WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

CREDIT CARD FRAUD DETECTION USING ML

***Aryansh Singh Dhakad*[1]**

[1]Student, Department of IT Maharaja Agrasen Institute of Technology (MAIT), New Delhi, India

ABSTRACT :

The exponential growth of online transactions has intensified the risk of credit card fraud, posing serious challenges to financial security. Traditional rule-based detection systems often fail to adapt to the dynamic nature of fraudulent behavior, resulting in delayed responses and significant financial losses. This paper explores an adaptive machine learning framework designed to detect credit card fraud with higher accuracy and efficiency. We systematically evaluate multiple supervised learning algorithms, including Random Forest, XGBoost, and Neural Networks, while addressing data imbalance through techniques like SMOTE and anomaly detection methods.

Keywords - Card-Not-Present frauds, Card-Present-frauds, Concept Drift

Introduction

Background

In today's highly digitized economy, credit cards have become one of the most common mediums for financial transactions due to their convenience and global acceptance. However, the growing dependence on electronic payments has been paralleled by a surge in fraudulent activities, causing billions of dollars in losses annually across the financial sector. Traditional fraud detection methods, largely based on manually crafted rules and static thresholds, are increasingly inadequate against the evolving tactics of cybercriminals who adapt quickly to system defenses.

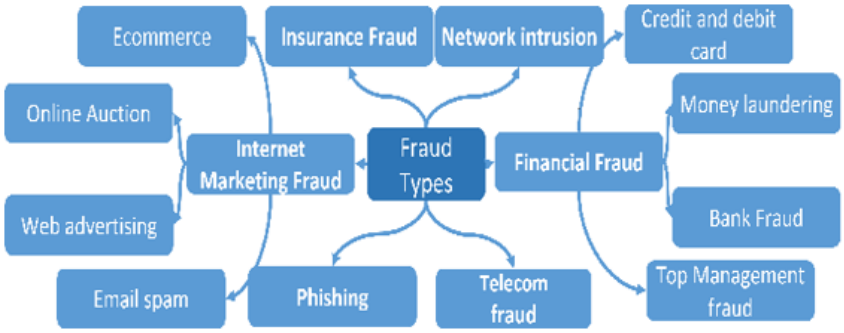

Fig. 1: Taxonomy for Frauds

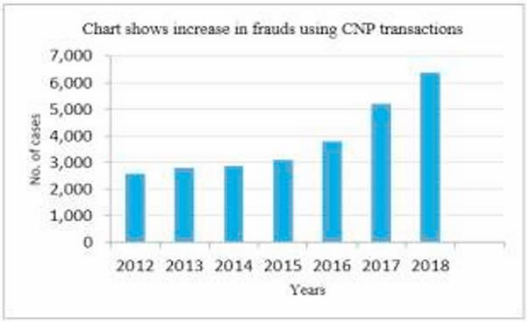

Fig. 2: Frauds Using Card Not Present Transaction

Literature Survey

Credit card fraud detection has evolved significantly, moving from traditional rule-based systems to advanced machine learning (ML) methodologies. Early systems depended heavily on manually crafted rules, but they struggled to adapt to new fraud patterns as criminals developed more sophisticated techniques.

Supervised learning models such as Logistic Regression, Decision Trees, Random Forests, and Support Vector Machines (SVM) have been widely investigated for fraud detection. Bhattacharyya et al. [1] demonstrated that ensemble methods like Random Forests achieve high accuracy and resilience against overfitting when applied to financial datasets. However, the severe class imbalance—where fraudulent transactions constitute a small fraction of total transactions—poses a major challenge. Dal Pozzolo et al. [2] emphasized that traditional accuracy metrics are misleading in this context, advocating for Precision, Recall, and the Area Under the Precision-Recall Curve (AUPRC) as more reliable performance indicators.

To mitigate class imbalance, data augmentation techniques like the Synthetic Minority Over-sampling Technique (SMOTE) and cost-sensitive learning have been employed successfully [3]. Ensemble learning methods, notably XGBoost and LightGBM, have also shown superior performance due to their ability to capture complex feature interactions and manage imbalanced datasets effectively [4].

