International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 6 Issue 7, November-December 2022 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Credit Cards Frauds and Cybersecurity Threats: Machine Learning Detection Algorithms as Countermeasures

Obodoeze Fidelis C.[1], Oliver Ifeoma Catherine[2], Onyemachi George Olisamaka[2], Udeh Ifeanyi Frank Gideon[3], Obiokafor, Ifeyinwa Nkemdilim[4]

[1]Department of Computer Engineering, Akanu Ibiam Federal Polytechnic Unwana, Ebonyi State, Nigeria
[2]Department of Computer Science, Akanu Ibiam Federal Polytechnic Unwana, Ebonyi State, Nigeria
[3]Department of Computer Science, Federal College of Agriculture, Ishiagu, Ebonyi State, Nigeria
[4]Department of Computer Science, Anambra State Polytechnic, Mgbakwu, Anambra State, Nigeria

ABSTRACT

Credit and Debit cards have become the choice mode of payment online as a result of the proliferation of electronic transactions and advancement in Information and Communication Technology (ICT). Because of the increased use of credit cards for payment online, the number of fraud cases associated with it has also increased; scammers and fraudsters are stealing credit card information of victims online and thereby stealing their monies. There is the need therefore to stop or abate these frauds using very powerful fraud detection system that detects patterns of credit card frauds in order to prevent it from occurring. In this paper we x-rayed the concept of credit card frauds and how they are carried out by fraudsters. Python 3.7.6 programming language, Jupyter Notebook 6.0.3 and Anaconda Navigator 1.9.12 were used as experimental test bed. Also, we implemented two different supervised machine learning algorithms on an imbalanced dataset such as Decision Tree and Random forest techniques. A comparative analysis of the credit card detection capabilities of these machine learning algorithms were carried out to ascertain the best detection algorithm using different performance evaluation metrics such as accuracy, precision, recall, f1 score, confusion matrix. Experimental results showed that Random Forest outperformed Decision Tree algorithm slightly in performance metrics used for performance evaluation.

KEYWORDS: *Credit Card frauds, Accuracy, f1 score, precision, recall, support, fraud detection, fraud patterns, machine learning algorithms*

How to cite this paper: Obodoeze Fidelis C. | Oliver Ifeoma Catherine | Onyemachi George Olisamaka | Udeh Ifeanyi Frank Gideon | Obiokafor, Ifeyinwa Nkemdilim "Credit Cards Frauds and Cybersecurity Threats: Machine Learning Detection Algorithms as Countermeasures" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-6 | Issue-7, December 2022, pp.940-948, URL: www.ijtsrd.com/papers/ijtsrd52440.pdf

IJTSRD52440

1. INTRODUCTION:

Cybersecurity is becoming increasingly significant in our daily lives. When addressing digital life security, the main issue is identifying anomalous behavior. When making purchases from online e-commerce stores or conducting business online, many people frequently prefer using credit cards as well as debit cards. Occasionally, we can make purchases even when we don't have the cash on hand thanks to credit card credit limitations.

On the other hand, scammers and online attackers abuse these features. To solve this problem, there is need for a system that can abort the transaction if it finds anything fishy or anomalous patterns in the whole financial transaction.

Here, a system that can monitor the patterns of all transactions is required, and if any patterns are abnormal, the transaction should be stopped or terminated.

Credit card information should always be kept private or confidential. Information about credit card privacy should not be compromised. Phishing websites, stolen or lost credit cards, fake credit cards, the theft of card information, intercepted cards, etc. are some examples of ways to steal credit card information (Anderson, 2007). The aforementioned activities should be avoided for security reasons. Online fraud simply requires the card information and takes place

remotely. At the time of purchase, neither a manual signature nor a PIN or card imprint are necessary. The legitimate cardholder is typically unaware that someone else has seen or stolen his or her card information.

The easiest way to spot this kind of fraud is to examine each card's purchasing habits and look for any deviations from the "normal" spending habits. The greatest strategy to lower the number of successful credit card frauds is to detect fraud by examining the current cardholder data purchases. Since the outcomes are not made public and the data sets are unavailable. The logged data and user behavior are two data types that can be used to identify fraud incidents. Currently, a variety of techniques, including data mining, statistics, and artificial intelligence, are used to detect fraud.

Currently, there are many supervised machine learning approaches based on Artificial Intelligence (AI) that can classify odd or anomalous transactions. The only prerequisites are historical data and an algorithm that can more closely match the data.

