Detecting Credit Card Fraud Transactions through Random Forest Machine Learning Model

B. SANTOSH KUMAR
Associate Professor, Department of MCA, Wesley PG College, Secunderabad, India.

Abstract - Credit card fraud poses a significant threat to financial institutions and cardholders alike, necessitating the development of robust and efficient fraud detection systems. This paper focuses on leveraging the Random Forest Classifier for the detection of credit card fraud. The Random Forest model is chosen for its ability to handle complex, high-dimensional datasets and provide accurate predictions while mitigating overfitting. The model begins by pre-processing the credit card transaction data, like feature scaling to enhance model performance. Subsequently, a Random Forest Classifier is trained on a labeled dataset comprising both legitimate and fraudulent transactions. The model is fine-tuned using cross-validation to optimize hyperparameters, ensuring generalizability to new and unseen data. The study evaluates the performance of the Random Forest Classifier in terms of key metrics such as accuracy, precision, recall, and F1 score. Comparative analyses with other machine learning models commonly employed in fraud detection are conducted to highlight the efficacy of the Random Forest approach. Results indicate that the Random Forest Classifier demonstrates superior performance in detecting credit card fraud, outperforming alternative models in terms of accuracy and robustness.

Keywords: Credit card fraud, Random Forest Classifier, feature scaling, hyperparameters, machine learning

I. INTRODUCTION

In today's digitalized financial environment, credit card theft has become a major global threat for both consumers and financial organizations. The widespread use of online transactions, along with advanced fraudulent methods [1], has led to a concerning increase in fraudulent activities, which present substantial risks to both financial stability and customer trust. The identification and mitigation of credit card fraud have emerged as a significant obstacle, demanding the implementation of strong and sophisticated measures [2].

The complexities and difficulties surrounding the detection of credit card fraud are many and significant. Fraudsters consistently develop novel methods and strategies to evade conventional fraud detection systems, leading to the emergence of more intricate and complex fraudulent operations [3]. The magnitude and intricacy of financial transactions conducted on a daily basis increase the challenge of differentiating between legitimate transactions and fraudulent ones [4]. Conventional rule-based systems sometimes have trouble quickly and effectively recognizing new fraud patterns, which makes them more susceptible to fraudulent assaults.

The use of machine learning has become more prominent in effectively tackling the intricate challenges associated with the identification of credit card fraud [5]. By using sophisticated algorithms and data-driven approaches, machine learning models has the capacity to examine extensive volumes of transactional data, detect intricate patterns, and distinguish abnormal behaviors that may indicate fraudulent activity [6]. These models demonstrate a capacity for adaptation, since they are able to acquire knowledge from past data in order to identify developing patterns of fraud. since a result, they provide a more proactive and efficient method of detecting fraud in comparison to systems that rely on established principles [7].

Machine learning techniques, including supervised learning algorithms, neural networks, and ensemble approaches, exhibit the capability to completely evaluate transactional data [8]. These models possess the capability to identify abnormalities, outliers, and suspicious patterns within extensive datasets, hence facilitating the detection of suspected fraudulent transactions with improved levels of accuracy and efficiency. Furthermore, it is worth noting that machine learning models possess the capability to perpetually acquire knowledge and adjust their algorithms to account for emerging fraud trends. This attribute significantly enhances their efficacy in promptly identifying instances of fraud in real-time circumstances. The capacity to adapt is of utmost importance when dealing with the ever-changing nature of fraudulent actions within the financial sector.

The present research explores the domain of credit card fraud detection, investigating the use of several machine learning methodologies to detect and alleviate instances of fraudulent behavior. This research seeks to examine the effectiveness of machine learning models in enhancing the security and resilience of financial transactions against fraudulent activities by using sophisticated algorithms and analyzing substantial transactional data.

