Date available online: 23-07-2025
Vol. 3, Issue 1 (January – June 2025)

DOI: https://doi.org/10.24312/ucp-jeit.03.01.444

Securing Financial Transactions: Leveraging Random Forest for Credit Card Fraud Detection

Abu Bakr Qazi[1], Arfan Ali Nagra[1], Khola Farooq[1], Muhammad Yousif[2], Muhammad Haseeb Zia [3]
[1] Department of Computer Science, Lahore Garrison University Lahore Pakistan
[2] School of Computer Science, Minhaj University Lahore Pakistan
[3] Department of Software Engineering Lahore Garrison University Lahore Pakistan

Corresponding author: Muhammad Haseeb Zia (e-mail: haseenzia@lgu.edu.pk).

ABSTRACT
It is a crucial responsibility in the financial sector to safeguard clients and businesses against financial losses by verification of credit cards. It is demonstrated that machine learning algorithms like random forest methods can detect fraud. Multiple decision trees are used in the Random Forest to create predictions. It is very suitable for fraud detection in credit card fraud due to its prowess with high-dimensional and huge datasets. With the help of training on labelled data and performance analysis, the Random Forest algorithm can accurately detect fraudulent transactions and help decrease financial risks. Due to its features of interpretability and durability against overfitting, it is well well-suited tool for firms wanting to improve their fraud detection systems due to. With the use of the strengths of the Random Forest algorithm, accurate analysis and categorization of complex patterns and minute abnormalities present in credit card transactions has become feasible. This strategy helps in the efficient and on-time identification of potential dangers which enables proactive measures to guard against fraudulent activity and increases the accuracy of detection. With this advantage of Random forests, institutions of finance can get an in-depth analysis of the causes that impact fraud incidents and enable them to enhance and improve their security systems. Despite of shifting dynamics of transactions and fraud strategies, the model can tackle overfitting and guarantees reliable performance. Therefore, with the addition of the Random Forest algorithm into card fraud detection frameworks, enterprises acquire the ability to strengthen their defense system and enhance the security and trust of both their clients and the overall financial ecosystem.

INDEX TERMS Random Forest Algorithm, Ensemble Learning, Credit Card, Defence Fortification, Fraud

I. INTRODUCTION
With the advancement of technology fraud in credit cards has grown to be a big issue in the financial sector that affects cardholders as well as financial institutions. To reduce financial losses and maintain the credibility of the system it is important to identify fraudulent transactions as early as possible [1]. With time fraud schemes are advancing in terms of complexity and sophistication which is why conventional rule-based approaches and manual monitoring have reached their limits [2]. RF algorithm is a learning method that uses the prediction of various decision trees and happens to be a very efficient algorithm in this aspect. The model has its versatility and handles big and complicated datasets efficiently and due to its robustness against over-fitting, Random Forest has been widely used in many fields. The model has generated promising results in detecting fraud in credit cards [3].

Over time with the advantage of the Random Forest technique decision trees are built and every tree is trained using a different set of sample data and feature set. Occurrence of fraudulent transactions and various characteristics form patterns. The system is trained by discovering these patterns and connections.

There are many advantages of using a random forest algorithm in detecting frauds of credit cards. First of all, it can manage unbalanced datasets, that have a high proportion of fraudulent transactions than genuine ones, by offering accurate predictions for both groups. In addition to that RF (Random Forest) provides a feature importance evaluation that enables investigators to identify the most important factors influencing fraud detection. The model is descriptive and enables analysts to understand the decision-making process efficiently [5].

This work explores the use of the random forest in detecting credit card fraud. The transaction data of credit cards is pre-processed, features selection is done and then the Random Forest model is trained on labeled data. After the training, the model is assessed with the use of pertinent performance measures. It is anticipated that reliable and effective identification of fraudulent transactions is done by utilizing the strengths of the Random Forest algorithm and it boosts the security and overall integrity of credit card systems [6].

In general, using the Random Forest algorithm to detect credit card fraud shows potential for enhancing fraud detection precision and lowering false positives, improving security for financial institutions and consumers against fraudulent actions.