In order to identify frauds and potential cyber risks, decision tree and random forest machine learning (ML) algorithms were utilized in this paper to identify unusual or odd and unexpected patterns in credit card transactions. The performance of the two ML algorithms is evaluated experimentally using a variety of performance evaluation criteria, including accuracy, precision, recall and F1 score**.**

1.1. How Credit Card Fraud works

Credit cards are very important in making purchases online especially when finances are not readily available. Credit cards are one of the most popular financial tools used to make online purchases and payments for commodities such as electronic gadgets such TVs, computer hardware and software, website domain registration and hosting, mobile phones, fuel, groceries, air ticket booking, books hotels and other items. When using credit cards for various purchases, they are most valuable because they offer numerous rewards in terms of points. Making payments with credit cards is equally easy and seamless. But the challenge of using credit cards for online payments is as a result of activities of hackers and scammers. According to ProjectPro (2022), today's credit card fraud falls into a number of different categories:

- **Lost or stolen cards:** Online shopping credit cards are stolen and used fraudulently on the owner's behalf. The process of canceling stolen credit cards and reissuing them is difficult for both customers and credit card providers. Several banking organizations limit the use of credit cards until it is certain that the card's legitimate owner has received it.
- **Card Abuse:** The customer uses a credit card to make purchases, but he or she has no intention of returning the money that the bank has charged for those purchases. When the due date for payment approaches, some customers quit returning calls. They even occasionally file for bankruptcy; every year, this kind of scam causes losses in the millions to banks.
- **Identity Theft:** Customers submit false information while applying for credit cards, and they may even steal the personal information of a real client to do so. Even card blocking cannot prevent the credit card from getting into the wrong hands in such circumstances.
- **Merchant Abuse:** Some online merchants display fictitious unlawful transactions to facilitate money laundering. Legal information of legitimate credit card customers is stolen to create counterfeit cards and be used for these illegal transactions.

Fig.1 shows a comprehensive list of credit card frauds that can compromise the cybersecurity of credit cards and financial systems.

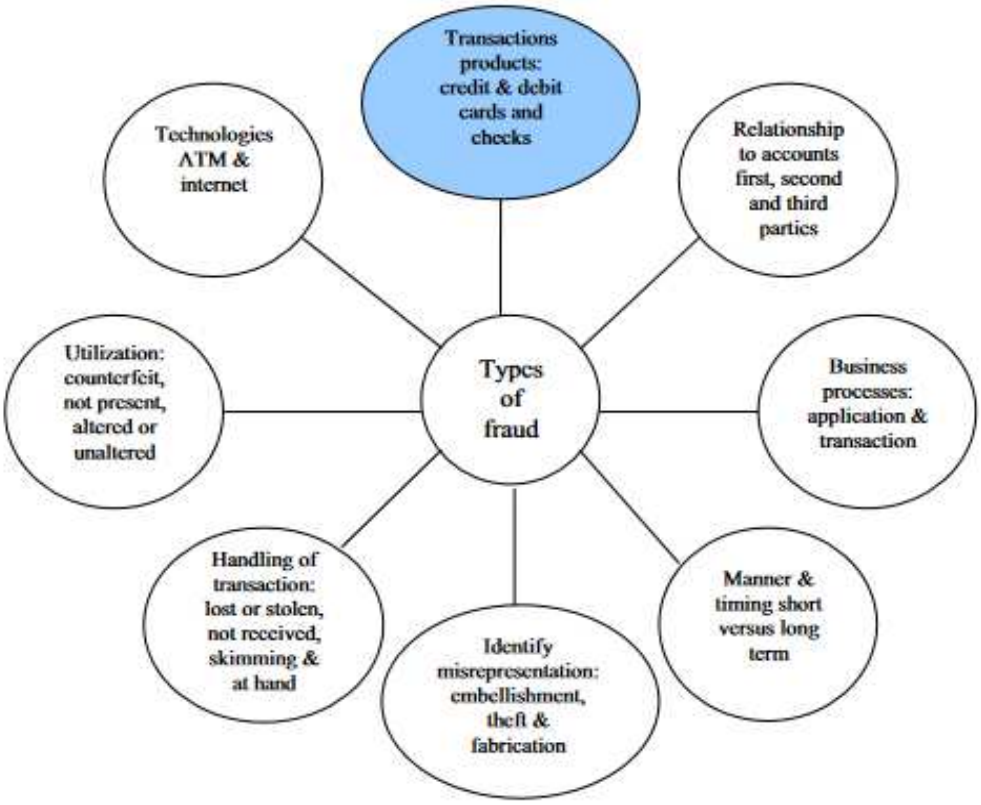

Fig.1. Types of Fraud (Anderson, 2007)

To identify credit card fraud, several traditional, obsolete techniques have been used since the dawn of time, including CVV verification, geolocation tracking, IP address verification, etc. However, since thieves improve their skills with time, it is challenging to put an end to them all using only traditional methods. In today's environment, when millions of transactions occur every second, human intelligence is incapable of processing all the data and identifying the patterns of behavior of fraudsters. Machine learning-based credit card fraud detection is essential in this situation.

