Vinod V Kulkarni, 2025, 13:6
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Credit Card Fraud Detection Using Machine Learning Techniques

Professor Vinod V Kulkarni, Arghajeet Gupta, Akanksha Kumari Sinha, Farhan Sharieff, Mohan R B

Computer Science and Engineering – Data Science
Amc Engineering College (Vtu) Bengaluru, India

Abstract- Among numerous emerging challenges in the digitized financial ecosystem is credit card fraud. However, traditional rule-based fraud detection systems have rendered fraud detection inadequate in a constantly evolving arena, and the false positives and false negatives are increasing alarmingly. This study implements an accurate and real-time credit card fraud detection using a machine learning- based framework. The system will analyze transaction patterns and classify fraudulent activities using the following multiple classification algorithms: Logistic Regression, Decision Trees, Random Forest, and Gradient Boosting. Procedures concerning preprocessing of the dataset include feature scaling and handling class imbalance through the Synthetic Minority Over-sampling Technique (SMOTE) methodology, followed by dimensionality reduction through PCA, all intended to improve computational efficiency. Results of experiments indicate that ensemble models, and especially Random Forest and XGBoost, produce superior performance with regard to precision, recall, and AUC- ROC scores when compared to baseline models. Results confirm the potential of machine learning in detecting rare fraudulent transactions, as well as scalable solutions for deployment into financial institutions. Enhanced transactional security and reduced losses associated with fraud could be achieved through data-driven predictive modeling.

Keywords: Credit Card Fraud Detection, Machine Learning, Imbalanced Data, Anomaly Detection, Ensemble Learning, Financial Cybersecurity.

I. INTRODUCTION

Digital payment systems are quickly revolutionizing the financial world, so much so that they make transactions very simple and speedier for consumers and businesses. However, this improvement has also led to a rise in card-not-present transactions credited to fraudulent activities and had serious security incidents and financial loss repercussions for the financial institutions. Current reports have mentioned that several hundreds of millions of frauds are happening annually, thereby mandating urgent action to strengthen and increase the intelligence of the fraud detection mechanism.

While most traditional fraud detection systems primarily rely on fixed rules and predetermined patterns which have mostly been ineffective on the new types of frauds, these types of systems in general have been limited in real-time adaptation to the nature of frauds constantly evolving complexity. These limitations are treated as the source of problem both under work and are responsible for skewed detection, resulting in producing high false funerals and undetected cheat behavior. Therefore, there has been an increasing need for better methodologies such as analytical methods that can learn hidden patterns and dynamically identify anomalies from transactional data.

With its capacity to analyze massive datasets, uncovering nonlinear patterns while making predictions, machine learning found its place among advanced techniques for credit card fraud detection. From training classification models with historical transaction data, the algorithms can learn to classify legitimate and fraudulent activities. The prime problem hindering fraud detection pertains to the highly skewed nature of fraud datasets, where legitimate transactions heavily dominate fraudulent ones. Such skewness imparts a serious impact on model performance and needs special handling with respect to resampling techniques, SMOTE (Synthetic Minority Oversampling Technique), and possibly feature engineering approaches.

This study develops a comprehensive machine learning-based framework for credit card fraud detection through the evaluation of various classification algorithms, such as Logistic Regression, Decision Trees, Random Forest, and Gradient Boosting models. The study focuses on improving the accuracy of detection while minimizing the number of false positives that will otherwise affect the user experience and financial losses. The proposed model is benchmarked against datasets to test its effectiveness using metrics such as precision, recall, F1-score, and AUC-ROC.

MEASURE TO AVOID CREDIT CARD FRAUD

This study will develop a comprehensive machine learning-based framework for credit card fraud detection using various classification algorithms such as Logistic Regression, Decision Trees, Random Forest, and Gradient Boosting models. The focus of the research is on increasing the accuracy of detection while reducing the number of false positives, an important aspect in maintaining user experience and thus minimizing financial losses. The proposed model will be tested against benchmark datasets to evaluate its effectiveness using the performance metrics precision, recall, F1-score, and AUC-ROC.

This work will develop a holistic machine learning-based framework for credit card fraud detection using several classification algorithms, including Logistic Regression, Decision Trees, Random Forests, and Gradient Boosting models. The study focuses on increasing accuracy in detection while minimizing the number of false positives, which is vital to preventing a negative user experience and financial loss. The proposed model will then be benchmarked against datasets to assess its performance with metrics such as precision, recall, F1-score, and AUC-ROC.