II. LITERTURE REVIEW
The article talks about how the growing usage of the internet has affected online card transactions and how this has become a reason for an increase in fraud in the

worldwide banking industry. Due to their static nature, traditional rule-based systems have shown to be ineffective at identifying fresh and unreported threats. In response, academics have concentrated on creating systems that use machine learning, particularly deep learning, to identify fraud in an adaptable manner. The development of robust models was hampered by the incomplete understanding of fraudulent card transaction features in earlier investigations. The authors created a dataset of 4 billion non-fraudulent and 245,000 fraudulent transactions from 35 banks in Turkey to fill this gap. They presented and assessed various models for fraud detection based on profiles like models based on type of cards, transaction characteristics, and amount. The efficiency of models against ageing and zero-day attacks was demonstrated through temporal and spatial analysis. By utilizing sophisticated profiling approaches and examining transaction patterns, this paper ultimately aims to improve fraud detection in online card transactions, aiding in the creation of more reliable and resilient fraud detection models. [1]

Credit card usage has significantly increased in the digital economy, which has increased credit card fraud, as this study explores. Although ML algorithms are already being used to identify credit card fraud, these algorithms struggle because of the constantly changing shopping habits of customers and the dataset's class imbalance issue.[2]

The effectiveness of transaction fraud detection techniques is examined, as well as how they affect user losses in online transactions. There is a high rate of misjudgment since it is difficult for current approaches to adequately de-scribe the transaction behaviours of low-frequency users with small transaction volumes. To improve accuracy for low-frequency users, the research presents a novel approach that generates individual transaction behaviours. To in-crease accuracy, this approach transfers the current transaction group behaviour and transaction status. With the help of previous transaction history benchmarks for users' unique transaction behavior is constructed by identifying the ideal risk threshold. To construct the common behavior of the current transaction group, behavioral traits from authentic as well as fraudulent samples are extracted by using the DBSCAN clustering algorithm. With the use of the sliding window method, the current transaction status is extracted from transaction records. A new transaction be-haviour is provided to the user by integrating these elements and with the use of the Naive Bayes method a multi-behavior detection model is recommended to determine the chances of a transaction being fraudulent. This method is suitable for low-frequency users. As the experimental results show the method effectively identifies fraud-lent transactions with a low misjudgment rate for genuine transactions.[3]

This research work explores the challenges that are involved in ensuring the trustworthiness and dependability of transactions in the autonomous as well as open environment of e-commerce in online social networks (ECOS). There is no guarantee of privacy or protection against fraud in ECOS network transactions. As an efficient solution to this problem, it is suggested that trust management strategies should be used.

To tackle the problem of trust in ECOS, this research work suggests a hybrid trust paradigm that is based on factor enrichment. The architecture suggested in this work uses three levels of trust to create a reliable view among people involved in the transaction. It defines private reputation as a dynamically changing perception of reliability. Moreover, it adds that common reputation is a group-wide, transferable factor of trust. It is strengthened by characteristics that increase reliability and consistency. In addition to that hybrid trust combines personal and public reputation to pro-vide cohesive and reliable impressions. Privacy and anti-fraud criteria are catered by the hybrid trust model to further evaluate the security of transactions. [4]

The results of this study show the performance and depict how well it can handle problems related to credit card data like imbalanced distribution of classes and overlapping class samples. [5]

This article states that credit card fraud is now a major problem in e-commerce technologies and caused businesses to suffer large financial losses. Ultimately these frauds prompt the creation of efficient fraud detection systems. It is a difficult task to accurately detect fraud because of the limitations of conventional machine learning methods and in-sufficient credit card information.

The proposed technique is compared with several algorithms like support vector machine (SVM), multi-layer perceptron (MLP), conventional AdaBoost, decision tree and LSTM to verify its performance. According to experimental findings, classifiers trained using resampled data perform better than those trained without it. The suggested LSTM ensemble classifier outperforms the previous techniques, with a sensitivity of 0.996 and a specificity of 0.998. [6]

The essay highlights the growing need for cutting-edge fraud prevention techniques in a cashless world, especially in light of the sizeable predicted global loss brought on by fraud.

