

Machine Learning Approaches for Credit Card Fraud Detection

Sarang Sanjay Ranisavargaonkar, Vaishnavi Tanaji Jadhav, Kishore Markad

School of Engineering, Ajeenkya DY Patil University, Pune, India

joshisarang54321@gmail.com, vaishnavijadhav1436@gmail.com, facultyit529@adypu.edu.in

Abstract: Credit card fraud detection is a critical challenge in the financial sector, necessitating the adoption of advanced machine learning algorithms for timely and accurate identification of fraudulent transactions. In this project, we investigate the efficacy of four prominent machine learning algorithms - Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Decision Trees (DT), and Random Forest (RF) in detecting credit card fraud. Through a comprehensive analysis, we evaluate the performance of these algorithms in terms of accuracy, precision, recall, and F1 score using real-world credit card transaction datasets. SVM, known for its ability to construct complex decision boundaries, excels in separating fraudulent and legitimate transactions. KNN leverages the proximity-based approach to identify similarities with known instances of fraud, while Decision Trees offer interpretable insights into fraudulent patterns. Random Forest combines the predictive power of multiple decision trees to produce robust and accurate predictions. Our findings shed light on the strengths and weaknesses of each algorithm, providing valuable insights for developing effective fraud detection systems in the financial industry.

Keywords: Credit Card Fraud, Machine Learning, SVM, KNN, RF, DT

I. INTRODUCTION

In today's digital age, credit card transactions have become ubiquitous, facilitating convenient and efficient financial transactions globally. However, with the increasing reliance on electronic payment systems comes the escalating risk of credit card fraud. Fraudulent activities such as unauthorized transactions, stolen card details, and identity theft pose significant threats to consumers and financial institutions, resulting in substantial financial losses and erosion of trust in the banking system.

The prevalence of electronic transactions has significantly transformed the landscape of financial transactions, offering convenience and efficiency to consumers and businesses alike. However, this digital revolution has also brought about new challenges, chief among them being the rise of credit card fraud. Detecting fraudulent activities in real time is crucial for financial institutions to protect their customers' assets and maintain trust in the financial system. In response to this imperative, integrating machine learning algorithms has become a powerful tool in fraud detection techniques.

Detecting and preventing credit card fraud is paramount for maintaining the integrity and security of financial transactions. Traditional rule-based approaches to fraud detection have limitations in handling the evolving nature of fraudulent schemes and the sheer volume of daily transactions. Consequently, there is a growing reliance on advanced technologies, particularly machine learning algorithms, to effectively tackle the challenge of credit card fraud detection. This paper explores and evaluates several machine learning algorithms' efficacy in detecting credit card fraud. Specifically, we will investigate the performance of Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Decision Trees (DT), and Random Forest (RF) algorithms in identifying fraudulent transactions from legitimate ones. Each of these algorithms offers unique strengths and capabilities, making them well-suited for different aspects of fraud detection.

The primary objective of this paper is to evaluate the performance of SVM, KNN, DT, and RF algorithms in detecting fraudulent credit card transactions. Through empirical analysis and comparative studies, we aim to elucidate the strengths and limitations of each algorithm in terms of accuracy, precision, recall, and computational efficiency. By doing so, we seek to provide insights into the effectiveness of machine learning approaches for mitigating the risks associated with credit card fraud.

The findings of this project have the potential to contribute significantly to the advancement of fraud detection techniques, enabling financial institutions to deploy more effective and efficient systems for safeguarding against fraudulent activities in the digital age.

