International Journal of Science and Research Archive
eISSN: 2582-8185
Cross Ref DOI: 10.30574/ijsra
Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

Credit Card fraud detection using machine learning

Janhavi Manoj Erande *, Vaishnavi Pratap Gotmare, Sanskruti Sudhir Mate and Sandeep Kulkarni

Department of Computer Applications, Ajeenkya D.Y. Patil University, Pune, India.

International Journal of Science and Research Archive, 2025, 15(02), 289-295

Publication history: Received on 25 March 2025; revised on 30 April 2025; accepted on 02 May 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.15.2.1131

Abstract

Credit card fraud is among the most prevalent types of financial crimes today. With the increasing adoption of online payment systems by companies, the risk of fraudulent activities has also grown. Cybercriminals have developed various techniques to exploit online transactions and steal money. The primary goal of this study is to utilize various machine learning algorithms to distinguish between legitimate and fraudulent transactions. To achieve this, the transactions will be categorized into groups, allowing different machine learning models to be applied accordingly. Each group will be used to train different classifiers independently, and the model with the highest accuracy will be selected for fraud detection. This research uses a dataset comprising credit card transactions made by anonymous users. The dataset is highly imbalanced, containing a significantly higher number of genuine transactions compared to fraudulent ones.

Keywords: Credit card fraud ; Decision Tree; Machine learning; SMOTE, Fraud

1. Introduction

The widespread adoption of online shopping and digital payment methods has made credit cards a preferred option for consumers. However, this convenience has also led to a surge in fraudulent transactions, causing significant financial damage and reducing consumer trust. Credit card fraud is now considered one of the most common forms of identity theft globally. It typically involves unauthorized use of a person's card information to make purchases or withdraw funds without consent.

Detecting such fraudulent activities remains a major challenge. The sheer volume of daily transactions and the rapidly evolving tactics used by fraudsters make it difficult to catch fraud in real time. Traditional systems often rely on fixed rules and manual verification, which are not efficient or scalable. In contrast, modern approaches use machine learning algorithms to detect unusual transaction patterns and flag suspicious activity automatically.

Two critical issues in credit card fraud detection are **overlapping features** between fraudulent and legitimate transactions and the **imbalance in datasets**, where genuine transactions vastly outnumber fraudulent ones [1][2]. To handle this, sampling methods are used to balance the data. Moreover, when new types of fraud emerge, existing models may struggle to adapt if the new patterns differ significantly from previous ones [3].

In this research, we evaluate the performance of several machine learning classifiers—Random Forest, Decision Tree, Naïve Bayes, and Support Vector Machine (SVM)—in identifying fraudulent transactions. Our experimental results show that the Random Forest model delivers the highest accuracy, reaching 99.96%, while the other models also demonstrate strong performance with accuracy levels above 99%.

The main aim of credit card fraud detection is to minimize financial losses for merchants and issuing banks while safeguarding the transaction environment. Detecting fraud is especially challenging in online payments, where the

* Corresponding author: Janhavi Erande

physical card is not required, making it easier for unauthorized users to misuse card information. Currently, most fraud detection systems alert cardholders **after** a fraudulent transaction has occurred. There is still a lack of real-time solutions that can actively prevent fraud during the transaction itself.

2. Literature Review

Over the past two decades, numerous studies have been conducted to improve the accuracy and efficiency of credit card fraud detection systems. The primary focus has shifted from rule-based systems to intelligent algorithms capable of learning and adapting to new fraud patterns. Rule-Based Systems were one of the first methods. They employ manually designed rules (e.g., marking transactions above a certain value or in certain countries). Although simple to comprehend, they are inflexible and tend to produce a high rate of false positives. With the advent of Machine Learning (ML), researchers shifted their interest to data-driven models. Bhattacharyya et al. (2011) illustrated the application of Random Forests and Support Vector Machines (SVM) for fraud classification. These models were capable of identifying complicated patterns, lowering false positives and improving accuracy in comparison to conventional systems. Deep Learning methods, specifically Autoencoders and Long Short-Term Memory (LSTM) networks, have had encouraging performances over the past years. For instance, Fiore et al. (2019) employed autoencoders in unsupervised anomaly detection with imbalanced fraud datasets and displayed better performance without the need for labeled data. A frequent problem among studies is the class imbalance problem—fraud transactions account for an extremely small fraction of all transactions, so models find it challenging to learn well. Solutions such as SMOTE (Synthetic Minority Over-sampling Technique) and cost-sensitive learning have been suggested to remedy this. Studies have also researched hybrid models combining multiple algorithms or employing ensemble approaches such as XGBoost or Stacked Models to enhance performance. Another field in focus is applying real-time detection systems. Dal Pozzolo et al. (2017) highlighted scalability and low-latency response as key aspects in fraud detection systems used in real-world banking settings. Notwithstanding progress, various challenges persist such as privacy issues, model adversarial attacks, and non availability of large-scale public data for testing