Financial organizations are increasingly depending on automated machine learning algorithms to make informed judgments and prevent large losses. These safety measures greatly reduce the risk involved in conducting online transactions. Machine learning algorithms use historical transaction data to appraise present and future transactions in a manner similar to how people do. Despite the fact that computers may not be as intelligent as people and may need some additional supervision, the speed at which data is processed and calculations are performed is an advantage. Machines are also more adept than people at recognizing and recalling patterns in vast volumes of data. Anomaly detection is the term most often used to describe these methods.

1.2. Credit Card Fraud Detection Techniques using Machine Learning

In the past, credit card fraud has been identified using the following machine learning techniques:

- **Unsupervised Learning** - Algorithms for machine learning, such as Isolation Forest, One-class SVM, LOF, etc., train models without the need of labeled training data. They look for patterns in the data and attempt to group the data points based on apparent similarities in patterns.
- **Supervised Learning –** These machine Learning Algorithms include KNN, Artificial Neural Networks (ANNs), Auto encoders, Random Forest, XGBoost, LightGBM, etc. These algorithms learn to anticipate the labels or patterns for the unobserved data by training on labeled data. It can be costly and difficult to collect labeled data for machine learning modeling.

2. Materials and Methods

In this paper, we used Supervised Learning ML algorithms such as Decision Tree, Random Forest and XGBoost to perform modeling experiments in Python 3.7.6 and Jupyter Notebook 6.0.3 in order to detect credit card patterns that are abnormal and unusual that may contain some frauds in the credit card dataset.

The historical credit card dataset used in the experiments contains transactions made by credit cards in September 2013 by European cardholders.

This dataset presents transactions that occurred in two days, where we have 492 frauds out of 284,807 transactions. The dataset was downloaded online at https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud. Fig. 2 shows the methodology adopted in the experiments.

The system architecture of the proposed machine learning method is shown in Fig.3.

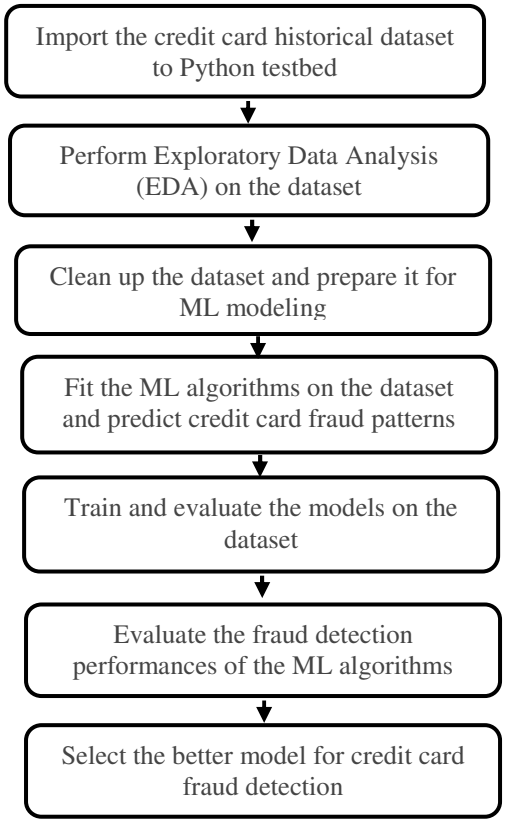

Fig. 2: Credit card fraud detection methodology using Machine Learning Algorithms