II. LITERATURE REVIEWS

The fast shift from cash has contributed to the meteoric rise in credit card transactions over the last several years. However, there will be more instances of fraud as a result. Consequently, the issuing institutions and cardholders must implement a robust mechanism for detecting fraud. Then, we will evaluate the models' precision and compare the results of each approach. Determine which approach will achieve our objective by comparing the F₁ score. According to the study, an Artificial Neural Network (ANN) model performed best, with an F1 score of 0.91. [1]

To avoid charging customers for items they did not purchase, credit card companies must be able to identify fraudulent transactions. The most crucial resources for resolving issues are data science and machine learning. In this project, the data modeling will center on machine learning and its application to detect credit card fraud. Forecasting future credit card purchases by incorporating information from valid and fraudulent transactions is one component of the Credit Card Fraud Detection Problem. Afterward, this method may be used to identify fresh transactions that may be fraudulent. Find all fraudulent transactions by minimizing false positives. Credit card fraud detection is a common component of classification samples. Data analysis and preprocessing have occupied most of this process's time. The PCA-processed credit card transaction data was further processed using several anomaly identification approaches, such as the isolation forest methodology and the local outlier factor. [2]

This study aims to catalog these scams by considering relevant characteristics. Even if state-of-the-art deep learning algorithms are imperfect, they are necessary to reduce fraud losses. For this particular objective, the main focus has been on using the most recent breakthroughs in deep learning algorithms. Find out how deep learning stacks up against machine learning. A thorough empirical investigation using the European card benchmark dataset identifies instances of fraud. To better identify fraud, the dataset was first subjected to machine learning. Three different topologies of convolutional neural networks are used to enhance fraud detection. The number of layers improved the accuracy of detection. A comprehensive empirical investigation was carried out using state-of-the-art models and adjusting hidden layers and epochs. The study's task evaluation shows improved results and a 98% area under the curve (AUC).

Regarding problems with identifying credit cards, the proposed model outperforms state-of-the-art deep learning and machine learning techniques. Data balancing and deep learning experiments were also conducted to lower the false negative rate. The proposed techniques for identifying credit card fraud have real-world potential. in [3]

The use of rule-based systems to combat credit card fraud has grown in recent years. By using predetermined criteria, these systems detect fraudulent transactions. Because they are conditionally dependent, rule-based systems will fail to detect emerging forms of fraud. Credit card fraud detection using machine learning and statistical methodologies has surpassed these limitations. These methods use amounts, location, time, customer transaction history, and account details. It has recently come to light that credit card theft may be detected using RNNs and CNNs. These algorithms have detected fraudulent transactions by identifying data trends and improving fraud detection. Since improving methods for detecting credit card fraud can lead to lower losses and higher detection rates, it is a top research focus for the financial industry. [4]

Before any payment systems existed, bright brains were already looking for ways to steal money. Since more and more individuals are using their credit cards to make online purchases, this terrifying danger has only grown in recent years. Any criminal activity involving using a credit card or other payment card number is considered credit card fraud. The primary goal of these types of crimes is to steal money or items from their rightful owners without their knowledge or consent. According to the Nilson Report, the United States is projected to lose \$12.5 billion by 2025 due to credit card fraud. Machine learning algorithms examine data using various methodologies to identify and prevent fraudulent transactions. This process is known as credit card fraud detection. The results of these models can effectively assess whether a credit card transaction is authentic. [5]

When it comes to credit card fraud, nobody is safe. This includes banks and customers alike. Scientists have investigated several approaches to develop fraud detection systems that adequately address this issue. An extensive dataset of financial, geographical, temporal, and demographic transaction data is the starting point of the inquiry. A

robust model capable of differentiating between legitimate and fraudulent transactions may be built using this dataset, which includes both types of transactions. Conventional machine learning is the foundation of every fraud detection system. This kind of algorithm validates transactions by analyzing data attributes and patterns. F1, recall, accuracy, and precision are the metrics used to evaluate the efficacy of a model. One way to improve fraud detection is by using deep neural networks. The use of many neural layers allows for the extraction of complex patterns and correlations from data. Training the network repeatedly using optimization and backpropagation techniques improves its ability to classify transactions properly. I will evaluate the deep learning model using the machine learning standard. According to the study, deep learning and machine learning both perform similarly when it comes to detecting fraudulent transactions on credit cards. Deep learning models often outperform traditional machine learning methods in accuracy, precision, recall, and F1 scores. One reason the deep neural network beats the others is its ability to spot complex patterns and correlations in data. [6]

