Kabale University Interdisciplinary Research Journal (KURJ)

Fraud detection model for illegitimate transactions

***Musibau Adekunle Ibrahim** and **Patric Ozoh**
Department of ICT, Osun State University, Nigeria

*Corresponding Author
ibrahima@uniosun.edu.ng

ISSN 2790-1394
KURJ

pp. 21 - 37
Vol 2. Issue 2.
Oct 2023

ABSTRACT

Due to advancements in network technologies, digital security is becoming a top priority worldwide. This project aims to study how machine learning techniques can be used to learn patterns in fraudulent and legitimate transactions in order to detect fraudulent transactions using Python programming language on Jupyter notebook as the integrated development environment (IDE). Scikit-learn was used to process the algorithm, and Streamlit and Heroku platforms were used for deployment of the algorithms. This was incorporated into a web application that allows the user to upload data that is analyzed by the system to detect fraud. The Classification report and Confusion matrix are used to evaluate each model's accuracy. The random forest model gave an accuracy of 99.95 %. At the end of this study, a web-based application was developed to allow users upload data and also to detect fraudulent online based transaction.

Keywords: *Fraud detection, Fraud prevention, Fraud statistical methods*

Introducton

Background Information

Fraud is an art and crime of deceiving and scamming people in their financial transactions. Credit card fraud is a broad term used to define fraud that is committed using a payment card (David Uejio 2021). The initial incident of credit card fraud occurs when a fraudster either steals a physical card, or illegally obtains a victim's card details.

Credit card generally refers to a card that is assigned to the customer (cardholder), usually allowing them to purchase goods and services within credit limit or withdraw cash in advance. It provides the cardholder an advantage of the time, i.e., it provides time for their customers to repay later in a prescribed time, by carrying it to the next billing cycle. The concept of fraud is present in the earliest writings of history and has since developed into an evolutionary subset of financial fraud (William and Marc-André, 2019). Fraud today comprises of many different types, such as consumer fraud, identity theft, credit card fraud etc. With different frauds mostly credit card frauds, often in the news

for the past few years, frauds are in the top of mind for most the world's population. Credit card dataset is highly imbalanced because there was more legitimate transaction when compared with a fraudulent one.

As use of online payment transactions continues to rise world-wide so does the fraud associated with them. Even with the measures put into place to stop these, fraudsters are continually changing the ways to which they exploit others therefore an efficient fraud detections method needs to be adopted which can detect and learn from past fraudulent transactions so that it can adapt to future methods of fraud in order to detect them before they occur (Mishra, 2016). Credit card fraud is defined as the unauthorized use of a payment card, this occurs when fraudsters obtain the physical card or the victim's card details (Shabad and Kavitha, 2018).

The growing development of online transactions have increased rapidly over the last decade due to advancements in network technologies making it the most popular payment method for online purchases, meaning that credit cards and other online payment models are involved. Businesses, Companies, Finance companies and Institutions now provide online services such as e-commerce in order to offer customers better efficiency and accessibility. Online transactions have some drawbacks because the card or cardholder do not need to be present for a transaction to be completed therefore making it difficult for merchants to determine if the customer is the genuine cardholder.

The scam usually occurs when someone accesses your credit or debit card numbers from unsecured websites or via an identity theft scheme to fraudulently obtain money or property. Due to its recurrence and financial institutions, it is crucial to take preventive measures as well as identifying when a transaction is fraudulent. Necessary prevention measures can be taken to stop this abuse of such fraudulent practices can be studied to minimize it and protect against similar occurrences in the future.

Fraud detection involves monitoring the activities of populations of users in order to estimate or avoid objectionable behavior, which consist of fraud, intrusion, and defaulting. This is a very relevant problem that demands the attention of communities such as machine learning and data science where the solution to this problem can be automated. It can be utilized to effectively identify suspicious patterns in transactions. Due to the advancement of fraudulent attacks, advanced fraud detection model (FDS) is required to detect fraudulent transactions (Benson and Annie, 2020).

Credit card usage has enormously been increased during the last years according to (Sudjianto *et al.* 2019), 120 million cards were created in Germany and brought into use from 2004 which led to total credit card purchases of €375 billion at the same year. With respect to usage from 2005, there was an increase of 4% on the overall credit card usage (Volinsky and Wilks 2019).

(Delamaire *et al.*, 2019) defined credit card as "a method of selling goods or services without the buyer having cash in hand". A credit card transaction involves four entities. The first entity is the consumer; that is the person who owns the card and who carries out the legitimate transactions. The second entity is the credit card issuer; that is usually the consumer's bank – also known as issuing bank – which provides the credit services to consumer. The credit card issuer sends the bill to the consumer in order to request a payment for their credit card transactions. The third entity is the merchant who sells goods or services to

the consumer by charging consumer's credit card. This charge is achieved through merchant's bank the forth entity which sends the request for the transaction to the issuing bank. The issuing bank will check whether the amount of the transaction does not reach the credit card's limit before authorizing that transaction. If the transaction is valid the issuing bank will block the requested amount from consumer's credit card account and send an authorization response to merchant bank. As soon as the authorization response is received by the merchant's bank, the merchant is notified; the transaction is marked as completed and the consumer can take the goods. The blocked amount on consumer's credit card account was transferred into merchant's bank account in the following days.

Although the use of credit cards as a payment method can be really convenient for our daily transactions; people must be aware of the risks that they impose themselves while using their credit cards. More precisely, the incremental usage of credit cards gave the opportunity to fraudsters to exploit their vulnerabilities (Delamaire *et al.*, 2019). Credit card fraud refers to any illegal and unauthorized activity on the use of credit cards which is undertaken by a fraudster. According to (Volinsky 2015) credit card fraud has been increased between 2015 and 2017. Moreover, Bolton *et al.* (2012) claim that in United Kingdom the total losses of credit card fraud, for 2020, were £286 million (Bolton, 2016). In United States the total losses for 2019 were as high as $3.56 billion; an increase of 10.2% comparing to the previous year. An interesting question arises as to who is responsible to pay for all those losses in case of a credit card fraud. (Delamaire *et al.*, 2019) claim that merchants are really vulnerable in case of a credit card fraud because they are required to pay for the losses due to the so-called charge-backs. Chargebacks are requested by the consumer's bank as soon as the consumer reports a transaction as unauthorized.

Aim and Objectives

This project aims to design and implement a model that detects credit card fraud. The objectives of this study are as follows:

i. To design a model to detect credit card fraud using machine learning.
ii. To implement the design of the model in (i) using Python language.
iii. To evaluate project work identifying success criteria and future work.