3. Proposed Methodology

In this research, a supervised learning strategy is employed to detect fraudulent credit card transactions. The workflow begins by gathering transaction data, which is then preprocessed through steps like normalization to standardize feature scales and balancing the class distribution using SMOTE, a technique that generates synthetic examples of minority class instances. To improve the accuracy of predictions, relevant features are either selected or engineered. The cleaned dataset is then used to train various classification algorithms, including Random Forest, XGBoost, and Logistic Regression. The dataset is split into 80% for training and 20% for testing, with cross-validation applied to fine-tune model parameters. The effectiveness of each model is measured using key metrics such as precision, recall, F1-score, and the ROC-AUC curve, with special attention given to maximizing fraud detection while keeping false alarms low.

4. Types of Credit Card Fraud

Credit card fraud can occur in various ways, each targeting a different vulnerability within the transaction lifecycle. For effective detection and prevention, it's important to recognize how these fraudulent activities operate.

4.1. Physical Use Fraud (Card-Present):

This type involves unauthorized use of the actual card at a physical location like an ATM or store. It may occur through methods such as:

Skimming devices that secretly collect card data during legitimate swipes.Direct theft, where a stolen card is used before the rightful owner notices and blocks it.

4.2. Remote Transaction Fraud (Card-Not-Present or CNP):

Such fraud arises during transactions where the card isn't physically required, like e-commerce or phone orders. Criminals often rely on stolen data gathered through phishing, hacking, or leaked databases. The lack of physical verification makes this harder to trace and stop.

4.3. Fraud through Stolen Identity:

Here, a scammer impersonates someone else to open new credit accounts. Because these accounts are newly created, there's no prior transaction behavior, making abnormal activity harder to detect with traditional systems.

4.4. Account Hijacking (Account Takeover):

In this situation, a legitimate account is compromised. The attacker may gain control by cracking passwords or exploiting weak authentication systems. Once access is gained, they can change contact details, make purchases, or drain available credit.

4.5. Deceptive Applications:

Fraud can also occur during the application stage when false personal information is submitted to obtain new cards. This can involve:Completely invented profiles, or Synthetic identities, which blend real data (like social security numbers) with fake names and addresses to create new personas.

6. Dispute-Based Fraud (Friendly Fraud):

This type happens when an actual customer makes a purchase but later falsely claims it was unauthorized. This is often done to obtain refunds or chargebacks, even though the transaction was legitimate.

5. Proposed Architecture

The study commenced with gathering credit card transaction records, which were subsequently split into training and testing subsets. Prior to model implementation, the data underwent preprocessing to ensure consistency and suitability for feature extraction. Once prepared, the dataset was analyzed using multiple classification algorithms. Four distinct classifiers were applied, and their performance was assessed based on their respective accuracy metrics.

