

Real Time Credit Card Fraud Detection and Reporting System Using Machine Learning

Jolaosho Ahmed Oluwatoyin¹, Solomon Akinola²,

¹Department of Computer Science, Faculty of Natural and Applied Sciences,
Lead City University, Ibadan, Oyo State, Nigeria,

²Department of Computer Science, Faculty of Natural and Applied Sciences, Lead City
University, Ibadan, Oyo State, Nigeria

doi: <https://doi.org/10.37745/ejcsit.2013/vol12n43656>

Published June 06, 2024

Oluwatoyin J.A.and Akinola S. (2024) Real Time Credit Card Fraud Detection and Reporting System Using Machine Learning, *European Journal of Computer Science and Information Technology*, 12 (4),36-56

ABSTRACT: *This study addresses the critical issue of real-time credit card fraud detection using machine learning. The primary goal is to develop a model that promptly identifies fraudulent transactions and alerts users. Two algorithms—Random Forest and Decision Tree Classifier were used, alongside various sampling techniques to balance the dataset and enhance performance. Six models were created, each with different accuracy levels in fraud detection. Key findings include a higher incidence of fraud among individuals over 75 years, likely due to less familiarity with modern transaction methods. Additionally, a majority of transactions involved females, indicating a potential higher fraud risk in these transactions. The Random Forest -SMOTE [Hyperparameter Tuned] model was the most effective, achieving a 97% accuracy rate, 95% F1 score, and 98% precision rate. For practical application, this model was integrated with Twilio for real-time fraud alerts, proving successful in sending timely, accurate notifications. The study highlights valuable insights and a robust solution for real-time fraud detection and response. Regular performance evaluations of the model are recommended to maintain its effectiveness against evolving fraud patterns.*

KEYWORDS—algorithm, credit card fraud, machine learning, real-time detection, twilio integration

INTRODUCTION

The widespread adoption of online banking platforms, which facilitate various financial activities such as cash transactions, bill payments, and online buying, has greatly enhanced the ease experienced by a large number of persons in their everyday lives. Despite the considerable benefits associated with conducting transactions online, customers are confronted with a substantial

challenge stemming from the occurrence of financial fraud. Fraud is the act of an unauthorised individual or organisation bypassing the security mechanisms of a financial institution and adopting the identity of a genuine customer in order to deceive and defraud the institution. Financial fraud is a pervasive phenomenon that is steadily increasing and carries substantial consequences inside the financial sector.

According to data from 2019, the worldwide population of individuals utilising credit cards amounted to approximately 2.8 billion. Moreover, a minimum of 70% of these individuals are in possession of at least one credit card (AlEmad, 2021). The United States experienced a notable rise in credit card fraud cases, with a 44.7% increase observed between 2019 and 2020. The number of reported incidents surged from 271,927 in 2019 to 393,207 in 2020. According to the most recent study, the global losses resulting from credit card fraud in 2021 reached a total of \$32.34 billion, exhibiting an increase of nearly 14% compared to the losses experienced in the previous year, which amounted to \$28.43 billion (Mullen, 2023). According to Mullen (2023), The aggregate losses due to fraudulent activities in the United States during the calendar year 2021 reached a sum of \$11.91 billion, indicating a notable increase of 18% compared to the \$10.09 billion reported in the year 2020. The occurrence of card not present fraud has exhibited a notable rise of 81% in comparison to point of sale fraud. Credit card fraud is a pervasive problem in the United States, as evidenced by the regular reporting of cases by banks, businesses, and cardholders. Indeed, the nation is responsible for 38.6% of the global recorded losses incurred from credit card fraud (Ashraf et al., 2022).

Between the months of January and September in the year 2020, financial services firms in Nigeria incurred a financial loss amounting to ₦5.2 billion as a result of fraudulent operations (NIBSS, 2021; Anowu et al., 2021). The predominant portion of the financial loss was suffered within the timeframe spanning from July to September 2020, wherein enterprises encountered losses amounting to as much as ₦3.36 billion. During the corresponding period in 2020, there was a notable escalation in the financial losses incurred as a result of fraudulent activities, exhibiting a substantial jump of 510% in comparison to the ₦550 million lost in the preceding year of 2019 (NIBSS, 2021)..

Machine Learning is a specialised domain within the study of Artificial Intelligence that facilitates the acquisition of knowledge and skills by computers through the process of learning from experience, without the need for direct human intervention. The primary aim of this endeavour is to forecast forthcoming results with a notable level of precision by employing various computational models. According to Saravanan & Sujatha (2018) and Nasteski (2017) Machine learning approaches can be classified into two primary categories: supervised learning and unsupervised learning. Machine learning algorithms utilise past data to train models capable of accurately predicting fraudulent transactions. It has become a widely used method for identifying financial fraud because of its capacity to evaluate large volumes of data and uncover intricate patterns that are challenging to detect using conventional techniques. Commonly employed

machine learning methods for fraud detection encompass logistic regression, decision trees, random forests, support vector machines, and neural networks (Kumar et al., 2020; Hasan et al., 2019).

This study aims to create a prototype model for real-time credit card fraud detection and notification using machine learning algorithms. The objective is to enhance the accuracy and efficiency of fraud detection and reporting. Two algorithms, namely Random Forest, and Decision Tree Classifier, will be employed to identify instances of credit card fraud based on transaction time and amount. Upon the identification of fraudulent activity, an automatic text message will be promptly dispatched to notify the cardholder of the detected anomaly.

LITERATURE REVIEW

Financial Fraud

There are different categories of financial fraud in which credit or debit card fraud is the most common. There are four types of Credit Card Fraud: Card not present, Skimming, Phishing and Lost/Stolen Card (Popat & Chaudhary, 2018).

In Card not Present (CNP) fraud, fraudster attempt to mislead the system by dissembling to be some other person (Popat & Chaudhary, 2018). Mail and the web are major routes for fraud against merchants who sell and ship merchandise, and affects legitimate mail order and web merchants. In Skimming, they are obtaining personal data regarding someone else's credit card utilized in an otherwise normal transaction (Ileberi et al., 2020). There is a tiny device (skimmer) which is used to swipe and store huge amount of victim's information. In phishing, Scammers might use a range of schemes to lure users into giving them their card info through tricks corresponding to websites simulation to be of a bank or payment system. When card is steal or lost, there are chances for a thief that he make unauthorized transaction before cardholder block the card (Popat & Chaudhary, 2018).