Literature Review

Machine learning uses algorithms to predict or classify data based on previous data therefore learning from past data characteristics to accurately classify or predict new data (Talabis, 2015). Algorithms used in machine learning to predict credit card fraud can be classified into two groups supervised and unsupervised learning.

In supervised learning, data is labelled i.e., fraud or genuine, this is used as a basis by the machine learning algorithm model to label unclassified data for example in credit card fraud detection past transaction data is marked as fraudulent or genuine, the characteristics of these transactions are then used to predict new records. It uses techniques such as linear regression and classification. Classification techniques can be used to recognize patterns in data which can by a machine learning model to learn characteristics of fraudulent transactions to accurately detect fraud (Talabis, 2015).

Unsupervised learning uses unlabeled data and classifies into structures that have common elements this can be used to detect account behavior such as amount spent, times of transaction and location, these methods can be used to build a behavioral model of legitimate account activity which can then be compared to new records to identify anomalies such as fraudulent activities (Talabis, 2015).

Artificial Neural Network is a hybrid form of machine learning that uses both supervised and unsupervised learning, the structure of this type of machine learning mimics the functions of a human brain, similarly to brain function it uses associative memory and pattern recognition to predict outcomes of future events. This machine learning model can be used for classification (Analysis of Credit Card Fraud Detection Techniques, 2016). According to the majority of fraud detection model studies are based on neural networks because of its ability to learn from the past therefore allowing it to get better with time as it fed more data (Zareapoor *et al.*, 2019).

Reducing Scalability Issues and improving Efficiency

(Mareeswari and Gunasekaran, 2016) has proposed a credit card fraud detection model that tackles scalability issues and imbalanced datasets in existing models. The main objective of the model is to reduce discrepancies such as scalability issues, low response time, and inefficiency. The model contains the dataset inputted for credit card fraud detection; the dataset is split into two before analysis. This model component was replicated in the design of the model for detecting fraud to reduce scalability and increase efficiency.

Wiese *et al.* (2019) suggest an implementation of Artificial Neural Networks (ANNs) for detecting credit card fraud. Their implementation takes into account a sequence of transactions that have occurred at some time in the past, in order to determine whether a new transaction is legitimate or fraudulent. They believe that "looking at individual transactions" only is misleading since it cannot face any periodical changes in spending behavior of a customer (Wiese and C. Omlin, 2019). They call their approach as "Long Short-term Memory Recurrent Neural Network (LSTM)".

Guo *et al.* (2018) suggest a different implementation of ANNs by converting the training samples into confidence values using a specific mathematical formula and then supply these values to train the ANN – instead of the original training samples. They call their approach as "confidence-based neural network" and they claim that it can achieve promising results in detecting credit card fraud.

Another implementation of ANNs is suggested by Patidar*et al.* (2020) "Credit Card Fraud Detection Using Neural Network,". They use the genetic algorithm; the details of which can be found in (Whitley, 2014) "A genetic algorithm tutorial," Statistics and Computing in order to derive the optimal parameters of ANN (Sharma, 2020) "Credit Card Fraud Detection Using Neural Network". Like many other data mining techniques, ANNs make use of a number of parameters which need to be specified by software developers. Although the values of theses parameters can seriously affect the predicting accuracy of ANN models; a standard practice for specifying these parameters has never been established. The use of genetic algorithm which is suggested by Patidar *et al.* (2020) "Credit Card Fraud Detection Using Neural Network," can help in deciding these optimal parameters. They call their approach as "Genetic Algorithm Neural Network (GANN)".

Chen *et al*. (2016) suggest an implementation of SVM which they call "Binary Support Vector Model (BSVS)". One of the main problems of data mining techniques arises in situations where the training samples have an imbalanced distribution also known as skewed distribution. In such a case the misclassification rate is increased whereas the predicting accuracy of the classifier is reduced. The approach of Chen*et al*. (2016) is insensitive to skewed distribution of training samples. An innovative implementation of SVMs for detecting credit card fraud is also suggested by Chen *et al*. (2014) "Detecting Credit Card Fraud by Using Questionnaire-Responded Transaction Model Based on Support Vector Machines,". They suggest from the issuing banks to ask their new customers to fill some questionnaires that can help them understand the spending habits of the customers. This is particularly useful since there is no any prior history on the spending behavior of new customers and therefore the detection techniques cannot spot fraudulent transactions at the initial stage. Therefore, the answers to the questionnaires can be used in a similar manner to the historical information of each customer. They call their approach as "Questionnaire-Responded Transaction Model" (QRT Model).

Maes *et al*. (2021) suggest an implementation of BBNs for detecting credit card fraud "Credit Card Fraud Detection Using Bayesian and Neural Networks,". They claim that their approach can detect up to 8% more fraudulent transactions than ANNs can do. To the best of writer's knowledge, this is the only article in literature which suggests the use of BBNs in credit card fraud.

Sahin *et al*. (2018) provide three different implementations of decision trees for detecting credit card fraud "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines,". These implementations are called C5.0, C&RT and CHAID. Their differences lie in the way in which they construct the tree as well as the pruning algorithm which they use to remove erroneous branches and nodes "Predicting business failure using classification and regression tree".

According to the experiments made by Sahin*et al*. (2017), the best predicting accuracy was achieved by C5.0 with an average of 92.80%, following by CHAID with 92.22% and finally by C&RT with 91.34% "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines,". In their experiments, the three DT implementations outperformed the SVM implementation which achieved an average accuracy of 88.38% "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines,".
YU *et al*. (2019) suggest an implementation of outlier detection technique, "Research on Credit Card Fraud Detection Model Based on Distance Sum,". The similarity metric that they use to detect outliers is called distance sum. This is mathematically explained in the research on Credit Card Fraud Detection Model Based on Distance Sum".

Yamanishi *et al*. (2014) suggest another implementation of outlier detection for detecting credit card fraud "On-Line Unsupervised Outlier Detection Using Finite Mixtures with Discounting Learning Algorithms,". They call their approach as "SmartSifter" and claim that it can be applied in real time. This means that a new transaction is checked as soon as it arrives before being authorized. This is not the case for most fraud detection models because real time detection is time consuming. Most of them will check the newly authorized transactions at some time in the future for example once a day in a batch processing mode. The main disadvantage of this approach is that a fraud is just detected but not prevented. If, for instance, a fraud was committed in a physical shop then the fraudster would take the products and run away before the bank discover this fraud. Therefore, somebody; either the legitimate cardholder or merchant or bank would need to pay the losses of this fraud.