II. LITERATURE

Dejan Varmedja et al [9] presented a variety of algorithms that may be used for the purpose of categorizing transactions as either fraudulent or legitimate. The study used the dataset on Credit Card Fraud Detection. The SMOTE approach was used to address the issue of dataset imbalance, since the dataset exhibited a significant imbalance. Additionally, a process of feature selection was conducted, followed by the division of the dataset into two distinct parts: the training data and the test data. The algorithms used in the experiment included Logistic

Regression, Random Forest, Naive Bayes, and Multilayer Perceptron. The findings indicate that all algorithms possess the capability to effectively identify credit card fraud, exhibiting a notable level of accuracy. The proposed model has the potential to be used for the identification of several additional anomalies.

Rishi Banerjee et al [10] investigated several classification models applied to a public dataset to assess the relationship between specific attributes and fraudulent activities. Additionally, it introduced improved metrics to evaluate false negatives and evaluates the impact of random sampling in mitigating dataset imbalances. Furthermore, the paper details the optimal algorithms suitable for datasets characterized by significant class imbalances. The research findings indicate that, in practical scenarios, the Support Vector Machine algorithm exhibits the highest performance in detecting credit card fraud.

Fabrizio Carcillo et al [11] introduced the Scalable Real-time Fraud Finder (SCARFF), a framework that amalgamates Big Data tools such as Kafka, Spark, and Cassandra, with a machine learning methodology designed to address issues related to imbalance, nonstationarity, and feedback latency. Through experiments conducted on an extensive dataset comprising real credit card transactions, the results demonstrate the scalability, efficiency, and accuracy of this framework when processing a substantial stream of transactions in real-time.

Ong Shu Yee et al [12] discussed the use of supervised classification techniques, namely Bayesian network classifiers such as K2, Tree Augmented Naïve Bayes (TAN), Naïve Bayes, logistics, and J48 classifiers.
Ishan Sohony et al [13] introduced an ensemble machine learning strategy as a potential resolution to the issue at hand. Their findings suggest that Random Forest exhibits greater accuracy in detecting normal instances, while Neural Network performs well in detecting instances of fraud. The proposed ensemble method, which integrates both Random Forest and Neural Network, capitalizes on the strengths of each approach, enabling high-accuracy and confident prediction of labels for new samples. The experimental validation conducted on real-world datasets supports and validates these observations.

Rafiq Ahmed Mohammed et al [14] proposed on conducting experiments to examine various machine learning approaches and assess their appropriateness as scalable algorithms for handling extremely unbalanced huge datasets, also referred to as "Big" datasets. The studies were performed on two datasets with significant class imbalance, using the Random Forest, Balanced Bagging Ensemble, and Gaussian Naïve Bayes algorithms. It was shown that several detection algorithms had satisfactory performance when applied to datasets of moderate size, but encountered difficulties in maintaining comparable predictive accuracy when confronted with much larger datasets.

John O.Awoyemi et al [15] analyzed how well logistic regression, k-nearest neighbor, and naive bayes perform on highly skewed credit card fraud data. The dataset used in this study comprises 284,807 credit card transactions obtained from European cardholders. The skewed data is subjected to a hybrid methodology that combines under-sampling and oversampling methods. The three strategies are implemented on both the raw and preprocessed data. The implementation of the task is conducted using the Python programming language. The evaluation of the approaches' performance is conducted by assessing many metrics, including accuracy, sensitivity, specificity, precision, Matthews correlation coefficient, and balanced classification rate.

Nuno Carneiro et al [16] explored the integration of human and automated categorization techniques, provides a comprehensive analysis of the whole development process, and conducts a comparative evaluation of several machine learning approaches. Therefore, this article has the potential to assist academics and practitioners in the development and execution of data mining systems for the purpose of fraud detection or comparable issues. This project has made a significant contribution by introducing an automated system and providing valuable insights to fraud analysts, so enhancing their manual review process and ultimately achieving a higher level of performance.