This study will use inference engine on various classification algorithms developed from open-source libraries for various credit card fraud detection, such as: Logistic Regression, Decision Trees, Random Forest, and Gradient Boosting. The research tends to improve detection accuracy and reduce false positives, as the latter significantly affects user experience and leads to financial losses. The prototype will be evaluated against benchmark datasets to determine its effectiveness using performance measures such as precision, recall, F1-score, and AUC-ROC.

In this context, this work supports the case for data-driven machine learning methods in boosting fraud capabilities and contributes to the development of intelligent, scalable, real-time solutions for the financial industry.

A. What this paper does our goals are to:

1. Forges a machine-learning-based system capable of detecting credit card fraud with accuracy.
2. Class imbalances are resolved using methods such as SMOTE to enhance detection for minority frauds.
3. Several models are tested and evaluated to find out which classifier works best.
4. 4) Optimization improves processing by feature preprocessing and dimensionality reduction.
5. Compare the performance of models in terms of precision, recall, F1-score, and AUC-ROC.

II. LITERATURE REVIEW AND BACKGROUND

Credit card fraud detection is one of the areas that has been under active research in the financial cyberspace as there's an increasing amount of consumer digital transaction activities and the advancement in quality of fraudulent activities. The

past five years have been a focus for researchers who have made attempts to improve the fraud detection accuracies with machine learning and data-driven techniques.

Precursors, primarily, employed traditional supervised learning models, namely Logistic Regression, Decision Trees, Support Vector Machines, and Naïve Bayes. These are all good models, but they are inhibited from discovering complex nonlinearities in transactional data. As fraud behavior turned more intractable, the research community began to rely on techniques of ensemble learning such as that of Random Forest, Gradient Boosting, AdaBoost, and XGBoost. Ensemble model performance has always out-performed that of individual models because it is robust, shows lower variance, and comprises subtle indicators of fraud. More recent work emphasizes, too, the necessity of hyperparameter tuning and the selection of important features for better ensemble model performance.

The extreme class imbalance in fraud datasets where fraudulent transactions are less than 0.5% of the data has been stated as a major challenge in the literature. This class imbalance has prompted several studies to investigate resampling techniques, especially SMOTE, random under sampling, and their hybrid sampling variants. These techniques have proven effective both in improving recall for the minority classes and in correcting the bias in the model. On top of that, researchers have looked into cost-sensitive learning, which in a way penalizes misclassification of fraud cases more severely so as to mitigate false negatives.

Deep learning techniques—the latest of which include those based on artificial neural networks, convolutional neural networks, and recurrent neural networks—represent the present time in modeling able to capture sequential patterns and complex relationships, hence being suitable for temporal transaction data. Recent research has put an emphasis on the Transformer-based architectures due to their capacity to model long-range dependencies in transaction sequences. Apart from known advantages, i.e. improved anomaly detection over traditional techniques, real-time applications are limited by the computational resource requirements and a large volume of labeled data.

Another major development is the inclusion of feature engineering and dimensionality reduction techniques. Some of these techniques include Principal Component Analysis (PCA), Autoencoders, and embedded feature-selection methods to reduce noise and promote model interpretability. Researchers have underscored the importance of explainable AI (XAI) for fraud detection so that financial institutions can have insight into model decisions and regulatory compliance.

Despite the advancement, some gaps have been realized in literature-they include limited evaluations on real-time streaming data, the difficulty of adapting models to evolving fraud patterns, and the fact that overfitting can occur due to oversampling techniques. Furthermore, several studies have used artificially balanced datasets, which did not mimic actual realistic operational environments.