Srivastava *et al*. (2018) suggest an implementation of Hidden Markov Model (HMM) which promises a good predictive accuracy and a minimal misclassification error "Credit Card Fraud Detection Using Hidden Markov Model,". However, their approach does not perform well on new customers where historical information is not available. Again there is no other implementation of HMM for credit card fraud to the best of writer's knowledge.

Chapter Summary

Card transactions are always unfamiliar when compared to previous transactions made by the customer. This unfamiliarity is a very difficult problem in real-world. The proposed model for this project is to design and create an application that uses machine learning algorithms that learns from previous fraudulent transactions in order to analyze online card transactions and detect fraudulent activity. A comprehensive survey conducted by (Clifton Phua, 2017) and his associates have revealed that techniques employed in this domain include data mining applications, automated fraud detection, adversarial detection. In another paper, Suman, Research Scholar, GJUS&T at Hisar HCE presented techniques like Supervised and Unsupervised Learning for credit card fraud detection. Even though these methods and algorithms fetched an unexpected success in some areas, they failed to provide a permanent and consistent solution to fraud detection.

A similar research domain was presented by Wen-Fang YU and Na Wang where they used Outlier mining, Outlier detection mining and Distance sum algorithms to accurately predict fraudulent transaction in an emulation experiment of credit card transaction data set of one certain commercial bank. Outlier mining is a field of data mining which is basically used in monetary and internet fields. It deals with detecting objects that are detached from the main model i.e., the transactions that aren't genuine. They have taken attributes of customer's behavior and based on the value of those attributes they've calculated that distance between the observed value of that attribute and its predetermined value. Unconventional techniques such as hybrid data mining/complex network classification algorithm is able to perceive illegal instances in an actual card transaction data set, based on network reconstruction algorithm that allows creating representations of the deviation of one instance from a reference group, an adequate proved has been shown for the inefficient typically on medium sized online transaction.
The proposed model was an effort to progress from a completely new aspect whereby there was improvement in the alert feedback interaction in case of fraudulent transaction. In case of fraudulent transaction, the authorized model would be alerted and a feedback would be sent to deny the ongoing transaction.

Research Methodology

Machine learning algorithms employ prior data to forecast or categorize data, therefore learning from past data features to properly classify or predict future data (Talabis, 2015). Machine learning algorithms used to forecast credit card fraud are divided into two categories: supervised learning and unsupervised learning. In supervised learning, data is labeled as fraudulent or genuine, and the machine learning algorithm model uses this as a foundation to label unclassified data. For example, in credit card fraud detection, past transaction data is labeled as fraudulent or genuine, and the characteristics of these transactions are then used to predict new records. It employs techniques like linear regression and classification. Classification techniques can be used to recognize patterns in data, which can then be

used by a machine learning model to learn characteristics of fraudulent transactions in order to detect fraud accurately (Talabis, 2015).

Unsupervised learning classifies unlabeled data into structures with common elements, which can be used to detect account behavior such as amount spent, time of transaction, and location. These methods can be used to build a behavioral model of legitimate account activity, which can then be compared to new records to identify anomalies such as fraudulent activity (Talabis, 2015).

Artificial Neural Networks (ANNs) are a type of machine learning that uses both supervised and unsupervised learning. The structure of this type of machine learning mimics the functions of the human brain, and it uses associative memory and pattern recognition to predict the outcomes of future events. According to the majority of fraud detection model research, neural networks are used because of their capacity to learn from the past, allowing them to improve over time as more data is fed into them (Zareapoor *et al*., 2012).

Neural Networks

A neural network can be used for machine learning to create a model that functions based on the human brain. Neurons are used in the network to analyze data and connect it to a multi-layered network (Raghavendra and Lokesh, 2011). The neural network will determine if the transaction is genuine or fraudulent in a logistic regression fashion by applying 0 for a genuine transaction, and 1 for a fraudulent transaction. The three layers of a neural network consist of an input layer, hidden layer, and output layer. The input layer contains the features of the data to analyze and the hidden layer contains the weights that determines the outcome in the output layer. The outcome (genuine or fraudulent) is then demonstrated in the output layer. An example model of a neural network implemented for credit card fraud detection is exhibited in figure 1 from the Raghavendra Patidar and Lokesh Sharma, 2011 publication. The artificial neural network is shown in figure 1 below.

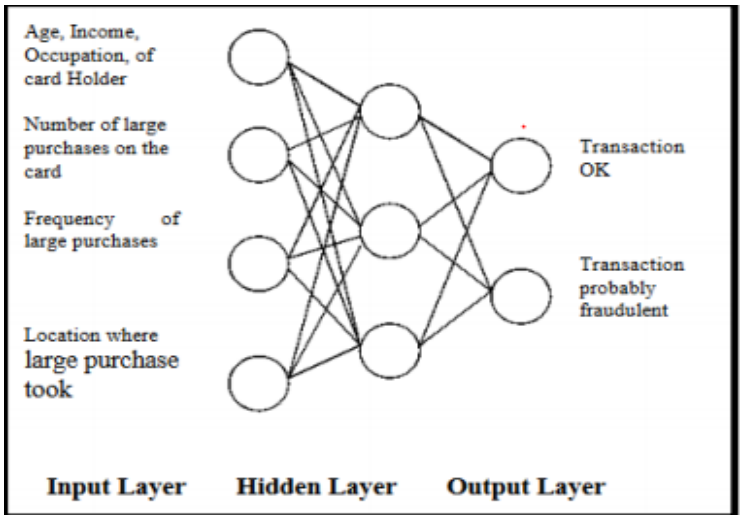

Figure 1: Artificial Neural Network for Credit Card Fraud Detection (Raghavendra Patidar and Lokesh Sharma, 2011).

(Suvasini *et al*, 2009) has developed a system to detect credit card fraud, it uses rule-based filters that are commonly used in velocity checks and then adds the transaction to conduct a belief analysis. If the transaction is deemed as suspicious, it is then then checked against a dataset that is split into two and then used to train the Bayesian learner before concluding that the transaction is genuine or fraudulent. This system also splits the datasets into two before being processed by a detection algorithm. This system uses the same velocity checks that are conducted during online transactions (Scott Stone, 2016); by implementing what is in this system to the proposed system, velocity checks can be used in fusion with a fraud detection algorithm, the algorithm chosen can then be incorporated with the same fusion approach.

