Quest Journals
Journal of Research in Humanities and Social Science
Volume 8 ~ Issue 2 (2020)pp.: 04-11
ISSN(Online):2321-9467
www.questjournals.org

Research Paper

Credit card fraud detection using Machine learning algorithms

Andhavarapu Bhanusri
(Assistant professor, Department of Information Technology , ANITS , Sangivalasa ,Visakhapatnam)
K.Ratna Sree Valli , P.Jyothi , G.Varun Sai , R.Rohith Sai Subash
(B.Tech , Department of Information Technology , ANITS , Sangivalasa ,Visakhapatnam)

Corresponding Author: Andhavarapu Bhanusri

ABSTRACT:*Due to a rapid advancement in the electronic commerce technology, the use of credit cards has dramatically increased. Since credit card is the most popular mode of payment, the number of fraud cases associated with it is also rising.Thus, in order to stop these frauds we need a powerful fraud detection system that detects it in an accurate manner. In this paper we have explained the concept of frauds related to credit cards.Here we implement different machine learning algorithms on an imbalanced dataset such as logistic regression, naïvebayes,random forest with ensemble classifiers using boosting technique. An extensive review is done on the existing and proposed models for credit card fraud detection and has done a comparative study on these techniques. So Different classification models are applied to the data and the model performance is evaluated on the basis of quantitative measurements such as accuracy, precision, recall, f1 score, support, confusion matrix. The conclusion of our study explains the best classifier by training and testing using supervised techniques that provides better solution.*

KEYWORDS:*Accuracy, f1 score, precision, recall, support, fraud detection, supervised techniques, credit card*

Received 04 Mar.,2020; Accepted 22Mar.., 2020 © The author(s) 2020.
Published with open access at ***www.questjournals.org***

I. INTRODUCTION

In recent years, the prevailing data mining concerns people with credit card fraud detection model based on data mining. Since our problem is approached as a classification problem, classical data mining algorithms are not directly applicable.This project is to propose a credit card fraud detection system using supervisedlearning algorithm. supervised algorithms are evolutionary algorithms which aim at obtaining better solutions as time progresses.Credit card is the most popular mode of payment. As the number of credit card users is rising world-wide, the identity theft is increased, and frauds are also increasing.In the virtual card purchase, only the card information is required such as card number, expiration date, secure code, etc. Such purchases are normally done on the Internet or over telephone. To commit fraud in these types of purchases, a person simply needs to know the card details. The mode of payment for online purchase is mostly done by credit card. The details of credit card should be kept private. To secure credit card privacy, the details should not be leaked. Different ways to steal credit card details are phishing websites, steal/lost credit cards, counterfeit credit cards, theft of card details, intercepted cards etc. For security purpose, the above things should be avoided. In online fraud, the transaction is made remotely and only the card's details are needed. A manual signature, a PIN or a card imprint are not required at the purchase time. In most of the cases the genuine cardholder is not aware that someone else has seen or stolen his/her card information. The simple way to detect this type of fraud is to analyze the spending patterns on every card and to figure out any variation to the "usual" spending patterns. Fraud detection by analyzing the existing data purchase of cardholder is the best way to reduce the rate of successful credit card frauds. As the data sets are not available and also the results are not disclosed to the public. The fraud cases should be detected from the available data sets known as the logged data and user behavior. At present, fraud detection has been implemented by a number of methods such as data mining, statistics, and artificial intelligence.

1.1 Types of Algorithms

Supervised learning is built to make prediction, given an unforeseen input instance. A supervised learning algorithm takes a known set of input dataset and its known responses to the data (output) to learn the regression/classification model.An algorithm is used to learn the dataset and train it to generate the model for prediction of frauds for the response to new data or test data. Supervised learning uses classification algorithms and regression techniques to developpredictive models.

1.**NAIVE BAYES:**Naive Bayes classifiers calculate the probability of a sample to be of a certain category, based on prior knowledge. They use the Naïve Bayes Theorem, that assumes that the effect of a certain feature of a sample is independent of the other features. That means that each character of a sample contributes independently to determine the probability of the classification of that sample, outputting the category of the highest probability of the sample. In Bernoulli Naïve Bayes the predictors are boolean variables. The parameters that we use to predict the class variable take up only values yes or no.The basic idea of Naive Bayes technique is to find the probabilities of classes assigned to texts by using the joint probabilities of words and classes.

