Detecting and Predicting Financial Fraud with Machine Learning: A Comprehensive Study

Yogeshchandra Puranik
Assistant Professor
MCA Department
PES Modern College of Engineering
Pune, Maharashtra
✉ ???

Ravikant Zirmite
Associate Professor
MES IMCC
Pune, Maharashtra
✉ ???

Sudarshan Saraswat
MCA Department
PES Modern College of Engineering
Pune, Maharashtra
✉ ???

ABSTRACT

This study focuses on the detection and prediction of financial fraud using machine learning algorithms. An assorted dataset of historical financial transaction records containing various types of fraud. Machine learning algorithms such as Support Vector Machines (SVM), Random Forest, Gradient Boosting, and Neuron Networks are being utilized to address the complexity and variability of fraudulent behaviours.

The analysis includes data preprocessing for handling missing values, outliers, and feature engineering to abstract relevant information from raw transactional data. A comparison evaluation of the performance of different machine learning algorithms is conducted in terms of accuracy, precision, recall, and F1- score.

Additionally, the study explores the interpretability of the models to gain insights into the underlying patterns of fraudulent behavior. Feature importance analysis and model explainability techniques such as SHAP (Shapley Additive Explanations) are employed to elucidate the factors contributing most significantly to fraudulent transactions. The feasibility of real-time fraud detection is also investigated by deploying trained models on streaming financial data. This enables assessments of the scalability and efficiencies of the proposed approaches in handling high-volume transactional data streams. The findings demonstrate the efficacy of machine learning techniques in detection and predication financial fraud, with promising results in terms of accuracies and scalability. These insights contribute to the development of robuster fraud detection systems, enhancing the resilience of financial institutions against fraudulent activities.

KEYWORDS: *Financial fraud, Machine learning, Detection, Predication, Algorithms, Analysis.*

INTRODUCTION

Financial fraud poses a significant threat to organizations globally, encompassing various illicit activities aimed at deceiving and exploiting financial systems for personal gain. The detection and prevention of financial fraud is crucial for maintaining the integrity, trust, and stability of financial institutions and markets. Traditional methods of fraud detection have proved insufficient in combatting the increasingly sophisticated tactics employed by fraudsters. Therefore, the applications of machine learning techniques have emerged as a powerful tool for enhancing fraud detection capabilities.

LITERATURE REVIEW

Financial fraud detection is a critical area of research that has garnered significant attention due to its implications for businesses and consumers. Machine learning algorithms have emerged as powerful tools in detecting and predicting fraudulent activities in financial transactions. Several studies have highlighted the importance of utilizing high-quality historical data to train machine learning models effectively [T1]. Without a sufficient amount of valid and invalid previous transaction data, the accuracy and performance of fraud detection models may be compromised. Dimensionality reduction and data enrichment strategies are commonly employed to enhance the quality of training data and improve model performance [T1].

In the realm of machine learning algorithms, various techniques such as Logistic Regression, Decision Trees, Support Vector Machines, and Random Forest have demonstrated high accuracies in detecting financial fraud [T2]. While these algorithms have shown promising results, researchers emphasize the potential benefits of implementing sophisticated preprocessing methods to further enhance their performance [T2]. Additionally, the use of deep learning techniques, such as artificial neural networks and autoencoders, has been proposed to improve the efficiency of machine learning models in fraud detection [T2].

Data preprocessing plays a crucial role in handling missing values, outliers, and feature engineering to extract relevant information from raw transactional data [T4]. By comparing the performance of different machine learning algorithms in terms of accuracy, precision, recall, and F1-score, researchers can gain insights into the effectiveness of these models in detecting financial fraud [T4]. Moreover, model interpretability techniques like SHAP (Shapley Additive Explanations) are employed to elucidate the factors contributing most significantly to fraudulent transactions, providing valuable insights into underlying patterns of fraudulent behavior [T4].

The literature also emphasizes the importance of real-time fraud detection by deploying trained models on streaming financial data [T4]. This approach enables researchers to assess the scalability and efficiency of machine learning techniques in handling high-volume transactional data streams, showcasing the efficacy of these methods in detecting and predicting financial fraud with promising results in terms of accuracy and scalability [T4].

