Credit Card Fraud Detection Using ML & DL

Murali Krishna Kodimenu[1], Dr Satyanarayana S[2], Dr Thayabba Katoon[3]

[1]*Student, MTech in ML&DL, Malla Reddy University*
[2]*Professor-AIML, Malla Reddy University*
[3]*Hod-AIML, Malla Reddy University*

---***---

Abstract - The ascent of the digital payments industry is accelerating as the global economy increasingly adopts online and card-based payment systems. This transition, however, brings with it an elevated risk of cyber threats and fraud, now more prevalent than ever before.

For banks and financial institutions, bolstering the detection of credit card fraud is of utmost importance. Machine learning (ML) is revolutionizing this domain, making the identification of fraudulent activities both simpler and more effective. ML-powered fraud detection systems are adept at identifying patterns and halting irregular transactions.

The hurdles faced in this area are significant: vast quantities of data are processed daily, with the vast majority of transactions (99.8%) being legitimate; the data, largely confidential, is not readily accessible; not all fraudulent activities are detected and reported; and fraudsters continually develop new strategies to outsmart the detection models.

Machine learning algorithms are capable of pinpointing atypical credit card transactions and instances of fraud, ensuring that cardholders are not billed for purchases they did not make. These ML algorithms outperform traditional fraud detection systems, capable of discerning thousands of patterns within extensive datasets. Moreover, ML provides valuable insights into consumer behavior through the analysis of app usage, payment, and transaction patterns.

The advantages of deploying machine learning in the fight against credit card fraud are manifold, including swifter detection, enhanced precision, and increased efficiency when dealing with large volumes of data.

Key Words: Credit Card Frauds, Fraud Detection, Correlation matrix, principal components, Random Forest.

1.INTRODUCTION *(Size 11, Times New roman)*

In today’s financial and corporate landscape, one of the most pressing challenges is the escalating threat of financial frauds, which have widespread implications across various sectors. A significant factor contributing to the surge in credit card fraud is the increasing reliance on credit cards for purchases, leading to a global spike in such fraudulent activities. Credit card transactions, which are now the preferred method for both online and offline payments, have seen a marked increase in fraud rates.

Credit card transactions can occur in two ways: physical and virtual. In physical transactions, the cardholder hands over the card to the merchant to complete the payment, which carries the risk of the card being stolen by an attacker. Virtual transactions, conducted via the internet or telephone, offer fraudsters a straightforward method to commit fraud on an international scale. The essential information needed to execute a fraudulent payment includes the CVV number, card number, and expiration date. With the rapid advancement of communication and information technology, financial frauds are proliferating, leading to significant financial losses worldwide. Online frauds, facilitated by the internet, have become the most common due to the ease of committing them and the formation of international networks among fraudsters.

Banks worldwide are recognizing the necessity of a unified global strategy that involves data sharing to combat these attacks. This collaboration forms the foundation of a global fraud detection framework. Additionally, local detection systems share information about attacks, thereby protecting the global financial network from being compromised by fraudsters. The main challenges in this system include:

1. Companies often conceal their data for competitive and financial reasons.
2. Transaction behavior databases require scalable machine learning systems.
3. The capability to detect fraud is distributed across models in a networked environment.

Credit card fraud has become increasingly prevalent in today’s digital landscape. With the convenience of having everything accessible from home, there’s been a surge in e-commerce usage, which in turn provides more opportunities for attackers and scammers to commit fraud. Fraudsters employ a variety of methods to carry out their schemes. Understanding these methods is crucial to prevent further fraudulent activities. Numerous studies have been conducted exploring a range of techniques for detecting and addressing credit card fraud.