By dividing users into old and new users, the research offers the idea of user separation rather than just concentrating on foretelling illegal transactions. For each user group, distinct models—CatBoost and Deep Neural Net-works—are used. The work also presents numerous ways to improve detection accuracy including dealing with the issue of imbalanced datasets, feature modification and feature engineering. The Deep Neural Network model achieved an AUC of 0.84 whereas the CatBoost model obtained a score of 0.97. That is why using these scores, one would expect counterfeit credit cards with higher accuracy. It gives an understanding of the user separation method for the detection of credit card frauds that employs CatBoost and a deep learning approach. Results demonstrate how effectively the

algorithm detects fake credit cards and highlight the methods that can be used to improve the precision of the detection. [7]

To enhance the efficiency, security as well as the effectiveness of the quickly growing private insurance business, this work calls for the adoption of technology. Traditional methods which rely on people are slow and can contain errors since they are not very efficient. To conclude, this paper provides a framework for a safe and automated insurance system to tackle these problems This approach tries to reduce losses, reduce contact with people, enhance secu-rity, indicate clients with high risks, and detect fake claims. It utilizes blockchain technology for secure transactions and data exchange among the insurance network agents. Also, it employs the extreme gradient boosting (XGBoost) method which is more effective than the rest in terms of performance and especially in detecting fake claims. In ag-gregate, by integrating blockchain technology and machine learning an extensive analytical framework can be turned into a set of powerful tools with benefits in terms of increased efficiency, enhanced accuracy, and enhanced protection of the insurance market.[8]

The paper is based on the issue of credit card fraud in electronic commerce systems and introduces. OLightGBM (Optimised Light Gradient Boosting Machine) is one of the latest smart techniques to detect fraud. With proper tuning of hyperparameters of LightGBM, the Bayesian-based hyperparameter optimisation also helps in fraud detection. From the testing carried out with real data, it's important to know that OLightGBM outperforms the other models. The proposed method acquires a precision of 97.34%, an AUC of 92.88% and an F1-score of 56.95%. It also achieved an accuracy of 98.40%. In conclusion, the study recommends a viable approach toward card fraudulent detection of credit cards.Transactions and reduce financial losses that use LightGBM and Bayesian-based hyperparameter-tuned optimization. [9]

The paper aims to cope with the issues related to the identification of fraud in online shopping as well as the in-creasing concern with it. Because of this, sophisticated deep-learning algorithms are necessary for utilization. The problem with applying machine learning techniques is that the calculations have finite accuracy. The article conducts a comparative analysis with the use of dataset i:e European Card Benchmark and shows appreciable enhancements in convolutional neural network architectures' fraud detection precision, accuracy, f1-score and AUC curves. The suggested models outperform conventional machine learning techniques and exhibit their efficacy in actual situations involving the detection of frauds of credit cards. The paper offers a thorough method that makes use of deep learning algorithms for more accurate and trustworthy credit card fraud detection. Overall, the research work demonstrates the suggested models' higher performance in comparison to conventional ML techniques [10].

To automate the detection process and decrease the number of false positive alerts, the article analyses the difficulties associated with the frequency of false positives in detection systems and advises the use of deep neural networks. Although sophisticated techniques like statistical modelling and models of machine learning are used by fraud detection systems, human intervention is still necessary to confirm fraud instances or rule out false positives, which results in inefficiencies and increased costs.

The study investigates how to interpret alerts produced by a fraud detection system using deep learning techniques, particularly deep neural networks, and assesses how accurate these techniques are at detecting false positives. We evaluate and contrast several neural network designs.

The findings show that the deep neural network's optimal configuration achieves a fraud detection rate of 91.79% while lowering the number of alerts by 35.16%. Since warnings identified by the neural network as false-positives would no longer require manual examination, the reduction in false-positive alerts has the potential to significantly lower the expenses associated with manual labour.

The proposed method holds the potential for automating fraud detection and advances the system in terms of the effectiveness of fraud detection systems by utilizing deep neural network capabilities. By lowering reliance on manual assessment of false-positive warnings, the findings emphasize the potential for cost savings and greater productivity. [11]

The paper emphasizes the need to identify financial fraud in the banking sector and recognizes the difficulties in doing so, including the need for interpretability and privacy legislation that restrict access to large-scale transaction data. To get beyond these restrictions, a lot of existing fraud detection techniques rely on manually created features. To address this, the authors suggest behaviour- and segmentation-based features that rely on statistical traits unique to fraudulent and non-fraudulent accounts. These characteristics offer clear cause-and-effect connections and show encouraging predictive outcomes.

The article also raises questions about the potential for unstable results when employing well-known boosting classifiers like XGBoost and LGBM because some features have time-inhomogeneous qualities. The authors used the Kolmogorov-Smirnov test to find and remove certain problematic characteristics to remedy this issue. As a result, XGBoost and LGBM classifiers have improved in terms of detection performance and resilience. According to experimental results, the suggested method performs better than competing classifiers like SVM and random forests.