III. PROPOSED MODEL

A machine learning classifier is essential for spotting fraudulent transactions in large datasets when it comes to credit card fraud detection. In general, a supervised learning methodology is used, whereby the classifier undergoes training using past credit card transactions in order to discern discernible patterns that are indicative of both legal and fraudulent operations. The model is trained using features such as the amount of transactions, the location of transactions, the time of transactions, and the frequency of transactions. Frequently used classification methods include logistic regression, decision trees, random forests, as well as more advanced models such as support vector machines or neural networks. The classifier that has undergone training evaluates incoming transactions in real-time, giving a probability or classification to each transaction, distinguishing between genuine and possibly fraudulent ones.

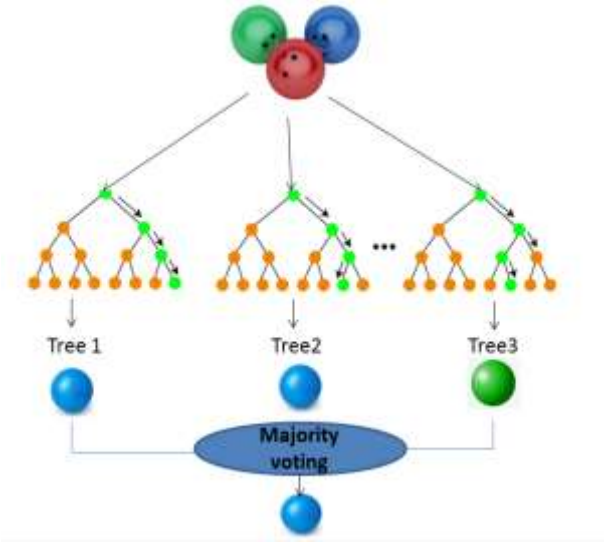

Figure 1: Random forest classifier architecture

The Random Forest algorithm is a kind of ensemble learning technique that is often used for classification problems, such as the detection of credit card fraud. The following is a comprehensive elucidation of the structural framework used by a Random Forest classifier:

a. **Ensemble Learning:** Ensemble learning refers to a method known as Random Forest, which involves the aggregation of predictions from numerous decision trees, so enabling the generation of a final prediction. Every decision tree is developed in an autonomous manner.

b. **Decision Trees:** Decision trees serve as the fundamental components of the Random Forest algorithm. Every tree may be seen as a structure like a flowchart, in which each internal node corresponds to a choice made based on the input attributes. The branches of the tree indicate the possible outcomes resulting from each decision, while the leaf nodes reflect the ultimate class label assigned to the input.

c. **Randomization in Feature Selection:** The Role of Randomization in Feature Selection: One important characteristic of the Random Forest algorithm is the use of randomness in the process of constructing individual decision trees. In the context of a tree structure, it is common practice to choose a random subset of characteristics at each node for the purpose of splitting, rather than examining all available features. This process aids in the decorrelation of the trees, hence enhancing the robustness of the ensemble.

d. **Bootstrapped Samples:** The Random Forest algorithm employs a method known as bootstrapped sampling to generate numerous training datasets for each decision tree. The process entails the use of random sampling with replacement to choose instances from the original dataset, resulting in the creation of various subsets that are used for training each individual tree. The presence of randomness in the ensemble adds to the variety seen among the individual trees.

e. **Voting:** The voting mechanism is an essential component of democratic systems. During the prediction phase, each individual tree inside the Random Forest algorithm autonomously generates a forecast for the class label. The ultimate prediction is then established via a majority voting technique, whereby the class that garners the most number of votes across all trees is designated as the prediction of the ensemble.

f. **Hyperparameters:** The Random Forest algorithm has hyperparameters that may be adjusted in order to enhance its performance. The parameters to consider in this context include the count of trees in the forest (`n_estimators`), the maximum depth of each tree (`max_depth`), the minimum number of samples necessary to split an internal node (`min_samples_split`), and the minimum number of samples needed to be present at a leaf node (`min_samples_leaf`), among other factors.

g. **Significance of Features:** The Random Forest algorithm offers a metric for feature significance, which quantifies the extent to which each feature contributes to the predictive performance of the model. The provided material has significant value in comprehending the many aspects that influence the detection of credit card fraud.

