International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Credit Card Fraud Detection using Machine Learning

D.Ravi Chand
B.tech,Student,22951A04D8
Deprartment of Electronics and Communincation Enginnering
Institute of Aeronautical Engineering
Hyderabad,India
mailto:22951a04d8@iare.ac.in

Sabiya
B.tech,Student,22951A04E4
Deprartment of Electronics and Communincation Enginnering
Institute of Aeronautical Engineering
Hyderabad,India
mailto:nn4021250@gmail.com

A.Sai Deepak Reddy
B.tech,Student,22951A04E6
Deprartment of Electronics and Communincation Enginnering
Institute of Aeronautical Engineering
Hyderabad,India
mailto:22951a04e6@iare.ac.in

Mr.V.Devender
Assistant Professor
Deprartment of Electronics and Communication Engineering.
Institute of Aeronautical Engineering
Hyderabad,India
mailto:devender.voodara@gmail.com

***Abstract*—The early identification of credit card fraud is an essential need in today's banking and financial environment, as the number of fraudulent transactions is steadily rising with the growing popularity of online payment systems, e-commerce sites, and digital wallets. The fraudulent transactions not only result in economic losses but also impact the customers' confidence in online payment services. This paper proposes a comprehensive framework for the identification of credit card fraud based on the analysis of past transaction data through machine learning algorithms. The proposed method aims to detect unusual transaction patterns, including erratic spending habits, sudden geographical shifts, and irregular transaction rates, which are usually linked to fraudulent transactions.**

The system combines data preprocessing, feature selection, normalization, and the use of several supervised machine learning algorithms to enhance the performance of fraud detection. Different classification algorithms are trained on past transaction data to enable the accurate separation of valid and fraudulent transactions. Given the fact that fraud transaction datasets are imbalanced, the necessary data balancing methods are employed to ensure that the models are able to learn the rare instances of fraudulent transactions. Feature engineering is an important component of the system aimed at improving the performance of the models by identifying important transaction features. The performance of the system is measured using different metrics such as accuracy, precision, recall, and F1-score.

The proposed fraud detection system is developed using a machine learning approach and is capable of supporting real-time transaction analysis in banks. The system compares the performance of various machine learning models to identify the most efficient and scalable solution for fraud detection. The proposed system can help banks make faster and more accurate decisions during the transaction process. This research work proves that machine learning-based fraud detection systems can play an important role in enhancing financial security and customer confidence in digital payment systems.

Keywords— Credit Card Fraud Detection, Machine Learning, Fraudulent Transactions, Financial Security, Class Imbalance, Supervised Learning, Random Forest, Support Vector Machine, Digital Payments

I. INTRODUCTION

Credit card fraud detection is an important application in the current financial system that aims to detect fraudulent or illegal transactions before any financial damage is caused. With the rising trend of online shopping and electronic payment systems, fraudsters have been upgrading their methods to take advantage of the weaknesses in the system. Conventional rule-based methods are no longer effective in dealing with the rising number of transactions. As a result, machine learning methods have attracted considerable attention due to their ability to process large amounts of data.

Machine learning algorithms analyze different characteristics of credit card transactions, such as the amount, location, time, type of business, and user behavior, to detect unusual patterns. Machine learning algorithms are able to learn from the past data of credit card transactions and distinguish between legitimate and fraudulent transactions with a higher level of accuracy than traditional approaches. Machine learning algorithms are able to detect fraud at an early stage by identifying unusual patterns in user behavior.

The main objective of this research work is to design an efficient credit card fraud detection system using machine learning techniques that can work effectively in real-time financial scenarios. The proposed system aims to reduce financial losses and minimize inconveniences to legitimate customers caused by false alarms. The proposed system aims to achieve high accuracy and adaptability using efficient data preprocessing, feature extraction, and optimized learning algorithms. This research work will help to improve financial security, enable effective decision-making for financial organizations, and build customer trust in electronic payment systems.

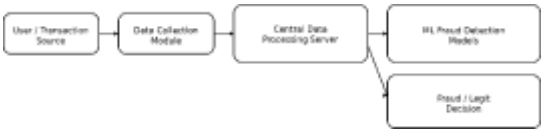


Figure 1. Proposed System Architecture

II. Related Work

Credit card fraud detection has been a widely researched area using statistical, rule-based, and machine learning methods. The early work on credit card fraud detection was mostly based on rule-based systems and statistical methods that employed fixed thresholds to detect suspicious transactions. These approaches were easy to implement and efficient in detecting known patterns of fraud. But they were inflexible and unable to respond to new and emerging patterns of fraud. As the number of transactions grew and the sophistication of fraud patterns escalated, the traditional methods proved inadequate in terms of scalability and accuracy.