2.LOGISTICREGRESSION: Logistic regression is basically a supervised classification algorithm. In a classification problem, the target variable(or output), y, can take only discrete values for given set of features(or inputs), X. The logistic regression model described relationship between predictors that can be continuous, binary, and categorical. Logistic regression becomes a classification technique only when a decision threshold is brought into the picture. The setting of the threshold value is a very important aspect of logistic regression and is dependent on the classification problem itself. It predicts the probability that a given data entry belongs to the category numbered as “1”. Just like Linear regression assumes that the data follows a linear function, Logistic regression models the data using the sigmoid function.

3.RANDOM FOREST: The random forest is a supervised learning algorithm that randomly creates and merges multiple decision trees into one “forest.” The goal is not to rely on a single learning model, but rather a collection of decision models to improve accuracy. The primary difference between this approach and the standard decision tree algorithm is that the root nodes feature splitting nodes are generated randomly.

4.**BOOSTING TECHNIQUE**: Boosting is an ensemble modeling technique which attempts to build a strong classifier from the number of weak classifiers. This procedure is continued, and models are added until either the complete training data set is predicted correctly, or the maximum number of models are added.**AdaBoost** was the first really successful boosting algorithm developed for the purpose of binary classification. Adaboost is short for Adaptive Boosting and is a very popular boosting techniquewhich combines multiple “weak classifiers” into a single “strong classifier”.

II. LITERATURE STUDY

2.1 The Uncertain Case of Credit Card Fraud Detection: Uncertainty is inherent in many real-time event-driven applications. Credit card fraud detection is a typical uncertain domain, where potential fraud incidents must be detected in real time and tagged before the transaction has been accepted or denied. We present extensions to the IBM Proactive Technology Online (PROTON) open source tool to cope with uncertainty. The inclusion of uncertainty aspects impacts all levels of the architecture and logic of an event processing engine. The extensions implemented in PROTON include the addition of new built-in attributes and functions, support for new types of operands, and support for event processing patterns to cope with all these. The new capabilities were implemented as building blocks and basic primitives in the complex event processing programmatic language. This enables implementation of event-driven applications possessing uncertainty aspects from different domains in a generic manner. A first application was devised in the domain of credit card fraud detection. Our preliminary results are encouraging, showing potential benefits that stemfrom incorporating uncertainty aspects to the domain of credit card fraud detection[1].(Author-Fabiana Fournier, Ivo carriea, Inna skarbovsky)

2.2A Comparative Analysis of Various Credit Card Fraud Detection Techniques: Fraud is any malicious activity that aims to cause financial loss to the other party. As the use of digital money or plastic money even in developing countries is on the rise so is the fraud associated with them. Frauds caused by Credit Cards have costs consumers and banks billions of dollars globally. Even after numerous mechanisms to stop fraud, fraudsters are continuously trying to find new ways and tricks to commit fraud. Thus, in order to stop these frauds we need a powerful fraud detection system which not only detects the fraud but also detects it before it takes place and in an accurate manner. We need to also make our systems learn from the past committed frauds and make them capable of adapting to future new methods of frauds. In this paper we have introduced the concept of frauds related to credit cards and their various types. We have explained various techniques available for a fraud detection system such as Support Vector Machine (SVM), Artificial Neural Networks (ANN), Bayesian Network, K- Nearest Neighbor (KNN), Hidden Markov Model, Fuzzy Logic Based System and Decision Trees. An extensive review is done on the existing and proposed models for credit card fraud detection and has done a comparative study on these techniques on the basis of quantitative measurements such as accuracy, detection rate and false alarm rate. The conclusion of our study explains the drawbacks of existing models and provides a better solution in order to overcome them[2].(Author-Yashvi Jain, Namrata Tiwari, ShripriyaDubey,Sarika Jain)

2.3 Credit Card Fraud Detection System-A Survey: The credit card has become the most popular mode of payment for both online as well as regular purchase, in cases of fraud associated with it are also rising. Credit card frauds are increasing day by day regardless of the various techniques developed for its detection. Fraudsters are so expert that they generate new ways for committing fraudulent transactions each day which demands constant innovation for its detection techniques. Most of the techniques based on Artificial Intelligence, Fuzzy logic, neural network, logistic regression, naïve Bayesian, Machine learning, Sequence Alignment, decision tree, Bayesian network, meta learning, Genetic Programming etc., these are evolved in detecting various credit card fraudulent transactions. This paper presents a survey of various techniques used in credit card fraud detection mechanisms[3]. (Author-Dinesh L. Talekar, K. P. Adhiya)

