR are the predominant models utilized for fraud detection, while DT, K-NN, NB and other models are also employed in this domain. Additionally, credit card fraud has emerged as the primary focus of scholarly attention, as evidenced by the largest number of related literatures on this type of fraud. In the following discussion, this paper focuses on the existing issues in current research, including the limited interpretability of models, data set imbalance and distribution differences, as well as privacy concerns arising from training data. The further study will also explore potential future improvements for these respective challenges, including LIME and SHAP to improve interpretability, incorporate transfer learning to address discrepancies, utilize SMOTE techniques to handle data imbalances, and implement Federated learning to tackle privacy concerns.

References

[1] *Madoff: The Monster of Wall Street – Release Date, Cast & News. (2023). Netflix. Retrieved from https://www.netflix.com/tudum/articles/madoff-the-monster-of-wall-street-release-date-cast-news*

[2] *A, R. R. S., G, S. K., & T. K. (2024). AI Precision on Rails Advanced Object Recognition for Train Track Safety – A Survey. In 2024 5th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp. 388-394). Tirunelveli, India.*

[3] *Ruke, S., Gaikwad, G., Yadav, A., Buchade, A., Nimbarkar, S., & Sonawane, A. (2024). Predictive Analysis of Stock Market Trends: A Machine Learning Approach. In 2024 4th International Conference on Data Engineering and Communication Systems (ICDECS) (pp. 1-6). Bangalore, India.*

[4] *Do Nascimento, E., & Lima De Castro, P. A. (2023). Mitigating Risk in Machine Learning-Based Portfolio Management: A Deep Reinforcement Learning Approach. In 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE) (pp. 628-634). Las Vegas, NV, USA.*

[5] *Aldosari, H. (2024). Garra Rufa Fish Optimization-based K-Nearest Neighbor for Credit Card Fraud Detection. In 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT) (pp. 1-5). Bengaluru, India.*

[6] *Pan, Y., Liang, B., Zhang, L., & Na, C. (2023). Dynamic Representation Learning for Unsupervised Fraud Identification in the Auto Insurance. In 2023 China Automation Congress (CAC) (pp. 4459-4464). Chongqing, China.*

[7] *Insurance Claims Fraud Detection [Dataset]. (2024, February 17). Kaggle. Retrieved from https://www.kaggle.com/datasets/mykeysid10/insurance-claims-fraud-detection*

[8] *Preetham, G., Siddu, K., Ramesh, B., Jabbar, M. A., & Sucharita, S. (2024). Insurance Claim Fraud Detection Using Hidden Naive Bayes. In 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT) (pp. 1-6). Bengaluru, India.*

[9] *Gupta, S. (2023, September 25). Car Insurance Fraud. Kaggle. Retrieved from https://www.kaggle.com/code/jwilda3/classifying-fraud-by-decision-trees/data*

[10] *SR. (2023, September 25). Fraudulent Claim on Cars Physical Damage. Kaggle. Retrieved from https://www.kaggle.com/datasets/surekharamireddy/fraudulent-claim-on-cars-physical-damage*

[11] *Shah, B. (2023, August 11). Auto Insurance Claims Data. Kaggle. Retrieved from https://www.kaggle.com/datasets/buntyshah/auto-insurance-claims-data*

[12] *Aiemsuwan, P., & Srikamdee, S. (2024). A Novel Hybrid Method for Imbalanced Automobile Insurance Fraud Detection. In 2024 16th International Conference on Knowledge and Smart Technology (KST) (pp. 12-17). Krabi, Thailand.*

[13] *Chirchi, K. E., & Kavya, B. (2024). Unraveling Patterns in Healthcare Fraud through Comprehensive Analysis. In 2024 11th International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 585-591). New Delhi, India.*

[14] *Zhou, J., et al. (2023). FraudAuditor: A Visual Analytics Approach for Collusive Fraud in Health Insurance. IEEE Transactions on Visualization and Computer Graphics, 29(6), 2849-2861.*

[15] *Sreekala, K., Sridivya, R., Rao, N. K. K., Mandal, R. K., Moses, G. J., & Lakshmanarao, A. (2024). A hybrid Kmeans and ML Classification Approach for Credit Card Fraud Detection. In 2024 3rd International Conference for Innovation in Technology (INOCON) (pp. 1-5). Bangalore, India.*

DOI: 10.54254/2754-1169/98/2024OX0125

[16] Jemai, J., Zarrad, A., & Daud, A. (2024). Identifying Fraudulent Credit Card Transactions Using Ensemble Learning. IEEE Access, 12, 54893-54900.

[17] Jahnavi, D., M. A., Pulata, S., Sami, S., Vakamullu, B., & Mohan G, B. (2024). Robust Hybrid Machine Learning Model for Financial Fraud Detection in Credit Card Transactions. In 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) (pp. 680-686). Bengaluru, India.

[18] Usman, A. U., Abdullahi, S. B., Liping, Y., Alghofaily, B., Almasoud, A. S., & Rehman, A. (2024). Financial Fraud Detection Using Value-at-Risk With Machine Learning in Skewed Data. IEEE Access, 12, 64285-64299.

[19] Awosika, T., Shukla, R. M., & Pranggono, B. (2024). Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection. IEEE Access.

[20] Dol, M., & Geetha, A. (2021). A Learning Transition from Machine Learning to Deep Learning: A Survey. In 2021 International Conference on Emerging Techniques in Computational Intelligence (ICETCI) (pp. 89-94). Hyderabad, India.

[21] Augenstein, C., Spangenberg, N., & Franczyk, B. (2017). Applying machine learning to big data streams: An overview of challenges. In 2017 IEEE 4th International Conference on Soft Computing & Machine Intelligence (ISCMI) (pp. 25-29). Mauritius.

[22] Jayaram, K. R., & Verma, A. (2022). Private parameter aggregation for federated learning. In Federated Learning (pp. 313-336). Springer International Publishing.