National College of Ireland

Online Payment Fraud Detection using Machine Learning Techniques

MSc Research Project
Data Analytics

Taranjyot Singh Chawla
Student ID: X21153078

School of Computing
National College of Ireland

Supervisor: Prof. Jorge Basilio

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Taranjyot Singh Chawla
Student ID:	X21153078
Programme:	Data Analytics
Year:	2022
Module:	MSc Research Project
Supervisor:	Prof. Jorge Basilio
Submission Due Date:	15/12/2022
Project Title:	Online Payment Fraud Detection using Machine Learning Techniques
Word Count:	XXX
Page Count:	19

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	1st February 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Online Payment Fraud Detection using Machine Learning Techniques

Taranjyot Singh Chawla
X21153078

Abstract

When it comes to the simplicity of making a payment while sitting anywhere in the world, online payments have been a source of attractiveness. Over the past few decades, there has been an increase in online payments. E-payments enable businesses earn a lot of money in addition to consumers. However, because electronic payments are so simple, there is also a risk of fraud associated with them. A consumer must ensure that the payment he is paying is going exclusively to the appropriate service provider. Online fraud exposes users to the possibility of their data being compromised, as well as the inconvenience of having to report the fraud, block their payment method, and other things. When businesses are involved, it causes some issues; occasionally, they must issue refunds in order to keep customers. Therefore, it is crucial that both consumers and businesses are aware of these internet scams. A model to determine if an online payment is fraudulent or not is put forth in this study. To determine if a certain Online payment is fraudulent or not, some features like the type of payment, the recipient's identity, etc. would be taken into account.

1 Introduction

Online payments have become more popular during the last few decades. This is because it's so simple to send money from anywhere, but the pandemic has also contributed significantly to the rise in e-payments. Numerous studies have demonstrated that e-commerce and online payments will continue to grow in popularity in the years to come. The risk of online payment fraud has also increased as a result of this rise in online payments. Online payment fraud has been shown to have increased over the past few years, making it crucial for consumers and service providers to be aware of these frauds. It is crucial for users to be certain that the payments they make are going to the legitimate recipients; otherwise, they run the risk of having to report fraud, freeze their payment method, and run the chance of having their data shared with criminals, which could occasionally result in more crimes. On the other hand, it's crucial for companies to check that their customers aren't giving money to these fraudsters. Businesses may have to repay money to clients in order to keep their patronage, which puts a strain on them. Even though firms have created and introduced numerous fraud detection programs, only a small number of them are effective in identifying online payment fraud. Although companies make every effort to make the payment method as secure as possible, fraudsters occasionally manage to circumvent security measures and commit these online payment scams. According to

studiesZanin et al. (2018), from 2014 to 2017, the cumulative losses from fraudulent bank card transactions increased globally. Other studiesKalbande et al. (2021) concentrate on idea drift, which refers to the possibility of change in the dataset's underlying distribution over time. Similar to how cardholders or users may alter their purchasing patterns over time, these fraudsters may modify their tactics. These fraudsters are always aware of the customers' payment methods and behavior, but occasionally their tactics become outdated with time as some professionals work round-the-clock to uncover these scams and shield people from them. Fraud is an illegal technique to obtain somethingYan et al. (2021), thus it's important to have in place an effective fraud detection system (FDS) that keeps track of all transactions and looks for any indication of fraud. The investigator looks into these potentially fraudulent transactions and reports back on whether or not the transaction was actually fraudulent. Machine learning techniques were used to determine if a transaction is fraudulent or not. Data mining techniques were typically used to analyze the patterns of fraudulent and non-fraudulent transactionsWang et al. (2015). Therefore, by analyzing the patterns of the data, a combination of data mining techniques and machine learning can be utilized to determine if transactions are fraudulent or real.
Hence, the research question for this study would be- "How far may machine learning methods be utilized to determine whether a specific online transaction is fraudulent or not based on selected features?".

2 Related Work

The synthesis of models for identifying fraudulent transactions in online payments is a challenging task given the large number of studies that have been conducted using various data sets and produced disparate results. These involve determining the issues with obtaining the data, getting the extracted data ready, selecting the appropriate processing procedure, deciphering the outcomes, and analyzing the same Kolodiziev et al. (2020). The actual payment data is incredibly sensitive because it contains very sensitive private information on customers or users, and only the companies in charge of handling these data are permitted access to this data. Ranjan et al. (2022)

2.1 Research on the variables that affect credit card theft in online transactions

It is crucial for consumers and organizations to ensure the security of transactions and the private data they include in today's world, when there are numerous transactions occurring every second.Rai and Dwivedi (2020) These thefts are typically carried out when utilizing credit cards to make purchases. This study focuses on credit card fraud detection when making online purchases.

2.2 Change in Techniques

These scammers' techniques change with time. Users learn that a certain transaction appears to be fraudulent as a result of the popularity of some approaches or procedures over time. The behavior of users or cardholders also evolves with time, making it challenging for new technology to keep up with fraud detection or protection. Therefore, it is crucial

that the algorithms are updated frequently to keep up with these shifts in fraudsters' strategies.Saputra and Suharjito (2019). In order to create models, real-time 3 data is needed, but obtaining this data is challenging since it contains private information that can only be shared with corporations that collect payments and third-party companies that store the data.

2.3 Protection of privacy

Numerous research are being conducted using the data in a way that protects privacy. One of the experiments was carried out using blockchain technology and machine learning techniques, according to Kalbande et al. (2021). The usage of block chain technology, however, can be helpful in protecting the privacy of the data, but we cannot ignore the fact that it is a decentralized solution and has some drawbacks along with it, such as scalability issues and high energy consumption. A supervised machine learning strategy utilizing block chain technology was developed by Thennakoon et al. (2019). Ethereum was employed by the author to implement block chain technology. 300,000 accounts were used in the study, and the outcomes were compared with a number of machine learning techniques. Additionally, studies utilizing the federated learning and gossip learning paradigms were conducted. Kolodiziev et al. (2020)It was determined that gossip learning is unsuccessful because it lacks a central management structure. However, because of its semi-decentralized nature, the federated learning technique, also known as the F.L., was deemed effective and performed better. According to Jain et al. (2020), the two transfers where frauds are most prevalent are Cash Out and the ones where money is transferred to a merchant before being transferred to users or occasionally, unknowingly, to fraudsters. The first transfer involves money being transferred from one user to another, a fraudster, or a customer. The second transfer is where frauds are most prevalent. In their assessment of various machine learning algorithms for the identification of frauds when using credit cards, Yee et al. (2018) Accuracy, precision, and specificity criteria were used to assess how well each technique performed in the study. This research also focuses on suggesting a model that makes use of the supervised Random Forest algorithm to improve the precision of identifying credit card payment fraud. Random Forest produced results with a precision of 99.7 percent and an accuracy of 96.2percent. Thennakoon et al. (2019) study of the fraud detection system, which consists of three key parts: the data warehouse, the API module, and the fraud detection models In this study, each of these elements played a simultaneous role. Real-time transactions must be passed between the fraud-detection model, data warehouse, and GUI via the API Module. The output of the machine learning models and the real-time transactions are both stored in a data warehouse. The GUIs, which display fraud alerts for real-time transactions, make it simple for consumers to interact with the fraud detecting system. When the model identifies a specific transaction as fraudulent, a message is displayed on the API module. Additionally, the user receives a message from the API, and their feedback is saved for later examination. The study by Singh et al. (2021) suggests an unique fraud detection system that can identify four different types of fraudulent transactions using the most appropriate algorithm. Rambola et al. (2018) studied the blending of data from many databases and stored it in a suitable format so that data mining techniques could be used on it. The information can be used by any organization where decision-making is necessary in order to identify the fraudulent transactions after further analysis of the data. Neural networks are also used in this study to identify fraudulent transactions.