The article also discusses the drawbacks of creating training and testing sets via random sampling since it misses time inhomogeneity and leads to inaccurate results of the accuracy of machine learning models. The

performance of resampling techniques used to address data imbalances in fraud detection is also impacted by the time-inhomogeneous traits found in fraud patterns. The authors find that due to the various modus operandi patterns, inappropriate linear interpolation in SMOTE-related techniques results in subpar performance. The essay contends that this problem can be solved by synthesizing false samples with generative adversarial networks (GANs) and straightforward oversampling. [12].

The article examines the rise in financial transactions and the associated rise in fraud instances, focusing in particular on credit card purchases made through online shopping sites. Due to the enormous expenses involved, finding fraudulent behavior in these transactions has become a top priority. The study uses Bayesian optimization to tune the involved hyperparameters while taking into account relevant factors like imbalanced data. For improving the efficiency of the LightGBM technique, it proposes weight-tuning as a pre-processing step for resolving data imbalance and offers a voting mechanism by merging CatBoost and XGBoost algorithms. For additional performance enhancement, deep learning techniques are used to fine-tune the hyperparameters with a focus on the suggested weight-tuning method.

The article's main focus is on the use of machine learning models to spot fraudulent transactions. Since the majority of systems often identify fraudulent acts after they have already occurred, it draws attention to how difficult it is to detect fraud in real-time or almost real-time. The highly unbalanced character of fraudulent transactions, which occur significantly less frequently than legitimate transactions, makes the task of fraud identification much more challenging.

The outcomes show that when applied to the highly unbalanced bank loan dataset, the quantum-enhanced support vector machine beats competing techniques in terms of speed as well as accuracy. However, its performance for Israel credit card transaction data is on par with other approaches. The study also shows that feature selection considerably increases detection speed while having a negligible effect on accuracy [13].

The article provides information on how to choose the best methods for a given dataset while taking into account the trade-offs between efficiency, precision, and expense in fraud detection activities. [14]

The article covers the issue of online fraud in e-commerce platforms and focuses on the value of reputation scores offered by platform users to assess vendors. To improve their earnings, sellers want to earn high reputation scores. But by combining it, scammers can misrepresent reputation scores and get unwary customers.

The study consists of conceptual propositions that refer to both people and indications of transactions and focus on fraud transaction attributes. To enhance the accuracy of fraud detection, two more independent variables – product type and product nature are added. Using a real-world undefined dataset, the effectiveness of these indications and the detection model is confirmed, enabling at least the separation between criminal and legitimate transactions

In conclusion, the research presented can be considered to contribute a usable and enriching conceptual frame-work concerning big data technologies and data mining approaches in an attempt to extract the relevant signs from fraud transactions in a bid to make the identification. These product attributes make fraud detection more accurate, and real-world data is deployed to evaluate the effectiveness of the recommended indicators and the model. [15]

The article is primarily devoted to the problem of class imbalance data classification, which has recently attracted the attention of researchers in science disciplines such as fraud detection, metabolomics, and cancer diagnosis. It stresses the undesirable consequences of sharing similarities in class-imbalanced learning performance, which needs to have methods that eliminate the overlaps and enhance the classification performance.

The paper suggests a model for feature selection that reduces data overlap and in turn increases classification ac-curacy. This method is based on enhanced R-value. These algorithms make use of sparse feature selection methods and, in the case of ROS and ROA, resample data. The algorithms were created primarily for binary classification jobs, it is important to note.

Results from simulations show how well the suggested techniques control the fluctuation in the false discovery rate when choosing the primary features for process modelling. Four credit card datasets are used in trials to assess the algorithms' performance. Evaluation measures like F-measure and G-mean demonstrate how much better the pro-posed algorithms are than conventional feature selection techniques.

To reduce overlap in class-imbalanced data classification, the study offers a feature selection technique based on enhanced R-value. The proposed approach can also be proved when testing on credit card datasets and showed higher accuracy than traditional feature selection methods. According to the study, the presented efficient feature se-lection method can also be applied to tackle overlapping issues in the context of other problems associated with class-imbalanced learning issues. [16]

Recall, precision, and accuracy are some metrics used to assess the models. The presented approach is further vali-dated with the use of a highly inclined synthetic credit card fraud dataset.

The result of experiments shows that using AdaBoost provides better results in terms of effectiveness. From the perspective of evaluation, the imposed alterations lead to increased effectiveness compared to the alternatives.