III. METHODOLOGY

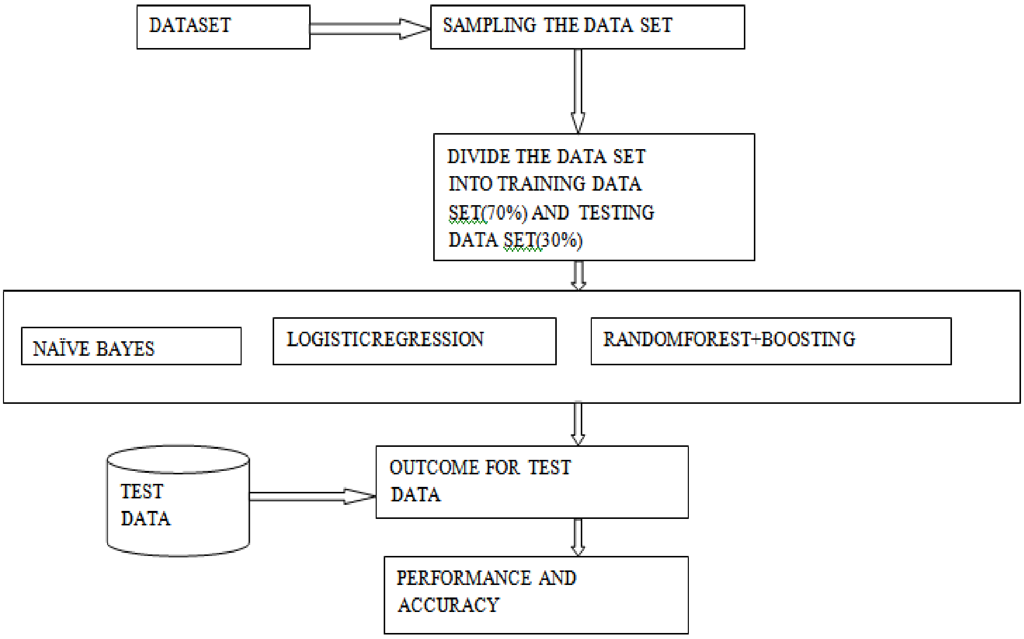


Figure 3.1System Architecture

Dataset: In this paper credit card fraud detection dataset was used,which can be downloaded from Kaggle.This dataset contains transactions,occurred in two days,made in September 2013 by European cardholders. The dataset contains 31 numerical features. Since some of the input variables contains financial information, the PCA transformation of these input variables were performed in order to keep these data anonymous. Three of the given features weren't transformed. Feature "Time" shows the time between first transaction and every other transaction in the dataset. Feature "Amount" is the amount of the transactions made by credit card. Feature "Class" represents the label and takes only 2 values: value 1 in case fraud transaction and 0 otherwise.

Sampling: Further the data set is minimized to 560 transactions.Where 228 fraud and 332 normal transactions.

Divide the dataset:The dataset is divided into trained data set and test data set. 70% of the data set is under training and the remaining 30% is under testing.Here we are using some supervised machine learning algorithms. The algorithms areNaive Bayes**,** Logistic RegressionandRandom Forest with boosting technique.

Naïve Bayes: Bayes theorem: Bayes theorem find probability of event occurring given probability of another event that has been alreadyoccurred.Naïve Bayes algorithm is easy and fast. This algorithm need less training data and highlyscalable

P (A/B) = (P (B/A) P (A)) / P (B)