According to Shakya (2018) , the total amount lost due to fraudulent activities in 2018 has reached \$22.8 billion. This figure represents a 4% increase compared to the losses incurred in 2015. Furthermore, it is anticipated that the losses will continue to rise significantly in the forthcoming years. In the United Kingdom, the total amount of unauthorised fraud losses incurred by payment cards, remote banking, and checks in the year 2022 amounted to £726.9 million (Connect, 2023). This figure represents a marginal decrease of less than one percent when compared to the same losses recorded in the year 2021. Remote purchase fraud, which involves the illicit utilisation of pilfered card information to make online, telephone, or mail order purchases, continues to account for the largest portion of financial losses, amounting to £395.7 million. However, it is worth noting that this figure has decreased compared to the previous year. The incidence of fraud on lost and stolen cards experienced a notable 30% increase, amounting to £100.2 million. Additionally,

instances of card identity theft, characterised by the unauthorised opening or takeover of a card account under another individual's name, nearly doubled, reaching £51.7 million (Connect, 2023).

Anowu et al. (2021) reported that financial services firms in Nigeria experienced a loss of ₦5.2 billion due to fraudulent activities over the period spanning from January to September 2020. The majority of this financial loss was incurred during the period from July to September 2020, with enterprises seeing a total loss of up to ₦3.36 billion (Paul, 2021). There was a significant increase of 510% in the amount lost to scammers, rising from ₦550 million in the corresponding period of 2019. Based on the 2021 fraud report published by the Nigerian Inter-Bank Settlement System (NIBSS), there was a significant surge in fraudulent activities in Nigeria, with a notable increase of 187% in the number of fraud attempts recorded between the years 2019 and 2020 (NIBSS Insight, 2021). In 2020, the primary sources of fraudulent activities were identified as the internet, accounting for 47% of reported cases, followed by mobile devices at 36%. ATM terminals accounted for 9% of reported fraud incidents, while point-of-sale (POS) terminals constituted 7% of the total cases (NIBSS, 2022)

Based on the data, the total amount of fraudulent activity amounted to \$5.6 billion in 2012. However, in 2018, the magnitude of fraud increased to \$9.1 billion, representing nearly 40% of the whole loss (Shakya, 2018). Specifically, 70% of the aforementioned fraudulent activities are to Card-Not-Present (CNP) transactions, which encompass fraudulent incidents occurring online or via telephone communication. Counterfeit transactions account for 20% of the total, while the remaining 10% of cases involve losses incurred as a result of lost or stolen cards (Shakya, 2018). The strategies for addressing fraud can be classified into two main categories: prevention, which entails measures aimed at averting fraud at its source, and detection, which involves actions conducted after to the occurrence of fraudulent activity. Nevertheless, some authors have undertaken efforts to combat this type of financial fraud.

Sudha & Akila (2021) proposed a Credit Card Fraud Detection system based on Operational & Transaction features using Support Vector Machine (SVM) and Random Forest (RF) classifiers. In this system, in the first phase, the operational features of users are extracted, and then a random forest classifier is used to classify the features into benign and suspected. In the second phase, the transaction features of users are extracted from the user records, and then the M-class SVM classifier is applied to classify the features into benign and suspected. The performance of the system is evaluated in terms of standard measures, accuracy, recall, and F-1 score. By results, it was shown that both RF and SVM classifiers achieve precision a higher detection rate with good accuracy. Abdulghani et al (2021) proposed some of the classification ML algorithms such as Logistic regression(LR), Linear Discriminant Analysis (LDA), and Naïve Bayes(NB), additionally, the boosting algorithm XGBoost to create models capable of detecting fraud. The dataset from Kaggle. The authors used performance metrics such as accuracy, precision, f1, recall, AUC confusion matrix to evaluate the models' performance. The XGBoost model presented the best results compared to other models

Lavanya (2023) detected credit card fraud using random forest classifier in comparison with logistic regression. Novel random forest classifier algorithm with sample size =09 and novel logiswhen compared to logistic regression algorithm efficiency(95.34%). The statistical significance difference(two-tailed) is 0.001($p < 0.05$). Their result showed that the Random tic regression algorithm with sample size =09 were evaluated many times to predict the efficiency percentage. The G power taken as 0.8 and a =0.05. Random forest classifier has been efficiency(97.12%) forest classifier with 97.12% has better accuracy than 95.34% Logistic regression in Credit card fraud detection. There is a statistical 2-tailed significant difference in accuracy for algorithms is 0.02($p < 0.05$) by independent t-test. Abdulghani (2022) proposed a model to detect fraudulent transactions based on some methods of machine learning such like Logistic regression (LR), NaiveBayes (NB), as well as the Linear Discriminant Analysis(LDA), in addition to XGBoost algorithm. The techniques used to generate the models of the suggested system, they were trained and evaluated on the basis of two different datasets. Where the first dataset was the European Cardholders, and the second dataset was the Turkish dataset provided by the Yapi Kredi Company. These datasets suffer from a big imbalance problem. Therefore, the authors used SMOTE to fix this issue. The system models' effectiveness was measured employing a variety of metrics, specifically the confusion matrix, accuracy, F1score, recall, precision as well as AUC. Also, the fuzzy membership function was adopted to the dataset in order to raise the system's efficiency. The final results showed the high efficiency of XGBoost.

Krishna (2022) identified the frauds committed using a payment card such as credit cards, debit cards, and also an experiment is performed to find the best suitable algorithm among Random forest and Logistic Regression. To stop the fraud detections using Random forest (N=10) and Logistic regression (N=10) with supervised learning that gives insights from the previous data. The precision of the random forest is 76.29% compared with Logistic regression with accuracy of 74.65% with statistical significance value $p = 0.03$ ($p < 0.05$) using Independent sample t test. Conclusion: This results proved that Random forest was significantly better for Fraud detection than Logistic regression within the study's limits. Ogundokun et al. (2021) proposed a credit card fraud discovery scheme to detect fraud. The ML techniques employed are Decision Tree (DT) and K-Nearest Neighbor (KNN) ML classification techniques. The performance outcomes of the two ML classification techniques are evaluated depending on accuracy, precision, specificity, recall, f1-score, and false-positive rate (FPR). The area under the ROC curve (AUC) of the receiver operating characteristics (ROC) curve was similarly drawn built on the confusion matrix for both classifiers. The two classification techniques were evaluated and compared using the performance metrics mentioned earlier and it was demonstrated that the KNN technique outperformed that of the DT with a greater ROC curve value of 91% for KNN and 86% for DT. It was concluded that KNN is considered a better ML classification technique that can be employed to discover credit card fraudulent activities.