DATASETS

Since credit card transaction information is personal and private, the information is harder to obtain, which poses a great challenge to researchers. Fortunately, Carcillo, Fabrizio [3] proposed a credit card fraud detection dataset. Many researchers presented algorithms based on these datasets for detecting fraudulent credit card transactions. There were a total of 284,807 transactions in this dataset over two days in September 2013 from cardholders in Europe, of which 492 are fraudulent. The validation of the proportion of positive and negative fraud samples in these datasets is not balanced due to the relatively small proportions of fraud cases in life, with fraud data representing 0.172% of all transactions. This dataset provides transaction time and transaction amounts as well as other PCA features to avoid privacy, and uses the Area of Precision Recall Curve (AUPRC) to evaluate the algorithm's performance. As Figure 1[3], in order to get the distributions of the fraud and norm transactions (normals:0; frauds:1) and checks for its class imbalance, it outputs the pie charts of their possibilities.

The credit card fraud data distribution graphs shown in Fig. 1, the red color indicates fraudulent data and the blue color indicates norm data. Owing to the low percentages of fraud samples, the serious sample imbalance problems, which bring great challenges to the credit card fraud detections tasks. As Figure 2[3], the relationship between time and fraud is observed by drawing two line graphs of the changes in non-fraudulent transaction counts over time and the changes in transactions counts with fraudulent behaviors over time.

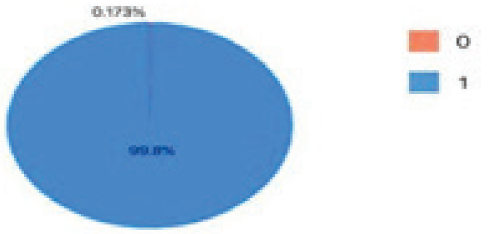

Figure 1. Distribution of Fraud and Normal Transactions.

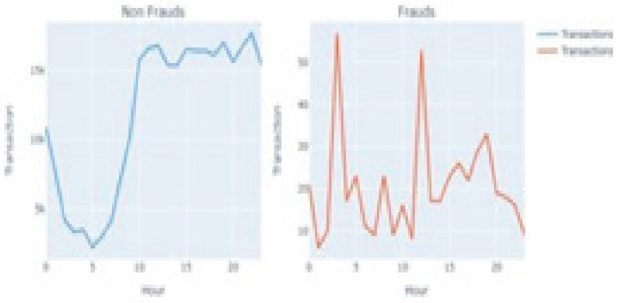

Figure 2. Transaction Count with Non Frauds and Frauds over Time.

METHOD

In the development history of credit card transaction fraud detections, there are numerous traditional methods, such as card security features, risk scores, and so forth. As artificial intelligence has grown so fast in the last several years, AI-related algorithms have found extensive applications in fraud detection systems, leading to significant enhancements in the accuracy and efficiencies of detection results.

Card Security Features

Faced with the occurrences of increasing cases of transactions fraud, enterprises, and banks use many tools and technologies to judge and detect fraud. For example, the credit card networks have developed many securities functions, including addresses authentications services [4], 3-D securities [5], CVV [6] card verifications, etc. These features are designed to determine whether a consumer is a cardholder by viewing or validating their personal identity or registration information. However, these securities functions will increase a certain degree of friction in the consumption process, slow down the consumption speeds of customers, and complicate the purchases process. For address authentication, the user's identity can be verified by comparing whether the user's consumption locations are consistent with previous records, or by asking the consumer to enter the mailing address and confirm whether it is correct. Even though the grid planning methodologies used in urban planning and the quantification of geographic areas through zip codes has made the delineation of the addresses system simple and clear in much of North America, there are still significant problems. For example, renaming of roads, construction of multiple residences at the same addresses, multiple different designations for the same residences, and errors in user input due to address information being too long can complicate the address validation process and cause great inconvenience to the user. For 3-D securities, it required customers to supply extra details of identifications, such as passwords or singles use codes, to successfully finalize a transaction, apart from the standard card information. These additional layers of security greatly reduces the feasibility of cybercriminals using stolen card information to conduct online transactions. Nevertheless, there are two significant drawbacks to 3D securities. Firstly, it can lead to customers abandoning their purchases during the checkouts processes due to its perceived complexities, resulting in a substantial decrease in conversion rates. Secondly, the implementation of 3D securities can be costly, as merchants may have to bear payments fees for each transaction. Another widely used verification method is CVV (Cards Verification Value). CVV is a three- or four- digits-code located on the back of the credit card, providing an additional layer of security when making online purchases. This code is only known to the cardholders. However, while shopping online, consumers may inadvertently expose their CVV to unfamiliar websites or malware, potentially leading to CVV theft. Additionally, during in-person transactions, if someone else sees the CVV, it increases the risk of later credit card theft. Therefore, some e- commerce companies led by Amazon cancel these verification steps like above, in order to ensure the purchasing experience of customers. If there are too many verification steps before payment, it leads to customer attrition; while if the identity of the customer cannot be accurately verified, it increases the likelihood of transaction fraud. So one of the challenges facing credit card fraud detection technology is how to confirm someone's identity before a transaction as concisely as possible.