Card transactions are always unfamiliar when compared to previous transactions made by the customer. This unfamiliarity is a very difficult problem in real-world. The proposed system for this project is to design and create an application model that uses machine learning algorithms that learns from previous fraudulent transactions in order to analyze online card transactions and detect fraudulent activity. This allows practitioners/users to upload transaction data and the results was displayed.

Data Collection

Data is collected from an online anonymized dataset from Kaggle. The dataset contains 984 transactions and 32 features. Because of the anonymity of the dataset, most features are represented as V1-V28 which are undisclosed. Table 1 below shows basic features that are captured when any transaction is made and would be utilized in this project.

Table 1: Raw features of credit card transactions.

Attribute name	Description
Transaction id	Identification number of a transaction
Cardholder id	Unique Identification number given to the cardholder
Amount	Amount transferred or credited in a particular transaction by the customer
Time	Details like time and date, to identify when the transaction was made
Label	To specify whether the transaction is genuine or fraudulent

Scikit-learn

Scikit-learn is a machine learning tool that uses Python to develop machine learning models (Fabian Pedregosa, 2011), the data processes much faster as Python is a general-purpose language. When Pedregosa analyzed the speed of the different machine learning algorithms it was found that Scikit-learn was the fastest when processing algorithms. Streamlit is an open-source Python library that makes it easy to create and share beautiful, custom web apps for machine learning and data science. It allows to build and deploy powerful data apps in minutes. This library is chosen to run the system. In order to successfully perform a sufficient data preparation step for the system model, a deep understanding of the data is needed, this ensures data quality and availability of quality data fed to the model for the model to have maximum performance. The dataset is collected from an online anonymized dataset from Kaggle. The data contains 419 fraudulent transactions out of 269 transactions. This difference between the fraudulent and normal transactions shows a large gap which tells us that the data is very imbalanced, this can have a negative effect on the model such that when it makes a prediction, it does so with high

accuracy while unknown to the users that the algorithm is only making predictions for only one class which is the dominating class. We will need to balance it so we can build a model capable of identifying fraudulent transactions.

SMOTE (Synthetic Minority Over-Sampling Technique) is used to perform the oversampling on the dataset by selecting 484 normal cases and 484 fraud transactions to make a balanced dataset.

Implementation and Evaluation

The following section explains the system development based on the modeling and designs specified in previous chapters. Code screenshots were used to highlight the functionalities of the system. It presents results for model-based machine learning techniques for predicting credit card fraud deployed using Heroku. From the data preparation, where the dataset was preprocessed and the synthetic minority over-sampling technique (SMOTE) was performed on it to make a balanced dataset. A screenshot of the code used to implement the data sampling is shown in figure 2.

```
182
183             # get train and test data
184             X_train_sfs=X_train[top_features]
185             X_test_sfs=X_test[top_features]
186
187             X_train_sfs_scaled=X_train_sfs
188             X_test_sfs_scaled=X_test_sfs
189
190             # set random seed
191             np.random.seed(42)
192
193             # set smote to handle imbalance class
194             smt = SMOTE()
195
196
197             st.subheader('Handling Imbalanced Class')
198             rect=smt
199             st.write('Shape of imbalanced y_train: ',np.bincount(y_train))
200             X_train_bal, y_train_bal = rect.fit_sample(X_train_sfs_scaled, y_train)
201             st.write('Shape of balanced y_train: ',np.bincount(y_train_bal))
202             st.subheader('Model Performance')
203             decisionTree(model,X_train_bal, y_train_bal,X_test_sfs_scaled,y_test)
204
205
```

Figure 2: Code screenshot on handling imbalanced data

The new sample is created as shown in the image below. The imbalance data has 303 normal observations and 484 fraud observations, while after oversampling, the balanced dataset has 484 normal transactions and 484 fraudulent transactions.

Modelling

The code below is used to create the random forest model, amongst the rest (KNN, Decision tree, neural network) before creating the model, the feature selection method is used to select features fed into the model based on their importance.

For Neural network and KNN, they are being modelled with all the features. The modelled data screenshot and a graph displaying the feature importance is shown in figure 3 and 4 below.

```
206         elif(choose_model == "Random Forest"):
207             #Feature selection through feature importance
208             model = RandomForestClassifier(random_state=42)
209             @st.cache
210             def feature_sort(model,X_train,y_train):
211                 # fit the model
212                 model.fit(X_train, y_train)
213                 # get importance
214                 imp = model.feature_importances_
215                 return imp
216
217             # Get feature importance and plot it
218             st.set_option('deprecation.showPyplotGlobalUse', False)
219             importance=feature_sort(model,X_train,y_train)
220             feats = {} # a dict to hold feature_name: feature_importance
221             for features, importances in zip(df.columns, importance):
222                 feats[features] = importances #add the name/value pair
223
224             importances_df= pd.DataFrame.from_dict(feats, orient='index').rename(columns={0: 'Gini-importance'})
225             importances_df.sort_values(by='Gini-importance').plot(kind='barh', rot=45)
226             plt.title('Feature Importance')
227             plt.xlabel('Importance')
228             plt.ylabel('Features')
229             st.pyplot()
230
231             # get top features from the feature importance list
232             feature_imp=list(zip(feat,importance))
233             feature_sort=sorted(feature_imp, key = lambda x: x[1])
234             n_top_features = st.sidebar.slider('Number of top features', min_value=5, max_value=20)
235             top_features=list(list(zip(*feature_sort[-n_top_features:]))[0])
236
237             if st.sidebar.checkbox('Show selected top features'):
238                 st.write('Top %d features in order of importance are: %s'%(n_top_features,top_features[::-1]))
239
```