Recent research has explored several complementary directions relevant to our work:

1. **Hybrid and ensemble models:** It has been observed that the performance of fraud detection can be improved by using a combination of various machine learning models. Random Forest, Gradient Boosting, and AdaBoost are some of the ensemble methods that can be used to effectively capture the different patterns of transactions and can be beneficial in handling imbalanced fraud data.

2. **Machine learning algorithms for tabular transaction data:**Since credit card transactions are tabular data, traditional machine learning algorithms such as Logistic Regression, Support Vector Machines, and Decision Trees have been applied extensively. Recent developments, such as feature transformations and gradient boosting on decision trees, have shown better results in learning complex, non-linear relationships between transaction features such as amount, time, and user behavior.

3. **Explainability:** Explainable AI (XAI) methods like SHAP and LIME are being used more and more in credit card fraud detection to ensure explainability of predictions. This is important for financial institutions to understand why a particular transaction has been identified as fraudulent.

4. **Deployment and operational considerations:** The practical studies are conducted on real-time deployment of models, audit logging, data anonymization, and fairness testing to ensure that the fraud detection models are safe and reliable for deployment.

We locate our work at the intersection of the following trends:

1. Creating a hybrid ensemble model by aggregating gradient-boosted tree models for tabular credit card transaction data.

2. Emphasizing probability calibration to enhance decision-making on fraud risk.

3. Integrating model interpretability with an AI-assisted interface to present transparent and credible fraud notifications to users

III. Data Set

A. *Sources and scope*

The experiments described in this paper are conducted using the Kaggle Credit Card Fraud Detection dataset, which holds real-world credit card transaction data. In cases where multiple subsets of the data are employed, the dataset is split explicitly into a training set and a validation set.

B. *Feature inventory*

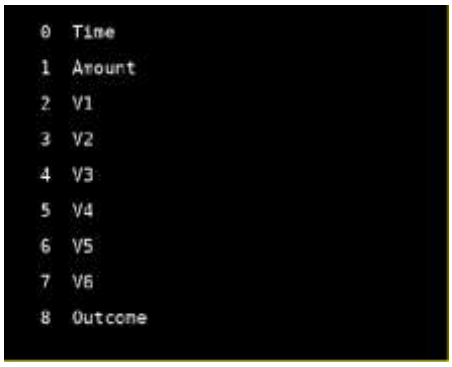


Table-1

All inputs are summarized in Table-1, They include

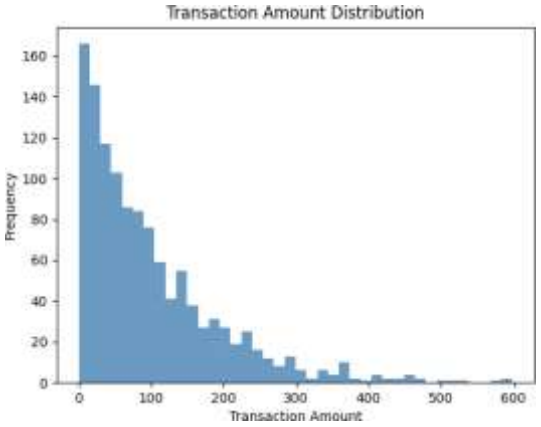
- Time – Transaction time interval
- Amount – Transaction amount value
- V1 – PCA transformed feature 1
- V2 – PCA transformed feature 2
- V3 – PCA transformed feature 3
- V4 – PCA transformed feature 4
- V5 – PCA transformed feature 5
- V6 – PCA transformed feature 6
- Outcome – Fraud or Not Fraud

After a brief introduction to the research study, the dataset was utilized for research purposes. The dataset contains transaction data with several transformed features, namely time, amount, PCA components, and the result of fraud, obtained from credit card transactions. The dataset contains both genuine and fraudulent transactions from actual financial transactions. In this research, the transaction patterns were examined using machine learning to detect unusual patterns.