Hence, the study concludes with a machine learning-based credit card fraud detection framework. The AdaBoost algorithm is incorporated into the system to enhance the feature’s classification and the system is

evaluated with re-al-world imbalanced data sets. The results acquired in the experiments depicted effectiveness in comparison to other approaches regarding credit card fraud detection. [17]

The article's main topic is credit card fraud, with a focus on the skimming method that fraudsters use to obtain card information. The suggested process entails numerous steps. In the beginning, principal component analysis (PCA) and autoencoder extractors are used to extract discriminative features. Next, using the K-Means method, comparable fraudulent transactions are clustered. The approach locates possible merchants implicated in the skimming scheme through retrospective analysis of all transactions by locating matched merchants within the created clusters.

Even with the lack of prior knowledge regarding existing skimming spots, experiments on real card transactions show encouraging results for the suggested strategy. Seven out of the nine locations of compromise that the bank had previously identified and reported were found after applying the approach. [18]

The article highlights the difficulty of detecting credit card fraud in online purchases and emphasises the need for flexible fraud detection systems (FDS). It is challenging to adapt current methods to new problems, such as fresh payment systems, other countries, or particular population segments, due to the varied nature of fraud behaviour.

The challenge of transfer learning, which entails adjusting current detection models to new contexts, is the subject of this research.

The study makes use of a dataset from an industry partner that includes around 200 million transactions within six months. With an emphasis on accuracy across various transfer contexts, the essay describes and contrasts 15 transfer learning strategies, spanning from fundamental baselines to cutting-edge and unique approaches. Two key conclusion emerge from the evaluation: (i) the availability of labelled samples in the target domain significantly influences the effectiveness of transfer methods, and (ii) an ensemble solution based on self-supervised and semi-supervised domain adaptation classifiers is proposed to address this challenge.

From the findings of the experiments, it can be observed that the proposed ensemble solution yields lesser sensitivity to the hoe much of labelled samples available in the target domain and it performs with amazing accuracy in credit card fraud detection. [19]

As a result, to resolve the problem of imbalanced classification in credit card fraud detection the study proposes a state-of-art method in oversampling. This approach is based on Deep learning methods and variational automatic coding (VAE). To generate several instances from the minority, the VAE approach is applied. The classification net-work is then trained using such generated samples. The baseline classification model performs greatly and performance is enhanced by the extended dataset that is produced using the VAE method. Performance is measured in terms of F measure, precision, specificity and accuracy.

The findings of the work suggest the proposed VAE-based oversampling technique is highly effective in addressing the imbalanced classification problem. This approach enhances the performance of the classification model and enhances the capability of detecting fraud samples as it generates many synthetic samples from minority classes. [20]

III. MATERIALS AND METHODOLOGY

A. DATA COLLECTION AND PREPROCESSING

The dataset [21] used in this work is gathered from the well-known sight “Kaggle”. To address the unequal class distribution in the dataset, the SMOTE-ENN i:e edited nearest neighbor method and the hybrid synthetic methodology of minority oversampling are also used. This method outperforms various models that are commonly used by machine learning classifiers and mentioned in the literature review in terms of performance. the below figure.1 working of flowchart explains how data is collected step by step and further on for preprocessing and finalizing the accuracy achieved.

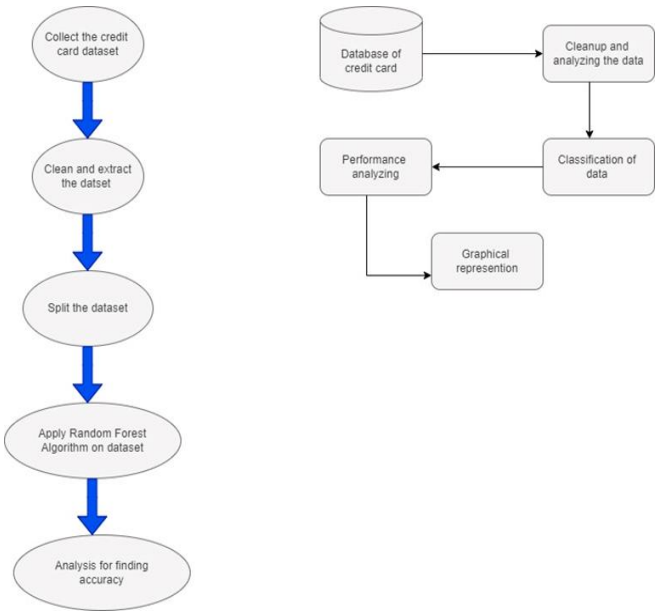

FIGURE 1: Data Collection and Preprocessing

B. DATA VISULIZATION

The dataset is plotted using the matplotlib library of Python was used. Following is the plot diagram of the respective dataset. To visually understand the dataset and look for discrepancies in it, we plot various graphs. Histogram, density plot, box plot, and scatterplot matrix. Dimensionality reduction is the following phase when we lower the number of dimensions in our data collection to enable visualization on a 2D or 3D display. Principal component analysis, or PCA, does this, so figure 2 display the class column which one is target showing fraud 1 and non-fraud 0.