Figure 3: Code screenshot of data modelling

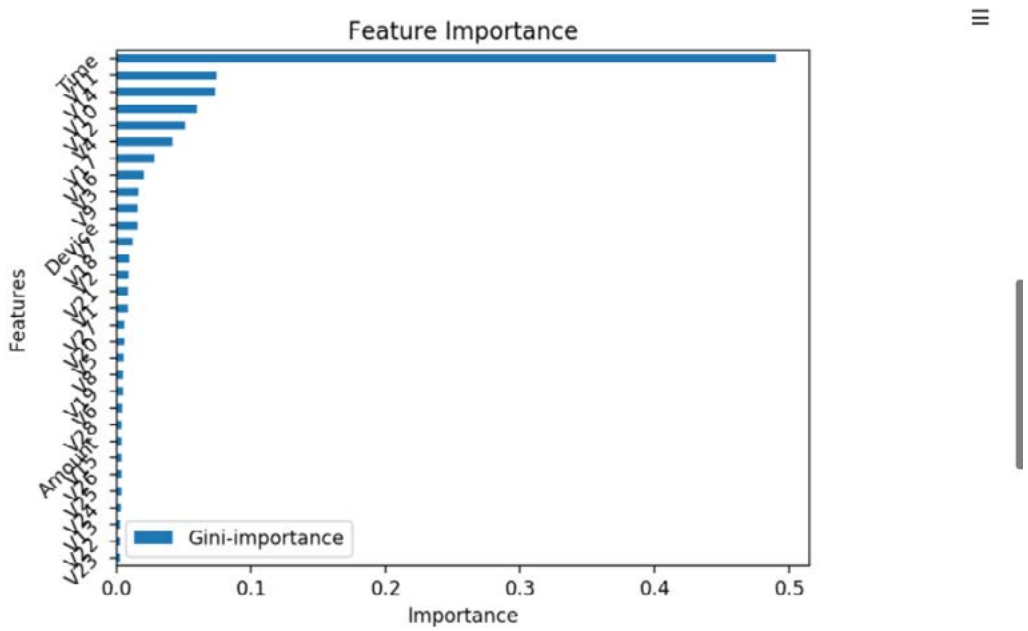

Figure 4: Graph displaying the Feature Importance of each feature in the dataset.

Implementation of a Web Application

The system has been fully built and is ready to be used. The images below show the GUI before a dataset is uploaded and after a dataset has been uploaded. The image below in figure 5 is the screenshot that shows the GUI welcome page of online credit card fraud detection after running it on a web application.

Figure 5: GUI welcome page of Online Credit Card Fraud Detection

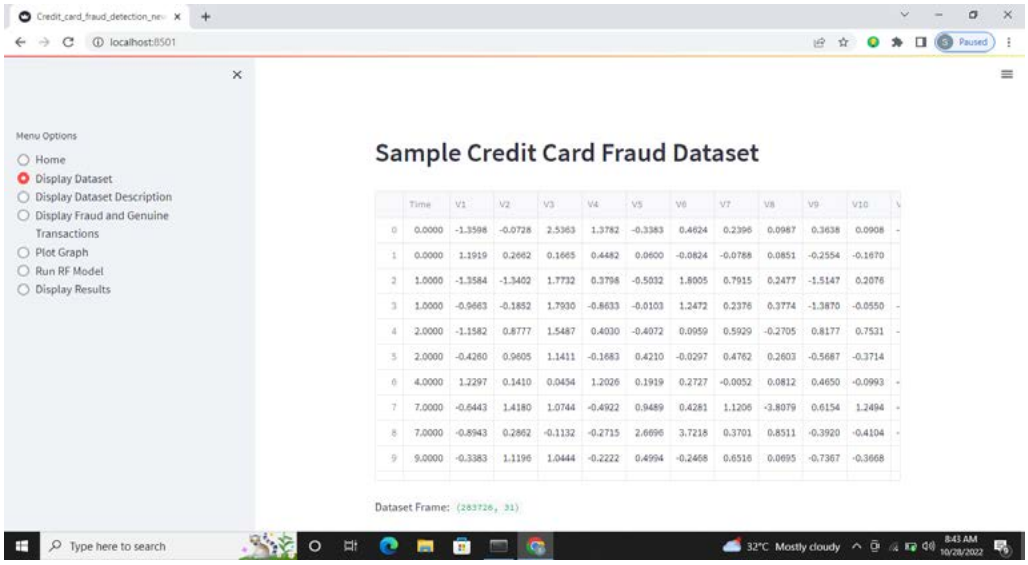

Figure 6: Sample Credit Card Fraud Dataset

Figure 6 above is the screenshot of the sample credit card fraud dataset with the time and volume and the dataset frame of (283726, 31)