The concepts of robustness and generalization are important factors to consider in several domains. The resilience of Random Forest against overfitting is attributed to its ensemble nature. The use of ensemble methods, such as pooling predictions from many trees, has been seen to enhance the generalization ability of models towards unknown data. This characteristic has contributed to the widespread adoption of such methods in diverse classification problems, including the detection of credit card fraud.

Advantages of using Random forest classifier in credit card fraud detection

- The concept of efficiency refers to the ability to accomplish a task or achieve a goal with the least amount of resources, time, or The Random Forest algorithm demonstrates computational efficiency, rendering it well-suited for managing large datasets and a multitude of characteristics often seen in credit card fraud detection.
- One notable advantage of this approach is its robustness against overfitting. The use of an ensemble approach in Random Forest mitigates the potential for overfitting, hence enhancing the model's ability to generalize well to novel data.
- The model offers a score indicating the relevance of each characteristic, facilitating the identification of the primary contributors to the detection of credit card fraud.

- The Random Forest algorithm is known for its effectiveness in handling class imbalance, which is particularly important in the context of credit card fraud detection because instances of fraudulent transactions are rather rare.
- Non-linearity refers to the absence of a linear relationship between variables or the deviation from a straight line pattern. The model effectively captures intricate and non-linear associations within the data, hence proving its significance in cases when fraudulent patterns deviate from linear trends.
- Ensemble learning refers to a machine learning technique that combines many models or algorithms to improve predictive performance. The use of the ensemble strategy enhances the overall accuracy of the model by amalgamating predictions derived from several decision trees.
- The Random Forest algorithm demonstrates a strong performance even in the presence of irrelevant or redundant characteristics, showcasing its adaptability to real-world datasets.
- One aspect that should be considered is the ease of use. The implementation process is characterized by its relative simplicity, since default hyperparameters often provide satisfying outcomes. Consequently, this approach proves to be viable in several domains, such as credit card fraud detection.

IV. EXPERIMENTAL RESULTS

This section presents a thorough examination of the outcomes derived from the simulations executed using the suggested technique. The dataset used in this investigation was obtained from Kaggle. The dataset was processed using the prescribed methodology. The dataset includes credit card transactions conducted by cardholders from Europe during the calendar year 2023. The dataset consists of more than 550,000 records, with the data being anonymized in order to safeguard the identity of the cardholders. The main purpose of this dataset is to support the development of fraud detection algorithms and models in order to identify possibly fraudulent transactions. Figure 2 shows the sample data from Dataset. The output characteristic of our class is denoted as 'Class', which serves to indicate if a transaction is fraudulent (1) or not fraudulent (0).

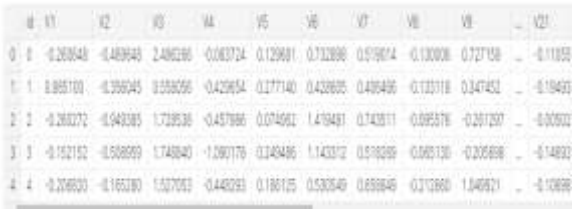

Figure 2: Sample true data from Dataset

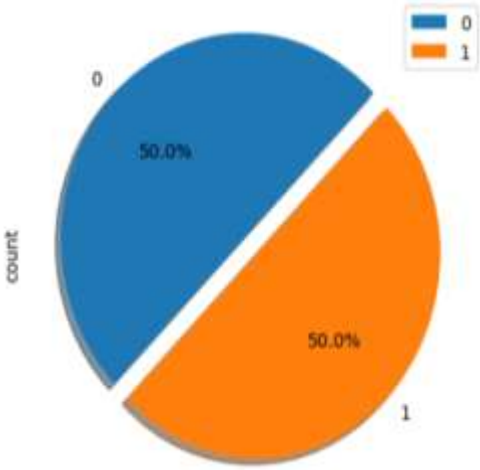

Figure 3: Count of the Class in Dataset

Figure 3 shows the distribution of class. Class 1 and Class 0 are balance.