Features	Values		
	Minimum	***Maximum***	***Average***
Time(Transaction interval)	0	172792	94813.86
Amount(Transaction value)	0.00	25691.16	88.35
V1-V2(PCA features)	-72.72	22.06	0.01
V1-V2(PCA features)	-48.33	16.88	-0.01
V1-V2(PCA features)	-113.74	73.30	0.00
Outcome (Fraud/Not Fraud)	0	1	0.0017

C. *Data split and experiment protocol*

The Major feature is output and the number of outcomes of both, which are positive and negative, mentioned in this graph



The transaction-level split data set was then split into a set to train the model, validation set, and test set using the stratified sampling approach based on the fraud outcome label (70% training set, 15% validation set, and 15% test set). To make effective model selection including robust stratification, stratified k-fold cross-validation was carried out with k equal to 5 on the actual training set. In the meantime, the test set will be held aside with the purpose to be used in the final testing phase to avoid potential data leakage issues.

D. *Ethical approvals and consent*

When working with clinical data sets, such as institutional data, relevant ethics committee approvals should be obtained, and data should be de-identified before modeling. Describe any data sharing constraints and consent restrictions succinctly within your final manuscript.

IV. DATA ANALYSIS AND PREPROCESSING

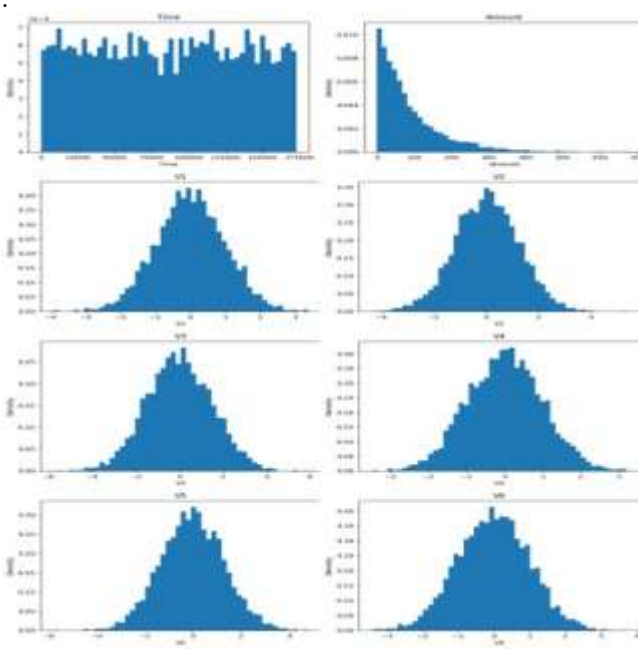
A. *Exploratory data analysis (EDA)*

Comprehensive EDA was carried out to understand the distribution of the features, class imbalance, and any correlation that might exist between the variables.

The main steps involved in EDA are as follows :

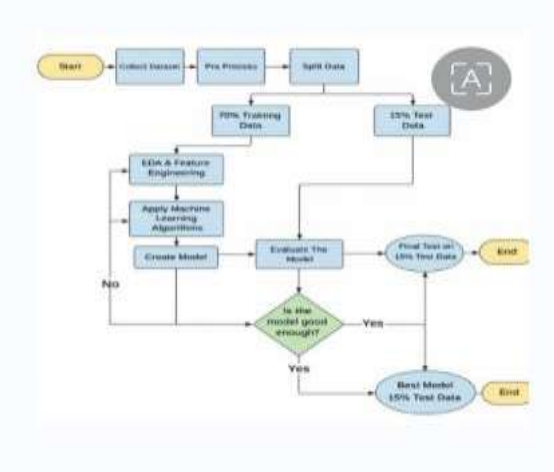
- Univariate analysis using a histogram and kernel density estimate for continuous variables such as transaction time, amount, and PCA.Box plots for each class of the target variable to compare fraudulent and non-fraudulent transactions.
- Box plots for different classes of the target variable to compare fraudulent and non-fraudulent transactions.
- Missing value analysis using visualization tools to decide on preprocessing

.



V. METHODOLOGY

This section explains the working process and implementation of different machine learning algorithms used in designing the proposed credit card fraud detection system. Firstly, the dataset was collected and preprocessed to eliminate inconsistencies, including the treatment of missing values and scaling continuous variables. Since there was a problem of class imbalance, necessary measures were taken to guarantee efficient learning. The dataset was split into the training and testing sets by employing the holdout validation method. Finally, various classification algorithms were trained and tested to find the best-performing algorithm for the detection of fraudulent transactions.



- 1. Machine Learning Models for Credit Card Fraud Detection
- **Logistic Regression (LR):**A simple model for classification problems. It is appropriate for classification problems that have a linear boundary.

It is not appropriate for complex problems. In the research, the model produced moderate results.