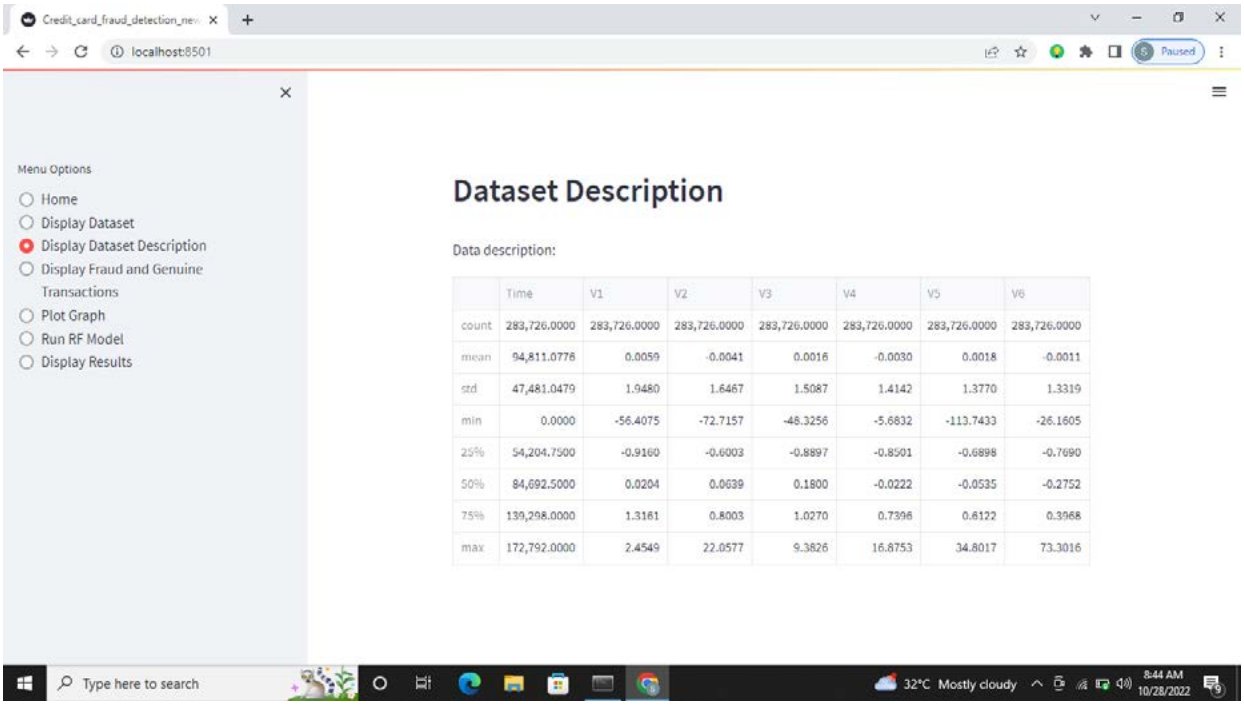

Figure 7: Dataset Description

The figure 7 above is showing the Dataset Description Table

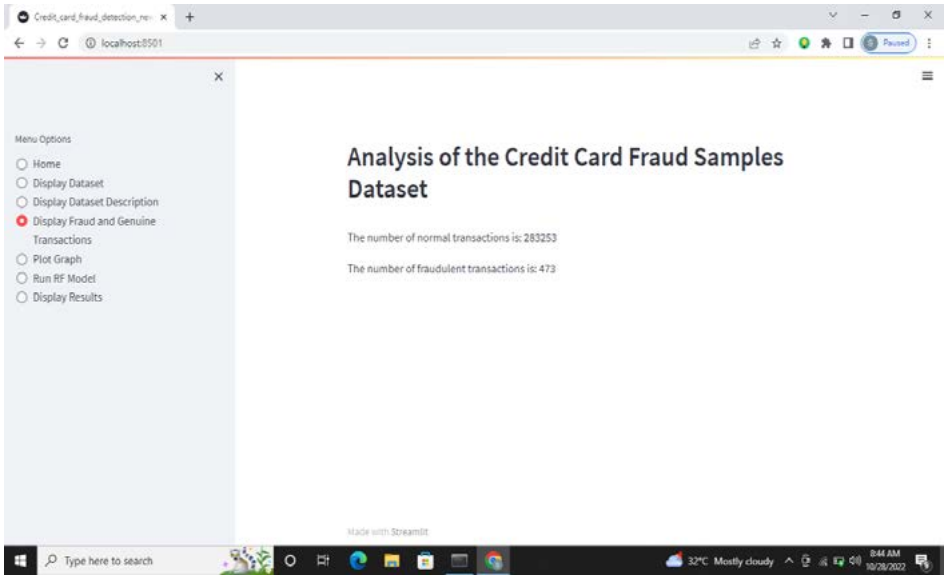

Figure 8: Analysis of the Credit Card Fraud Samples Dataset

The above image figure 8: showcase the screenshot of the analysis of credit card fraud dataset sample. The number of normal transaction is 283253 and the number of fraudulent transaction is 473.

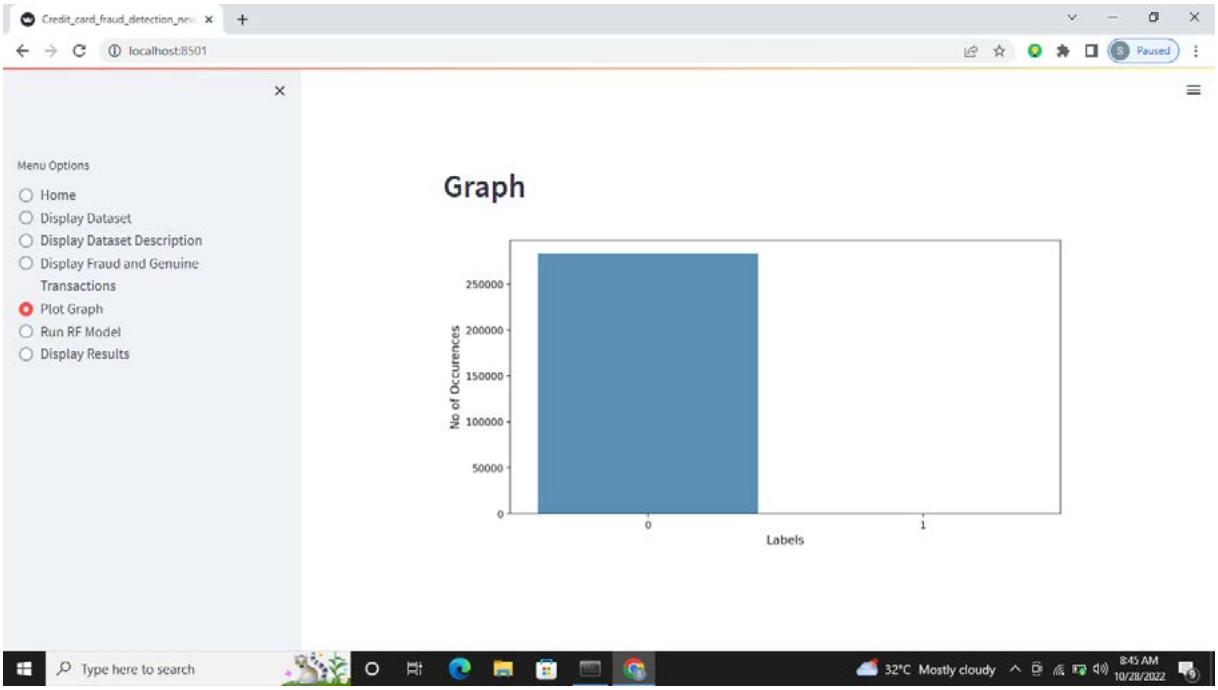

Figure 9: Graph of the Dataset

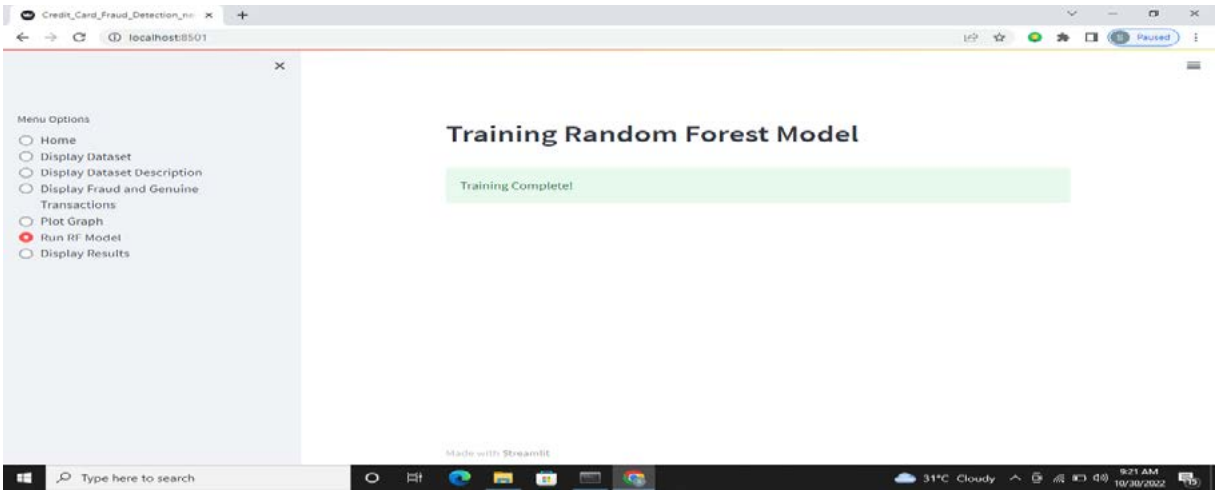

Figure 10: Random Forest Model

Figure 10 above shows the training of the Random Forest Model is complete.