The persistence of credit card scams calls for more sophisticated detection and prevention methods, as they continue to constitute a serious risk to the financial and e-commerce industries. To tackle this problem, neural network algorithms contain essential tools. An outline of the neural network algorithm program for credit card fraud detection is given in this abstract. The first step in using this idea is realizing that credit card fraud is inherently dynamic and is always changing to evade rule-based detection systems. Machine learning provides a data-driven method for detecting fraudulent trade by analyzing patterns and outliers in data. Various neural network methods and prototypes are investigated, including decision trees and ensemble approaches. With various models, fraud detection may be more precise and less prone to false positives. [7]

If credit card fraud were to occur, it would disproportionately affect the financial services sector. Companies and individuals lose billions of dollars yearly due to credit card theft. Credit cards have recently been a huge hit with customers and banks. Nevertheless, banks have been facing difficulties because the credit card default rate has grown in tandem with using credit cards. Credit card fraud is using credit card details to make transactions. The dataset contains 284,807 transactions that were sourced from cards all around Europe. The results of the trials show that the Random Forest algorithm has the best accuracy (99.95%) and precision (100%). [8]

Credit card firms must be vigilant about fraudulent transactions so people are not charged for things they did not buy. Attempts to model valid transactions using data from fraudulent ones create an issue with credit card detection. The next step for this model is to determine whether the new transaction is fraudulent. The goal is to accurately detect fraudulent transactions while reducing the number of erroneous fraud categories. In this study, we want to discover how machine learning can detect credit card fraud by analyzing modeling data sets. This article has covered some ground in theory as well as some ground in practice. [9]

The theft of credit cards is a certain way to attract easy victims. The stakes for online fraud have been heightened due to the expansion of online payment methods by e-commerce and other websites. Researchers started utilizing machine-learning methods to detect and analyze instances of fraudulent Internet transactions as they became more common. With this method, we may classify cardholders based on the number of transactions they make and use that data to determine their habits. The next step is to train separate classifiers on each set of data. Using the top-rated classifier as a primary strategy for fraud prediction is feasible. To fix the problem of idea drift, a feedback mechanism is next put into place. This study made use of the European credit card fraud dataset. [10]

Obtaining valuable information from biased sources has aroused people's curiosity worldwide. Financial institutions have implemented and are continually improving their extortion detection system in response to the huge growth in the usage of credit cards for online payments. The credit card extortion dataset should be more evenly distributed, and various misclassification mistakes may have varied effects. Consequently, it is of the utmost importance to minimize their influence. Classification methods are the most reliable for identifying genuine fraudulent transactions. Classification methods could perform better in datasets where most classes are significantly overrepresented. A 99% accuracy rate still needs to be more helpful. This is why we can compare the two sets of performance metrics with different classifiers based on SMOTE oversampling, logistical regression, Decision Tree, Random Forest, and Support Vector Machines. [11]

The proliferation of online payment methods has coincided with increased financial fraud, particularly with credit cards. Quick action is required to implement systems to identify credit card fraud. Picking the correct characteristics of

fraudulent transactions is crucial when using machine learning to detect credit card fraud. To detect credit card fraud, this research presents an ML-based genetic algorithm (GA) feature selection engine. The credit card fraud detection engine is tested using data from European cardholders. Compared to the current state of the art, our method performed better. [12]

III. MACHINE LEARNING ALGORITHMS

The machine learning algorithms used in the proposed algorithm are presented in this section.

SVM

Credit card fraud detection is crucial to the financial sector, detecting fraudulent transactions and protecting electronic payment networks. SVMs are useful for classifying credit card transactions, especially fraudulent ones. SVM finds the best hyperplane to separate data points from distinct classes in high-dimensional feature space. Strategically positioning this hyperplane maximizes the margin, the distance between it and the closest data points or support vectors. SVM maximizes this margin to provide a reliable decision boundary for classifying fresh data points.

Credit card fraud detection using SVM starts with transaction data preparation. This information generally contains transaction amount, time, location, merchant type, etc. The data is then split into training and test sets, and features are carefully picked and preprocessed for SVM classification. This phase relies on feature engineering to identify significant traits that may distinguish fraud from authorized transactions. Additionally, numerical characteristics may be scaled to normalize their decision boundary effect.