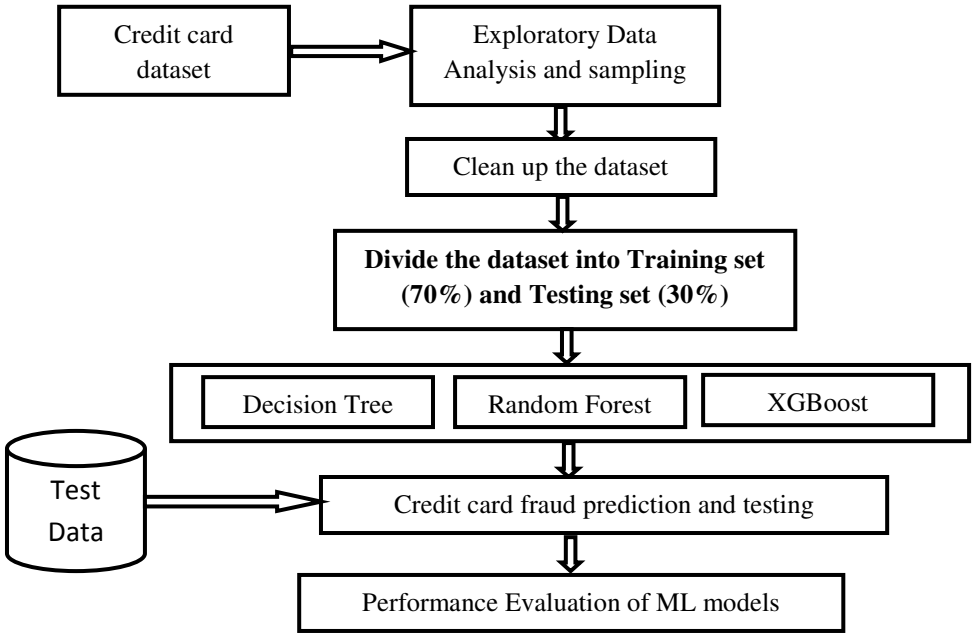

Fig. 3: Credit card fraud detection system architecture

The following tools were used for the programming and modeling of the credit card detection models using machine learning algorithms:

- Python – 3.7.6
- Numpy – 1.19.2
- Scikit-learn – 0.24.1
- Matplotlib – 3.3.4
- Anaconda Navigator 1.9.12
- Jupyter Notebook 6.0.3

Algorithm steps for finding the Best algorithm for Credit fraud detection:

Step1: Import the credit card dataset into Pandas data frame
Step2: Convert the data into data frames format suitable for machine learning modeling
Step3: Do random sampling
Step4: Split dataset into training set (70%) and testing set (30%)
Step5: Fit the training dataset to the machine learning algorithms
Step6: Apply the algorithms to the training dataset and create the prediction models
Step7: Make Credit card fraud prediction for test dataset for each algorithm
Step8: Compute the performance metrics for each machine learning algorithm

Random Forest ML algorithm:

Random forest (one of the most popular algorithms) is a supervised machine learning algorithm. It creates a "forest" out of an ensemble of "decision trees", which are normally trained using the "bagging" technique. The bagging method's basic principle is that combining different learning models improves the prediction outcome.

To get a more precise and reliable forecast, random forest creates several decision trees and merges them. Fig.4 shows the Random Forest algorithm's anomaly detection technique using majority class rule.

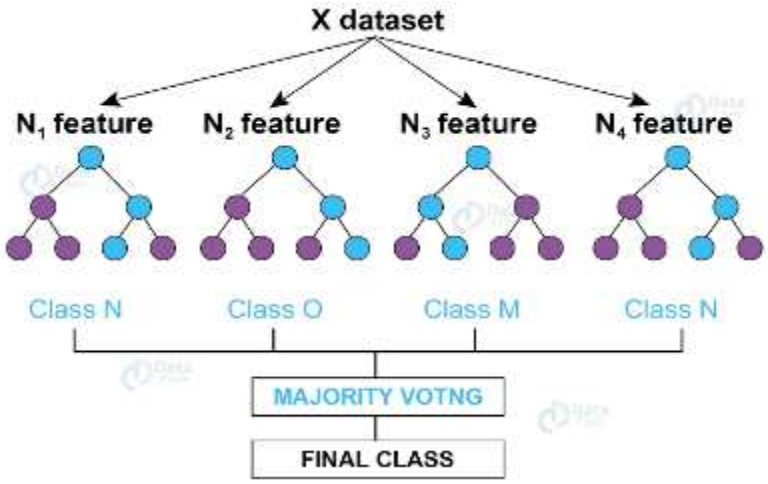

Fig 4: Random Forest anomaly detection using Majority class technique

Decision Tree ML algorithm:

A decision tree is a non-parametric supervised learning algorithm, which is utilized for both classification and regression tasks. It has a hierarchical, tree structure, which consists of a root node, branches, internal nodes and leaf nodes (IBM, 2022).