System Evaluation

Evaluation of the model is carried out to determine the model performance - if it is good or bad; if it can be used effectively on other datasets and produce a good outcome. The accuracy is determined by comparing the predicted and actual data, it is the ratio of number of correct predictions to the total number of input samples. The accuracy works well when we have a balanced dataset where the number of predictions in each class is equal. Each model has its own accuracy. The accuracy of the random forest model is shown in figure 11 below.

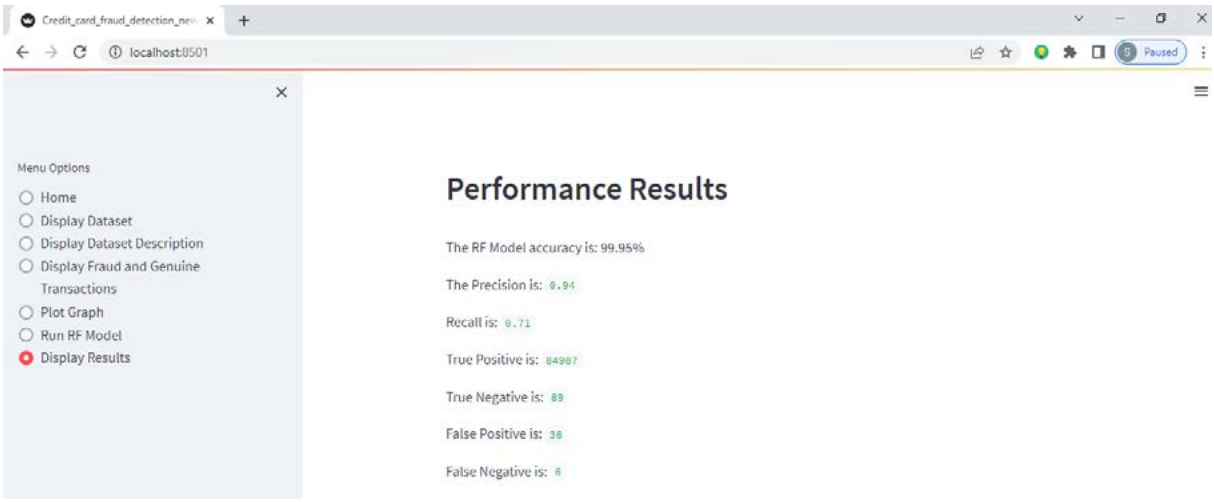

Figure 11: Accuracy of the random forest model.

Classification Report

A classification report is used to measure the quality of predictions from a classification algorithm. The classification report shows Precision, Recall and the F1 score.

Precision

This is the ability of a classifier not to label an instance positive that is actually negative. It is the ratio of the true positives to the sum of the true and false positives.

TP= True Positives
FP= False Positives
Precision – Accuracy of positive predictions.
Precision = TP / (TP + FP)

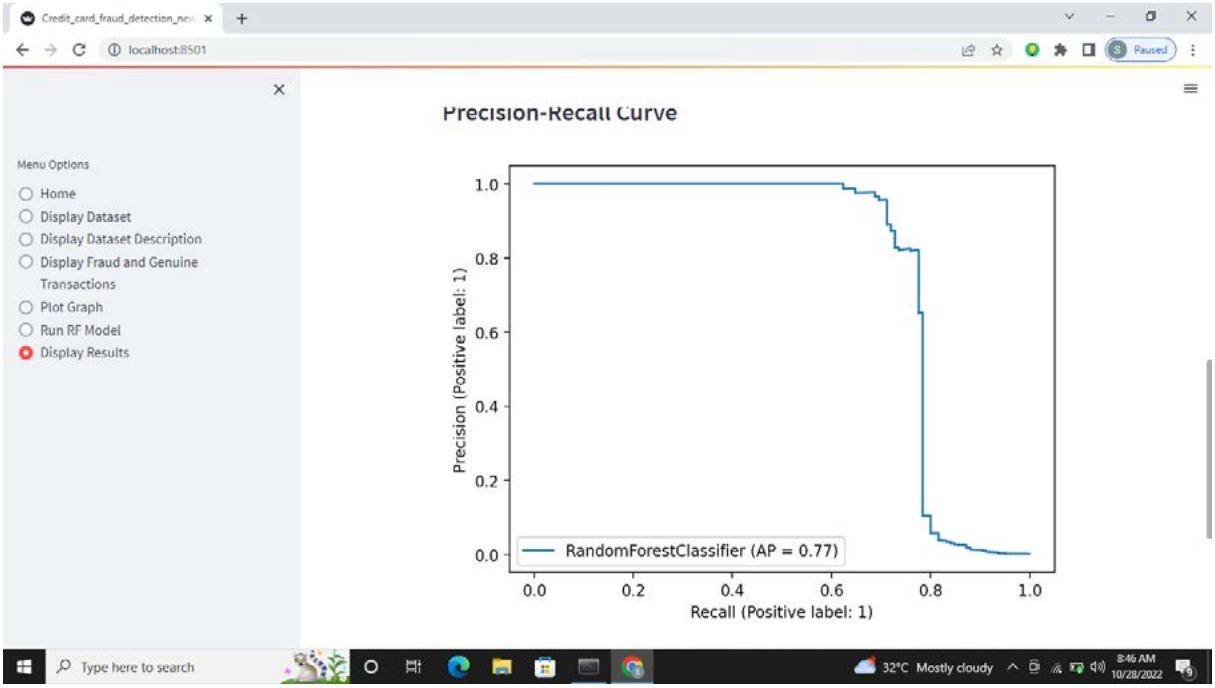

Figure 12: Precision for data analysis

Recall

Recall is the ability of a classifier to find all positive instances. it is defined as the ratio of true positives to the sum of true positives and false negatives.

FN= False Negatives
Recall -Fraction of positives that were correctly identified
Recall = TP/(TP+FN)

F1 Score

The F1 score is a weighted harmonic mean of precision and recall such that the best score is 1.0 and the worst value is 0.0, F1 scores are considered lower than accuracy measure because they enbed both precision and recall into their computation. The weighted average of F1 is used to only compare classifier models, which in this case, is one. The classification report of the model is given in by figure 13 below.