Abakarim et al. (2018) proposed a live credit card fraud detection system based on a deep neural network technology. The proposed model is based on an auto-encoder and it permits to classify,

in real-time, credit card transactions as legitimate or fraudulent. To test the effectiveness of our model, four different binary classification models are used as a comparison. The Benchmark shows promising results for our proposed model than existing solutions in terms of accuracy, recall and precision. Also, Kumar et al. (2021) proposed a real time fraud detection system based on service oriented architecture (SOA) to analyze the fraudulent activities in credit card transactions. The architecture is designed on the basis of Apache Kafka tool, which is used for real time streaming of transactional data to detect the fraudulent transactions. This process considers different services which form the backbone of SOA. Further, five different machine learning classifiers namely support vector machine (SVM), multilayer perceptron (MLP), random forest regressor, autoencoder and isolation forest have been considered to identify the fraudulent activities instantly with the help of SOA based real time architecture.

THEORETICAL BACKGROUND

Below, we explain the classification algorithms that were used in this paper.

Decision Tree

A decision tree is a form of supervised machine learning that may be used for classification or regression tasks. It is particularly useful when the data can be separated based on specific parameters, and it provides a visual depiction of the potential answers. All decisions were contingent upon a multitude of conditions. The process begins at the root node and then diverges into several solutions, resembling a tree structure. The tree originates from the root, subsequently extending branches and progressively increasing in size. The primary concept is constructing a tree T based on our collection of observations S . If every element in set S is a member of class C , then the node is considered a leaf node and is assigned a label. Otherwise, the algorithm proceeds to the next characteristic that provides the most relevant information and constructs sub-trees until the desired objective is achieved. Firstly, it is necessary to establish the most informative attribute by utilising the entropy approach, which quantifies the uniformity of the collected data (Mohamed et al., 2020).

$$\text{Entropy } S = - \sum P(x) \log_2 P(x)$$

1

Also, the information gain that measures the relative change in entropy with respect to the independent attribute is given as:

$$\text{Gain}(S, A) = \text{Entropy}(S) - \sum_{v \in A} \frac{|S_v|}{S} \times \text{Entropy}(S_v)$$

2

Random Forest Algorithm

Random forest is a supervised ensemble method that uses a collection of numerous decision trees to make predictions (Shaik & Srinivasan, 2019). Random Forest is a classifier consisting of a set of tree-structured classifiers with identically distributed independent random vectors and each tree casting a unit vote at input x for the most popular class (Reis et al., 2018). A random vector that is independent of the previous random vectors of the same distribution is generated and a tree is generated using the training test, an upper bound is extracted for Random Forests to get the generalization error in terms of two parameters Exactitude and interdependence of individual classifiers (Yigin et al., 2020)

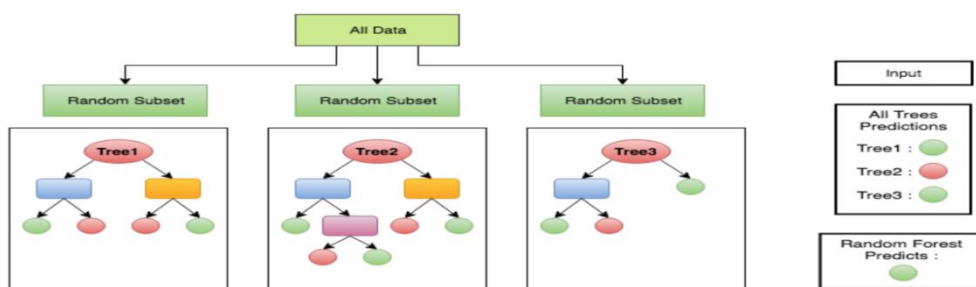


Figure 1: Random Forest Flow Chart (Arista, 2022).

The RF algorithm is very efficient, as it handles datasets that contain continuous variables, as well as categorical variables robustly. An RF classifier contains subsets of various tree classifiers $\{h(x, \Theta_k), k = 1, 2, \dots\}$ where the Θ_k are independently and identically distributed random vectors, with each tree being able to specify the modal class at input x (Tretiak et al., 2023). The performance index, which solely approximates the confidence interval (CI) of the RF model is given as

$$mg(x, y) = av_k I(h_k(x, \Theta_k) = y) - \max_{j \neq y} av_k I(h_k(x, \Theta_k) = j) \quad 3$$

where $I(\cdot)$ denotes an indicator function, and $av(\cdot)$, the average value. It is observed that as the margin increases, the confidence level also increases. The generalisation error becomes

$$PE^* = P_{x,y}(mg(x, y) < 0), \quad 4$$

where $P(\cdot)$ denotes probability. With an increase in trees for all sequences Θ_k , PE^* converges to

$$P_{x,y}(P_{\Theta}(h(x, \Theta) = y) - \max_{j \neq y} P_{\Theta}(h(x, \Theta) = j) < 0)$$

5

Convergence of this generalisation error proves that the RF model does not overfit as more trees are introduced. The upper bound for the generalisation error is given as

$$PE^* \leq \frac{\bar{\rho}(1-s^2)}{s^2},$$

6

where $\bar{\rho}$ is the average correlation value, s is the strength of each tree in the model. An increased strength of individual trees and a low correlation between them produces more accurate prediction results

MATERIALS AND METHODS

The system is designed such that, credit card comprehensive data will be collected from a simulated credit card transaction dataset containing legitimate and fraud transactions and preprocessed to normalize the data. Data sampling (Oversampling, undersampling and SMOTE) was done to cater for imbalanced data that may affect the performance of the model. Relevant features and variables were also identified that may influence the credit card fraud detection rate through exploratory data analysis and domain expertise. Machine learning models was built using two algorithms (Random Forest and Decision Tree) to detect credit card fraud, thus sending a real time notification of any fraudulent activity. The performance of the system was evaluated and interpreted using the evaluation metrics (Accuracy, F1 Score, Recall and Precision).