The sum of all bank transactions is combined to identify clusters. According to Zanin et al. (2018), similar customers are grouped together to have the same data for similar types of customers, which makes it easier to analyze the data further. For example, if one customer or user of a particular area and job requests some specific service from the financial institute. The consumer behavior of each individual user is examined by Bahnsen et al. (2016) as they build a fraud detection model. Additionally, it shows that by pre-processing the data and including recent user behavior, the model's performance improves by roughly 200 percent when compared to the raw data from the transactions. Wang et al. (2015). This work suggests two ensemble learning approaches, OOB and UOB, by using re sampling and a time-decayed measure in order to address the issue of online class imbalance. The sampling rate appears to be commensurate with the degree of imbalance in the data stream. The data distribution turns out to be a significant element determining the models' performance. Saputra and Suharjito (2019). Most of these fraud detection systems produce positive results, but many of them produce false positive results, or in other words, they flag particular transactions as fraudulent even though they are not.Behera and Panigrahi (2015) . Companies find it difficult since they don't want their customers to feel constrained all the time. This study suggests using neural networks and fuzzy clustering. It groups related data sets using the fuzzy c-means clustering technique, and then employs the neural network technique to reduce the classification rate. The investigation is conducted by using the fuzzy c-means technique to input vectors.

2.4 Study on factors influencing frauds in online transaction using credit cards

In order to predict fraudulent transactions, Singh et al. (2021) concentrated on using machine learning techniques like KNN, SVM, and Random Forest. When compared to the other algorithms employed in this study, Random Forest comes out to be the most accurate, with a 99.9 percent accuracy rate. Random forest also comes out to have the lowest rate of false alarms related to fraudulent transactions. Although Jain et al. (2020) did not use real-time data, it may still be useful in the future to help organizations like banks become aware of these scams. Ileberi et al. (2021)applied the AdaBoost method in addition to some supervised machine learning techniques like logistic regression, decision trees, and support vector machines (SVM) (2021). AdaBoost was primarily used to increase the performance of classifiers when employed singly in terms of performance metrics like accuracy and area under the curve (AUC). The XGB-AdaBoost produces an MCC of 0.99 and addresses the dataset's class imbalance as well. It might be argued that using AdaBoost has a beneficial impact on machine learning models. ? It focuses on the confusion matrix, which serves as a basis for performance measurement, and studies the identification of fraudulent transactions when using a credit card. Multiple measurements are provided, including sensitivity, specificity, accuracy, and error rate. In this study, Logistic Regression and XGBoost were applied, and it was discovered that the cross validation score for LR was 94.16 percent and the cross validation score for XGBoost was 93.76 percent. While XGBoost's AUC score was 93.55 percent, LR's was 94 percent. However, since just 10percent of the transactions in the dataset were used, a lot of information was reported to have been lost in this study, which still has room for development. The outcomes might alter if the same techniques were used on the entire dataset. For financial institutions and IT specialists, resolving the issue of rising

criminality due to online payments is a big challenge. Kaur et al. (2021). This study focuses on using machine learning to address this problem. Additionally, it employs a number of data mining algorithms, including CART, C4.5, Naive Bayes, and many others. Using various patterns found by machine learning models, the study seeks to distinguish between legitimate and illegal transactions.Yan et al. (2021)