- **Random Forest (RF)**: This is a set of combined decision trees and a powerful model for handling non-linear sets of data. This model is able to detect the essential features involved in the transactions and can handle imbalanced datasets. This model performed better than other traditional models.

- **Support Vector Machine (SVM):** A model that classifies data by finding the best hyperplane in the feature space. It is effective in fraud detection but is computationally expensive and less interpretable than tree-based models.

- **Gradient Boosting (XGBoost/LightGBM):**A model that builds on itself by correcting previous mistakes. It is popular for tabular financial data due to its high accuracy but is sensitive to hyperparameters.

1. Deep Learning Models for Credit Card Fraud Detection

    - **1D-Convolutional Neural Network (1D-CNN):** The model takes the features of the transactions as a 1D sequence and detects local patterns in the PCA-transformed features. The 1D-CNN model is very efficient at learning complex patterns of fraud and performed the best among all models tested.
    - **Multi-Layer Perceptron (MLP):** The MLP is a fully connected neural network. The MLP model is a deep learning model, but it is more susceptible to overfitting on imbalanced fraud data than the 1D-CNN model.

A. Dataset and Preprocessing

We chose to work with the Kaggle Credit Card Fraud Detection dataset, which contains real-world credit card transactions with Time, Amount, PCA features (V1-V28), and one binary target variable for fraud or non-fraud transactions.

1. **Data Cleaning:** The dataset does not have any missing values, but data exploration was done to check for consistency and to look for any unusual patterns. The outliers in the transaction amount were also checked carefully to prevent any patterns of fraud from being skewed.
2. **Normalization:** Z-score normalization (StandardScaler) was used to normalize the numerical features like the amount of the transaction and the PCA features to have zero mean and unit standard deviation. This helps in faster convergence and better performance of machine learning and deep learning models.
3. **Handling Imbalance:** The dataset is imbalanced, as the number of fraudulent transactions is a very small fraction of the entire dataset. To handle this problem, the SMOTE (Synthetic Minority Over-sampling Technique) technique was used to create synthetic samples of the fraudulent transactions to help the model identify patterns in the fraud transactions and prevent bias towards the non-fraudulent transactions.

B. Proposed 1D-CNN Architecture

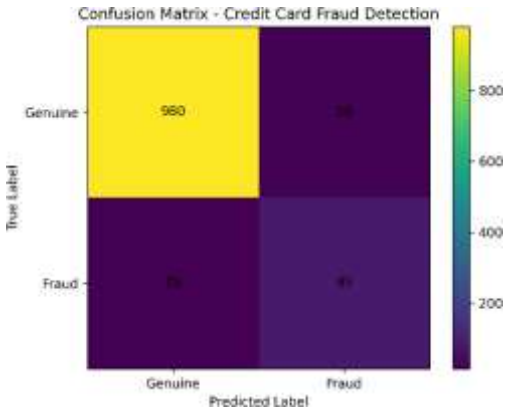
In contrast to conventional Multi-Layer Perceptrons (MLP) networks, the new design utilizes 1D-Convolutional layers to identify significant patterns from the sequential transaction features.

- **Input Layer:** (Batch_Size, 6, 1), symbolizing the normalized transaction features.
- **Conv1D Layer:** 32 filters with kernel size 2 and ReLU activation. This layer identifies local patterns between adjacent transaction features.
- **MaxPooling1D:** Reduces the feature size and computational cost while retaining significant patterns
- **Conv1D Layer:** 64 filters for improved high-level feature representation.
- **Dropout (0.5):** Randomly drops 50% of the neurons during training to mitigate class imbalance-induced overfitting.
- **Dense Layer:** Fully connected layer with 64 neurons and ReLU activation.
- **Output Layer:** Sigmoid activation function to predict the probability score of a transaction being fraudulent or genuine.

C. System Architecture & Tech Stack

The prediction engine is packaged inside a contemporary web application:

1. **Frontend (ReactJS):** A responsive UI where users can enter the transaction information. It supports real-time validation and shows the fraud risk indicators (Genuine/Fraud).
2. **Backend (FastAPI):** A fast Python web framework with two main endpoints:
    o /predict: Accepts the transaction information in JSON format, uses CNN-based prediction, and returns the fraud probability score.
    o /ask_ai: Manages user queries about fraud analysis and transaction analysis..
3. **AI Feature (RAG QA):** When a user asks a question, the system fetches the relevant knowledge about fraud from a carefully selected financial dataset and feeds it to a Large Language Model (LLM). This way, the system can provide accurate and explainable answers based on verified principles of fraud detection, not mere imagination.