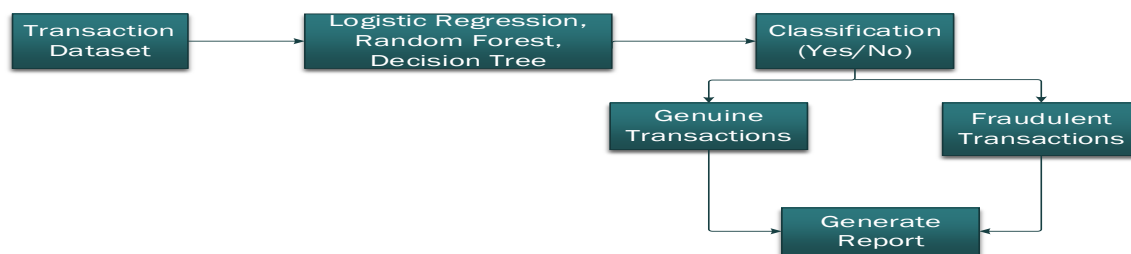


Figure 2: Design Framework

Data splitting: The dataset was divided into two distinct subsets: a Training set of 70% and a Test set of 30% of the data. The training set was for resampling, hyperparameter tuning, and training the model and the test set was used to test the performance of the trained model.

Data Resampling: This is use to handle the imbalanced dataset. If an imbalanced dataset is used, the model built tends to be biased towards the legitimate transactions, and hence, it results in the

poor performance of model when tested in an unseen data. To tackle this problem, three resampling techniques was used such as random undersampling, random oversampling, SMOTE. The resampling technique was implemented on the training data separately to make it balanced.

Algorithm Models: Random Forest and Decision Tree Classifier models was designed and trained using the preprocessed dataset. Three (3) sampling techniques was used (over sampling, undersampling and SMOTE) in order to balance the dataset.

Evaluation Metrics

Evaluation metrics is used for evaluating the performance of the model depending on the nature of the problem (whether it is a regression or classification). This thesis is limited to evaluation metrics related to the classification problem.

Confusion Matrix : It is the most commonly used evaluation metrics in predictive analysis mainly because it is very easy to understand and it can be used to compute other essential metrics such as accuracy, recall, precision, etc (Shakya, 2018). It is an NxN matrix that describes the overall performance of a model when used on some dataset, where N is the number of class labels in the classification problem (Tiwari, 2022). A confusion matrix is composed of statistics such as True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) which are calculated using the combination of actual and predicted values (Anand, Velu & Whig, 2022).

True Positive (TP) is a case where the actual value was positive (e.g., fraud) and the predicted value is also positive.

False Positive (FP) is a case where the actual value was negative (e.g., normal) but the predicted value is positive.

True Negative (TN) is a case where the actual value was negative (e.g., normal) and the predicted value is also negative.

False Negative (FN) is a case where the actual value was positive (e.g., fraud) but the predicted value is negative.

Recall: Recall, also known as sensitivity, is the fraction of true positives to the actual positive cases, which is shown in equation 7. In simple terms, recall is how many of true positives were found (recalled) out of all the true positive cases.

$$\text{Recall} = \frac{TP}{TP+FN}$$

7

Precision: As shown in equation , precision is the fraction of true positives over the true positives and false positives. In simple terms, precision is how many of the found cases were true positives.

$$\text{Precision} = \frac{TP}{TP+FP}$$

8

F1 Score: F1 Score also called F score or F-measure is the harmonic mean of the recall and precision (Hand, Christen & Kirielle, 2021). Its value ranges from 0 to 1, where 0 is considered worst, and 1 is considered best. It can be calculated as follows.

$$F1 = \frac{2 * (Precision * Recall)}{(Precision + Recall)}$$

9

Real Time Reporting: Twilio was be used in generating a real time text message if fraud is detected. Twilio is a web application programming interface (API) that can be used to add communications such as phone calling, messaging into Python applications.

Data Description

We utilised the open source data available at kaggle.com, namely the fraudTrain.csv file (Credit Card Transactions Fraud Detection Dataset, 2020). This file contains a simulated credit card transaction dataset that includes both valid and fraudulent transactions. It spans the period from 1st Jan 2019 to 31st Dec 2020 and includes the credit cards of 1000 customers who made transactions with 800 merchants. We imported required packages and plotted the distribution of each variable *trans_date_trans_time*, *cc_num*, *merchant*, *category*, *amt*, *first*, *last*, *gender*, *street*, *city*, *state*, *zip*, *lat*, *long*, *city_pop*, *job*, *dob*, *trans_num*, *unix_time*, *merch_lat*, *merch_long*, *is_fraud*. Also, analyzed the transaction patterns of the customers as shown in figure 3.

The numeric values in the dataset was looked into, to get a sense of what it was like. The output of the describe function on the dataset is shown in Figure 4.3.

	cc_num	amt	zip	lat	long	city_pop	unix_time
count	1296675.000000	1296675.000000	1296675.000000	1296675.000000	1296675.000000	1296675.000000	1296675.000000
mean	417192042079641088.000000	70.351035	48800.671097	38.537622	-90.226335	88824.440563	1349243636.726123
std	1308806447000789248.000000	160.316039	26893.222476	5.075808	13.759077	301956.360689	12841278.423360
min	60416207185.000000	1.000000	1257.000000	20.027100	-165.672300	23.000000	1325376018.000000
25%	180042946491150.000000	9.650000	26237.000000	34.620500	-96.798000	743.000000	1338750742.500000
50%	3521417320836166.000000	47.520000	48174.000000	39.354300	-87.476900	2456.000000	1349249747.000000
75%	4642255475285942.000000	83.140000	72042.000000	41.940400	-80.158000	20328.000000	1359385375.500000
max	4992346398065154048.000000	28948.900000	99783.000000	66.693300	-67.950300	2906700.000000	1371816817.000000

Figure 3: Snapshot of the Numerical Values in the Dataset (Describe Function Analysis)