The experiments were carried out in Anaconda Navigator running Python 3.0 and Tensorflow environment as shown in Fig. 5.

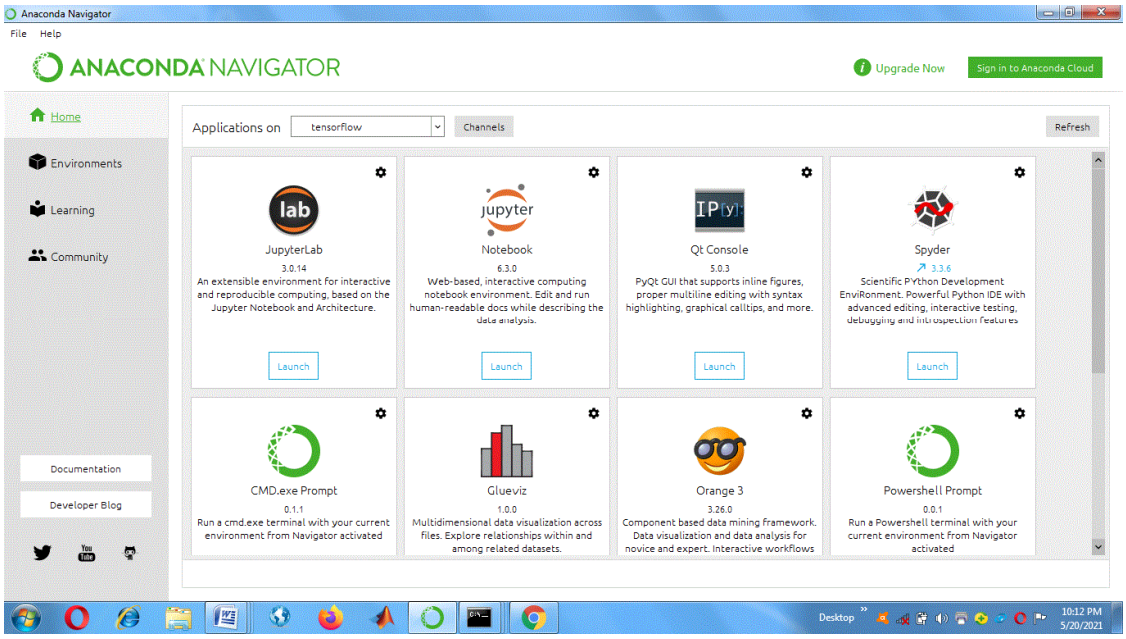

Fig.5: Anaconda Navigator Development Environment for Python

2.1. Exploratory Data Analysis

Exploratory data analysis (EDA) was carried out in Python 3, Jypyter Notebook and several statistical data analysis tool. Figs. 6 and 7 show the credit card data analysis carried out in Pandas dataframe.