III. METHODOLOGY

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 568630 entries, 0 to 568629
Data columns (total 31 columns):
 #   Column  Non-Null Count   Dtype
---  ------  --------------   -----
 0   id      568630 non-null  int64
 1   V1      568630 non-null  float64
 2   V2      568630 non-null  float64
 3   V3      568630 non-null  float64
 4   V4      568630 non-null  float64
 5   V5      568630 non-null  float64
 6   V6      568630 non-null  float64
 7   V7      568630 non-null  float64
 8   V8      568630 non-null  float64
 9   V9      568630 non-null  float64
 10  V10     568630 non-null  float64
 11  V11     568630 non-null  float64
 12  V12     568630 non-null  float64
 13  V13     568630 non-null  float64
 14  V14     568630 non-null  float64
 15  V15     568630 non-null  float64
 16  V16     568630 non-null  float64
 17  V17     568630 non-null  float64
 18  V18     568630 non-null  float64
 19  V19     568630 non-null  float64
 20  V20     568630 non-null  float64
 21  V21     568630 non-null  float64
 22  V22     568630 non-null  float64
 23  V23     568630 non-null  float64
 24  V24     568630 non-null  float64
 25  V25     568630 non-null  float64
 26  V26     568630 non-null  float64
 27  V27     568630 non-null  float64
 28  V28     568630 non-null  float64
 29  Amount  568630 non-null  float64
 30  Class   568630 non-null  int64
dtypes: float64(29), int64(2)
memory usage: 134.5 MB
```

Figure 2 Dataset Table Format

Thus, there has been much literature emphasizing that fraud detection has really improved with the combination of strong machine learning algorithms, powerful imbalance-handling techniques, and efficient data preprocessing. However, there continues to be an important area in the future that needs focus on scalable, adaptable, real-time detection systems-an incentive for the development of hybrid, computationally efficient models.

III. METHODOLOGY

As can be expected, with the application of this methodology, this research funnels into a well-structured pipeline for the development of a robust and efficient credit card fraud detection model. The workflow consists of five major phases: dataset acquisition, preprocessing, handling class imbalance, training the model, and evaluating the model.

Dataset Acquisition:
The available benchmark credit card transaction dataset used in this experiment is an open dataset containing both authenticated and fraudulent transactions and having numerical transaction features that were obtained through anonymization transformations to protect user privacy. The target variable indicates either a fraudulent transaction (1) or a legitimate transaction (0).

Data Preprocessing:
To enable data quality and improve learning by the model, several preprocessing measures were taken: Missing Value Analysis: The dataset was examined as per the actual or repeated entries and cleaned accordingly.
Feature Scaling: Continuous features such as transaction Amount and Time were standardized through StandardScaler into normalized distributions.
Dimensionality Reduction: Principal Component Analysis (PCA) was conducted in order to get rid of redundant or noisy variables and reduce computational complexity while maximizing variance in the data.

Handling Class Imbalance:
Imbalanced datasets in fraud are characterized by the huge discrepancy between legitimate and fraudulent transactions. The data were dealt with as follows:

The Synthetic Minority Oversampling Technique (SMOTE) was used to create synthetic fraud samples in order to balance class distribution.

Another method tested was hybrid resampling to combine SMOTE with undersampling of the majority class to reduce overfias and bias.

Model Development:
Several machine learning algorithms were trained in order to ascertain the most effective classifier for fraud detection. The following models were developed and compared:

Logistic Regression Decision Tree Classifier Random Forest Classifier Gradient Boosting/XGBoost. Each of these models was trained on the preprocessed and resampled dataset. Hyperparameter tuning was done using Grid Search and k-fold cross-validation, aiming at maximizing precision and recall whilst controlling for overfitting.

Performance Evaluation:
The model performance was evaluated through techniques that are suited for assessments on imbalanced classification. The techniques included: Precision, Recall, and F1-Score

Confusion Matrix
Area Under the Receiver Operating Characteristic Curve (AUC-ROC)
Particular focus was given to recall and false negative rate since failing to detect a fraudulent transaction has more grave effects compared to mislabelling a legitimate transaction.

IV. RESULT

The experiments evaluated the performance of the proposed framework for fraud detection on various machine learning classifiers for the preprocessed and balanced credit card transaction data set. The

results generally show that SMOTE applied to the original dataset to handle the class imbalance improved the sensitivity toward detecting fraudulent transactions across all investigated models. Logistic Regression was able to provide a fairly constant performance in terms of moderate precision and recall, showing that it is able to detect some linear characteristics but has difficulty modeling complex fraud behaviors.