Where, P (A) – Priority of A P (B) – Priority of B

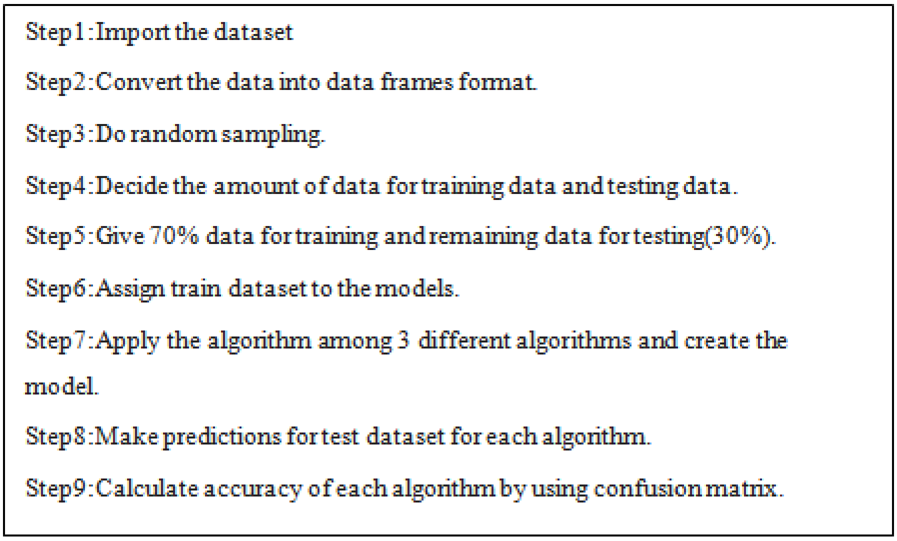
P (A/B) – Posteriori priority of B

LogisticRegression: This algorithm similar to linear regression algorithm.But linear regression issued for predict / forecast values and Logistic regression is used for classificationtask.This algorithm easy for binary and multivariate classification task. Binomial is of 2 possible types (i.e. 0 or 1) only. Multinomial is of 3 or possible types and which are not ordered and Ordinal is in ordered in category (i.e. very poor, poor , good, very good).

Random Forest: First, start with the selection of random samples from a given dataset.Next, this algorithm will construct a decision tree for every sample. Then it will get the prediction result from every decision tree. Then voting will be performed for every predicted result. So finally, select the most voted prediction result as the final prediction result.

AdaBoost: AdaBoost is a machine learningalgorithm. Mainly developed for binary classification.For AdaBoost, Each instance in the training dataset is weighted. Initial weight is set To:
Weight (xi)= (1/n)Where, xi – i^{th} traininginstance
n– Number of training instance

Algorithm steps for finding the Best algorithm:



Step1:Import the dataset

Step2:Convert the data into data frames format.

Step3:Do random sampling.

Step4:Decide the amount of data for training data and testing data.

Step5:Give 70% data for training and remaining data for testing(30%).

Step6:Assign train dataset to the models.

Step7:Apply the algorithm among 3 different algorithms and create the model.

Step8:Make predictions for test dataset for each algorithm.

Step9:Calculate accuracy of each algorithm by using confusion matrix.

Test data:After training is done on the datasetthen testing process take place.

Outcome for test data: We will get the respective results for each algorithm and performance is displayed in graphs.

Accuracy results: Finallyresults of each algorithm are shown with accuracy and the best algorithm is identified.

Evaluation: There are a variety of measures for various algorithms and these measures have been developed to evaluate very different things .So it should be criteria for evaluation of various proposed method. False Positive(FP),False Negative(FN),True Positive(TP),True Negative(TN) and the relation between them are quantities which usually adopted by credit card fraud detection researchers to compare the accuracy of different approaches. The definitions of mentioned parameters are presented below:

- **True Positive(TP):**The true positive rate represents the portion of the fraudulent transactions correctly being classified as fraudulent transactions.

True positive=Tp/TP+FN

- **TrueNegative(TN):**The true negative rate represents the portion of the normal transactions correctly being classified as normal transactions.

True negative=TN/TN+FP

- **False Positive (FP):**The false positive rate indicates the portion of the non-fraudulent transactions wronglybeing classified as fraudulent transactions.

False positive=FP/FP+TN

- **False Negative (FN):**The false negative rate indicates the portion of the non-fraudulent transactions wrongly being classified as normal transactions.

False negative=FN/FN+TP

- **Confusion matrix:** The confusion matrix provides more insight into not only the performance of a predictive model, but also which classes are being predicted correctly, which incorrectly, and what type of errors are being made.The simplest confusion matrix is for a two-class classification problem, with negative and positive classes. In this type of confusion matrix, each cell in the table has a specific and well-understood name

Predicted	Positive	Negative
Positive	TP	FN
Negative	FP	TN

- **Accuracy:**Accuracy is the percentage of correctly classified instances.It is one of the most widely used classification performance metrics.

$$\text{Accuracy}=\frac{\text{Number of correct predictions}}{\text{Total Number of predictions}}$$

Or for binary classification models.The accuracy can be defined as:

$$\text{Accuracy}=\frac{TP+TN}{TP+TN+FP+FN}$$

- **Precision and recall:**Precision is the number of classifiedPositive or fraudulent instances that actually are positive instances.

Precision = Tp/(Tp+Fp)

- Recall is a metric that quantifies the number of correct positive predictions made out of all positive predictions that could have been made.Unlike precision that only comments on the correct positive predictions out of all positive predictions, recall provides an indication of missed positive predictions.Recall is calculated as the number of true positives divided by the total number of true positives and false negatives.