Unsupervised and semi-supervised approaches, such as Autoencoders and Isolation Forests, have proven valuable when labeled data is scarce. Fiore et al. [5] explored deep Autoencoders for reconstructing normal transaction patterns and detecting deviations indicative of fraud. Additionally, recurrent models like Long Short-Term Memory (LSTM) networks have been employed to model sequential transaction behavior for real-time fraud detection.

Proposed Method

This study proposes a hybrid machine learning approach for effective credit card fraud detection, focusing on maximizing detection rates while minimizing false positives. The framework consists of four major stages: data preprocessing, feature engineering, model training, and evaluation.

In the preprocessing phase, data cleaning is performed to handle missing values and outliers. Class imbalance, a key challenge in fraud detection, is addressed using a combination of Synthetic Minority Over-sampling Technique (SMOTE) and Tomek links to enhance minority class representation without introducing noise.

Table 1: Raw features of credit card transactions

Attribute name	Description
Transaction id	Identification number of a transaction
Cardholder id	Unique Identification number given to the cardholder
Amount	Amount transferred or credited in a particular transaction by the customer
Time	Details like time and date, to identify when the transaction was made
Label	To specify whether the transaction is genuine or fraudulent

Dataset Description

A publicly available credit card fraud dataset is used. It contains transaction details such as amount, time, and anonymized features. Each transaction is labeled as fraud (1) or non-fraud (0). The dataset is highly imbalanced, with fraudulent transactions being a small percentage of the total data.

Table 2: Attributes of European dataset

S. No.	Feature	Description
1.	Time	Time in seconds to specify the elapses between the current transaction and first transaction.
2.	Amount	Transaction amount
3.	Class	0 - not fraud 1 – fraud

Methodology

The proposed methodology for credit card fraud detection integrates data preprocessing, model training, and evaluation phases. Initially, the dataset undergoes cleaning to address missing values and outliers. To counteract class imbalance, SMOTE combined with Tomek Links is applied.
Feature engineering is performed by extracting time-based and behavior-driven attributes, enhancing the model's ability to differentiate between normal and fraudulent transactions. Dimensionality reduction using PCA is optionally used to simplify complex data patterns.
Three machine learning models—Random Forest, XGBoost, and an Autoencoder for anomaly detection—are trained independently. Their outputs are combined through a stacking ensemble technique, with a Logistic Regression model serving as the meta-classifier to improve overall predictive performance.
The system is evaluated using metrics appropriate for imbalanced data, including Precision, Recall, F1-Score, and AUPRC. Model explainability is achieved through SHAP analysis, ensuring the transparency and trustworthiness of predictions.

Conclusion

This study demonstrates that machine learning techniques, when combined with careful data balancing, feature engineering, and ensemble modeling, significantly improve the accuracy and reliability of credit card fraud detection systems. By integrating multiple models and using interpretability tools like SHAP, the proposed approach not only enhances detection performance but also builds trust for real-world deployment. Future work can explore deep learning architectures and adaptive learning systems to further strengthen fraud prevention efforts against evolving threats.

REFERENCES

[1] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," *Decision Support Systems*, vol. 50, no. 3, pp. 602–613, Feb. 2011.

[2] A. Dal Pozzolo, O. Caelen, Y.-A. Le Borgne, S. Waterschoot, and G. Bontempi, "Learned lessons in credit card fraud detection from a practitioner perspective," *Expert Systems with Applications*, vol. 41, no. 10, pp. 4915–4928, Aug. 2014.

[3] N. Chawla, K. Bowyer, L. Hall, and W. Kegelmeyer, "SMOTE: Synthetic Minority Over-sampling Technique," *Journal of Artificial Intelligence Research*, vol. 16, pp. 321–357, 2002.

[4] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," in *Proc. 22nd ACM SIGKDD Int. Conf. Knowl. Discov. Data Min.*, 2016, pp. 785–794.

[5] Datasets from Kaggle