3 Methodology

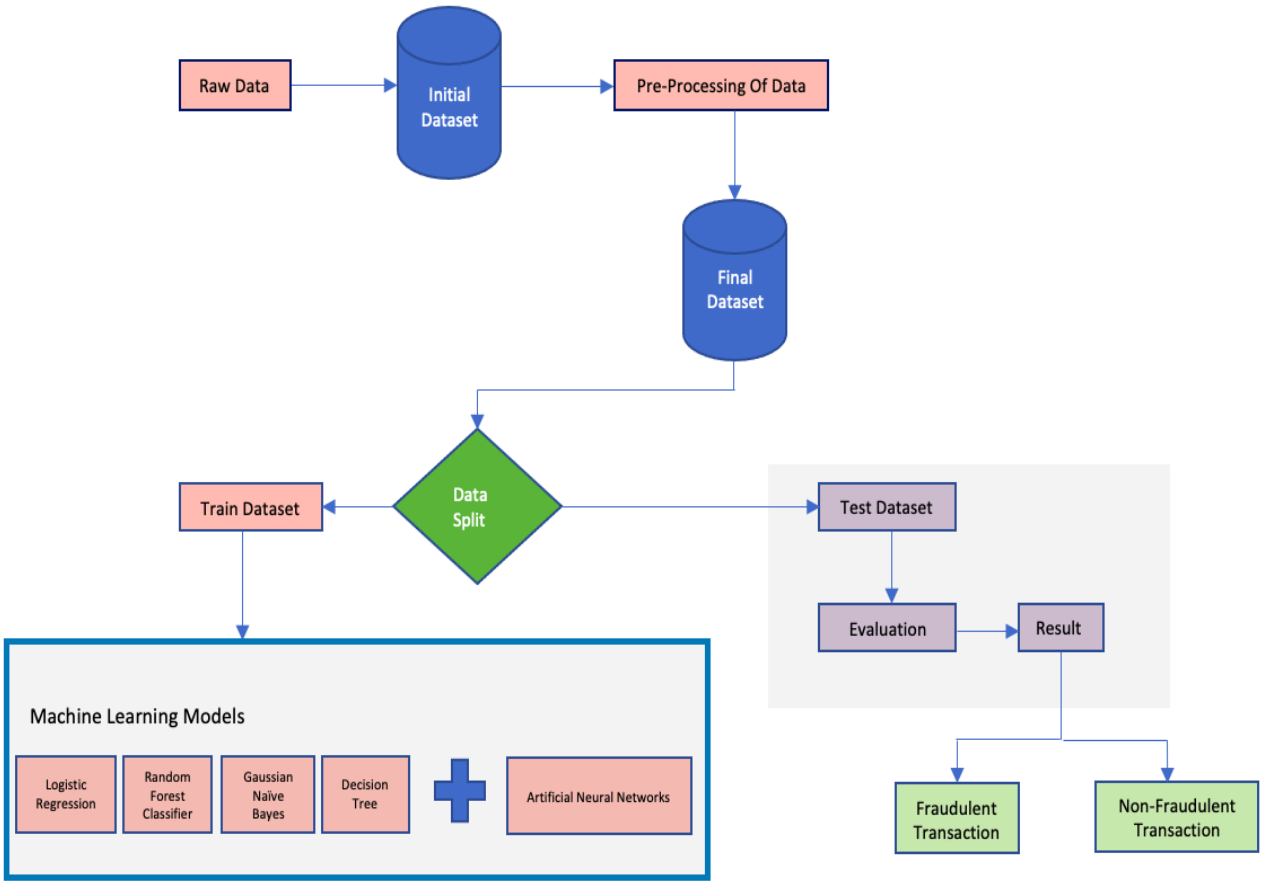

Figure 1: Flowchart of Proposed Implementation

When it comes to finding fraudulent online payment transactions, data analysis is crucial. Banks and other financial institutions can adapt the required defences against these frauds with the aid of machine learning techniques. Many businesses and organizations are investing a lot of money in the development of these machine learning systems to determine whether a specific transaction is fraudulent. Machine learning techniques assist these organizations in identifying frauds and preventing their clients who may be at risk for such frauds and occasionally sustain losses as a result.
The research's data set came from the open platform "kaggle." Due to privacy concerns, it is challenging to obtain real-time data sets; therefore, a data collection big enough to conduct the research was taken. The data set has 1048576 records and 11 columns. This data set includes attributes like type (type of payment), amount, "nameOrig" (customer initiating the transaction), "pldbalance- Org" (balance before the transaction), "newbalanceOrig" (balance after the transaction), "nameDest" (recipient of the transaction),

"pldbalanceDest" (initial recipient balance prior to the transaction), "newbalanceDest" (the new balance recipient after the transaction), and isFraud which (0 if the transaction is legitimate and 1 if the transaction is fraudu- lent). The figure2. shows all the features

step	type	amount	nameOrig	oldbalanceOrg	newbalanceOrig	nameDest	oldbalanceDest	newbalanceDest	isFraud	isFlaggedFraud
1	PAYMENT	9839.64	C1231006815	170136.00	160296.36	M1979787155	0.0	0.00	0	0
1	PAYMENT	1864.28	C1666544295	21249.00	19384.72	M2044282225	0.0	0.00	0	0
1	TRANSFER	181.00	C1305486145	181.00	0.00	C553264065	0.0	0.00	1	0
1	CASH_OUT	181.00	C840083671	181.00	0.00	C38997010	21182.0	0.00	1	0
1	PAYMENT	11668.14	C2048537720	41554.00	29885.86	M1230701703	0.0	0.00	0	0
1	PAYMENT	7817.71	C90045638	53860.00	46042.29	M573487274	0.0	0.00	0	0
1	PAYMENT	7107.77	C154988899	183195.00	176087.23	M408069119	0.0	0.00	0	0
1	PAYMENT	7861.64	C1912850431	176087.23	168225.59	M633326333	0.0	0.00	0	0
1	PAYMENT	4024.36	C1265012928	2671.00	0.00	M1176932104	0.0	0.00	0	0
1	DEBIT	5337.77	C712410124	41720.00	36382.23	C195600860	41898.0	40348.79	0	0

Figure 2: Dataset

in the dataset. Whether a particular transaction is fraudulent or not depends highly on the type of the trasaction, figure 3 below shows the types of transactions and the percentage of the same in our dataset.

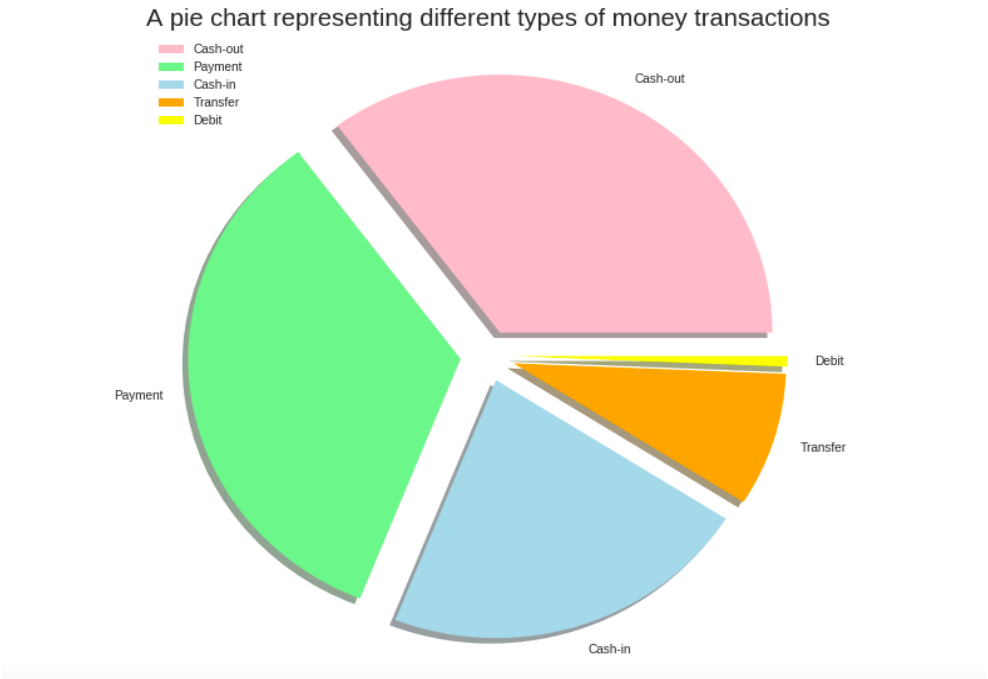

Figure 3: Dataset

3.1 Analysing Missing values:

Before using the data in the model, it is important to pre-process the data downloaded from the dataset. The next step is to check for any missing values in our dataset. It can be seen in the figure 4. that there are no missing values in our dataset.