Recall = Tp / (Tp + Fn)

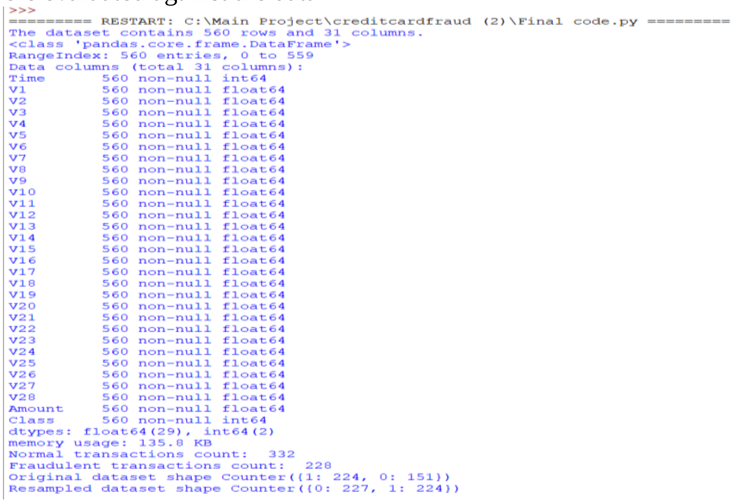
- **F1 score:** F1 Score is the weighted average of Precision and Recall. Therefore, this score takes both false positives and false negatives into account.

F1 Score = 2*(Recall * Precision) / (Recall + Precision)

- **Support:** The support is the number of samples of the true response that lie in that class.Support is the number of actual occurrences of the class in the specified dataset. Imbalanced support in the training data may indicate structural weaknesses in the reported scores of the classifier and could indicate the need for stratified sampling or rebalancing. Support doesn’t change between models but instead diagnoses the evaluation process.

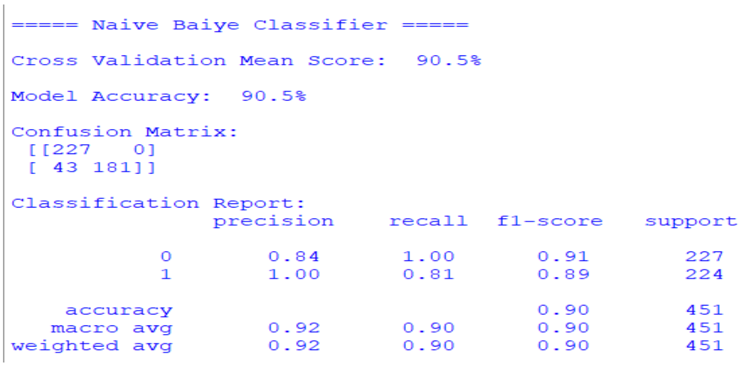
IV. RESULTS AND DISCUSSIONS:

The following results were observed as the models - naive bayes , logistic regression and random forest with boosting technique were evaluated against the data



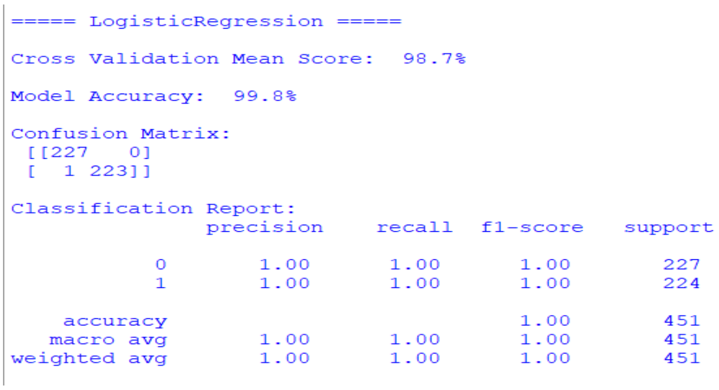
```
>>>
========= RESTART: C:\Main Project\creditcardfraud (2)\Final code.py =========
The dataset contains 560 rows and 31 columns.
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 560 entries, 0 to 559
Data columns (total 31 columns):
Time       560 non-null int64
V1         560 non-null float64
V2         560 non-null float64
V3         560 non-null float64
V4         560 non-null float64
V5         560 non-null float64
V6         560 non-null float64
V7         560 non-null float64
V8         560 non-null float64
V9         560 non-null float64
V10        560 non-null float64
V11        560 non-null float64
V12        560 non-null float64
V13        560 non-null float64
V14        560 non-null float64
V15        560 non-null float64
V16        560 non-null float64
V17        560 non-null float64
V18        560 non-null float64
V19        560 non-null float64
V20        560 non-null float64
V21        560 non-null float64
V22        560 non-null float64
V23        560 non-null float64
V24        560 non-null float64
V25        560 non-null float64
V26        560 non-null float64
V27        560 non-null float64
V28        560 non-null float64
Amount     560 non-null float64
Class      560 non-null int64
dtypes: float64(29), int64(2)
memory usage: 135.8 KB
Normal transactions count:  332
Fraudulent transactions count:  228
Original dataset shape Counter({1: 224, 0: 151})
Resampled dataset shape Counter({0: 227, 1: 224})
```