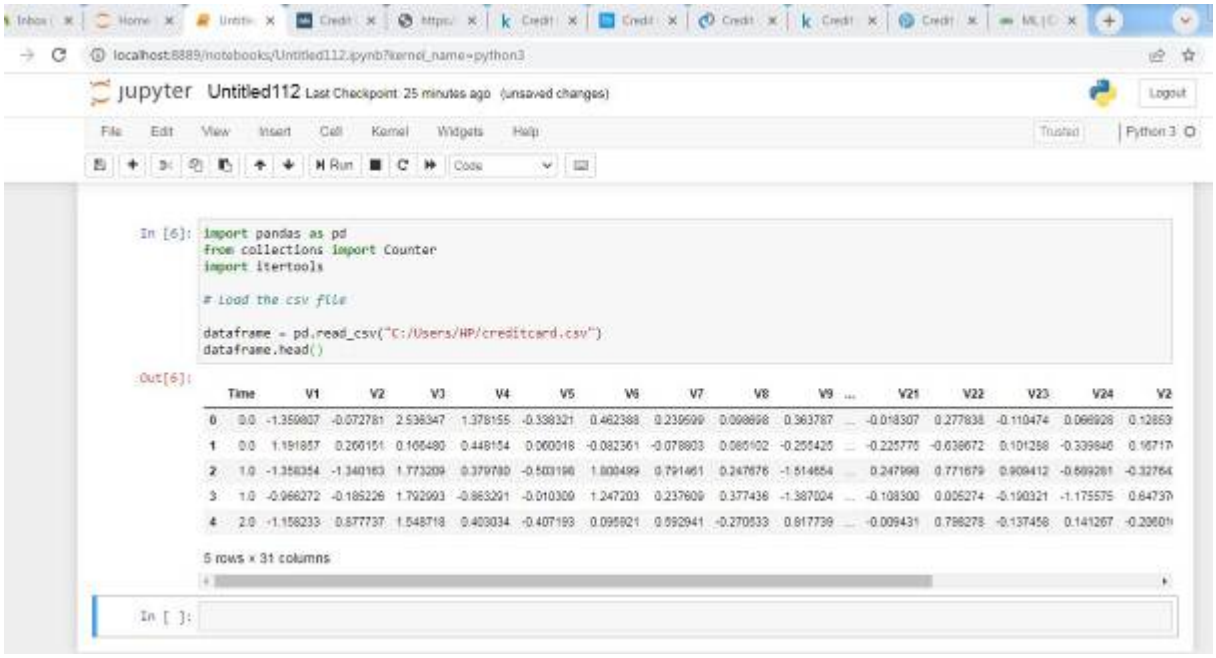

Fig. 6: Data Analysis showing credit card dataframe in Pandas

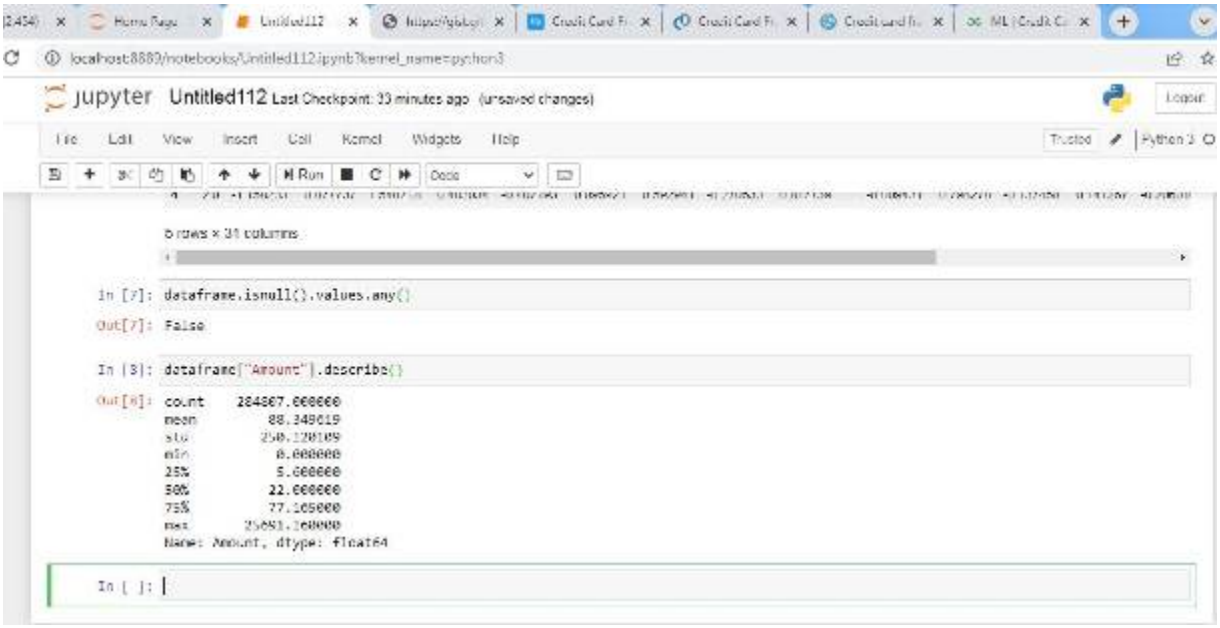

Fig.7: Data Analysis showing data types in Pandas

Fig.8 shows the printout of the percentage of credit card frauds in the database used for the experiments.