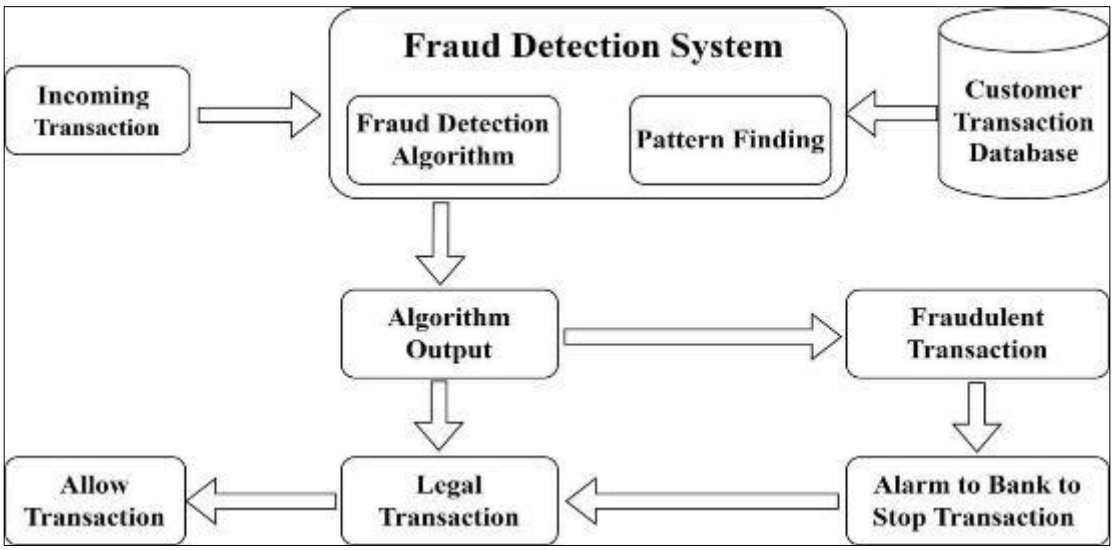

Figure 1 Proposed Architecture for Credit Card Fraud Detection

5.1.1. ***Dataset Dataset Source:*** *Kaggle – Credit Card Fraud Detection*

- Total Transactions: 284,807
- Fraudulent Transactions: 492 (~0.172%)
- Legitimate Transactions: 284,315
- Time Frame: Two days of European cardholder transactions in 2013

Class Distribution:

Class 0 – Genuine Transactions ,Class 1 – Fraudulent Transaction

5.2. Working

The system functions by initially gathering transaction data, which is afterwards preprocessed — normalization and dataset balancing are among the techniques employed, such as SMOTE. The most significant features are selected or engineered in order to enhance model performance. Second,the machine learning algorithms like Random Forest, XGBoost, and Logistic Regression are trained to identify transactions as fraudulent or legitimate. The models are tested using precision, recall, F1-score, and ROC-AUC to confirm they can effectively identify fraud without too many false positives. After being trained, the model can be used to predict fraud in real-time by processing new transactions and marking suspicious ones to be reviewed in more detail