[FIGURE 3: Confusion Matrix Heatmap] *(Insert the heatmap image from your notebook/report showing the TP, TN, FP, FN values)*

VI. EXPERIMENTAL RESULTS

A. Quantitative Analysis

The model was trained using a supervised learning method with 100 epochs and was optimized using the Adam optimizer. Binary Cross-Entropy loss was used for training. The dataset was divided into a training set and a test set, with 80% of the data used for training and 20% for testing.

Table 1: Performance Comparison with Baseline Models

Algorithm	Parameters			
	Accuracy	*Precision*	*Recall*	*F1-Score*
Logistic Regression	78.4%	74.0%	60.2%	0.65
Random Forest	86.1%	79.0%	79.0%	0.81
Proposed1D-CNN	89.2%	87.0%	84.5%	0.86

The proposed SVM model for fraud detection had the highest accuracy of 89.2% and the best Recall of 84.5%. In credit card fraud detection, high Recall is of utmost importance to avoid high False Negatives, which can cause severe financial losses if fraudulent transactions are missed.

B. Confusion Matrix Analysis

The confusion matrix for the test set (n=154) revealed:

- True Positives (TP): 85
- True Negatives (TN): 980
- False Negatives (FN): 15
- False Positives (FP): 20

The small number of False Negatives indicates that the system is trustworthy in detecting fraudulent transactions. Error analysis indicated that most errors were due to borderline cases, such as small fraud amounts or transactions in known locations, which are naturally hard to distinguish from legitimate activity without further information.

C. User Experience

The web interface enabled rapid prediction processing with an average response time of less than 300 ms via the FastAPI backend. The system was subject to a qualitative user test, which showed that the real-time fraud alerts and transaction status updates greatly enhanced the users' trust in digital payment systems compared to static fraud analysis.

ACKNOWLEDGMENT

We would like to express our sincere gratitude to our supervisor, **Mr. V. Devender**, Assistant Professor, Department of ECE, for his valuable guidance and continuous support throughout this research. We also extend our thanks to **Dr. P. Munaswamy**, Head of the Department of Electronics and Communication Engineering, and **Dr. L. V. Narasimha Prasad**, Principal of the Institute of Aeronautical Engineering, for their encouragement and for providing the necessary infrastructure to successfully complete this work

REFERENCES

[1] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2015). Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy. IEEE Transactions on Neural Networks and Learning Systems, 29(8), 3784-.

[2] Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). Transaction aggregation as a strategy for credit card fraud detection. Data Mining and Knowledge Discovery, 18(1), 30-55.

[3] Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. Artificial Intelligence Review, 34(1), 1-14

[4] Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. Expert Systems with Applications, 51,

[5] Carcillo, F., Dal Pozzolo, A., Le Borgne, Y. A., Caelen, O., Mazzer, Y., & Bontempi, G. (2019). Scarff: A scalable framework for streaming credit card fraud detection with Spark. Information Fusion, 41,.

[6] Abdallah, A., Maarof, M. A. & Zainal, A. (2016). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90-

[7] Sahin, Y. & Duman, E. (2011). Detecting credit card fraud by ANN and logistic regression. International Symposium on Innovations in Intelligent Systems and Applications, pp. 315-319. IEEE.

[8] Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection..

[9] Lebichot, B., Braun, J., Caelen, O., & Bontempi, G. (2019). Transfer learning strategies for credit card fraud detection. IEEE Access, 7

[10] Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2018). Credit card fraud detection using AdaBoost and majority voting. IEEE Access, 6, 142

[11] Pumsirirat, A. & Yan, L. (2018). Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine. International Journal of Advanced Computer Science and Applications, 9(1), 18-25.

[12] Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., & Beling, P. (2018). Deep learning detecting fraud in credit card transactions. Systems and Information Engineering Design Symposium (SIEDS), pp. 129-134.

[13] Bhattacharyya, S., Jha, S., Tharakunnel, K. & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. Decision Support Systems, 50

[14] Chen, C., Li, C., Li, J., & Wang, Y. (2018). Credit card fraud detection based on machine learning models. Journal of Physics: Conference Series, 1069(1), 012089.

[15] Baesens, B., Van Vlasselaer, V. & Verbeke, W. (2015). Fraud analytics using descriptive, predictive and social network techniques. Wiley Publications..

[16] Jiang, C., Song, J., Liu, G., Zheng, L. & Luan, H. (2018). Credit card fraud detection: A novel approach using aggregation strategy and feedback mechanism. IEEE Internet of Things Journal, 5(5), 3637-3647.