Table 1: Classification report

	Precision	Recall	F1-score
Class 0	1.00	1.00	1.00
Class 1	1.00	1.0	1.00

The classification report in Table 1 includes metrics that assess the performance of a classification model on two distinct classes, namely Class 0 and Class 1. The metrics of precision, recall, and F1-score are presented for every individual class. Precision is a statistic that quantifies the correctness of positive predictions, while recall assesses the model's capability to identify all positive cases. The F1-score is a composite measure that incorporates both precision and recall, providing a balanced assessment of the model's performance. In the above table, it can be seen that for both Class 0 and Class 1, the precision and recall metrics exhibit a perfect score of 1.00. This signifies that the model has attained impeccable accuracy and recall for both classes. The elevated results indicate that the model's predictions were precise and thorough, underscoring its efficacy in categorizing cases from both Class 0 and Class 1.

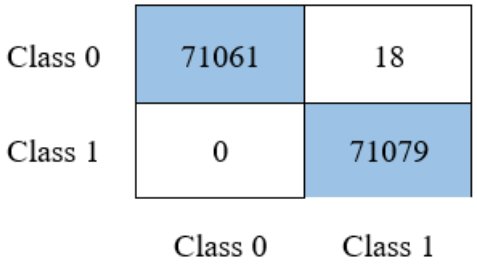

Figure 4: Confusion Matrix

The provided figure 4 shows the confusion matrix and depicts the performance of a binary classification model, where "Class 0" and "Class 1" represent the two possible classes. The top-left cell indicates that 71,061 instances of "Class 0" were correctly classified, while the top-right cell

shows that 18 instances of "Class 0" were incorrectly predicted as "Class 1." The bottom-left cell indicates that none of the instances of "Class 1" were incorrectly predicted as "Class 0," and the bottom-right cell signifies that 71,079 instances of "Class 1" were correctly classified. This matrix provides a clear summary of the model's accuracy, revealing the true positive and true negative predictions along with false positives and false negatives.

Table 2: Comparative analysis

Methods	**Accuracy**
LogisticRegression	0.96
XGBRFClassifier	0.97
XGBRFClassifier+HperTuning	0.97
Random Forest Classifier	**1.00**

Table 2 displays a comparative examination of several methodologies used for a certain job, evaluated based on their correctness. The Logistic Regression technique attained a classification accuracy of 0.96, whilst the XGBRFClassifier demonstrated a somewhat superior accuracy of 0.97. Furthermore, the XGBRFClassifier with hyperparameter tuning, referred to as XGBRFClassifier+HyperTuning, also attained a classification accuracy of 0.97. The Random Forest Classifier demonstrated superior performance compared to the other techniques, with a flawless accuracy score of 1.00.

V. CONCLUSION

In conclusion, the utilization of the Random Forest Classifier for credit card fraud detection has demonstrated remarkable success, achieving a staggering accuracy of 100%. This outcome underscores the effectiveness of the model in accurately distinguishing between legitimate and fraudulent transactions within the credit card dataset. The inherent capability of the Random Forest model to handle complex, high-dimensional datasets, coupled with its adeptness in mitigating overfitting, has proven instrumental in creating a robust and reliable fraud detection system.

VI. REFERENCES

[1] Dal Pozzolo, Andrea, Giacomo Boracchi, Olivier Caelen, Cesare Alippi, and Gianluca Bontempi. "Credit card fraud detection: a realistic modeling and a novel learning strategy." *IEEE transactions on neural networks and learning systems* 29, no. 8 (2017): 3784-3797.