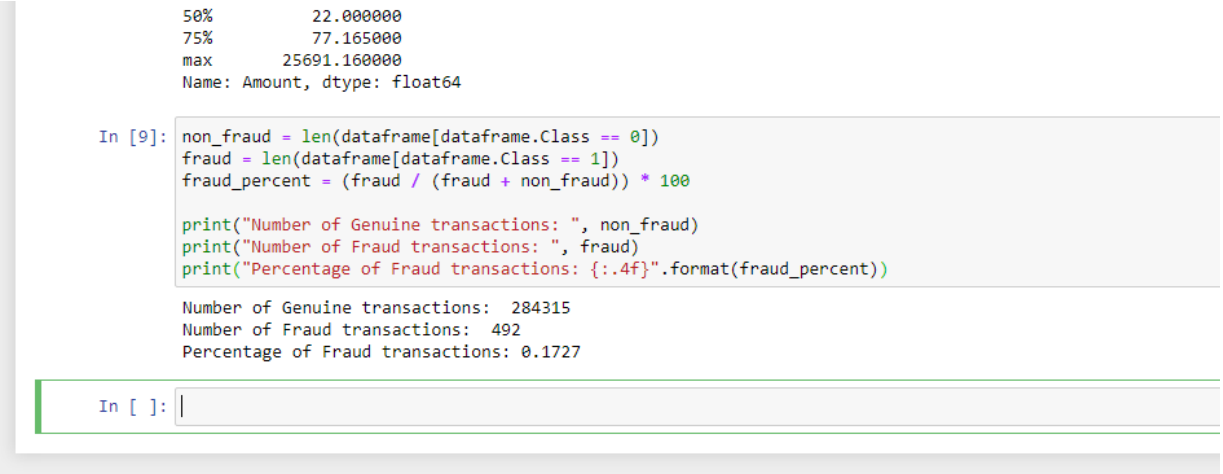

Fig.8: Data Analysis showing percentage of credit card incidences in the dataset

Fig.9 shows the printout of the dataset ratio split used for the experiments. The dataset was divided into two sets, training set was allocated 70% while testing and evaluation set was allocated 30%.

```
Y = dataframe["Class"]
X = dataframe.drop(["Class"], axis= 1)

In [12]: from sklearn.model_selection import train_test_split

         (train_X, test_X, train_Y, test_Y) = train_test_split(X, Y, test_size= 0.3, random_state= 42)

         print("Shape of train_X: ", train_X.shape)
         print("Shape of test_X: ", test_X.shape)

         Shape of train_X:  (199364, 29)
         Shape of test_X:  (85443, 29)

In [ ]: |
```

Fig.9: The Dataset split into Training and Testing ratio

Performance Evaluation Tools:

The following performance evaluation metrics were used to evaluate the credit card prediction performances of the machine learning algorithms used in this paper. These metrics (Accuracy, Precision, Recall and F1- Score) are calculated using True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN) parameters.

When TP is likely to cause most kidney issues in a kidney patient; FPs will likely find that the rate at which kidney disease is detected is the rate at which a healthy person is found. TN hopes to reveal that a person with kidney disease is healthy. FN is prescribed when a healthy man or woman has kidney disease.

Accuracy:

Accuracy is the proportion of instances that are accurately classified. It is one of the most popular performance measures for machine learning categorization.

$$\text{Accuracy} = \frac{\text{Number of correct predictions}}{\text{Total Number of predictions}} = \frac{TP+TN}{TP+TN+FP+FN} \quad \ldots\ldots\ldots\ldots (1)$$

Where TP, TN, FP and FN are referred to as True Positives, True Negatives, False Positives and False Negatives respectively as used in binary classification machine learning tasks.

Precision:

Precision is the number of classified Positive or fraudulent instances that actually are positive instances.

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

Recall:

Recall is a metric that measures the proportion of accurate positive predictions among all possible positive predictions. Recall gives an indicator of missed positive predictions, unlike precision, which only comments on the accurate positive predictions out of all positive predictions. The number of true positives divided by the sum of true positives and false negatives is used to determine recall.

$$Recall = \frac{TP}{TP+FN} \quad \ldots\ldots\ldots\ldots (3)$$

F1-Score:

F1 Score is the weighted average of Precision and Recall. Therefore, this score takes both false positives and false negatives into account.

$$F1\text{-}Score = \frac{2*(Recall * Precision)}{(Recall + Precision)} \quad \ldots\ldots\ldots\ldots (4)$$

3. Results and Discussions

This section describes the results obtained from several experiments as carried out in the testbed. Fig. 9 shows the modeling prediction of credit card fraud by Decision Tree and Random Forest machine learning algorithms.

```
#Decision Tree
decision_tree = DecisionTreeClassifier()

# Random Forest
random_forest = RandomForestClassifier(n_estimators= 100)
```

```
In [15]: decision_tree.fit(train_X, train_Y)
predictions_dt = decision_tree.predict(test_X)
decision_tree_score = decision_tree.score(test_X, test_Y) * 100

random_forest.fit(train_X, train_Y)
predictions_rf = random_forest.predict(test_X)
random_forest_score = random_forest.score(test_X, test_Y) * 100

print("Random Forest Score: ", random_forest_score)
print("Decision Tree Score: ", decision_tree_score)
```

```
Random Forest Score:  99.96137776061234
Decision Tree Score:  99.93211848834895
```

```
In [ ]:
```

Fig. 10: Modeling prediction results for credit card frauds by Decision Tree and Random Forest Algorithms

From Fig.10, it is clear that Random Forest algorithm outperformed the Decision Tree Algorithm by Accuracy Score of 99.96% while Decision Tree scored 99.93%.