4.1 Model Evaluation Results



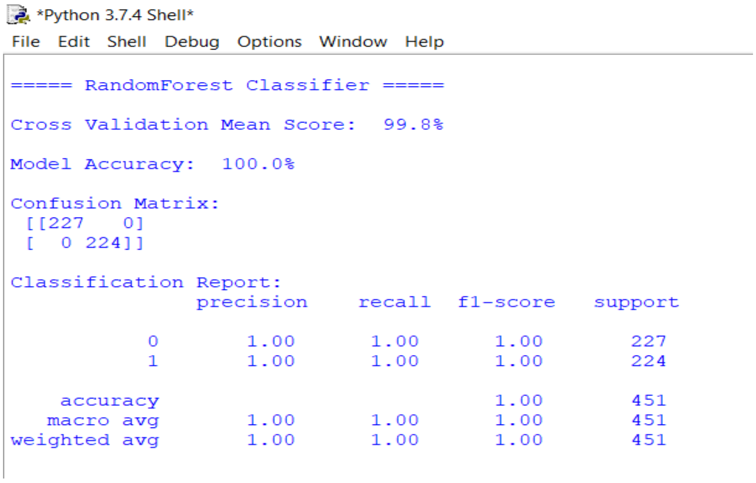
```
===== Naive Baiye Classifier =====

Cross Validation Mean Score:  90.5%

Model Accuracy:  90.5%

Confusion Matrix:
 [[227   0]
 [ 43 181]]

Classification Report:
              precision    recall  f1-score   support

           0       0.84      1.00      0.91       227
           1       1.00      0.81      0.89       224

    accuracy                           0.90       451
   macro avg       0.92      0.90      0.90       451
weighted avg       0.92      0.90      0.90       451
```

Fig 4.1.1: metrics for naïve bayes classifier model



```
===== LogisticRegression =====

Cross Validation Mean Score:  98.7%

Model Accuracy:  99.8%

Confusion Matrix:
 [[227   0]
 [  1 223]]

Classification Report:
               precision    recall  f1-score   support

           0       1.00      1.00      1.00       227
           1       1.00      1.00      1.00       224

    accuracy                           1.00       451
   macro avg       1.00      1.00      1.00       451
weighted avg       1.00      1.00      1.00       451
```

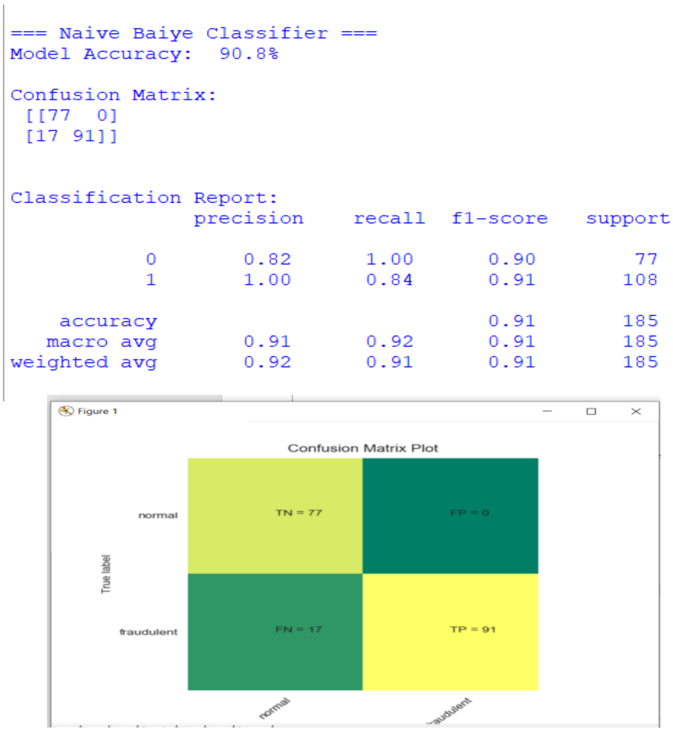
Fig 4.1.2: metrics for logistic regression classifier model



```
===== RandomForest Classifier =====

Cross Validation Mean Score:  99.8%

Model Accuracy:  100.0%

Confusion Matrix:
 [[227   0]
 [  0 224]]

Classification Report:
               precision    recall  f1-score   support

           0       1.00      1.00      1.00       227
           1       1.00      1.00      1.00       224

    accuracy                           1.00       451
   macro avg       1.00      1.00      1.00       451
weighted avg       1.00      1.00      1.00       451
```