[2] Fu, Kang, Dawei Cheng, Yi Tu, and Liqing Zhang. "Credit card fraud detection using convolutional neural networks." In *Neural Information Processing: 23rd International Conference, ICONIP 2016, Kyoto, Japan, October 16–21, 2016, Proceedings, Part III 23*, pp. 483-490. Springer International Publishing, 2016.

[3] Dornadula, Vaishnavi Nath, and Sa Geetha. "Credit card fraud detection using machine learning algorithms." *Procedia computer science* 165 (2019): 631-641.

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

[5] Jiang, Changjun, Jiahui Song, Guanjun Liu, Lutao Zheng, and Wenjing Luan. "Credit card fraud detection: A novel approach using aggregation strategy and feedback mechanism." *IEEE Internet of Things Journal* 5, no. 5 (2018): 3637-3647.

[6] Zanin, Massimiliano, Miguel Romance, Santiago Moral, and Regino Criado. "Credit card fraud detection through parenclitic network analysis." *Complexity* 2018 (2018).

[7] de Sá, Alex GC, Adriano CM Pereira, and Gisele L. Pappa. "A customized classification algorithm for credit card fraud detection." *Engineering Applications of Artificial Intelligence* 72 (2018): 21-29.

[8] Lebichot, Bertrand, Fabian Braun, Olivier Caelen, and Marco Saerens. "A graph-based, semi-supervised, credit card fraud detection system." In *International Workshop on Complex Networks and their Applications*, pp. 721-733. Cham: Springer International Publishing, 2016.

[9] Varmedja, Dejan, Mirjana Karanovic, Srdjan Sladojevic, Marko Arsenovic, and Andras Anderla. "Credit card fraud detection-machine learning methods." In *2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH)*, pp. 1-5. IEEE, 2019.

[10] Banerjee, Rishi, Gabriela Bourla, Steven Chen, Mehal Kashyap, and Sonia Purohit. "Comparative analysis of machine learning algorithms through credit card fraud detection." In *2018 IEEE MIT Undergraduate Research Technology Conference (URTC)*, pp. 1-4. IEEE, 2018.

[11] Carcillo, Fabrizio, Andrea Dal Pozzolo, Yann-Aël Le Borgne, Olivier Caelen, Yannis Mazzer, and Gianluca Bontempi. "Scarff: a scalable framework for streaming credit card fraud detection with spark." *Information fusion* 41 (2018): 182-194.

[12] Yee, Ong Shu, Saravanan Sagadevan, and Nurul Hashimah Ahamed Hassain Malim. "Credit card fraud detection using machine learning as data mining technique." *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)* 10, no. 1-4 (2018): 23-27.

[13] Sohony, Ishan, Rameshwar Pratap, and Ullas Nambiar. "Ensemble learning for credit card fraud detection." In *Proceedings of the ACM India joint*

international conference on data science and management of data, pp. 289-294. 2018.

[14] Mohammed, Rafiq Ahmed, Kok-Wai Wong, Mohd Fairuz Shiratuddin, and Xuequn Wang. "Scalable machine learning techniques for highly imbalanced credit card fraud detection: a comparative study." In *PRICAI 2018: Trends in Artificial Intelligence: 15th Pacific Rim International Conference on Artificial Intelligence, Nanjing, China, August 28–31, 2018, Proceedings, Part II 15*, pp. 237-246. Springer International Publishing, 2018.

[15] Awoyemi, John O., Adebayo O. Adetunmbi, and Samuel A. Oluwadare. "Credit card fraud detection using machine learning techniques: A comparative analysis." In *2017 international conference on computing networking and informatics (ICCNI)*, pp. 1-9. IEEE, 2017.

[16] Carneiro, Nuno, Gonçalo Figueira, and Miguel Costa. "A data mining based system for credit-card fraud detection in e-tail." *Decision Support Systems* 95 (2017): 91-101.