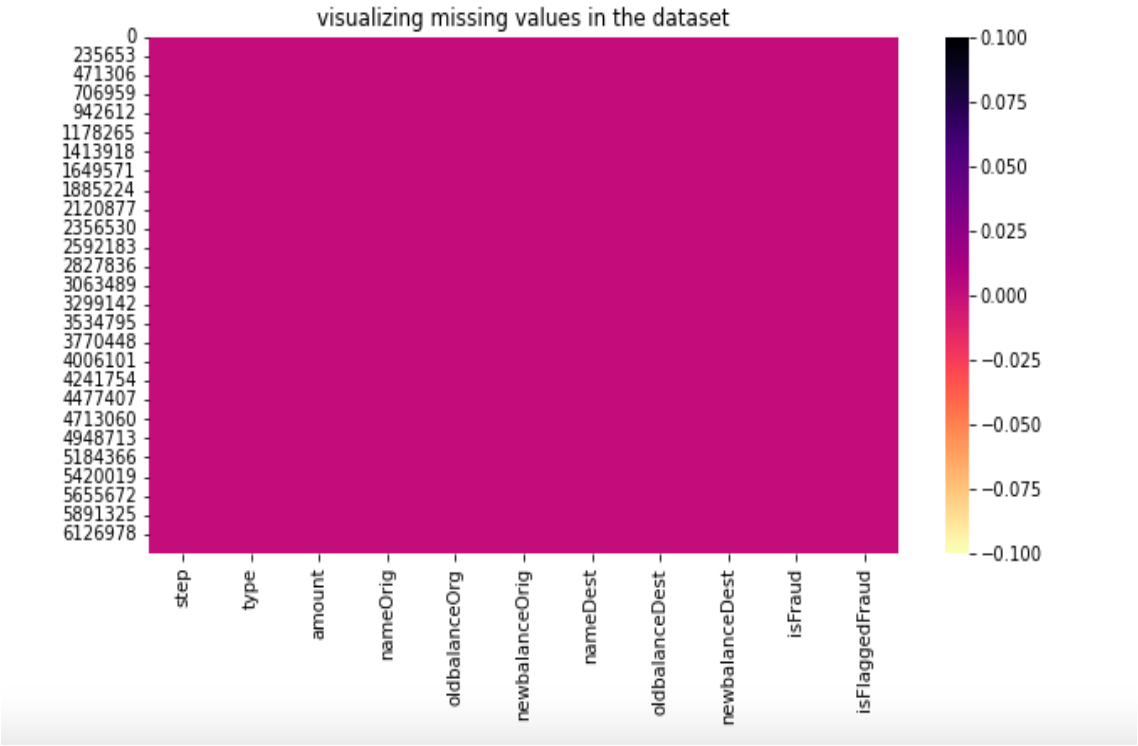

Figure 4: Missing Values

3.2 Investigating target distribution:

By looking at the distribution of our target feature "isfraud" it is clear that there is a huge class imbalance in our data.

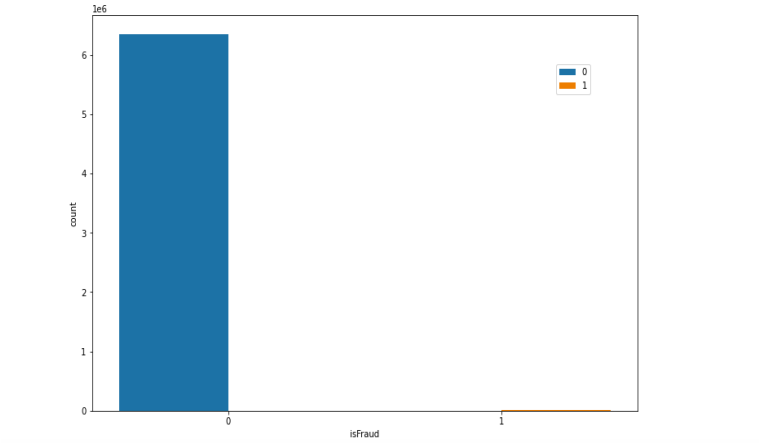

Figure 5: Class Imbalance

As shown in the figure 5 only 8213 transactions are recorded to be fraudulent while 6354407 transactions are recorded to be Non Fraudulent, We would take care of this imbalance between classes in later stages to make sure it does not have any negative impact on our machine learning models.

3.3 Investigating the Correlation between the Features:

Even though our data has a large number of features, not all of them are contributing to our target feature. Figure 5 shows how the features are related to each other. With the help of the correlation matrix, we have narrowed down the list of important features that can help us predict our target feature.However, we will again train the models including all the features which were rejected earlier to compare the results of the models.