Machine learning offers a wide-ranging application in the realm of credit card fraud detection, encompassing various facets of electronic payment systems. Key areas where machine learning proves beneficial include:

- Transaction Monitoring: Machine learning algorithms are capable of scrutinizing vast amounts of transaction data in real-time to identify fraudulent activities.
- Risk Assessment: Machine learning models can evaluate the risk level of transactions, users, or merchants, aiding credit card companies in focusing their fraud prevention efforts.
- User Behavior Analysis: These algorithms can examine patterns in user behavior to spot anomalies, such as unusual login locations, shifts in spending habits, or repeated account creations from a single device.
- Fraud Trend Analysis: Machine learning can also be instrumental in detecting new patterns and trends in fraud, enabling credit card companies to take preemptive measures against future fraud attempts and reduce financial losses.

Credit card fraud detection is a highly confidential process that few are privy to. To address this issue, a proposed system for detecting fraud in credit card transactions will be developed using machine learning techniques, providing investigators with reliable and targeted fraud alerts.

2. Related Work

Credit card fraud manifests in various forms. It can involve the theft of the physical card or the unauthorized acquisition of sensitive information such as the account number, CVV, card type, among others. Fraudsters may exploit this data to authorize substantial transactions, often spending large sums before the cardholder becomes aware. Consequently, companies are implementing diverse machine learning strategies to discern between legitimate and fraudulent transactions. As credit cards grow more prevalent for both online and in-person transactions, the incidence of fraud is likely to increase.

The traditional manual methods for detecting fraudulent activities are often slow and error-prone, making them impractical in the era of big data. Consequently, financial institutions have shifted towards more intelligent methods. These advanced fraud detection techniques are based on computational intelligence (CI) and are divided into two main categories: supervised and unsupervised methods. Supervised methods involve modeling based on examples of both fraudulent and legitimate transactions to accurately classify them. In contrast, unsupervised methods detect potential fraud by identifying statistical outliers in transaction data without prior labeling.

Classification of credit card transactions is generally a binary classification problem . In this scenario, a transaction is either classified as fraudulent (negative class) or legitimate (positive class). A unique aspect of credit card transaction data is that both legitimate and fraudulent transactions often exhibit similar features. Fraudsters are constantly devising new methods to mimic the spending patterns of genuine cardholders, leading to an ever-evolving profile of legitimate and fraudulent behaviors. This dynamic nature results in a lower detection rate of actual fraud within the dataset, creating a distribution heavily skewed towards the negative class (legitimate transactions).

The objective of fraud detection is often viewed as a data mining classification task, requiring accurate differentiation between legal and fraudulent transactions. In practice, there are two primary approaches to detecting credit card fraud. The first involves manual data mining, which is labor-intensive and prone to error. The second employs rule-based systems, also known as machine learning techniques or expert systems, which store and update knowledge on fraud to interpret data effectively and address fraudulent activities. These systems are categorized into supervised, unsupervised, and semi-supervised learning.

Supervised fraud detection methods use models trained on examples of both fraudulent and legitimate transactions to classify new transactions. Unsupervised fraud detection identifies outlier transactions as potential fraud. A combination of both methods is known as semi-supervised learning. The random forest algorithm is frequently used to tackle the challenge of credit card fraud detection.

A significant challenge in this field is the imbalanced nature of datasets, where the majority of transactions are non-fraudulent. This imbalance can cause supervised learning algorithms to predominantly predict non-fraudulent transactions. Despite this, the F1 score is regarded as the most reliable metric for evaluating the performance of algorithms.

2.1 Features Utilized for Detecting Credit Card Fraud

a) Principal Component Analysis (PCA): PCA is an unsupervised learning algorithm employed for reducing dimensions in machine learning. It uses orthogonal transformation to turn correlated variables into a set of uncorrelated variables known as Principal Components.

b) Decision Tree: This supervised learning method is versatile, suitable for both classification and regression tasks, though it is predominantly used for classification. It features a tree-like model where internal nodes denote dataset attributes, branches represent decision-making rules, and each leaf node signifies a result.

c) Random Forest Algorithm: As a supervised learning algorithm, Random Forest is effective for both classification and regression challenges. It operates by creating multiple decision trees on different data subsets and averaging their predictions to enhance the dataset's overall predictive accuracy.

d) Correlation Matrix: This statistical tool measures how two variables move in tandem. The correlation coefficient, symbolized as “r,” varies from -1 to 1, reflecting the strength and direction of the linear relationship between the variables.