We also carried out another experiment to comprehensively evaluate the performance of the Decision Tree and Random Forest algorithms using standard performance evaluation metrics such as Accuracy, precision, Recall and f1-score. Fig.11 and Table 1 shows the performance evaluation results obtained for Decision Tree algorithm. Decision Tree performed very well in credit card pattern detection with Accuracy score of 0.99932 or 99.93% and Precision of 0.76712, Recall=0.82353 and F1-score of 0.79433.

```
In [17]: print("Evaluation of Decision Tree Model")
print()
metrics(test_Y, predictions_dt.round())
```

```
Evaluation of Decision Tree Model

Accuracy: 0.99932
Precision: 0.76712
Recall: 0.82353
F1-score: 0.79433
```

```
In [ ]:
```

Fig. 11: Modeling prediction performance evaluation for Decision Tree Algorithm

Table 1: Decision Tree credit card fraud detection results

Performance Metric	Score
Accuracy	0.99932
Precision	0.76712
Recall	0.82353
F1-score	0.79433

Fig.12 and Table 2 show the performance evaluation results obtained for Random Forest algorithm. Random Forest performed very well (better than Decision Tree algorithm) in credit card pattern detection with Accuracy score of 0.99961or 99.96% and Precision of 0.94783, Recall=0.80147 and F1-score of 0.86853.

```
In [19]: print("Evaluation of Random Forest Model")
print()
metrics(test_Y, predictions_rf.round())
```

```
Evaluation of Random Forest Model

Accuracy: 0.99961
Precision: 0.94783
Recall: 0.80147
F1-score: 0.86853
```

```
In [ ]:
```

Fig. 12: Modeling prediction performance evaluation for Random Forest Algorithm

Table 2: Random Forest credit card fraud detection results

Performance Metric	Score
Accuracy	0.99961
Precision	0.94783
Recall	0.80147
F1-score	0.86853

Table 3 shows the comparative prediction performances between Decision Tree and Random Forest algorithms. It is very clear here that Random Forest outperformed Decision Tree algorithm in credit card fraud detection with higher Accuracy, Precision and F1-score and lower Recall score.

Table 3: Comparison of credit card frauds prediction performances between Decision Tree and Random Forest algorithms

Performance Metric	Score	ML Algorithm
Accuracy	0.99932	Decision Tree
	0.99961	Random Forest
Precision	0.76712	Decision Tree
	0.94783	Random Forest
Recall	0.82353	Decision Tree
	0.80147	Random Forest
F1-score	0.79433	Decision Tree
	0.86853	Random Forest

4. Summary and Conclusion

In this paper, we built a binary classifier using three machine learning algorithms such as Random Forest and Decision Trees classifiers to detect credit card fraud transactions. Through this project, we understood and applied techniques to address the class imbalance issues and achieved an accuracy of more than 99%.

We applied different performance evaluation metrics such as Precision, Recall, f1-score, support and accuracy to evaluate the performance of the two Machine learning algorithms. Our comparative performance evaluation shows that Random Forest outperformed the Decision Tree algorithm in credit card fraud patterns detection.

The results obtained from the experiments show that Machine learning classification algorithms such as Decision Tree and Random Forest are well suited to detect any credit card fraud before it occurs.

4.1. Future Scope

Future experiments will be carried to determine the performances of hybrid ensemble machine learning algorithms by combining ensemble algorithms such as XGBoost, Random Forest with Decision Trees algorithm in carrying out fraud detection in credit cards.

References:

[1] Anderson, R. 2007. The Credit Scoring Toolkit: theory and practice for retail credit risk management and decision automation. New York: Oxford University Press.

[2] IBM (2022).” What is a decision Tree?”. Retrieved online at https://www.ibm.com/topics/decision-trees

[3] ProjectPro (2022).”How does Credit Card Fraud work?”. Accessed online at https://www.projectpro.io/article/credit-card-fraud-detection-project-with-source-code-in-python/568