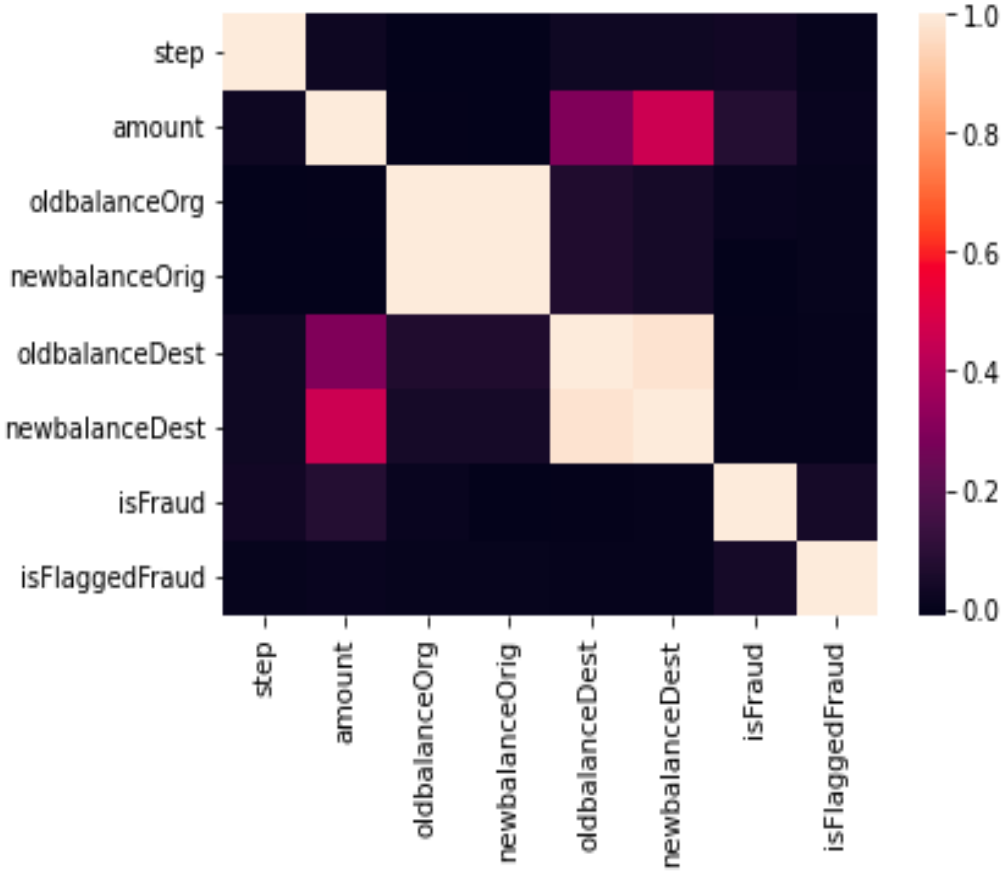

Figure 6: Correlation Matrix

3.4 Data Preparation:

For the machine learning model to give accurate, high-quality results, the data used to train and test it should be well-prepared. One of the most important steps in data mining is getting the data ready. There are many things to consider, such as how to deal with missing data, duplicate values, removing redundant features from data using correlation matrix and feature selection methods, how to deal with the fact that data isn't balanced, etc. The quality of the techniques used to prepare the data has a lot to do with how well machine learning works. If the data is not prepared well, it could take a long time to run the models and cost a lot of money. Because of all of these things, the most difficult and time-consuming part of the data mining process is getting the data ready.

3.4.1 Feature Selection

Feature selection is one of the approaches that helps models perform even better after data cleansing and feature correlation analysis. This method is used to eliminate unnecessary variables, which leads to a smaller feature space and could improve the performance of the model.
In our dataset two features "namedest" and "nameOrig" were of less significance as compared to other features, however to compare the same we will be running the models without these features and then including these two features.

3.4.2 Handling Class Imbalance

One of the key issues in the field of fraud detection is the class imbalance, which was covered in the sections above. Algorithms for machine learning are created to work optimally when taught on sufficient examples from both classes. The performance of machine learning models is vulnerable to skewed outcomes and overfitting due to the rarity of fraud transactions within the overall data. For the class samples with lower representation, this could lead to incorrect classification. There are a number of sampling approaches that can help with this problem, each with its own set of benefits and drawbacks. These strategies either focus on oversampling the minority class, undersampling the dominant class, or a mix of the two.
In order to handle the class imbalance in our dataset, we have used undersampling tech-

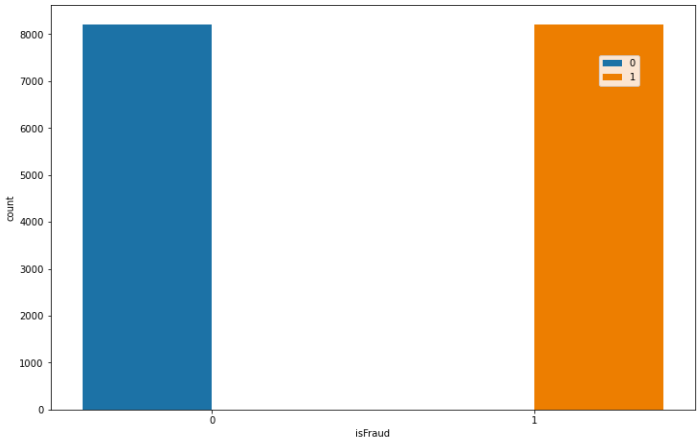

Figure 7: Target Feature count after the undersampling

nique. As the dominant class in our dataset was having 6354407 records, we randomly undersampled our dominant class to 8213 records. The target class distribution after the undersampling is shown in the figure 7.

3.5 Modelling Approach

Modelling is a very important aspect in machine learning. After the final data preparation, which includes steps like handling the class imbalance and feature selection, the proposed models are implemented on the processed or prepared data. The detailed explanation and working of the proposed models are discussed in this section:

3.5.1 Logistic Regression

Logistic Regression is the classification of algorithm into multiple categorical values. It includes the use of multiple independent variables which are used to predict a particular outcome of a variable which is dependent on all the independent variables use to train the model. Logistic Regression is similar to linear regression, it predicts a target field rather than a numeric one Zanin et al. (2018). Like predicting True or False, successful or unsuccessful in our case it is fraudulent or non fraudulent. The figure below explains the logistic regression:

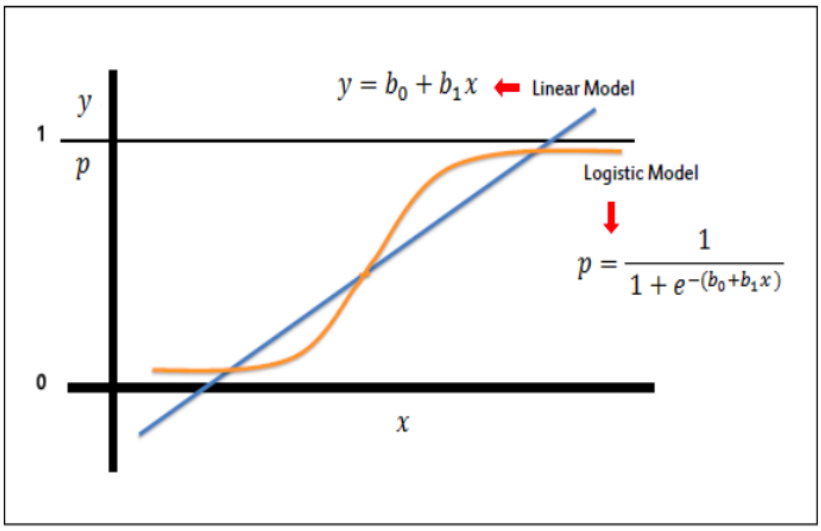

Figure 8: Logistic Regression

3.5.2 Random Forest Classifier

The random forest model is made up of many decision trees that are all put together to solve classification problems. It uses methods like feature randomization and bagging to build each tree. This makes a forest of trees that don't have anything in common with each other. Every tree in the forest is based on a basic training sample, and the number of trees in the forest has a direct impact on the results.Bahnsen et al. (2016)
Tsest
fdfdf

3.5.3 Decision Tree

Decision tree is a supervised machine learning algorithm which uses a combination of rules to make a particular decision, just like a human being. The motive behind decision tree is that one uses the dataset features to create yes or no questions and split the dataset until and unless we isolate all the datapoints those belong to each class.Choi and Lee (2017)