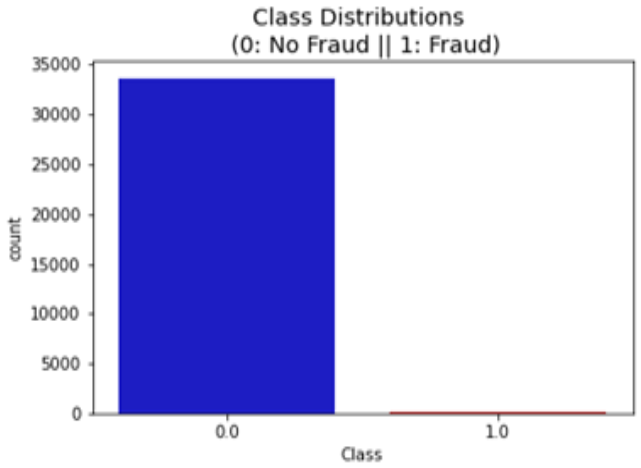

FIGURE 2: FIGURE OF FRAUDLUENT TRANSACTIONS

C. FEATURE SELECTION

To reduce overlap in class-imbalanced data classification, the study offers a feature selection technique based on enhanced R-value. Experiments on credit card datasets show that the suggested algorithms perform better than traditional feature selection techniques. According to the article, this efficient feature selection method can be used to tackle overlapping issues in other class-imbalanced learning issues.

D. RANDOM FOREST ALGORITHM

When compared to the client's prior exchanges, card exchanges are consistently new. It is recognized as an idea float issue in reality and this newness is a very difficult problem [1]. Idea float can be thought of as a variable that alters gradually and erratically over time. High levels of information irregularity are caused by these variables. The main goal of our investigation is to resolve the problem of Concept Float's inability to operate in certain circumstances. Table 1, [1] lists the fundamental components that are observed during any trade. Figure 3 demonstrate the workflow of credit card Transactions fraud history according to profile of customer and make it sure for final result.

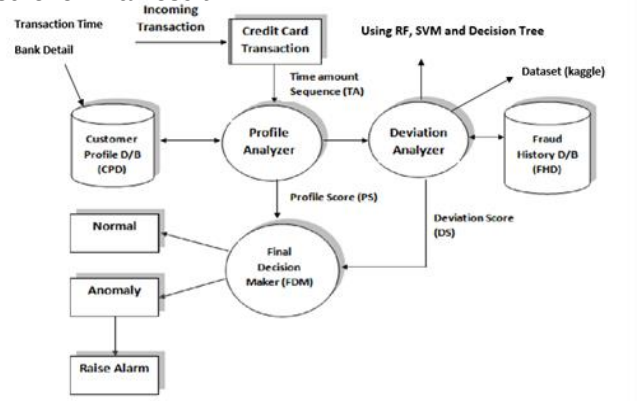

FIGURE 3: System Design for Credit Card Farud Detection using Random Forest classifiers

E. MODEL TRAINING AND EVALUATION

Separate the training and testing sets from the preprocessed dataset. Describe in detail how to use the training set to train a Random Forest model. Also, go over the hyperparameter tweaking procedure for model optimization. Discuss additional evaluation methods like cross-validation to ensure model effectiveness.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

$$MCC = \frac{TP * TN - FP * FN}{((TP + FP)(TP + FN)(TN + FP)(TN + FN))^2} \quad (3)$$

In the above equations parameters are used as:
TP represent as True Positive
TN represent as True Negative
FP represent as False Positive
FN represent as False Negative

IV. RESULTS

The algorithm puts out the number of false benefits it has identified and contrasts it with the true characteristics. This is used to determine the calculations' correctness and exactness score. 10% of the whole dataset was the little portion of data we used for quicker testing. Near the end, the entire dataset is also used, and both results are printed. These results, along with the arrangement report for each calculation, are provided in the result as follows, where class 0 denotes that the results are not certain to be significant and class 1 denotes that the method is not completely established as an extortion exchange. To look for false positives, this result was compared to the class values.