3. Machine Learning Methods

Machine learning techniques are frequently employed in evaluating credit scoring systems due to their minimal reliance on assumptions and their ability to enhance the accuracy of observations.

3.1 Supervised Learning

The method aims to learn from past instances that are introduced during the training phase. Therefore, if the dataset is pre-labeled, it falls under the category of supervised learning. Supervised learning techniques encompass a variety of algorithms such as decision trees, support vector machines (SVM), neural networks (NN), and linear regression (LR), all of which have been applied, including the use of neural networks, to identify credit card fraud.

Random Forest: Among ensemble methods, Random Forest (RF) stands out as an effective technique for enhancing both accuracy and precision in artificial intelligence and machine learning algorithms. Proposed by researcher Breiman, this classifier helps identify relevant independent variables, allowing the system to make informed selections. Numerous studies have highlighted its importance in selecting multiple candidates for each tree, and empirical research confirms its superior predictive accuracy

3.2 Unsupervised Learning

Unsupervised learning is a subset of machine learning methods that are used to detect patterns in data. These methods autonomously analyze the data to uncover intriguing structures. The most commonly used unsupervised learning techniques include the K-means algorithm, the Self-Organizing Map (SOM), and the Hidden Markov Model (HMM).

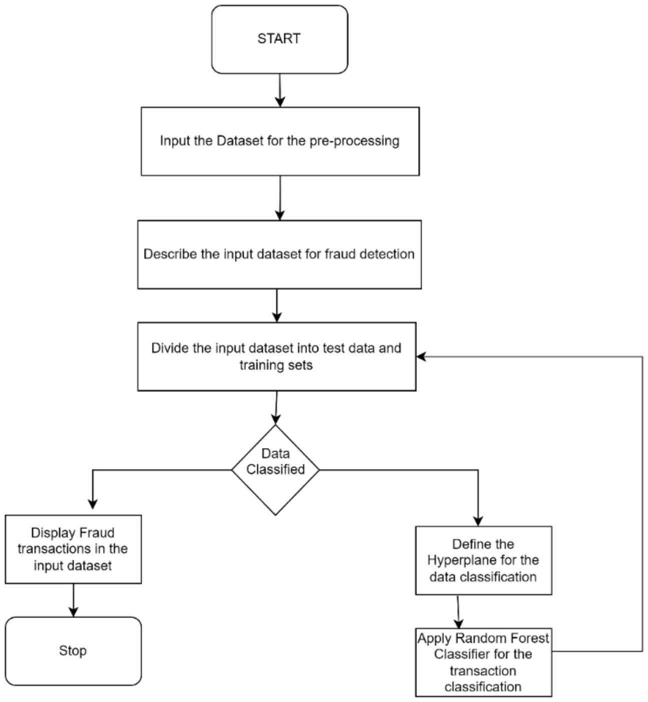
4. Challenges of Credit Card Fraud Detection

The task at hand is to recognize fraudulent transactions to ensure that customers of merchant accounts are not billed for purchases they did not make. In the field of credit card fraud detection, there are several challenges that still need to be addressed, some of which we will discuss here.

The primary challenges in detecting credit card fraud include:

- The vast amount of data that is collected daily, which requires the detection system to be fast and responsive enough to accurately identify fraud.
- The imbalance in data, where the vast majority of transactions (98.9%) are legitimate, making it difficult to pinpoint fraudulent ones.
- The issue of misclassified data, as not all instances of fraud are detected or reported.
- The adaptive strategies employed by fraudsters to circumvent detection systems.