Feature Engineering

The number of fraud per month was identified and analyzed as shown in figure 4.4

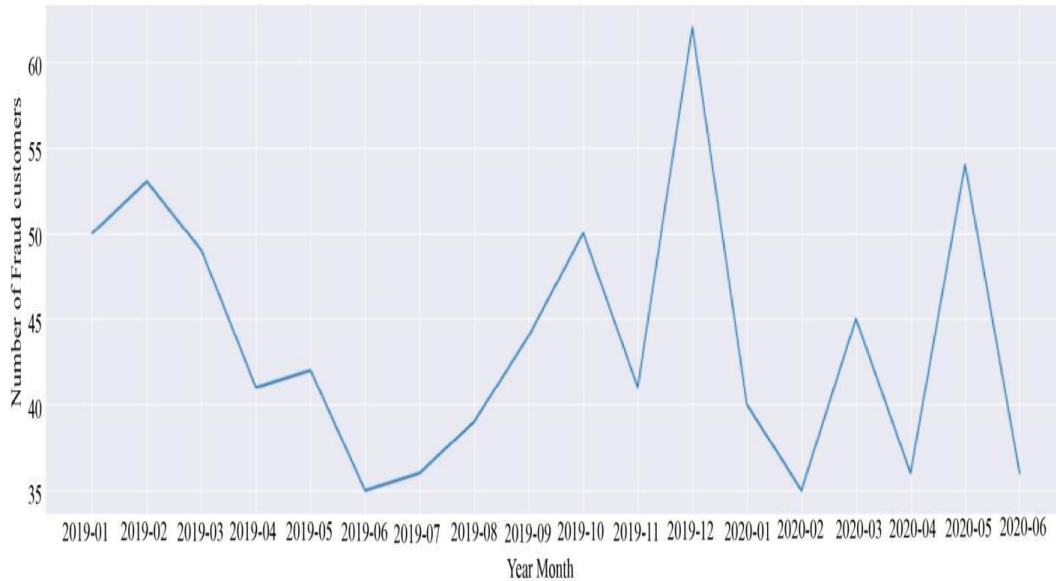


Figure 4: Number of Fraud Per Month

From the above visualizations it can be deduced that,

- i. Moreover, according to the 'trans_year_month' data, most transactions have happened in the January, February, October, December months of 2019 and in the May month of 2020.
- ii. Also, it can be noted that the number of fraud customers and the number of fraud transaction have increased in the time of December, which again is the holiday season.

Gender fraud distribution was grouped and plotted and age-fraud distribution was created as shown in Figures 5 and 6

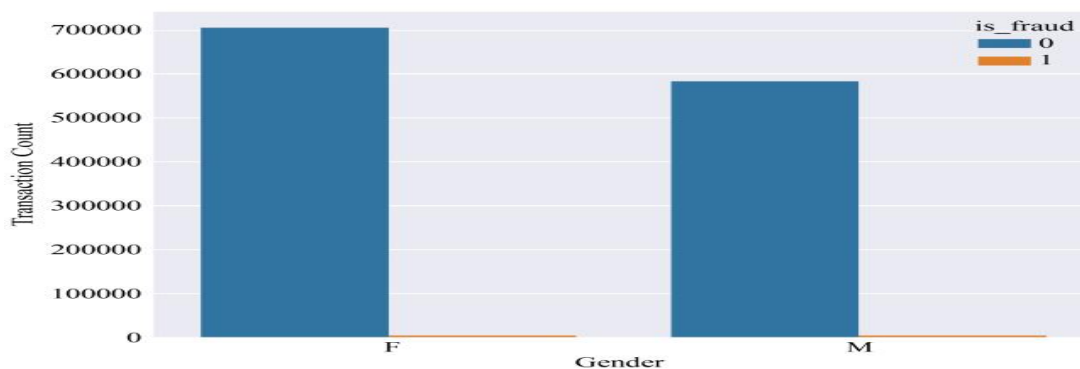


Figure 5: Distribution of Fraud Over Gender Chart

From the above visualization it can be observed that women contribute the most to the amount of the transaction frequencies. Although women do participate in fraud, the amount of women involved in fraud with respect to the number of transactions involving women is 0.52% whereas the same for men is about 0.64%. It can be concluded that women are involved in most of the transactions and hence, they be more prone to frauds.

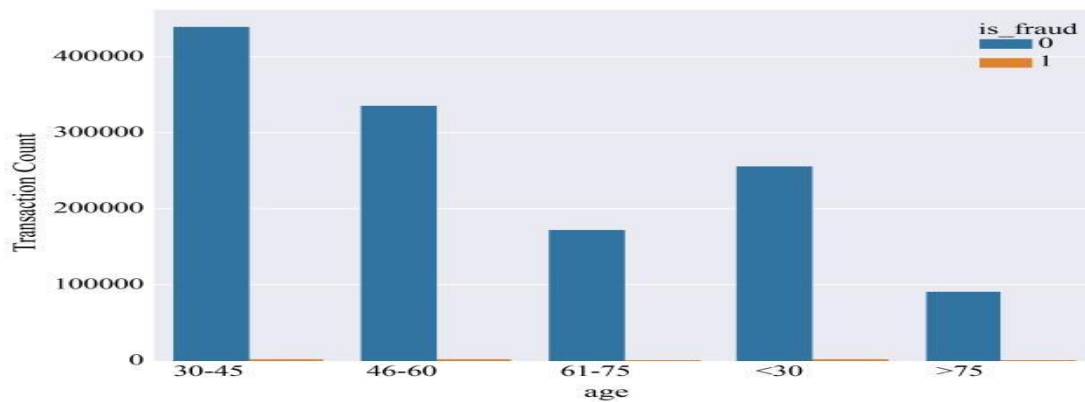


Figure 6: Age-Fraud Distribution Chart

From the plots it can be observed that the most number of transactions in the dataset have been done by the people in the 30-45 age group. Also, the 46-60 age group has done significant number of transactions. With respect to the total number of transaction made by a particular age group the people in the >75 age group are the most affected, wherein, about 1% transaction made by these people have been fraudulent.

3.3 Correlation Analysis of the Numeric Features

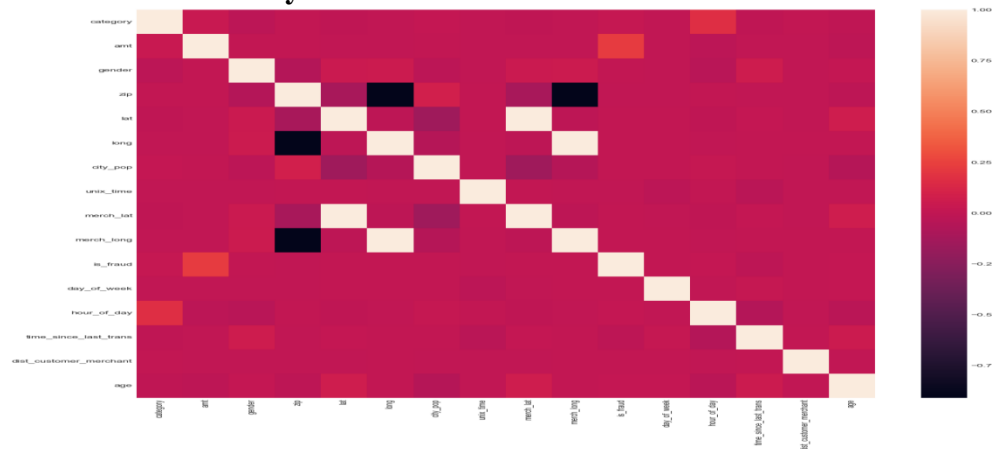


Figure 7: A Correlation Matrix of the Numeric Features

The main focus is on the correlation of the is_fraud column (indicating fraud) with other columns. The highest correlation value is approximately 0.22, indicating a positive correlation between the amt (transaction amount) and the likelihood of fraud (is_fraud). This suggests that higher transaction amounts might be associated with a slightly higher likelihood of fraud. There are some strong positive correlations, as indicated by coefficients close to 1: Strong positive correlation between unix_time (correlation of approximately 0.999). Strong positive correlation between long and merch_long, as well as between lat and merch_lat. This is likely due to the relationship between transaction locations and merchant locations. Most other correlations are close to 0, indicating weak or no linear relationships between the variables. For example, there are weak correlations between transaction locations (lat, long) and the target variable (is_fraud).