RISK SCORES

Risk scores determine the likelihood of transaction fraud by using statistical models to evaluate many factors in each transaction. Typically, these models produce numerical scores that signify the probabilities of a transaction being fraudulent. A higher score suggests a more suspicious order. Merchants can use these risk scores to make educated guesses about specific user actions to minimize potentially fraudulent transactions, or to use additional security measures to ensure that every transaction is risky again. If the risk score of any one transaction is greater than a set threshold, it will be defined as fraudulent or rejected. In order to determine the risk scores as accurately as possible, we need to consider and test a variety of risk factors, such as bank identification numbers, country matching, city/state and zip code matching, proxies detection, distance between IP address and billing address, IP address in high-risk countries, and so on, which are derivated from past transactions. Subsequently, this data undergoes preprocessing, which includes tasks such as data cleaning to eliminate duplicate entries, address missing values, and identify any anomalous data points. Following preprocessing, machine learning algorithms [8] like dimensionality reductions, logistic regressions, Natives Bayes, decision trees, and support vector machines come into play to construct risk-scoring models. These models learn patterns and trends related to potential risks by analyzing historical data. Once the model is constructed, it undergoes a training and validation phase. To evaluate the model's performance and validities, a number of metrics are examined, such as F1-score, accuracies, precision, and recalls. Finally, upon deployment of the models in real-world settings, transactions are continuously monitored in real-time to detect potential risky behaviors. If a suspicious transaction is identified, the model generates an associated risk score to indicate the level of potential risk. Organizations utilising risk scoring can capitalize on precise fraud scores to establish an appropriate strategy for responding to risks. This approach aims to lower the probabilities of fraudulent incidents that transpiring and mitigate the aftermath in cases where fraud does take place. At the same time, transaction fraud can be comprehensively evaluated and prioritized with just a singles number, greatly reducing the cost of manual reviews. In essence, this tool aids in safeguarding merchants against the detrimental effects of credit card fraud, which encompasses financial losses, harriers to reputation, strains relationships with payment processors and card issuers, and more.

AI FRAUD DETECTION SYSTEM

Machine learning has a significant impact on the field of identification and prevention of online fraud. It involves employing a set of artificial intelligence (AI) algorithms that are educated using historical data from your records. These algorithms then propose risk-related rules that can be enforced. These rules serve to either authorize or block specific user actions, such as instances of suspicious logins, identity thefts, or fraudulent transactions. During the training processes of the machine learning systems, it's essential to flag paste instances of both fraudulent and legitimacies cases. These steps are crucial to minimize instances of false positives and enhance the precision of the risk rules. In practice, the algorithmic models can be continuously optimized by user generated data, and finally, the prediction accuracies of the models can be improved over time. In the early stages of research on machine modeling, researchers used simple algorithms for abnormal transaction detections like logistic regressions, k-nearest neighbors, decision trees, etc. With the passage of time and advancement in technology, researchers have improved and developed more advanced algorithms, such as neurons networks. A study was carried out by Khatri et al. to assess how well different machine-learning methods detect fraudulent credit card transactions. It explores several machine learning approaches including decision trees, K-nearest neighbors, logistic regressions, random forests, and native Bayes. The researchers employed a dataset created by European cardholders that was substantially class-imbalanced to evaluate the effectiveness of these methods. Precisions, which were calculated for each classifier in their experiments, served as the main performance metrics. The findings of the experiments showed that DT achieved a precisions of 85.11%, KNN reached 91.11%, LR showed 87.5%, and RF exhibited 89.77% precisions, while NB lagging behind with a precisions of 6.52%. We could see because KNN considers neighbors, its result is 3.61% higher than LR's.