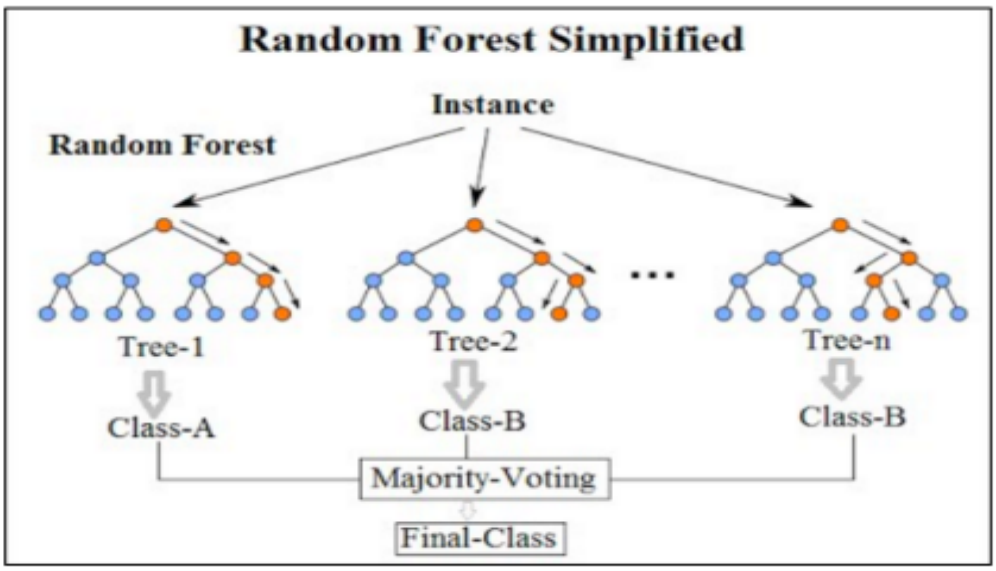

Figure 9: Random Forest

Decision tree is a tree like structure having branch node, leaf node and the root node. The top most node is called the root node.

3.6 Artificial Neural Networks

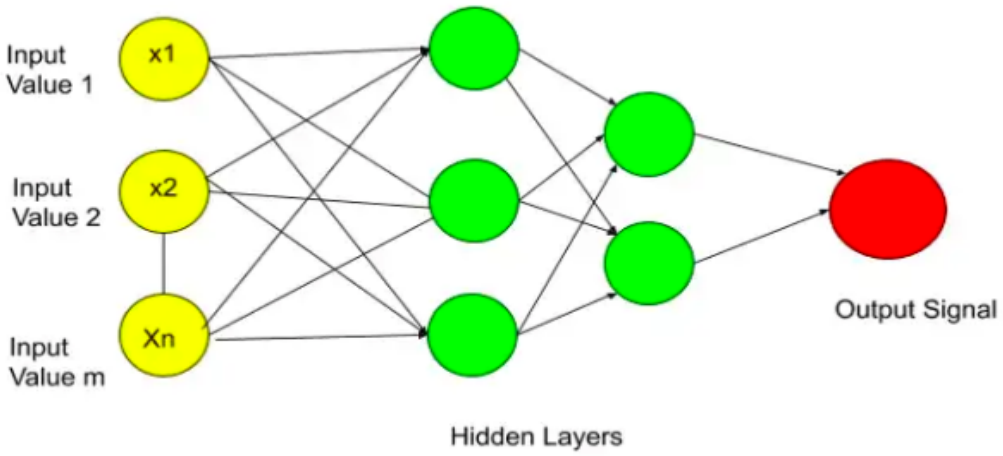

Figure 10: Artificial Neural Networks

All the circles in the figure are called neurons and ANN is fully connected with all the neurons.Information is sent to the input layer. The following layer, which is a hidden layer, was then given access to this data by the input layer. The hidden layer carries out certain tasks. then transmit the outcome to the output layer.

4 Design Specification

We begin by gathering data from the source, which is followed by pre-processing and EDA (explanatory data analysis) stages. These comprise removing duplicate and null values as well as uncovering hidden patterns in the data. We are filtering our features afterwards to maintain only the columns that are important to our analysis, however for the comparison we are running the models again including all the features which were filtered initially. The training of our baseline models on the training data set came next after we had divided our data into the train, and test datasets.

5 Implementation

The implementation procedures used in the contemplated research effort are discussed in depth in this section. Additionally, it describes the methods used to choose pertinent features and the procedures used for processing datasets.The Python programming language (v.3.7) has been utilized throughout the whole implementation of the suggested technique, and Google Colab has been used as the integrated development environment (IDE). Python has been chosen as the ideal option for our implementation because of its extensive online support community, simple yet effective features, and excellent code readability. Python has been a popular choice for machine learning applications because of its high availability libraries for data handling and pre-processing.
The data set which we are using for our research is available publicly in CSV format. The data set contains 11 features in total, which includes the target variable class also, which implies whether a particular transaction is fraudulent or not.We used Python to load the data into pandas data frame. After cleaning and scaling the data, we used visualizations to look for patterns and correlations in the data. After looking at how all of the features are related to the target variable, we found the important features that are highly related to the target variable.After that we implemented one hot encoding to convert all the categorical variables information into a form that machine learning algorithms can use to make better predictions. Once we had the final data set, we split it into train, validation, and test sets so we could use it in our models.As we've looked at our data, we've found that our target variable has a huge class imbalance. To get reliable results from machine learning models and to keep them from becoming too specific, we have applied under sampling of our majority class. We have under sampled our majority class from 6354407 records to 8213 records which is equal to our minority class.Then, we used different classifier models on our balanced data to decide whether a given sample was a fraud or not. In our approach, we used the Python sklearn library's Random Forest,Logistic regression, decision tree calssifier and Gaussian Naive Bayes. we also implemented Artificial Neural Networks to predict the fraudulent transactions.We are comparing the performance of all classifier models implemented using all the features and without the two not so relevant feature which are "namedest"(Name of the destination) and "nameorig"(Name of the orgin of transaction) as Kolodiziev et al. (2020) compared the results of classifier models on both unbalanced and balanced data using two different case studies.The research uses specificity, sensitivity, F1- score, AUC-ROC score, and geometric mean as ways to measure how well something works. In our case the best way to find the accuracy of the prediction is to evaluate the confusion matrix so that the false positive and false negative scores can be analyzed which is very important in our research. The figure below shows a standard confusion matrix.