RESULTS AND DISCUSSIONS

Machine Learning Models and Performance Evaluation

Two algorithms were used on the processed dataset and three(3) sampling techniques (Oversampling, Undersampling and smote) to balance the dataset was used. Six (6) different models were created and used for the prediction of credit card fraud. The features 'zip', 'lat', 'long', 'city_pop', 'unix_time', 'merch_lat', and 'merch_long' have been assumed to provide no significant information in the model-building phase.

Decision Tree Classifier

Confusion Matrix for Decision Tree Classifier

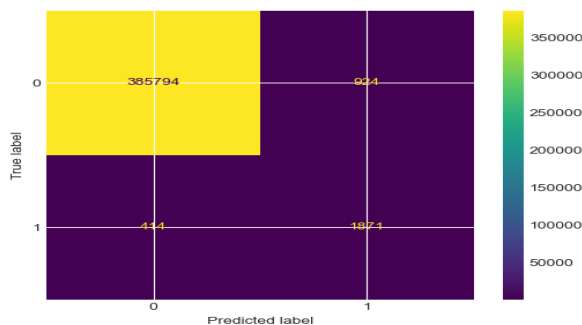


Figure 7: Decision Tree Confusion Matrix

From the figure 7 the model correctly identified 1871 instances as "isfraud", correctly identified 385794 instances as "notfraud", the model made 924 false positive predictions and the model made 414 false negative predictions.

Random Forest

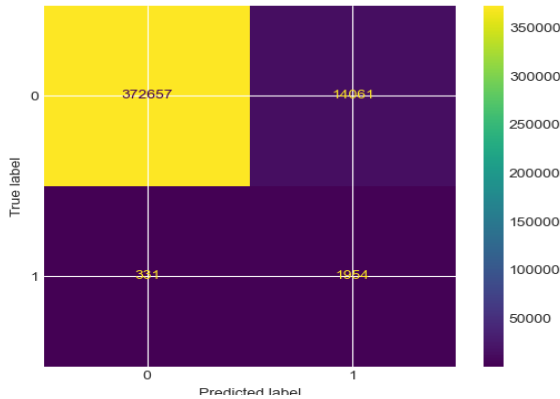


Figure 8: Confusion Matrix for Random Forest Classifier

From figure 8, implies that the model correctly identified 1954 instances as "isfraud".The model correctly identified 372657 instances as "notfraud", the model made 14061 false positive predictions and the model made 331 false negative predictions.

Table 1: Summary of all Classification Model

	Model Name	Trainin g Score	Testing Score	Accurac y	F1 Score	Precisio n	Recall
1	Decision Tree - imbalance class	0.99862	0.95426	0.998026	0.99794	0.89037	0.75711
2	Decision Tree -Random Under Sampling	0.98743	0.95426	0.954263	0.95426	0.95137	0.95729
3	Decision Tree -Random Over Sampling	0.99129	0.94610	0.946100	0.94610	0.93726	0.95524
4	Decision Tree -SMOTE[Hyperparameter Tuned]	0.99494	0.94021	0.940217	0.94021	0.95054	0.93010
5	Random Forest - imbalance class	0.99999	0.99825	0.998257	0.99814	0.95421	0.73873
6	Random Forest - Random Under Sampling	1.00000	0.96580	0.965808	0.96580	0.95511	0.95373
7	Random Forest - Random Over Sampling	1.00000	0.95497	0.954978	0.95496	0.96714	0.94117
8	Random Forest -SMOTE [Hyperparameter Tuned]	1.00000	0.95380	0.973804	0.95380	0.95511	0.95340

We used underfitting and overfitting, especially the imbalance dataset, to build and benchmark the model against those built with the SMOTE Hyperparameter dataset because

- i. To Evaluate Model Robustness: By comparing models trained on imbalanced datasets (which might lead to underfitting or overfitting) with those trained on SMOTE-enhanced datasets, we evaluated the robustness of the model. This comparison helps in understanding how well the model can generalize from the training data to unseen data.
- ii. To Demonstrate the Effectiveness of SMOTE: By benchmarking against models trained on imbalanced datasets, we demonstrated the effectiveness of SMOTE in improving model performance, especially in terms of metrics like precision, recall, and F1-score.
- iii. To Highlight the Challenge of Imbalanced Datasets: Imbalanced datasets are a common challenge in machine learning, where one class significantly outnumbers the other. By showing how models perform poorly on imbalanced datasets, we highlighted the need for techniques like SMOTE.
- iv. To Understand Model Behavior: Observing how a model overfits or underfits in the context of an imbalanced dataset can provide insights into its learning behavior. It can help in tuning the model or choosing a more appropriate model or technique for the given problem.

From table 1 a total of eight distinct models have been generated. Among the eight (8) models constructed, determine which model is the best based on Accuracy, F1 Score, Precision, and Recall, Random Forest - SMOTE [Hyperparameter Tuned] the highest accuracy (0.973804), the highest F1 Score (0.953805), which is a balanced measure of precision and recall, the highest precision (0.977211), indicating that when it predicted "isfraud," it was usually correct, highest recall (0.953737), indicating that it was effective at capturing a large proportion of "isfraud" cases. Therefore, Random Forest Classifier - SMOTE sampling with hyperparameter tuning is the optimal model for predicting credit card fraud in this work exhibiting an accuracy rate of 97.4%

Real Time Notification

Twilio was used in generating a real time text message if fraud is detected. The steps below was used to integrate Twilio the fraud detection system:

Detect Fraudulent Activity: The machine learning model (RF hyperparameter Tuned) will continuously monitor transactions or activities for signs of fraud.

Trigger an Alert: When the fraud detection system identifies a potentially fraudulent transaction or activity, it then an alert to notify the appropriate personnel or system.