A. COMPARISON WITH MACHINE LEARNING ALGORITHMS

Table1 shows the comparison of the current model with some other machine learning models on which Credit Card Fraud detection had been performed previously

TABLE 1: PRECISION, ACCURACY, AND MCC VALUES

Method	Precision	Accuracy	MCC
SVM	0.782	0.997	0.5267
LR-Logistic	0.876	0.990	0.6786
Decision Tree classifier	0.884	0.944	0.8156
Random Forest Classifiers	0.9350	0.994	0.8368

In the Figure 4 The plot displays the ratio of Fraud and no fraud performance with the classifier model (2X2)

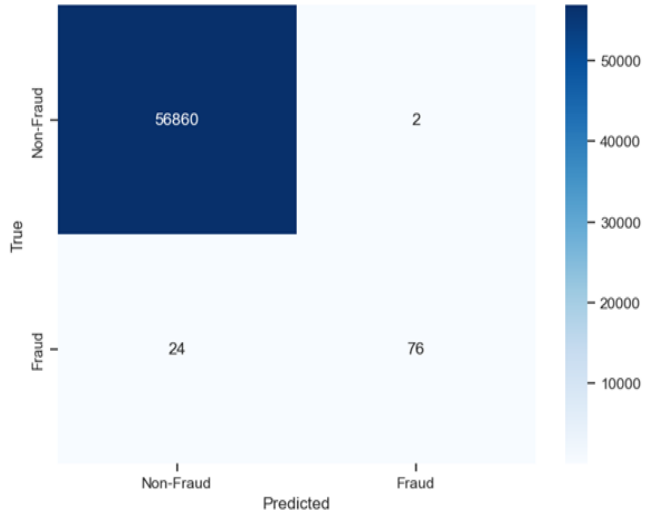

FIGURE 4: Confusion Matrix

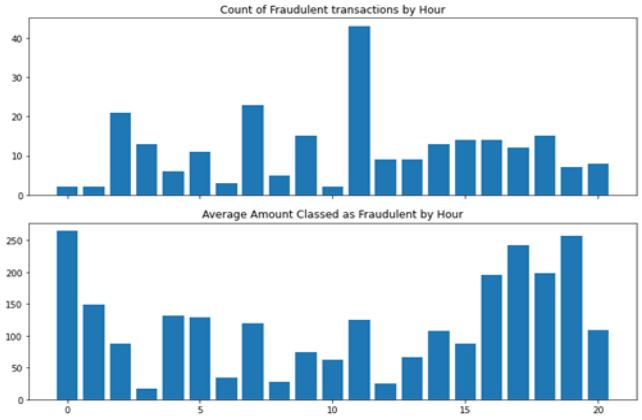

FIGURE 5: Histogram Plot

In the Figure 5 Given graph demonstrates the ratio of fraudulent transactions is a lot more than the original ones.

The aforementioned graphs in Figure 5, depict how fraudulent transactions were distributed throughout the days' time(hr) and hour banks.

Figure 6 display the Interpreting correlation with debit card transitions positive correlation and negative correlation.

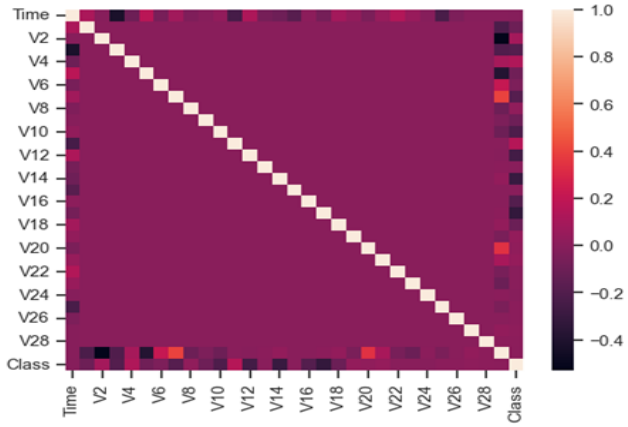

FIGURE 6: Interpreting correlation with Debit card Fraud

V. CONCLUSIONS

In this work we developed a new method for the detection of credit card fraud where users are gathered because of their transactions and focus on moral principle to develop a profile for each cardholder.