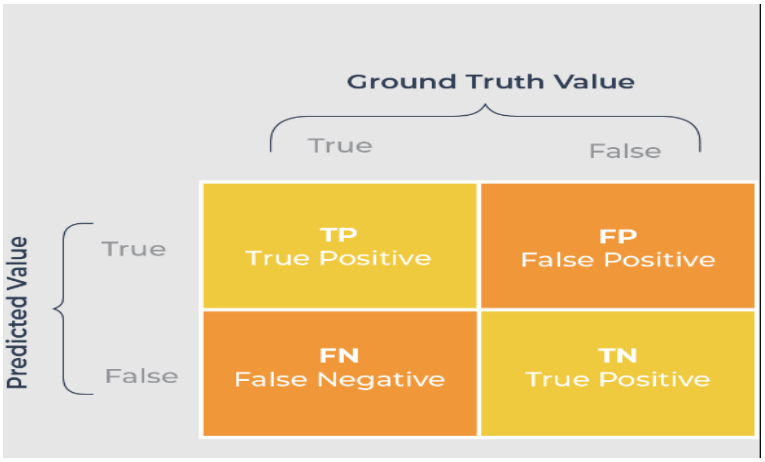

Figure 11: Confusion Matrix

6 Evaluation

The main goal of this research is to use supervised machine learning techniques and Artificial Neural Networks together and see if our proposed method improves the model's performance more than other state-of-the-art methods.For the comparative study, we did the following two experiments: [1] Figuring out how well a model works by training it on all of the features in the dataset. [2] Figuring out how well the model works by training it on certain features (Eliminating namedest and name orig features).We chose metrics like recall, specificity, F1-score, AUC score, AUC-ROC curve, and the geometric mean of recall and specificity so that we could compare how well our models worked.Because our data isn't balanced, we can't judge how well models work based on how accurate they are.Rambola et al. (2018) also compares the results based on the confusion matrix as in this case it is better to compare the True Positive and True negatives and decide based on that that how much accuracy is achieved in our models.The confusion matrix is explained below:

- True Positive(TP):It shows that the given model has done a good job of figuring out non-fraudulent cases as non-fraud (positive).
- False Positive(FP): It shows that the model didn't get the prediction right, fraudulent cases were identified as non-fraud (positive).
- False Negative(FN):It shows that the model didn't get the prediction right, non-fraudulent cases were identified as fraudulent (negative).
- True Negative(TN):It shows that the model has been able to accurately predict fraudulent cases as fraudulent (negative).

Precision and specificity show the number of transactions that are considered to be fraud and are frauds. On the other hand, recall/sensitivity values show what percentage of real fraud transactions are correctly classified.F1-score is the average of the notes between Precision and Recall and for better classification, should be close to 1 Kalbande et al. (2021).The geometric mean is the sum of both specificity and sensitivity. We chose this metric to judge our models because it works well with unbalanced data Bahnsen et al.

(2016). Due to how unbalanced our data is, the most important evaluation metric in our research is the recall and AUC score. We've used the confusion matrix to figure out the above evaluation metrics. the equations that follow:- After using the different data

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

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

$$\text{F1-Score} = \frac{2 * Recall * Precision}{Recall + Precision}$$

$$\text{Geometric Mean(GM)} = \sqrt{Sensitivity * Specificity}$$

Figure 12:

preparation methods talked about in the above sections, we now have our final dataset to use with our chosen models.To see how well our proposed method of using undersampling for handling Imbalance in data works and eliminating two fetaures(namedest and nameorig),We have done two different case studies for each of the algorithms and used the above-discussed evaluation metrics to rate them.

6.1 Experiment 1: Model Performance with all the fetaures

In our first experiment, we used all of the features to train a base model for each classifier. This was done after using feature selection and data split to get the final data.

6.1.1 Logistic Regression

The logistic Regression gave accuracy of 89.9 percent precision of 86 percent. The confusion matrix of the logistic regression is shown below: The ROC vlue of the model comes

Out[48]:

	Predicted Negative(0)	Predicted Positive(1)
Actually Negative(0)	1490	153
Actually Positive(1)	177	1466

Figure 13: Confusion Matrix

out to be 95 percent and the graph is shown below:

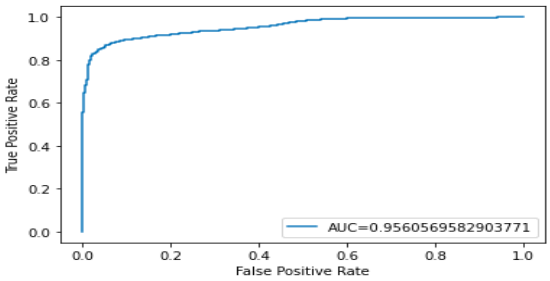

Figure 14: ROC curve for Logistic Regression

6.1.2 Random Forest Classifier

The second classifier was Random Forest and gave the accuracy of 87 percent, precision of 96.3 and AUC of 99 percent. The confusion matrix of the same is shown below:

Out[62]:

	Predicted Not Fraud(0)	Predicted Fraud(1)
Actually Not Fraud(0)	1598	45
Actually Fraud(1)	34	1609

Figure 15: Confusion Matrix for Random Forest

Algorithm	Accuracy	Precision	Recall	F1 Score
Logistic Regression	89.8	86.18	89	90
Random Forest	97.59	96.3	97	98
Gaussian Naive Bayes	73	80	97	78
Decision Tree	99	98	98	99

Figure 16: Comparison of all the model results

6.1.3 Artificial Neural Netwroks

We also implemented Artificial Neural Networks to our dataset. Yan et al. (2021) also compared the performance of machine learning models and Neural Networks for fraud detection.

```
([[1270816,      65],
  [    522,    1121]])
```

Figure 17: Confusion Matrix for ANN

We got a good accuracy of 99 percent by implementing ANN and the confusion matrix is shown in the figure 16. The transactions which were actually Fraudulent but were predicted Non-Fraudulent comes out to be 65 while the transactions which were actually fraudulent and were predicted non-fraudulent were 522.

6.2 Experiment 2:Model Performance when eliminating some fetaures

As discussed above, after training the models on all of the features we implemented the same models eliminating two features those are "namedest" and "nameorig" which were not that relevant to train our models as compared to other features. In other words, these two features did not have that impact on our target variable as compared to above features.

6.2.1 Logistic Regression

The logistic Regression gave accuracy of 89.9 percent precision of 86 percent. The ROC value of the model comes out to be 95.6. The confusion matrix of the logistic regression is shown below:
As compared to the confusion matrix of logistic regression when the model was trained

Out[85]:

	Predicted Negative(0)	Predicted Positive(1)
Actually Negative(0)	1490	153
Actually Positive(1)	177	1466

Figure 18: Confusion Matrix for Logistic Regression

without eliminating any features as shown in the figure 9. there is no significant effect on the model performance if we eliminate the "nameorig" and "namedest" features.