Figure 13: Classification report

Conclusion

This research has listed out the most common methods of fraud along with detection methods and reviewed recent findings in this field. This paper has also explained in detail, how machine learning can be applied to get better results in fraud detection along with the algorithm, code screenshots, explanation and its implementation. By applying the SMOTE, to balance the dataset, it was observed that the models performed better, Decision tree, Random Forest, Neural network and K-nearest neighbor and algorithms was used to fit and train the data. They also appear in the system to allow user select a model of choice. The Random Forest gave an accuracy of 99.58, however, the efficiency decreases when trained with imbalanced transaction datasets.

References

Benson S., Edwin Raj A., Annie Portia, (2020). Analysis on credit card fraud detection methods. *International Conference on Computer, Communication and Electrical Technology (ICCCET)*, IEEE, 152-156. [Accessed 24 January 2020].

Berk, R. (2010). What you can and can't properly do with regression. *Journal of Quantitative Criminology,* 26, 481-487.

Bhatia, S., Bajaj, S., & Hazari, S. (2016). Analysis of Credit Card Fraud Detection Techniques. International *Journal of Science and Research (IJSR)* 5(3)

Bhingarde, A., Bangar, A., Gupta, K. and Karambe, S., (2015). Credit Card Fraud Detection using Hidden Markov Model. *IJARCCE*, pp.169-170.

David Uejio (2021). *Bureau of consumer financial protection consumer credit card market report*. International Conference on Computer, Communication and Electrical Technology (ICCCET).

Erich F., Chintan Amrit, Maya Daneva (2014). Construction of a Model Dynamics model to achieve a" repetitive, risk-free and effortless Continuous Delivery Process" is described in DevOps Literature Review, University of Twente.

Erich Gamma, John Vlissides, Richard Helm and Ralph Johnson, (2014). *Design Patterns: Elements of Reusable Object-Oriented Software*. United States: Addison-Wesley.

Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., ... & Duchesnay, É. (2011). Scikit-learn: Machine learning in Python. *Journal of machine Learning research*, 12, 2825-2830.

Hand D. J., (2019), "Fraud Detection in Telecommunications and Banking: Discussion of Becker, Volinsky and Sudjianto*et al*., (2019)," *Techno metric*s, vol. 52, no. 1, pp. 34-38.

James V Stone, (2013). *Bayes' Rule - A Tutorial Introduction to Bayesian Analysis*. Sheffield, UK: Sebtel Press.

Kültür, Y. and Çağlayan, M., (2016). Hybrid approaches for detecting credit card fraud. *Expert Models,* 34(2), p. e12191.

Mishra, C., (2016). Analysis of Credit Card Fraud Detection Techniques. *International Journal of Science and Research (IJSR)*, 5(3), pp.1302-1307.

Melo-Acosta, German E.,*et al*., (2017). "Fraud Detection in Big Data Using Supervised and Semi-Supervised Learning Techniques." *2017 IEEE Colombian Conference on Communications and Computing (COLCOM)*.

Mohammed, Emad, and Behrouz Far., (2018) "Supervised Machine Learning Algorithms for Credit Card Fraudulent Transaction Detection: A Comparative Study." *IEEE Annals of the History of Computing, IEEE*.

Maniraj, S. P., Aditya Saini, Shadab Ahmed and Swarna Sarkar, (2019). Credit Card Fraud Detection using Machine Learning and Data Science. *International Journal of Engineering Research*, 08(09).

Mason, S., (2020). Looking at debit and credit card fraud. *Teaching Statistics*,34 (3), pp.87-91.

Meadowcroft, P., (2015). Combating cardholder not present fraud. *Card Technology Today*, 17(7-8), pp.12-13.

Richard J. Bolton and David J. Hand, 2001. *Unsupervised Profiling Methods for Fraud Detection*. London: Imperial College London.

Raghavendra Patidar, Lokesh Sharma, (2019). Credit Card Fraud Detection Using Neural Network. *International Journal of Soft Computing and Engineering (IJSCE)*, 13-14 May 2011, Jaipur, India.

Shabad, M. and Kavitha, M., (2018). Credit Card Fraud Detection Using Neural Networks at Merchant Side. *Journal of Computational and Theoretical Nanoscience*, 15(11), pp.3373-3375.

Shiyang Xuan ; Guanjun Liu ; Zhenchuan Li ; Lutao Zheng ; Shuo Wang ; Changjun Jiang, (2018). Random forest for credit card fraud detection. *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*, 27-29 March 2018, Zhuhai, China.

Srivastava, A., Kundu, A., Sural, S. and Majumdar, A., (2018). Credit Card Fraud Detection Using Hidden Markov Model. *IEEE Transactions on Dependable and Secure Computing*, 5(1), pp.37-48.

Suvasini Panigrahia, Amlan Kundua, Shamik Surala, A.K. Majumdarb, (2019). Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning. *Information Fusion*, 10 (4), 354-363.

Scott Stone, 2016. *Velocity Checks and Fraud Prevention*. Available from: https://chargeback.com/velocity-checksfraud-prevention/ [Accessed 8 March 2019].

Talabis, M., (2015). *Information Security Analytics,* pp.1-12. Waltham: Syngress.

Tyagi, C. S., Parwekar, P., Singh, P., & Natla, K. (2020). Analysis of Credit Card Fraud Detection Techniques. *Solid State Technology*, 63(6), 18057-18069.

UK Finance, (2018). *Fraud the Facts*. London: UK Finance. Fraud-the-Facts. [Accessed 26 January 2019].

V.Mareeswari, (2016). *Prevention of Credit Card Fraud Detection based on HSVM*. International Conference on Information Communication and Embedded System.

William Brock, Marc-André Boutin, (2019). *Fraud: History, Issues, Tools and Challenges*. DWPV: Davies.Davies-Academy-November-06-2012.pdf [Accessed 24 January 2019].

Xuan, S., Liu, G., Li, Z., Zheng, L., Wang, S., & Jiang, C. (2018, March). Random forest for credit card fraud detection. In *2018 IEEE 15th international conference on networking, sensing and control (ICNSC)* (pp. 1-6). IEEE.

Zareapoor, M., Seeja.K. S., and Afshar Alam, M., (2021). Analysis on Credit Card Fraud Detection Techniques: Based on Certain Design Criteria. *International Journal of Computer Applications*, 52(3), pp.35-42.