V. Dornadula, S. Geetha et al [11] also applied a number of machine learning algorithms to tackle the challenges of credit card fraud. In order to address the dataset's significant skew, the researchers utilized SMOTE sampling techniques. They considered several machine learning methods, including DT, LR, and Isolation Forest (IF). The primary performance metric examined was accuracies. Through their improvements, the outcomes revealed that DT achieved an accuracies of 97.08%, while LR reached an accuracies of 97.18%. Navanshu Khare et al developed a system for credit card transactions fraud detection by employing multiple machine learning algorithms, which included LR, DT, RF, and support vector machines (SVM). To gauge the effectiveness of every machine learning approach, the researchers utilized classification accuracies as their performance metrics. The experimental results indicated that LR achieved an accuracies of 97.70%, DT reached 95.50%, SVM showed 97.50%, and RF excelled with an accuracies of 98.60%. Despite these favorable outcomes, the authors maintained that implementing sophistication pre-processing methods could potentially further enhance the performance of these classifiers. Different machine learning methods have similar accuracies and have achieved good results so far. It models the elements to be observed, which includes KNN, SVC, NB, DTC, RFC, XGB, LGB, GGC, ABC, and LR, produces statistical plots of theirs correlated predictions and actuals results with their precisions, recalls, f1-scores, and supports respectively, and summarizes the accuracies of all models.

In addition to these common algorithms, with the joint efforts of Warren McCulloch, Geoffrey Hinton, and other researchers, deep learning, a branch of machine learning, has been proposed to significantly improve the work efficiency of the machine models. Within deep learning, various techniques and architectures are employs, including artificial neurons networks [14], autoencoders, deep beliefs networks, generative adversarial networks, convolutional neurons networks, and recurrence neurons networks. Deep learning harnesses the neurons' networks to mimic the human brain's ability to process data and make decisions. In the above algorithms, the artificial neurons networks algorithms (ANN) are separated into the trainings part and the testings part. The first step of the training part is to load and read the datasets and then it will be scaled, normalized, and segmented. After preprocessing the data, ANN starts training and analyzing the models and predicting fraudulent behaviors. When getting the results, the trained data is stored for testing later. The testing part of the process is roughly the same as the training part, and the only difference is that the stored training models will be used to test and classify the data. Compared to the SVMs and KNNs algorithms, ANN is able to achieves 99.92% [10] accuracies and is most appropriate for detecting credit card frauds. However, even though ANN could reach such a high accuracies rate, its precisions and recalls are lower than SVM.

Method	Description	Advantages	Disadvantages
3D Security	A security feature requiring additional verification during online transactions.	Provides an extra layer of security by confirming the identity of the cardholder.	Can lead to abandoned purchases due to complexity, resulting in decreased conversion rates. Implementation can be costly.
CVV Verification	Requires entering a three- or four-digit code from the back of the credit card for online transactions.	Adds an additional layer of security that is known only to the cardholder.	Risk of CVV exposure to unfamiliar websites or malware, leading to potential theft. If seen during in-person transactions, it increases the risk of credit card theft.
Risk Scores	Uses statistical models to evaluate multiple factors in each transaction, producing numerical scores indicating the likelihood of fraud.	Allows for educated guesses about user actions to minimize fraudulent transactions. Can be used to establish appropriate strategies for responding to risks.	Requires careful consideration and testing of various risk factors to ensure accurate risk scores.
AI Fraud Detection System	Employs machine learning algorithms to detect and prevent online fraud by analysing historical data to propose risk-related rules.	Can be continuously optimized by user- generated data, improving prediction accuracyover time.	Early-stage models may have higher instances of false positives, requiring continuous refinement to enhance precision.

Machine Learning Models	Various algorithms such as Support Vector Machines (SVM), Random Forest, Gradient Boosting, and Neural Networks used to detect fraudulent credit card transactions.	Capable of handling complex and variable fraudulent behaviours. Provides promising results in terms of accuracy and scalability.	Requires extensive data preprocessing and feature engineering. Training and validation phases are crucial for ensuring model performance.
Feature Importance Analysis	Uses techniques like SHAP (Shapley Additive Explanations) to interpret models and understand the factors contributing to fraudulent transactions.	Enhances the interpretability of models, providing insights into underlying patterns of fraudulent behavior.	Requires sophisticated techniques and expertise to implement effectively.
Real-Time Fraud Detection	Deploys trained models on streaming financial data to assess the scalability and efficiency of fraud detection approaches in handling high-volume transactional data streams.	Enables real-time monitoring and detection of potentially risky behaviors, reducing the cost of manual reviews.	Implementation in real-world settings may pose challenges in terms of computational resources and infrastructure requirements.