Integrate Twilio: Integrate Twilio's API into the model. Twilio provides APIs for sending SMS messages programmatically.

Craft the Message: The default message was defined to notify when a fraud is detected. For this research, the crafted message is "Fraudulent transaction detected on your credit card! Please contact your bank immediately".

Testing and Validation: The model was tested with integration with Twilio to ensure that messages are sent accurately and in a timely manner. The snippet code for the testing and validation is given below

```
# Make a prediction using the trained model
prediction = model.predict(transaction_data)

# If fraud is detected, send a text message alert
if prediction == 1:
    message = client.messages.create(
        body="Fraudulent transaction detected on your credit card! Please conta
        from_=' ',
        to=' '
    )
    print(message.sid)
```




Figure 9: Sample of Simulated SMS Alert

DISCUSSION

Various features of the data set have been analyzed and several insights have been obtained. The 'trans_date_trans_time' feature has been broken down into several components like 'Age', 'day of the week', 'month' in order to facilitate our analysis. These features have been thoroughly analyzed. It has been found that old age people above 75 years are more susceptible to frauds. This is because, fraudsters might try to take advantage of their lack of knowledge about the constantly changing ways of how transactions are made.

The 'Female' gender people have been observed to do much of the transaction according to the dataset. Hence, transactions involving might be much prone to fraud. Also, by analyzing several demographic variables like city, state, zip etc it has been found that, several places like 'DE' state has 100% fraud rate and about 50 zip codes and 70 cities have 100% fraud rate. There might be some ill practices happening at the ground level at these places since all the transactions happening there are shown as fraudulent.

Two (2) different algorithms have been implemented upon the processed dataset. Three sampling techniques in order to balance the dataset have also been implemented. The algorithms have also been implemented upon the dataset before balancing the dataset for demonstration purposes. Hence, six (6) different models have been created the results of which have been summarized above. Out of the 6 models that have been built, the Random Forest Classifier built using the SMOTE sampling technique after hyper parameter tuning has provided the most preferable model

with a accuracy of 0.97, f1 score of 0.95 and precision of 0.98. Hence, it can be said the the Radom Forest Classifier - SMOTE [Hyperparameter Tunned] sampling is the best model. Further, the model (Radom Forest Classifier - SMOTE [Hyperparameter Tunned]) was tested with integration with Twilio and the message was sent accurately and in a timely manner.

The result of this study has higher accuracy compared to a result of Thennakoon et al. (2019) that reported that the machine learning models (LR, NB, LR and SVM) used in detecting credit card fraud captured the four fraud patterns (Risky MCC, Unknown web address, ISOResponse Code, Transaction above 100\$)with an accuracy rate of 74%, 83%, 72% and 91% accuracy rates respectively. This findings also corroborates the result in More et al. (2021) that reported an accuracy of 97% when compared with Decision Tree and Naive Bayes Technique for credit card fraud detection using supervised learning approach.

CONCLUSION AND RECOMMENDATION

The analysis and model development for fraud detection have provided valuable insights and a robust solution for real time identifying and responding to fraudulent activities. The combination of data analysis, feature engineering, and the selection of an effective machine learning model has resulted in a powerful fraud detection system. The "Random Forest Classifier - SMOTE [Hyperparameter Tuned]" model, along with Twilio integration, provides a comprehensive solution for detecting and responding to fraud in a timely and accurate manner. This system is well-equipped to safeguard against fraudulent transactions and protect both the business and its customers. Based on the findings from this study, the following recommendations were made:

- i. Continuous use and deploy the "Random Forest Classifier - SMOTE [Hyperparameter Tuned]" model as the primary fraud detection model. It has demonstrated strong performance across multiple metrics, including accuracy, F1 score, and precision
- ii. Maintain the integration with Twilio for real-time SMS alerts. This is to ensure that the alerting system is continuously monitored and tested to confirm its reliability and responsiveness.
- iii. Perform periodic evaluations of the fraud detection model's performance to ensure its effectiveness in detecting evolving fraud patterns. Revisit and retrain the model as necessary to adapt to changing circumstances.
- iv. Continue to explore and engineer features that could enhance the model's predictive capabilities by considering additional data sources or variables that may provide valuable insights into fraud detection.
- v. Implement a robust monitoring and reporting system to track the model's performance in a real-world environment. Ensure that alerts are acted upon promptly and that false positives/negatives are reviewed and addressed

Contributions and Limitation

The work demonstrates the application of various machine learning models and data sampling techniques for fraud detection. It provides insights into which techniques are most effective in handling imbalanced datasets and improving the accuracy of fraud detection systems. It also showcases the importance of feature engineering and in-depth data analysis in understanding transaction patterns and identifying potential fraud indicators. Breaking down transaction timestamps and analyzing demographic variables offer valuable insights. The integration of the fraud detection model with Twilio for real-time SMS alerts demonstrates a practical and proactive approach to fraud prevention. It showcases how technology can be leveraged to respond swiftly to potential fraudulent activities. The emphasis on continual improvement underscores the dynamic nature of fraud detection. It encourages organizations to adapt and evolve their strategies to stay ahead of fraudsters.

However, the research is limited by the availability of real life and historical data credit fraud data. The data used was an open source dataset for training and evaluating the machine learning algorithms. Also, another limitations is the potential challenges associated with adapting the model to evolving fraud patterns and the need for continuous model updates. Another limitation of the research is the potential for false positives, where legitimate transactions are incorrectly flagged as fraudulent.

Suggestion for Further Studies

More research can be done to explore the application of deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), for fraud detection. Deep learning models can capture intricate patterns in data and may improve fraud detection accuracy. Further research can be done by combining multiple data sources, such as transaction data, user behavior data, and network logs, to create a multi-modal fraud detection system. Fusion techniques can improve accuracy by leveraging complementary information. More work can be done to investigate the challenges and opportunities of fraud detection in real-time data streams, where transactions and events are continuously generated. Implement stream processing techniques for timely detection. Investigation of advanced feature engineering techniques can be explored, including natural language processing (NLP) for analyzing transaction descriptions and customer reviews, to extract valuable information for fraud detection.

REFERENCES

- Abakarim, Y., Lahby, M. and Attioui, A., 2018, October. An efficient real time model for credit card fraud detection based on deep learning. In Proceedings of the 12th international conference on intelligent systems: theories and applications (pp. 1-7).
- Abdulghani, A., 2022. Employing machine learning techniques and fuzzy membership for detecting fraud transactions in credit card (Master's thesis, Altınbaş Üniversitesi/Lisansüstü Eğitim Enstitüsü).