5. Methodology


START
Input the Dataset for the pre-processing
Describe the input dataset for fraud detection
Divide the input dataset into test data and training sets
Data Classified
Display Fraud transactions in the input dataset
Stop
Define the Hyperplane for the data classification
Apply Random Forest Classifier for the transaction classification

The diagram illustrates the operational process of our application. We have utilized various classification methods such as logistic regression, decision tree, random forest, and KNN for the purpose of detecting fraud. We evaluate these models to determine which one most effectively discerns the link between the features and identifies fraudulent transactions. Following the training phase, we will introduce an ensemble model that operates as a voting classifier, integrating the strengths of the other classification methods. The goal is to minimize the inaccuracies inherent in individual models, thereby enhancing the predictive capabilities of the ensemble model. If we denote the classifiers as

$C1,C2,C3,C4,$and $C5$

, then the ultimate classifier,
Ct

, will be determined by the majority vote:

$$Ct=Majority\{C1,C2,C3,C4,C5\}$$

.Subsequent stages include:

- Data Collection: Gathering and storing credit card transaction data in a database, which includes details like transaction amount, date and time, merchant ID, and cardholder information.

- Data Pre-processing: Refining the raw data for analysis, potentially involving the elimination of extraneous or repetitive data, data format unification, and standardization of data fields.

- Data Analysis: Employing statistical and machine learning methods on the pre-processed data to pinpoint fraudulent transactions, which may encompass anomaly detection, clustering, and classification algorithms.
- Model Building: Creating a model based on the outcomes of data analysis, trained to recognize fraudulent behavior patterns, useful for detecting future fraud.
- Model Validation: Evaluating the model's performance using a distinct dataset to verify its precision and effectiveness.
- Deployment: Implementing the validated model in a live environment to oversee credit card transactions in real-time.
- Monitoring and Updates: Continuously observing the operational model to maintain its efficacy.

5.1 Steps in Credit Card Fraud Detection

Begin by collecting the available data and uploading the dataset of credit card transactions. Implement one-class classifiers and the Matthews correlation coefficient to enhance data pre-processing and verify the presence of imbalances within the dataset. Generate a Correlation Matrix for the entire dataset. Divide the dataset into training and testing subsets, for instance, 70% for training and 30% for testing. Employ a machine learning classification approach. Compute various evaluation metrics, including the confusion matrix, accuracy, precision, recall (or True Positive Rate), F1-score, and False Positive Rate, using the following formulas:

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive + False Positive}}$$

$$\text{Recall} = \frac{\text{True Positive}}{\text{True Positive + False Negative}}$$

$$\text{F1 Score} = \frac{2 \text{ x (Precision x Recall)}}{\text{Precision + Recall}}$$

$$\text{Accuracy} = \frac{\text{True Positive + True Negative}}{\text{TP+ TN+ FP + FN}}$$

$$\text{Recall or True Positive Rate} = \frac{\text{True Positive}}{\text{True Positive + False Negative}}$$

$$\text{False Positive Rate} = \frac{\text{False Positive}}{\text{False Positive + True Negative}}$$

The confusion matrix is structured as below:

Actual Value	Predicted Positive(1)	Predicted Negative (0)
Positive(1)	TP	FP
Negative(0)	FN	TN

Implement a feedback mechanism to enhance the detection rate and accuracy. Iterate the process from steps 4 to 6 with different classifiers to compare their performance.

5.2 Modeling and Analysis

Upon examining the dataset, we employ a variety of classification methods, such as KNN and Random Forest, to determine whether the values are fraudulent. We create visual representations like graphs and a correlation matrix from this data. Additionally, we conduct a comparative analysis of different machine learning algorithms to ascertain the most effective classification technique. The correlation matrix visually demonstrates the interrelationships between features, aiding in the identification of the most significant predictors for fraud detection. A confusion matrix is a tool that encapsulates the accuracy of a machine learning model on test data. Commonly used for evaluating classification models tasked with assigning categorical labels to each data point, the matrix outlines the counts of true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) generated by the model during testing.