Charge card extortion is undoubtedly a sign of criminal unreliability. The most well-known extortion techniques, along with their methods of discovery, have been thoroughly examined in this article, which also looked at recent developments in the subject. Additionally, this study has shown in detail how AI may be used to improve extortion identification along with computation, pseudocode, clarification of its execution, and trial-and-error outcomes. Even if the computation has an accuracy of more than 99.6%, it is still only 28% accurate when only a tenth of the informational index is taken into account.

REFERENCES

[1] Luo, B., Zhang, Z., Wang, Q., Ke, A., Lu, S., & He, B. (2023). Ai-powered fraud detection in decentralized finance: A project life cycle perspective. ACM Computing Surveys.

[2] Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities. Computer Science & IT Research Journal, 5(6), 1505-1520.

[3] Mienye, I. D., & Jere, N. (2024). Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions. *IEEE Access*.

[4] Parkar, E., Gite, S., Mishra, S., Pradhan, B., & Alamri, A. (2024). Comparative study of deep learning explainability and causal ai for fraud detection. International Journal on Smart Sensing and Intelligent Systems, 17(1).

[5] Rezvani, S., & Wang, X. (2023). A broad review on class imbalance learning techniques. Applied Soft Computing, 143, 110415.

[6] Leevy, J. L., Hancock, J., & Khoshgoftaar, T. M. (2023). Comparative analysis of binary and one-class classification techniques for credit card fraud data. Journal of Big Data, 10(1), 118.

[7] Prabhakaran, N., & Nedunchelian, R. (2023). Oppositional Cat Swarm Optimization-Based Feature Selection Approach for Credit Card Fraud Detection. Computational Intelligence and Neuroscience, 2023(1), 2693022.

[8] Ralli, R., Jugran, G., Gaurav, M., & Goyal, M. (2024, August). An Ensemble based Fraudulent Blockchain Account Detection System. In Proceedings of the 2024 Sixteenth International Conference on Contemporary Computing (pp. 337-342).

[9] Taha, A. A., & Malebary, S. J. (2020). An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. IEEE access, 8, 25579-25587.

[10] Khalid, A. R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J., & Adejoh, J. (2024). Enhancing credit card fraud detection: an ensemble machine learning approach. Big Data and Cognitive Computing, 8(1), 6.

[11] Baria, J. B., Baria, V. D., Bhimla, S. Y., Prajapati, R., Rathva, M., & Patel, S. (2024). Deep Learning based Improved Strategy for Credit Card Fraud Detection using Linear Regression. *Journal of Electrical Systems*, *20*(10s), 1295-1301.

[12] Bao, Q., Wei, K., Xu, J., & Jiang, W. (2024). Application of Deep Learning in Financial Credit Card Fraud Detection. Journal of Economic Theory and Business Management, 1(2), 51-57.

[13] Du, H., Lv, L., Wang, H., & Guo, A. (2024). A novel method for detecting credit card fraud problems. Plos one, 19(3), e0294537.

[14] Zhu, K., Zhang, N., Ding, W., & Jiang, C. (2024). An Adaptive Heterogeneous Credit Card Fraud Detection Model Based on Deep Reinforcement Training Subset Selection. IEEE Transactions on Artificial Intelligence.

[15] Chatterjee, P., Das, D., & Rawat, D. B. (2024). Digital twin for credit card fraud detection: Opportunities, challenges, and

fraud detection advancements. Future Generation Computer Systems.
[16] Chhabra, R., Goswami, S., & Ranjan, R. K. (2024). A voting ensemble machine learning based credit card fraud detection using highly imbalance data. Multimedia Tools and Applications, 83(18), 54729-54753.
[17] Ning, W., Chen, S., Lei, S., & Liao, X. (2023). Amwspladaboost credit card fraud detection method based on enhanced base classifier diversity. IEEE Access.
[18] Salekshahrezaee, Z., Leevy, J. L., & Khoshgoftaar, T. M. (2023). The effect of feature extraction and data sampling on credit card fraud detection. Journal of Big Data, 10(1), 6.
[19] Jemai, J., Zarrad, A., & Daud, A. (2024). Identifying Fraudulent Credit Card Transactions using Ensemble Learning. IEEE Access.
[20] Zioviris, G., Kolomvatsos, K., & Stamoulis, G. (2024). An intelligent sequential fraud detection model based on deep learning. The Journal of Supercomputing, 80(10), 14824-14847.