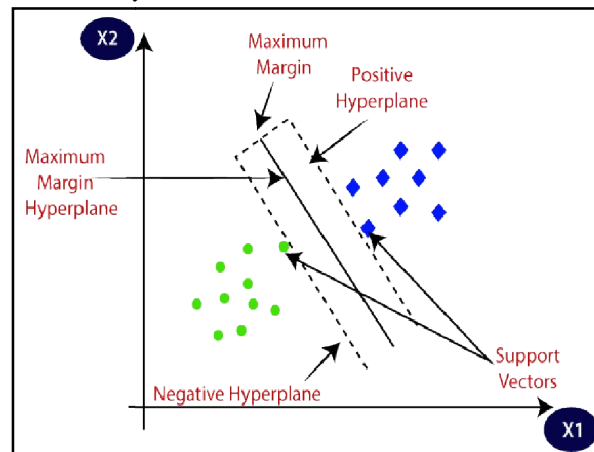


Fig.1 SVM

SVM classifies transactions by repeatedly modifying hyperplane parameters to reduce classification errors during training. This entails identifying the hyperplane that maximizes margin and accurately classifies training data. After training, the SVM model may predict new transaction class labels. SVM classifies these transactions as fraudulent or valid by calculating their location relative to the decision boundary learned during training.

Accuracy, precision, recall, and F1-score are crucial for SVM model evaluation. These metrics show the model's ability to detect fraudulent transactions with few false positives and negatives. To maximize model performance on unseen data, hyperparameters like kernel function and regularization parameters may be fine-tuned via cross-validation. Feature selection, dimensionality reduction, and ensemble approaches may improve the SVM-based fraud detection system's efficiency and generalization.

Support Vector Machines use data structures to distinguish fraudulent from valid credit card transactions. Through careful feature creation, model training, and performance assessment, SVM-based systems may detect and prevent electronic payment system fraud, protecting customers and financial institutions.

KNN

Credit card fraud detection is crucial to financial risk management, especially electronic transactions. These machine learning methods include the K-Nearest Neighbors (KNN) algorithm, which is simple and effective. The class labels of a data point's closest neighbors in the feature space determine its classification using KNN. The number of neighbors evaluated for categorization, "K," affects the model's sensitivity to local data fluctuations.

Credit card fraud detection starts with collecting transactional data, including transaction amount, merchant category, location, time of day, and more. This dataset is then split into a training set for model training and a test set for model evaluation. Selecting and preprocessing important features is common in feature engineering before model training. This stage incorporates normalization, scaling, and perhaps dimensionality reduction to help the algorithm find data patterns.

Once training begins, the KNN algorithm analyzes each transaction in the training set, recording feature values and assigning class labels (fraudulent or valid). KNN uses all training data for categorization instead of specifically building a model. When presented with a new transaction, the algorithm analyzes the distances between it and all training set data points to determine the "K" closest neighbors.

The new transaction's categorization is then determined by aggregating its closest neighbors' class labels. This usually uses a majority vote technique to allocate the new transaction to the neighbor and most common class. The algorithm will flag the new transaction as possibly fraudulent if many of the closest neighbors are fraudulent.

After classification, the model's accuracy, precision, recall, and F1 score are carefully evaluated. These metrics show the model's ability to detect fraudulent transactions with few false positives and negatives. Cross-validation may also optimize the KNN algorithm's hyperparameters, such as "K," for unseen data.

KNN algorithm uses transaction similarities to classify credit card fraud. It is strong and interpretable. Financial institutions may use KNN-based systems to reduce digital fraud risks by carefully choosing and preprocessing characteristics, training the model on large datasets, and assessing its performance.