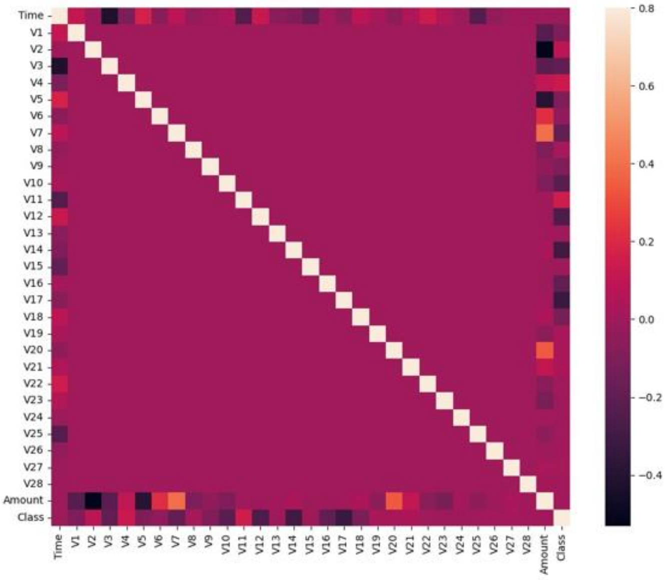


Fig: Correlation Matrix

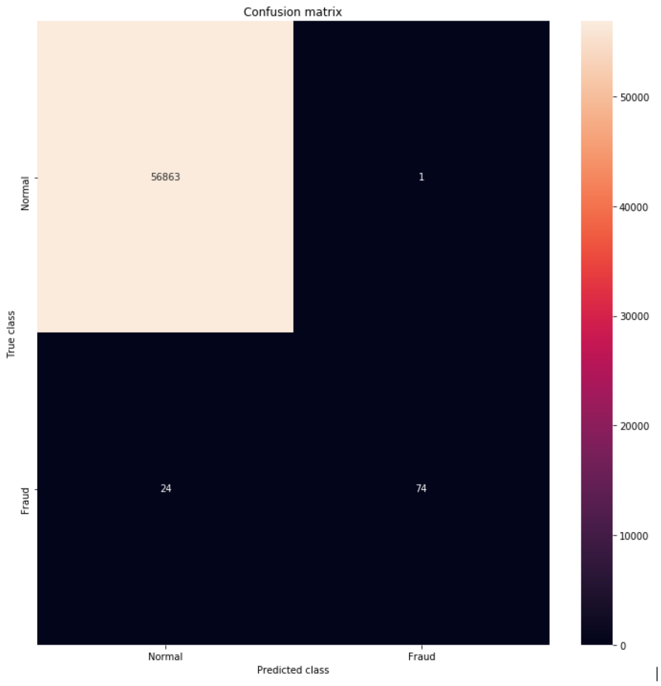


Fig: Confusion Matrix.

Random Forest is a sophisticated ensemble learning technique that builds numerous decision trees and merges their outcomes to reach a consensus decision. More intricate than KNN, it is adept at processing extensive datasets replete with irregular data. It is capable of managing missing data points and complex, non-linear feature relationships. While Random Forest is a potent tool for fraud detection, its intricate decision-making process can be opaque. To sum up, no single algorithm reigns supreme for detecting credit card fraud; the optimal choice hinges on the unique characteristics of the problem and data involved. It is advisable to trial various algorithms to discern the most effective one for the task at hand.