APPLICATION

Running an AI-driven method for credit card transaction fraud detection requires meeting several crucial conditions to ensure the model achieves the best detection score possible. To train high-quality machine learning models effectively, a substantial number of internal historical records are necessary. Without a sufficient amount of valid and invalid previous transactions data, it is impossible to run the models and obtain accurate results. In other words, the quality of the input determines the performance of the training process. Using dimensionality reductions and data enrichment strategies is a common approach since the training set rarely contains two classes of medium volume data samples. The quality of previous data can skew the models. This argument implies that if the information collector does not organize the data neatly and appropriately or mixes the data of fraudulent transactions with norm transactions, significant deviations in the output results can occur. Fraud detection will only be effective if there is an adequate number of well-organized and impartial data, as well as business logic that exactly matches the machine learning models chosen. Therefore, the use of machine learning in AI models should be based on excellent datasets.

CONCLUSION

Machine learning algorithms have been founded to be effective in detecting and predicting financial fraud. These algorithms analyze large volumes of datums to identify patterns and anomalies that may indicate fraudulent activity. Despite their effectiveness, machine learning algorithms' face several challenges.

One challenge is the quality of the data used to train these algorithms. The data must be comprehensive, accurate, and up-to-date to ensure that the algorithms can effectively identify fraudulent behaviors. What's more, the algorithms may struggle with unbalanced datasets, where the numbers of fraudulent transactions are significantly lower than legitimacy transactions.

Another challenge is the interpretability of the algorithms. While machine learning models can accurately detect fraud, understanding how they reach their decisions can have complexities. This lack of transparencies can make it difficult for organizations to trust the results of these algorithms.

Despite these challenges... ongoing research is focused on addressing these issues and improving the effectiveness of fraud detection systems. Researchers are exploring ways to improve the quality of training data, develop more interpretation models, and enhance the overall performance of machine learning algorithms in detecting financial fraud.

By using machine learning techniques, organizations can improve their fraud detection capabilities. These techniques can help organizations identify fraudulent activity more quickly and accurately, thereby protecting their assets and maintaining the trust of consumers and stakeholders. What's more, machine learning can enable organizations to automate fraud detection processes, reducing the need for manually intervention and improving overall efficiencies."

REFERENCES

1. Barker, Katherine J., Jackie D'amato, and Paul Sheridon. "Credit card fraud: awareness and prevention." Journal of financial crime 15.4 (2008): 404-405.
2. Bhatla, Tej Paul, Vikram Prabhu, and Amit Dua. "Understanding credit card fraud. Cards' business review 1.6 (2003): 13.
3. Bouch, Anthony. "3-D Secure: A critical review of 3-D Secure and its effectiveness in preventing card not presenting fraud." University of London, Londra, erişim 8 (2011): 39-63.
4. Dal Pozzolo, Andrea, et al. "Learned lessons in credit card fraud detection from a practitioner perspective." Expert systems with applications 41.10 (2014): 4915-4928. [5]. Dornadula, Vaishnavi Nath, and Sa Geetha. "Credit card fraud detection using machine learning: A comprehensive review." International Journal of Recent Technology and Engineering (IJRTE) 8.1 (2019): 231-239.
6. Ileberi, Emmanuel, Yanxia Sun, and Zenghui Wang. "A machine learning based credit card fraud detection using the GA algorithm for feature selection." Journal of Big Data 9.1 (2022): 1-5.
7. Khatri, Samidha, Aishwarya Arora, and Arun Prakash Agrawal. "Supervised machine learning algorithms for credit card fraud detection: a comparison." 2020 10th International conference on cloud computing, data science & engineering (confluence). IEEE(2020): 680-683.
8. Komuves, Flavio L. "We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers." J. Marshall, J. Computer & Info. L. 16 (1997): 525-537.
9. Popat, Rimpal R., and Jayesh Chaudhary. "A survey on credit card fraud detection using machine learning." 2018 2nd, International conference on trends in electronics and informatics (ICOEI). IEEE, 2018: 3-5.
10. Save, Prajal, et al. "A novel idea for credit card fraud detection using decision tree." International Journal of Computer Applications 161.13 (2017): 3. Proceedings of the 4th International Conference on Signal Processing and Machine Learning DOI: 10.54254/2755-2721/51/20241172 79.
11. Yenouskas, Joseph F., and Tierney E. Smith. "Fair Credit Reporting Act Litigation Developments on Standing." Business Lawyer 76 (2021): 2-3.