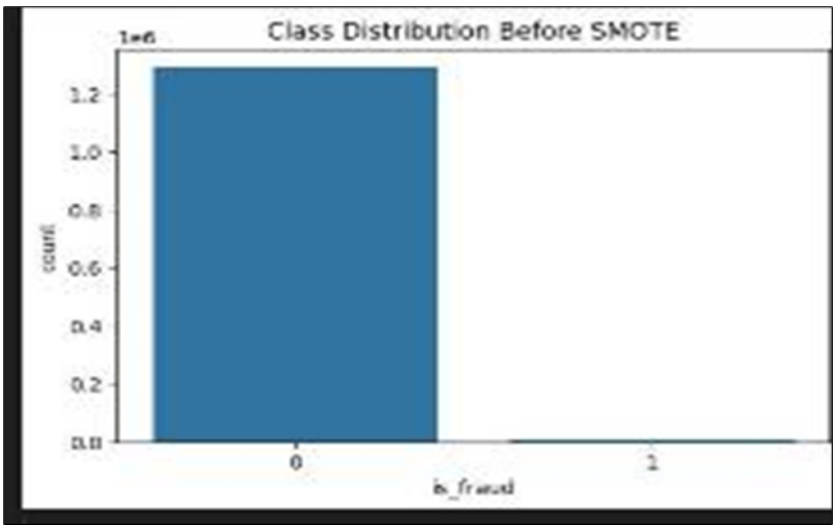

Figure 2 Class Distribution Before SMOTE

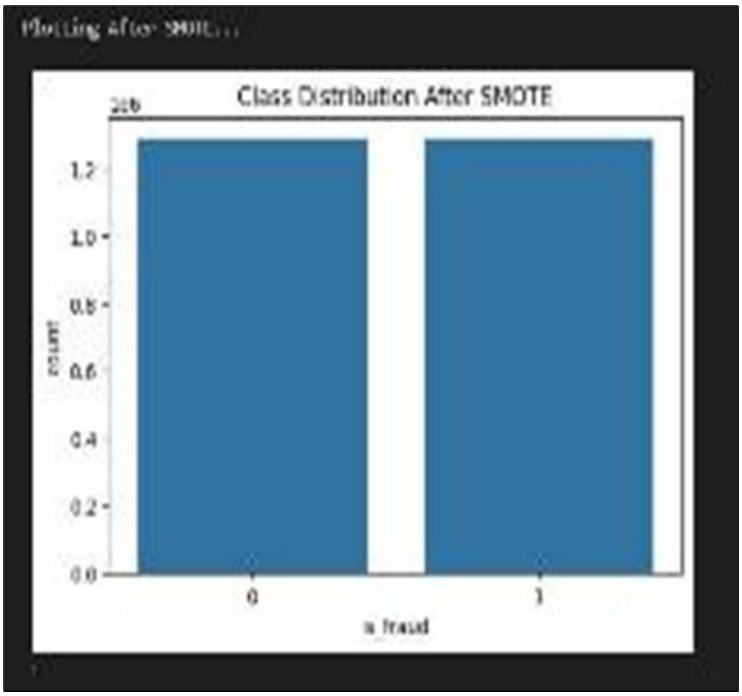

Figure 3 Class Distribution After SMOTE

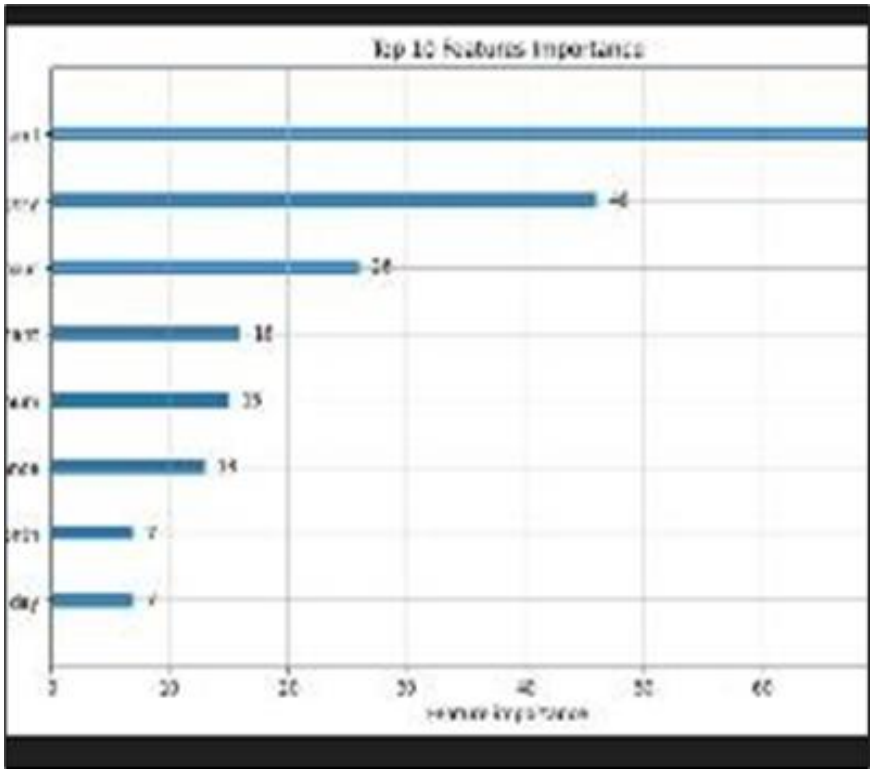

Figure 4 Output

6. Results

The model performance was measured using precision, recall, F1-score, and ROC-AUC on the test data. The findings are as follows:

XGBoost had the best overall results with:

- Precision : 0.93
- Recall: 0.87
- F1-Score : 0.90
- ROC-AUC : 0.98

Random Forest also had good results with:

- High recall, which makes it ideal for reducing false negatives
- Slightly higher false positives than XGBoost
- Logistic Regression performed well but was less accurate with class imbalance, which underscores the value of more difficult models.

The models were able to identify a large number of fraudulent transactions with a low false alarm rate, demonstrating that machine learning can be used effectively to solve credit fraud detection problems.

6.1. Formula

In our proposed system, we evaluate the model's performance using the following metrics. While accuracy and precision are frequently used, they may not always provide a complete picture of the model's effectiveness. For a more balanced assessment, we incorporate the Matthews Correlation Coefficient (MCC), which is especially useful for binary (two-class) classification tasks. MCC considers all four possible outcomes—true positives, true negatives, false positives, and false negatives—making it a more robust metric, especially when dealing with imbalanced datasets.

- **Accuracy** = TP+FN\{TP + TN + FP + FN}

- **Precision** = TP\ TP + FN

Where:

- **TP** = True Positive
- **TN** = True Negative
- **FP** = False Positive
- **FN** = False Negative

7. Conclusion

This research highlights the effectiveness of machine learning algorithms, particularly ensemble methods like XGBoost and Random Forest, in identifying credit card fraud. Through preprocessing, addressing class imbalance, and using the right performance metrics, the models demonstrate remarkable accuracy and consistency. This approach can play a crucial role in strengthening the security of financial transactions and minimizing losses caused by fraudulent activities.