6. CONCLUSIONS

Credit card fraud is undeniably a form of criminal deceit. Identifying fraud is a complex challenge that demands considerable expertise, which is significantly alleviated by the application of machine learning algorithms. The deployment of machine learning and artificial intelligence serves to protect customers' funds from unauthorized use. The research paper in question presents an efficient fraud detection system based on machine learning techniques, incorporating a feedback mechanism. This feedback loop is designed to improve the detection capabilities and efficiency of the classifier. A comparative analysis has been performed on various machine learning approaches, including random forest, decision trees, artificial neural networks, support vector machines, Naïve Bayes, logistic regression, and gradient boosting classifiers. Several performance metrics such as precision, recall, F1-score, accuracy, and false positive rate percentage have been evaluated. The method that excels in these performance metrics is considered the most effective. Currently, the random forest classifier demonstrates superior performance over other machine learning classifiers. Future work includes implementing and testing the proposed method on larger, real-time datasets using additional machine learning techniques.

ACKNOWLEDGEMENT

The heading should be treated as a 3rd level heading and should not be assigned a number.

REFERENCES

[1] Awoyemi, J.O., Adetunmbi, A.O. and Oluwadare, S.A., 2017, October. Credit card fraud detection using machine learning techniques: A co parative analysis. In 2017 International Conference on Computing Networking and Informatics (ICCNI) (pp. 1-9). IEEE.

[2] Adewumi, A.O. and Akinyelu, A.A., 2017. A survey of machine-learning and nature-inspired based credit card fraud detection techniques. International Journal of System Assurance Engineering and Management, 8(2), pp.937-953

[3] Fu, K., Cheng, D., Tu, Y. and Zhang, L., 2016, October. Credit card fraud detection using convolutional neural networks. In International Conference on Neural Information Processing (pp. 483-490). Springer, Cham.

[4] Yee, O.S., Sagadevan, S. and Malim, N.H.A.H., 2018. Credit card fraud detection using machine learning as data mining technique. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 10(1-4), pp.23-27.

[5] Khan, A.U.S., Akhtar, N. and Qureshi, M.N., 2014. Real-time credit-card fraud detection using artificial neural network tuned by simulated annealing algorithm. In Proceedings of International Conference on Recent Trends in Information, Telecommunication and Computing, ITC (pp. 113-121).

[6] Carneiro, N., Figueira, G. and Costa, M., 2017. A data mining based system for credit-card fraud detection in e-tail. Decision Support Systems, 95, pp.91-101.

[7] Dhankhad, S., Mohammed, E. and Far, B., 2018, July. Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study. In 2018 IEEE International Conference on Information Reuse and Integration (IRI) (pp. 122-125). IEEE.

[8] Adewumi, A.O. and Akinyelu, A.A., 2017. A survey of machine-learning and nature-inspired based credit card fraud detection techniques. International Journal of System Assurance Engineering and Management, 8(2), pp.937-953.

[9] Fiore, U., De Santis, A., Perla, F., Zanetti, P. and Palmieri, F., 2019. Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences, 479, pp.448-455.

[10] Bahnsen, A.C., Stojanovic, A., Aouada, D., and Ottersten, B., 2014, April. Improving credit card fraud detection with calibrated probabilities. In Proceedings of the 2014 SIAM international conference on data mining (pp. 677-685). Society for Industrial and Applied Mathematics.

[11] Popat, R.R. and Chaudhary, J., 2018, May. A survey on credit card fraud detection using machine learning. In 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 1120-1125). IEEE.

[12] Patil, S., Nemade, V. and Soni, P.K., 2018. Predictive modelling for credit card fraud detection using data

analytics. Procedia computer science, 132, pp.385-395.

[13] Malini, N. and Pushpa, M., 2017, February. Analysis on credit card fraud identification techniques based on KNN and outlier detection. In 2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication, and Bio-Informatics (AEEICB) (pp. 255-258). IEEE.

[14] Zareapoor, M. and Shamsolmoali, P., 2015. Application of credit card fraud detection: Based on bagging ensemble classifier. Procedia computer science, 48(2015), pp.679-685.

[15] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C. and Bontempi, G., 2015, July. Credit card fraud detection and concept-drift adaptation with delayed supervised information. In 2015 international joint conference on Neural networks (IJCNN) (pp. 1-8). IEEE.