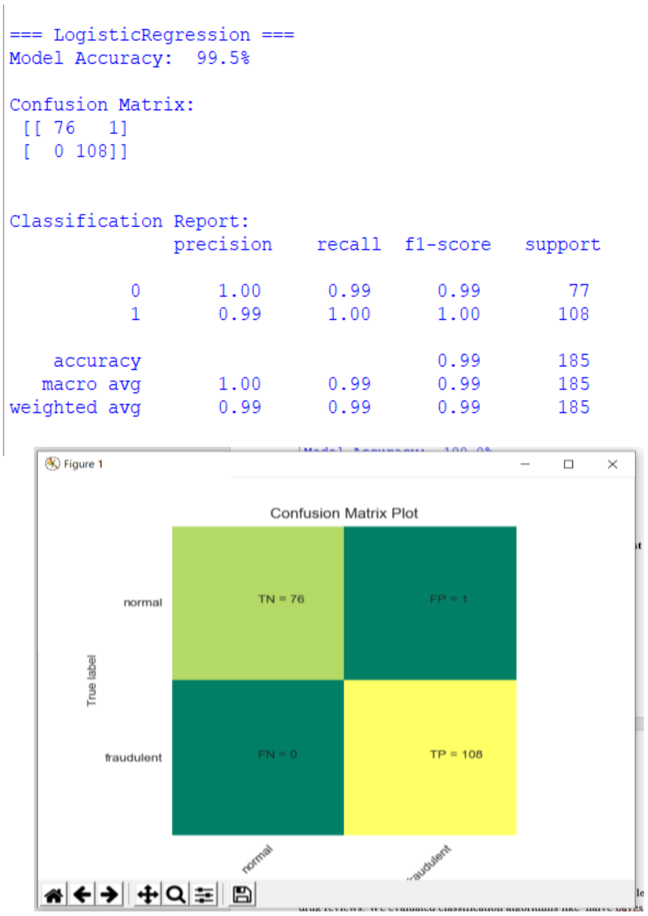
Fig 4.1.3: metrics for random forest classifier model

4.2 Model Test Results And Graphs



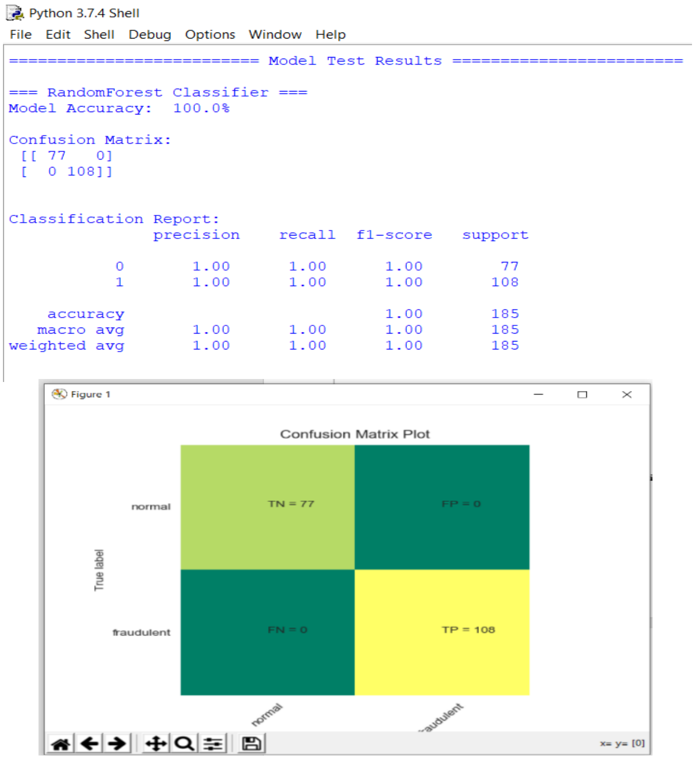
```
=== Naive Baiye Classifier ===
Model Accuracy:  90.8%

Confusion Matrix:
 [[77  0]
 [17 91]]


Classification Report:
               precision    recall  f1-score   support

           0       0.82      1.00      0.90        77
           1       1.00      0.84      0.91       108

    accuracy                           0.91       185
   macro avg       0.91      0.92      0.91       185
weighted avg       0.92      0.91      0.91       185
```