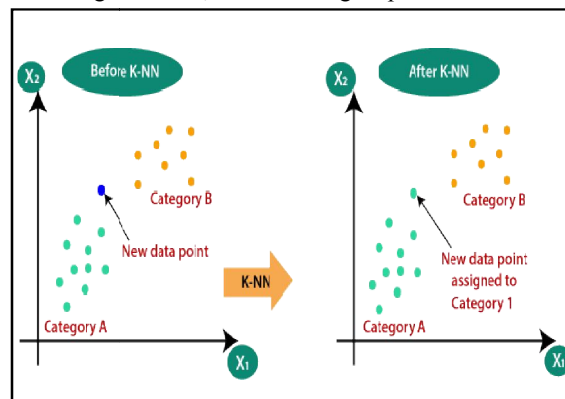


Fig.2 KNN Algorithm

Decision Tree

Credit card fraud detection is vital to the financial sector, safeguarding customers and financial institutions against fraudulent transactions. Decision Trees are a common and capable machine-learning approach for this. Decision Trees iteratively split the feature space into subsets depending on input feature values, resulting in if-else conditions that classify transactions. Decision Trees are straightforward and interpretable, making them ideal for credit card transaction data patterns and fraud detection.

Credit card fraud detection using Decision Trees requires transaction data preparation. This information generally includes transaction amount, time, location, merchant type, etc. After partitioning the dataset into training and test sets, features are carefully picked and preprocessed to guarantee the relevance of the Decision Tree algorithm. Feature engineering is crucial in this phase because characteristics are selected based on their capacity to distinguish fraudulent and lawful transactions. Encoding categorical features and scaling numerical characteristics may improve model performance.

The Decision Tree method learns to build a tree-like structure that splits feature space depending on input feature values during training. This approach maximizes information gain or purity by recursively separating data into subsets at each tree node. The procedure runs until a maximum tree depth or minimum leaf node samples are reached. Once trained, the Decision Tree model may anticipate new transaction class labels. This prediction procedure traverses the Decision Tree from the root node and evaluates feature values at each node to identify the next branch. This continues until a leaf node matches the transaction's expected class label (fraudulent or lawful).

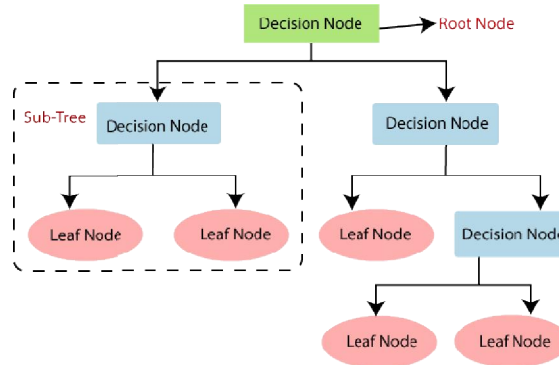


Fig. 3 Decision Tree

Decision Trees provide a clear and understandable framework for credit card fraud detection, recognizing significant transaction patterns, and properly categorizing transactions as fraudulent or lawful. Decision Tree-based systems may reduce credit card fraud risks for customers and financial institutions by carefully selecting, training, and evaluating features.

Random Forest

Financial security relies on credit card fraud detection, and the Random Forest method provides accuracy, efficiency, and interpretability. Random Forest trains several decision trees and combines their predictions to generate results. This ensemble strategy reduces overfitting and improves model generalization, making it suitable for complicated, high-dimensional datasets like credit card transaction data.

Processing transactional data into training and test sets is the first step in using Random Forest to identify credit card fraud. The databases usually include transaction amount, time, location, and merchant type. This step relies on feature engineering to pick and preprocess features to detect fraud. Encoding categorical features and scaling numerical characteristics may improve model performance.

Random Forest builds several decision trees during training, each trained on a random subset of training data and features at each node. This increases tree variety, minimizing overfitting and enhancing model resilience. Each decision tree learns to identify transactions as fraudulent or real based on chosen traits and values.