6.2.2 Random Forest

We impemented random forest classifier after eliminating the two features(namedest and nameorig) and following confusion matrix was obtained: As Compared to the results of random forest classifier in figure 11 for our first experiment where all the features were used to train the model,we can say that the eliminated features("namedest" and "nameorig") have a huge impact on the results for Random Forest Classifier.
The true Negative which were also predicted negative was 1598 but after eliminating two features it comes out to be 1618. The transactions which were not fraudulent but were

Out[99]:

	Predicted Not Fraud(0)	Predicted Fraud(1)
Actually Not Fraud(0)	1618	25
Actually Fraud(1)	15	1628

Figure 19: Confusion Matrix for Random Forest

predicted positive or fraudulent were 45 and in the second experiment comes out to be 25. The transactions which were actually fraudulent but were predicted non fraudulent were 34 in our first experiment but in the second experiment comes out to be 15 for Random Forest Classifier. Thus for Random Forest Classifier we can say that eliminating the two features in our experiment 2 increases the efficiency and performance of our model.

6.3 Discussion

In any financial company, where the daily number of transactions of their customers are in millions, they can't afford to classify any transactions which is a fraudulent as non-fraudulent or vice-versa. It brings along a huge loss to their customers as well as to these companies also. As they have to refund the amount to the customers some time because the transaction was fraudulent but was predicted as non-Fraudulent.
To ensure this, we have considered the confusion matrix and recall as a crucial evaluation metric in this research. While F1 score tells the overall model performance as it gives the balance between the precision and the recall scores. The higher the F1 value of a model is the lower is the errors in predicting fraudulent and non fraudulent transactions.Saputra and Suharjito (2019)
After analysing the results from the confusion matrix above, we can say that Random Forest in experiment 2 where we eliminated two of the features("namedest" and "nameorig") outperforms all other classifiers and proved to be a better performing classifier than others. The transactions which were actually fraudulent but were predicted non-fraudulent were just 15 and transactions which were actually non fraudulent but were predicted fraudulent were 25, which is better than all other classifiers in our study.
It can be determined from the ROC Curve's value and graphic depiction that for each of the models, the false positive rate for both fraudulent and non-fraudulent transactions decreases as the true positive rate rises. Thennakoon et al. (2019)
To answer our research question "How far may machine learning methods be utilized to determine whether a specific online transaction is fraudulent or not based on selected features" we can say that the performance of the algorithm can be improved by using feature selection techniques to extract the most pertinent and useful variables from the data set. This will also improve each model's capacity for identifying and separating true-positive fraudulent and legitimate transactions from false-positive fraudulent and non fraudulent credit card transactions.Behera and Panigrahi (2015)

7 Conclusion and Future Work

Online payment fraud has been identified as one of the leading frauds in the past few decades, In this research paper, we discussed the concept of online payment fraud detection. It was seen that feature selection techniques are very important and can be implemented to attain lower false positive rate. We implemented various machine learning algorithms like logistic regression, Random Forest in order to predict if a particular transaction is fraudulent or not. A good fraud detection system should accurately be able to predict if a given transaction is fraudulent or not.
To improve the performance of the models, various techniques such as handling class imbalance, feature selection was used in order to extract the most relevant data. Confusion matrix was used to evaluate the performance of our models, however we did not attain 0 False Positive and false negative score. It is important for a financial organization to attain 0 false positive and negative score as we discussed it impacts on the customer retention and costs lot of money for the refunds. More future works can be done on this research in order to attain the 0 false positive and negative score. Combination of models can be used to attain high accuracy in predicting the transactions as fraudulent and non fraudulent.

References

Bahnsen, A. C., Aouada, D., Stojanovic, A. and Ottersten, B. (2016). Detecting credit card fraud using periodic features.

Behera, T. K. and Panigrahi, S. (2015). Credit card fraud detection: A hybrid approach using fuzzy clustering neural network.

Choi, D. and Lee, K. (2017). Machine learning based approach to financial fraud detection process in mobile payment system, *IT CoNvergence PRActice (INPRA)* **5**.

Ileberi, E., Sun, Y. and Wang, Z. (2021). Performance evaluation of machine learning methods for credit card fraud detection using smote and adaboost, *IEEE Access* **9**.

Jain, V., Agrawal, M. and Kumar, A. (2020). Performance analysis of machine learning algorithms in credit cards fraud detection.

Kalbande, D., Prabhu, P., Gharat, A. and Rajabally, T. (2021). A fraud detection system using machine learning.

Kaur, P., Sharma, A., Chahal, J. K., Sharma, T. and Sharma, V. K. (2021). Analysis on credit card fraud detection and prevention using data mining and machine learning techniques.

Kolodiziev, O., Mints, A., Sidelov, P., Pleskun, I. and Lozynska, O. (2020). Automatic machine learning algorithms for fraud detection in digital payment systems, *Eastern-European Journal of Enterprise Technologies* **5**.

Rai, A. K. and Dwivedi, R. K. (2020). Fraud detection in credit card data using unsupervised machine learning based scheme.

Rambola, R., Varshney, P. and Vishwakarma, P. (2018). Data mining techniques for fraud detection in banking sector.

Ranjan, P., Santhosh, K., Kumar, A. and Kumar, S. (2022). Fraud detection on bank payments using machine learning.

Saputra, A. and Suharjito (2019). Fraud detection using machine learning in e-commerce, *International Journal of Advanced Computer Science and Applications* **10**.

Singh, P., Chauhan, V., Singh, S., Agarwal, P. and Agrawal, S. (2021). Model for credit card fraud detection using machine learning algorithm.

Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S. and Kuruwitaarachchi, N. (2019). Real-time credit card fraud detection using machine learning.

Wang, S., Minku, L. L. and Yao, X. (2015). Resampling-based ensemble methods for online class imbalance learning, *IEEE Transactions on Knowledge and Data Engineering* **27**.

Yan, T., Li, Y. and He, J. (2021). Comparison of machine learning and neural network models on fraud detection.

Yee, O. S., Sagadevan, S. and Malim, N. H. A. H. (2018). Credit card fraud detection using machine learning as data mining technique, *Journal of Telecommunication, Electronic and Computer Engineering* **10**.

Zanin, M., Romance, M., Moral, S. and Criado, R. (2018). Credit card fraud detection through parenclitic network analysis, *Complexity* **2018**.