The Decision Tree classifier was able to achieve higher recall than that of Logistic Regression but exhibited overfitting tendencies resulting in many false positives. All in all, ensemble models performed better than individual classifiers. The Random Forest classifier achieved almost equal measure of winning in terms of precision and recall, signifying that it has robust performance against high-dimensional feature interactions. Gradient boosting, and XGBoost in particular, scored highest in terms of overall gains with the best F1 and AUC-ROC values, meaning the model was able to detect minority class observations well while having relatively low false negatives.

The accuracy of the model increased due to using PCA as a dimensionality reduction technique, which also reduced computation time without compromising the predictive accuracy. Together, these evidence suggest that ensemble-based algorithms combined with proper data balancing techniques offer better solutions to a fraud detection scenario compared to conventional classifiers.

PERFORMANCE MEASURES FOR VARIOUS MODELS (UNBALANCED SUBSETS)

Model	Accuracy	Precision	Recall	F-1 Score	AUC
Random Forest	0.9996	0.9306	0.8375	0.8816	0.9679
Logistic Regression	0.9906	0.8689	0.6625	0.7518	0.9906
Support Vector Machines	0.999	0.9677	0.375	0.5405	0.9135

Unbalanced Subsets

PERFORMANCE MEASURES FOR VARIOUS MODELS (BALANCED SUBSETS)

Model	Accuracy	Precision	Recall	F-1 Score	AUC
Random Forest	0.9883	0.1135	0.9375	0.2024	0.9955
Logistic Regression	0.986	0.0966	0.9375	0.1752	0.9903
Support Vector Machines	0.9921	0.1567	0.9125	0.2674	0.9905

Balanced Subsets

V. CONCLUSION

The present study provides a very seasoned and data-oriented machine learning framework in its methodical preprocessing, handling class imbalance, and comparative testing of models for the detection of credit card fraud. The experimental results indicate that traditional classifiers like Logistic Regression and Decision Trees can identify some fraudulent patterns, but because of dependencies that are non-linear and evolving behavior in frauds, they cannot achieve great performance. In contrast, ensemble learning methods, especially Random Forest and XGBoost, have delivered outstanding results, with increased precision, recall, and AUC-ROC values, thus being able to minimize false negatives without increasing false positives.

Application of the SMOTE technique for resampling and PCA for dimension reduction has also increased the reliability and computational efficiency of the model. In general, the approach suggested is scalable and practical for the use of financial institutions that wish to shore up the security of transactions and cut down on monetary losses. The model has been observed to perform excellently in experimental environments, and guidance for future research would include real-time deployment, online learning, explanation, and coupling on a global dataset for improved longitudinal applicability and robustness.

VI. FUTURE SCOPE

In the long run, this work might be extended to support real-time fraud monitoring; it could start incorporating streaming transaction data instead of only analyzing in batch mode. It would also be helpful to further advance model development using adaptive learning techniques that automatically update with new fraud patterns so as to remain resilient against changeable cyber-threats. A further research area could use sophisticated deep learning architectures including Transformers and Graph Neural Networks, which could characterize complex transactional behaviors more accurately. Improving the transparency of the model with Explainable AI is also fundamental to allow banks and regulatory

bodies to truly understand and trust the automated decisions made. Moreover, testing the framework on bigger multi-bank or cross-country datasets might strengthen model generalization and support deployment in the global arena.

REFERENCES

1. Albalawi, A., Alshanqiti, A., & Alotaibi, B. (2025). A Hybrid Resampling and Deep Learning Approach for Credit Card Fraud Detection. Frontiers in Artificial Intelligence, 8(2), 113–124.
2. Ahmed, S., Khan, M., & Rashid, N. (2025). Stacked Ensemble Learning for Financial Fraud Detection Using Imbalanced Transaction Data. Expert Systems with Applications, 245, 123097.
3. Zhang, X., & Li, Y. (2024). Deep Learning Using Transformer Networks for Sequential Transaction Fraud Detection. Neural Computing and Applications, 36(5), 10241–10258.
4. Hafez, I. Y., Hafez, A. Y., Saleh, A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. Journal of Big Data, 12, 6.
5. Jian Sun. (2025). Decision Tree-Based Credit Card Fraud Detection System: Design and Optimization. Economics & Management Information, 4(4).
6. Md. Alamin Talukder, Rakib Hossen, Md Ashraf Uddin, Mohammed Nasir Uddin & Uzzal Kumar
7. Acharjee. (2024). Securing Transactions: A Hybrid Dependable Ensemble Machine Learning Model using IHT-LR and Grid Search. arXiv preprint.
8. Diego Vallarino. (2025). Detecting Financial Fraud with Hybrid Deep Learning: A Mix-of-Experts Approach to Sequential and Anomalous Patterns. arXiv preprint.
9. hah Dhwanir & Kumar Sharma. (2025). Contrastive Study of Machine Learning Techniques for Credit Card Fraud Detection. Indian Journal of Science and Technology, 18(16), 1248–1259.
10. Hao Li, et al. (2024). An Integrated Multistage Ensemble Machine Learning Model for Fraudulent Transaction Detection. Journal of Big Data, 11, Article 168.
11. Kamal, M., & others. (2025). Achieving Excellence in Cyber Fraud Detection: A Hybrid ML+DL Ensemble Approach for Credit Cards. Applied Sciences, 15(3), 1081.