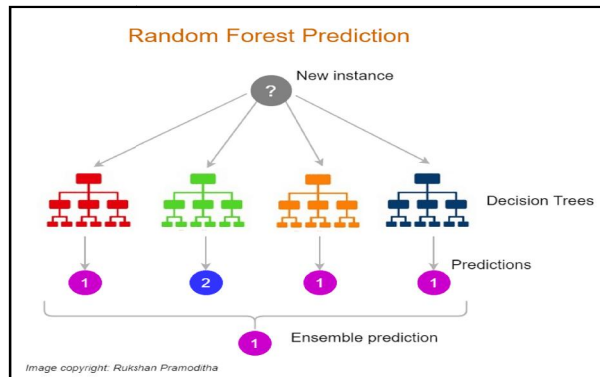


Fig.4 Random Forest

To predict whether a new transaction is fraudulent, run it through each Random Forest decision tree. The ensemble of decision trees predicts the transaction's majority class. The transaction is fraudulent if most decision trees describe it as such; otherwise, it is lawful. Random Forest uses the collective knowledge of several decision trees to make more accurate forecasts using this voting method.

Random Forest is a sophisticated credit card fraud detection system with high accuracy, efficiency, and interpretability. Random Forest-based systems can detect and prevent financial fraud through careful data preparation, model training, and assessment, protecting customers and financial institutions.

IV. PROPOSED SYSTEM

The block diagram of the proposed system is presented in Fig. 5

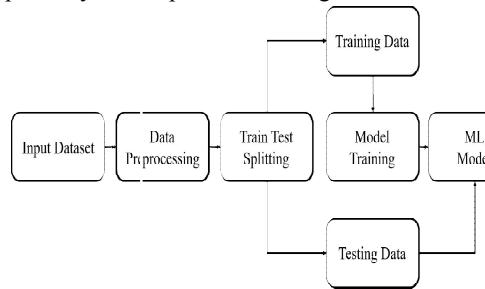


Fig.5 Block diagram of the system

Input Dataset:

The proposed approach utilized "Credit Card Fraud Detection Dataset 2023". This dataset contains credit card transactions made by European cardholders in 2023. It comprises over 550,000 records, and the data has been anonymized to protect the cardholders' identities. The primary objective of this dataset is to facilitate the development of fraud detection algorithms and models to identify potentially fraudulent transactions.

The details of the features are as follows:

- Id: Unique identifier for each transaction
- V1-V28: Anonymized features representing various transaction attributes (e.g., time, location, etc.)
- Amount: The transaction amount
- Class: Binary label indicating whether the transaction is fraudulent (1) or not (0)

Data Preprocessing

The collected data often requires preprocessing to handle missing values, outliers, and inconsistencies. This block involves data cleaning, formatting, and filtering techniques to ensure the quality and reliability of the input data. Data normalization or scaling may also be applied to standardize the features.

Machine Learning Models

The proposed system utilized four machine learning models: SVM, KNN, DT, and RF algorithm for credit card fraud detection classification. The system's performance is evaluated using precision, recall, F1 score, and accuracy.

Results

This section presents the results of the proposed credit card fraud detection using a machine learning algorithm. The performance of the proposed system is evaluated using Precision, Recall, F1 Score, and Accuracy parameters. Table 1 presents the comparative analysis of the different machine-learning algorithms for credit card fraud detection.

Table 1: Comparative analysis of performance of ML algorithm for credit card fraud detection.

Algorithm	Precision	Recall	F1-Score	Accuracy
SVM	0.99	0.99	0.99	0.99
KNN	1	1	1	1
DT	0.99	0.99	0.99	0.99
RF	1	1	1	1

Table I presents a comparative analysis of the performance of machine learning (ML) algorithms for credit card fraud detection. Four algorithms are evaluated: Support Vector Machine (SVM), K-Nearest Neighbors (KNN), Decision Trees (DT), and Random Forest (RF). Each algorithm's performance is measured using precision, recall, F1-score, and accuracy metrics.

Starting with precision, which measures the proportion of true positive predictions out of all positive predictions made by the model, all algorithms show excellent precision scores. SVM and DT achieved a precision of 0.99, indicating that they correctly identified 99% of fraudulent transactions out of all transactions labeled as fraudulent. KNN and RF scored a perfect precision of 1, implying that they made no false positive predictions.