Fig 4.2.1: Test Resultand confusion matrix plot for naive bayes classifier model



```
=== LogisticRegression ===
Model Accuracy:  99.5%

Confusion Matrix:
 [[ 76   1]
 [  0 108]]


Classification Report:
               precision    recall  f1-score   support

           0       1.00      0.99      0.99        77
           1       0.99      1.00      1.00       108

    accuracy                           0.99       185
   macro avg       1.00      0.99      0.99       185
weighted avg       0.99      0.99      0.99       185
```

Fig 4.2.2: Test Result and confusion matrix plot for logistic regression model



```
========================= Model Test Results ========================

=== RandomForest Classifier ===
Model Accuracy:  100.0%

Confusion Matrix:
 [[ 77   0]
 [  0 108]]


Classification Report:
               precision    recall  f1-score   support

           0       1.00      1.00      1.00        77
           1       1.00      1.00      1.00       108

    accuracy                           1.00       185
   macro avg       1.00      1.00      1.00       185
weighted avg       1.00      1.00      1.00       185
```

Fig 4.2.3: Test Result and confusion matrix plot for random forest model

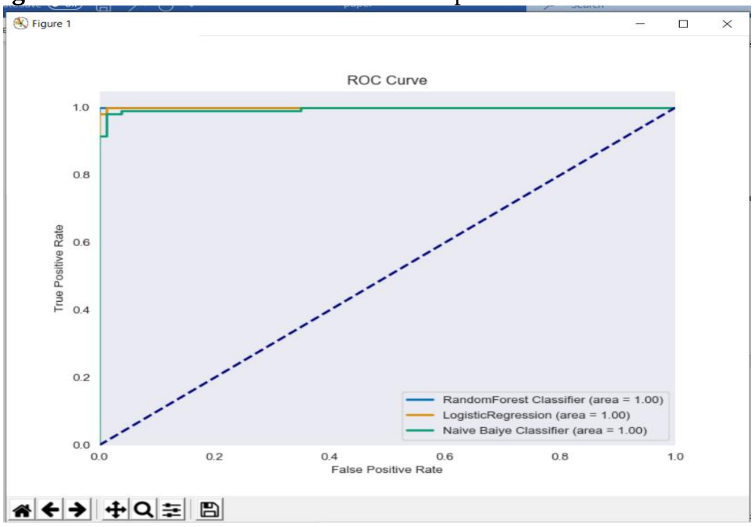


Fig 4.2.4: ROC Curve for all the three models

V. CONCLUSION

In this paper, we studied applications of machine learning like Naïve Bayes, Logistic regression, Random forest with boosting and shows that it proves accurate in deducting fraudulent transaction and minimizing the number of false alerts. Supervised learning algorithms are novel one in this literature in terms of application domain. If these algorithmsare applied into bank credit card fraud detection system, the probability of fraud transactions can be predicted soon after credit card transactions. And a series of anti-fraud strategies can be adopted to prevent banks from great losses and reduce risks. The objective of the study was taken differently than the typical classification problems in that we had a variable misclassification cost. Percision,recall.f1-score,support and accuracy are used to evaluate the performance for the proposed system. By comparing all the three methods, we found that random forest classifier with boosting technique is better than the logistic regression and naïve bayes methods.

FUTURE SCOPE

From the above comparative analysis of the various credit card fraud detection techniques it is clear that Random Forest with Boosting technique performs best in this scenario. But the drawbacks of this paper by using the abovethree algorithms we cannot determine the names of fraud and unfraud transactions for the given dataset using machine learning. For the further development of the project we can work to solve this problem by using various methods.

REFERENCES

Papers:

[1]. Fabiana Fournier, Ivo carriea, Inna skarbovsky, The Uncertain Case of Credit Card Fraud Detection, The 9th ACM International Conference On Distributed Event Based Systems(DEBS15) 2015.

[2]. Yashvi Jain, Namrata Tiwari, ShripriyaDubey, Sarika Jain, A Comparative Analysis of Various Credit Card Fraud Detection Techniques, Blue Eyes Intelligence Engineering And Sciences Publications 2019

[3]. Dinesh L. Talekar, K. P. Adhiya, Credit Card Fraud Detection System-A Survey, International journal of modern engineering research(IJMER) 2014.

[4]. SamanehSorournejad, Zahra Zojaji, Reza Ebrahimi Atani, Amir Hassan Monadjemi, A Survey of credit card fraud detection techniques: Data and techniques oriented perspective.

[5]. Lakshmi S V S S, Selvani Deepthi Kavila, Machine learning for credit card fraud detection system, International Journal Of Applied Engineering Research ISSN 2018.

Andhavarapu Bhanusri "Credit card fraud detection using Machine learning algorithms" *Quest Journals Journal of Research in Humanities and Social Science, vol. 08(02), 2020, pp. 04-11.*