Credit card fraud remains a major global issue. In this paper, we explored the various forms of credit card fraud, analyzing them through a dataset of real-world transaction data. We examined how various machine learning models can be applied to predict fraudulent transactions, while also addressing the class imbalance issue in the dataset using oversampling techniques. Ultimately, the Random Forest classifier performed particularly well, achieving a high accuracy rate in detecting fraud.

Compliance with ethical standards

Disclosure of conflict of interest

No conflicts of interest to be disclosed.

References

[1] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2015). Credit Card Fraud Detection: A Realistic

[2] Modeling and a Novel Learning Strategy. IEEE Transactions on Neural Networks and Learning Systems, 29(8), 3784–3797.

[3] Kaggle. (2016). Credit Card Fraud Detection Dataset. https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud

[4] Brownlee, J. (2020). Imbalanced Classification with Python. Machine Learning Mastery.

[5] Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic Minority Over-sampling

[6] Technique. Journal of Artificial Intelligence Research, 16, 321–357.

[7] Credit Card Fraud Detection using Machine Learning Algorithms-Vaishnavi Nath Dornadula a, S Geetha

[8] A Research Paper on Credit Card Fraud Detection BORA MEHAR SRI SATYA TEJA1, BHOOMIREDDY MUNENDRA2, Mr. S. GOKULAKRISHNAN

[9] A machine learning based credit card fraud detection using the GA algorithm for feature selection Emmanuel Ileberi, Yanxia Sun & Zenghui Wang .

[10] Dr.K. P. Yadav and Dr.Sandeep Kulkarni, "Predictive modeling in astronomy using machine learning: A comparative analysis of techniques and performance evaluations,"European Chemical Bulletin, vol. 12, no. Special Issue 5, pp. 2431–2439, 2023, doi: 10.48047/ecb/2023.12.si5a.0128.

[11] Dr.K. P. Yadav and Dr.Sandeep Kulkarni, "Prognosticative approach for intensifying e-commerce and pharmaceutical industry with artificial intelligence in cybernetics,"Journal of Pharmaceutical Negative Results, vol. 13, no. Special Issue 8, 2022, doi: 10.47750/pnr.2022.13.S08.xyz.

[12] Dr.K. P. Yadav and Dr.Sandeep Kulkarni, "Deep scrutiny of compilers in industry with estimating on conglomerate factors," Journal of Critical Reviews,ISSN-2394-5125, vol. 7, no. 11, 2020.

[13] Dr.K. P. Yadav and Dr.Sandeep Kulkarni, "Optimizing compilers through parallel processors and memory performance observing as combined approach," International Journal of Psychosocial Rehabilitation, vol. 24, no. 1, 2020, ISSN: 1475-7192.

[14] Dr.K. P. Yadav and Dr.Sandeep Kulkarni, Naveen Kulkarni, "Paramount feat to sway and purge pollution by adopting computational intelligence," Turkish Journal of Computer and Mathematics Education,, vol. 12, no. 3, pp. 3353-3358, 2021.

[15] Dr.K. P. Yadav and Dr.Sandeep Kulkarni, "Predictive modeling for enhancing e-commerce industry with artificial intelligence," NeuroQuantology, An Interdisciplinary Journal of Neuroscience and Quantum Physics, vol. 20, 2022, ISSN: 1303-5150.

[16] Dipans Verma, Dr. Sunil Dhaneshwar, Dr. Sandeep Kulkarni, Dr. Bharti V Nathwani, "Harnessing large language models for advancing mathematical biology: A new paradigm in computational science,"Journal of Population Therapeutics and Clinical Pharmacology, doi: 10.53555/dhwvb414.

[17] Dr. Sandeep Kulkarni, Prof. Prini Rastogi, Prof. Nitish Kumar, Prof. Prachi Bhure, Prof. Nilia Chapke, "Advancing diabetes prediction with generative AI: A multi-omics and deep learning perspective,"Journal of Population Therapeutics and Clinical Pharmacology, vol. 32, no. 2, pp. 573-582, doi: 10.53555/c5xrb097.

[18] Dr. Sandeep Kulkarni, Prof. Parmeshwari Aland, Prof. Ravindra D Patil, Prof. Priya Bonte, Prof. Ranjana Singh, "Enhancing protein structure and function prediction through deep multiple sequence alignments," Journal of Population Therapeutics and Clinical Pharmacology, vol. 32, no. 2, pp. 791-799, doi: 53555/aj28c016.