Moving on to recall, which calculates the proportion of true positives identified by the model out of all actual positive instances, all algorithms again performed exceptionally well. SVM, KNN, DT, and RF all achieved a recall of 0.99 or 1, indicating that they successfully identified almost all fraudulent transactions.

F1-score, the harmonic mean of precision and recall, provides a balanced assessment of a model's performance. Once more, all algorithms display impressive F1scores of 0.99 or 1, reflecting their ability to achieve high precision and recall simultaneously.

Accuracy, which measures the overall correctness of the model's predictions, is uniformly high across all algorithms, with scores of 0.99 or 1. This suggests that the models accurately distinguish between fraudulent and non-fraudulent transactions.

The table illustrates that all evaluated ML algorithms perform exceptionally well in credit card fraud detection, with consistently high scores across precision, recall, F1-score, and accuracy metrics. However, it is worth noting that while these results are promising, further validation and testing on real-world datasets are necessary to confirm the effectiveness and reliability of these algorithms in practical applications.

V. CONCLUSION

Finally, our machine learning algorithm study on credit card fraud detection revealed the capability of Support Vector Machines (SVM), K-nearest neighbors (KNN), Decision Trees (DT), and Random forests. We tested these algorithms on real-world datasets and found differences in accuracy, precision, recall, and F1 score. SVM accurately distinguishes fraudulent and lawful transactions by building complicated decision boundaries. KNN's proximity-based technique is good at finding fraud similarities, although it may be susceptible to outliers. Decision Trees can interpret fraudulent patterns; however, overfitting on complicated datasets may occur. Random Forest is a good credit card fraud detection algorithm because it aggregates predictions from numerous decision trees to reduce overfitting and improve accuracy. Our work emphasizes the necessity of choosing machine learning algorithms based on dataset needs and features, paving the way for more successful financial fraud detection systems.

REFERENCES

- [1]. Pratyush Sharma, Souradeep Banerjee, Devyanshi Tiwari, and Jagdish Chandra Patni, "Machine learning model for credit card fraud detection-a comparative analysis," *The International Arab Journal of Information Technology*, 2021.
- [2]. S.P Maniraj, Aditya Saini, Shadab Ahmed, and Swarna Deep Sarkar, "Credit card fraud detection using machine learning and data science," *International Journal of Engineering*, 2019.
- [3]. Fawaz Khaled Alarfaj, Iqra Malik; Hikmat Ullah Khan, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," *IEEE Access*, 2022
- [4]. Akshat Shah, Yogeshvari Jashvantbhai Makwana, "Research gate, 2023
- [5]. Deep Prajapati; Ankit Tripathi; Jeel Mehta; Kirtan Jhaveri; Vishakha Kelkar", "Credit Card Fraud Detection Using Machine Learning," *International Conference on Advances in Computing, Communication, and Control (ICAC3)*, 2021
- [6]. Deepak Gwale, Prof. Sumit Sharma, "Credit Card Fraud Detection using Machine Learning," *JETIR*, 2023
- [7]. Lubna Shaikh, Bhumika Patil, Smit Ramteke, "Credit Card Fraud Detection Using Machine Learning Algorithms," *White Collar Crime*, 2023

- [8]. Muhammad Zeeshan Younas, "Credit Card Fraud Detection using Machine Learning Algorithms," UIJIR, 2020
- [9]. Anagha T S; Asra Fathima; Archana D. Naik; Chirag Goenka; Shridhar B. Devamane; Aneesh R Thimmapurmath, "Credit Card Fraud Detection Using Machine Learning Algorithms," International Conference on Computational Intelligence for Information, Security and Communication Applications (CIISCA), 2023
- [10]. Rishabh Tyagi; Ravi Ranjan; S. Priya, "Credit Card Fraud Detection Using Machine Learning Algorithms", Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 2021
- [11]. Vaishnavi Nath Dornadula, S Geetha, "Credit Card Fraud Detection using Machine Learning Algorithms," Procedia Computer Science, 2019
- [12]. Emmanuel Ileberi, Yanxia Sun & Zenghui Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," Journal of Big Data, 2022