- Abdulghani, A.Q., Uçan, O.N. and Alheeti, K.M.A., 2021, December. Credit card fraud detection using XGBoost algorithm. In 2021 14th International Conference on Developments in eSystems Engineering (DeSE) (pp. 487-492). IEEE.
- AlEmad, M., 2022. Credit Card Fraud Detection Using Machine Learning.
- Anand, M., Velu, A., & Whig, P. (2022). Prediction of loan behaviour with machine learning models for secure banking. *Journal of Computer Science and Engineering (JCSE)*, 3(1), 1-13.
- Anowu, D.N., Nyor, T., Agbi, S.E., Nelson, A.I. and Saliu, A.N., 2021. Financial forensic analysis and fraud deterrence in listed deposit money banks in NIGERIA. *Gusau Journal of Accounting and Finance*, 2(4), pp.18-18.
- Arista, A., 2022. Comparison Decision Tree and Logistic Regression Machine Learning Classification Algorithms to determine Covid-19. *Sinkron: jurnal dan penelitian teknik informatika*, 7(1), pp.59-65.
- Ashraf, M., Abourezka, M. A., & Maghraby, F. A. (2022). A Comparative Analysis of Credit Card Fraud Detection Using Machine Learning and Deep Learning Techniques. In *Digital Transformation Technology: Proceedings of ITAF 2020* (pp. 267-282). Springer Singapore.
- Connect, C. (2023, May 12). Over £1.2bn Lost to Fraud in 2022. Credit Connect. Retrieved November 30, 2023, from <https://www.credit-connect.co.uk/news/consumer-lending/fraud/over-1-2bn-lost-to-fraud-in-2022/>
- Credit Card Transactions Fraud Detection Dataset*. (2020). Kaggle. <https://www.kaggle.com/datasets/kartik2112/fraud-detection?select=fraudTrain.csv>
- Fraud in Nigerian Financial Services” 2021 <https://nibss-plc.com.ng/media/PDFs/post/NIBSS%20Insights%20Fraud.pdf>
- Hand, D. J., Christen, P., & Kirielle, N. (2021). F*: an interpretable transformation of the F-measure. *Machine Learning*, 110(3), 451-456.
- Hasan, M., Islam, M.M., Zarif, M.I.I. and Hashem, M.M.A., 2019. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*, 7, p.100059.
- Ileberi, E., Sun, Y. and Wang, Z., 2022. A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, 9(1), pp.1-17.
- Krishna, M.V. and Praveenchandar, J., 2022, October. Comparative analysis of credit card fraud detection using logistic regression with random forest towards an increase in accuracy of prediction. In 2022 International Conference on Edge Computing and Applications (ICECAA) (pp. 1097-1101). IEEE.
- Kumar, A., Prusti, D., Purusottam, I.S. and Rath, S.K., 2021, July. Real time SOA based credit card fraud detection system using machine learning techniques. In 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
- Lavanya, K., 2023. A Comparison of Logistic Regression Classifier and Random Forest Classifier for the Accurate Classification of Credit Card Fraudulent Transactions. *Journal of Survey in Fisheries Sciences*, 10(1S), pp.2008-2017.

- Mohamed, S., Ashraf, R., Ghanem, A., Sakr, M. and Mohamed, R., Supervised Machine Learning Techniques: A Comparison.
- More, R., Awati, C., Shirgave, S., Deshmukh, R., & Patil, S. (2021). Credit card fraud detection using supervised learning approach. *International journal of scientific & technology research*, 9(10), 216-219.
- Mullen, C. (2023). *Card industry's fraud-fighting efforts pay off: Nilson Report*. Payments Dive. <https://www.paymentsdive.com/news/card-industry-fraud-fighting-efforts-pay-off-nilson-report-credit-debit/639675/>
- NIBSS Insight, "fraud in nigerian financial services" 2021 <https://nibss-plc.com.ng/media/PDFs/post/NIBSS%20Insights%20Fraud.pdf>
- Ogundokun, R.O., Misra, S., Ogundokun, O.E., Oluranti, J. and Maskeliunas, R., 2021. Machine learning classification based techniques for fraud discovery in credit card datasets. In *Applied Informatics: Fourth International Conference, ICAI 2021, Buenos Aires, Argentina, October 28–30, 2021, Proceedings 4* (pp. 26-38). Springer International Publishing.
- Paul, E. (2021). In 2020, Nigeria Lost ₦5b to Fraud in 9 Months: What You Need to Watch Out For. *Techpoint Africa*. Retrieved November 30, 2023, from <https://techpoint.africa/2021/02/22/nigeria-lost-5b-fraud-2020/>
- Popat, R.R. and Chaudhary, J., 2018, May. A survey on credit card fraud detection using machine learning. In *2018 2nd international conference on trends in electronics and informatics (ICOEI)* (pp. 1120-1125). IEEE.
- Reis, I., Baron, D. and Shahaf, S., 2018. Probabilistic random forest: A machine learning algorithm for noisy data sets. *The Astronomical Journal*, 157(1), p.16.
- Shaik, A.B. and Srinivasan, S., 2019. A brief survey on random forest ensembles in classification model. In *International Conference on Innovative Computing and Communications: Proceedings of ICICC 2018, Volume 2* (pp. 253-260). Springer Singapore.
- Shakya, R. (2018). *Application of machine learning techniques in credit card fraud detection* (Doctoral dissertation, University of Nevada, Las Vegas).
- Sudha, C. and Akila, D., 2021, January. Credit card fraud detection system based on operational & transaction features using svm and random forest classifiers. In *2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM)* (pp. 133-138). IEEE.
- Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., & Kuruwitaarachchi, N. (2019, January). Real-time credit card fraud detection using machine learning. In *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 488-493). IEEE
- Tiwari, A. (2022). Supervised learning: from theory to applications. In *Artificial intelligence and machine learning for EDGE computing* (pp. 23-32). Academic Press.
- Tretiak, K., Schollmeyer, G. and Ferson, S., 2023. Neural network model for imprecise regression with interval dependent variables. *Neural Networks*, 161, pp.550-564.

European Journal of Computer Science and Information Technology, 12 (4),36-56, 2024

Print ISSN: 2054-0957 (Print),

Online ISSN: 2054-0965 (Online)

Website: <https://www.eajournals.org/>

Publication of the European Centre for Research Training and Development -UK

Yigin, B.O., Algin, O. and Saygili, G., 2020. Comparison of morphometric parameters in prediction of hydrocephalus using random forests. Computers in Biology and Medicine, 116, p.103547.