International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 1679-1685 www.ijaem.net ISSN: 2395-5252

Credit card Fraud detection using Machine learning Algorithm.

Smitha N[1,4], Shivaprasad B.J [1,5], Mr. Ganesh Babu[2] and Dr. Renuka A[3]

[1]*MTech CSE, Department of Computer Science and Engineering, MIT, MAHE, Manipal*
[2]*Professor, Department of Computer Science and Engineering, MIT, MAHE, Manipal*
[3]*Professor, Department of Computer Science and Engineering, MIT, MAHE, Manipal*

Submitted: 05-06-2022 Revised: 17-06-2022 Accepted: 20-06-2022

ABSTRACT
Credit card is the commonly used payment mode in the recent years. As the technology is developing, the number of fraud cases are also increasing and finally poses the need to develop a fraud detection algorithm to accurately find and eradicate the fraudulent activities. This study proposes a variety of machine learning algorithms such as logistic regression, random forest, and Naive Bayes for handling the highly unbalanced dataset. Finally, this research work will calculate the accuracy, precision, recall, f1 score, confusion matrix, and Roc-auc score.

Keywords: Fraud detection, Credit card, Machine learning, Accuracy, F1 score, Precision, Recall Roc-auc score, Confusion matrix.

I. INTRODUCTION

This research is primarily concerned with identifying the fraudulent credit card transactions. To achieve this goal, the fraudulent and non-fraudulent transactions must be classified. Using machine learning based classification algorithms, the primary goal is to develop a fraud detection algorithm that finds fraud transactions in less time while maintaining high accuracy. Due to technology's rapid advancement, payments by cash are being reduced and online payments being increased, allowing fraudsters to make anonymous transactions.

Online payments may require only card number, expiration date, and CVV, and this information can be lost without the merchant's knowledge, sometimes without them even knowing. In the case of online purchases, fraudsters abuse phishing techniques to gain our details. Our systems may have been compromised at the time you provide us with data. A fraudster needs only the user's credit card information for some purchases to carry out fraud, and the user may not even know that the information has been leaked. While card information should be kept confidential, sometimes it is out of our hands. To determine whether a transaction is fraud or not, The customer's spending pattern must be determined. Phishing websites may leak information, and the card itself may be lost or stolen. Machine learning can be used to identify whether a is genuine and based on existing data.

Types of Frauds: -

- Data phishing
- Application Fraud
- Card Theft
- Online and Offline
- Telecommunication Fraud

II. RELATED WORK

There are many studies that try to find whether a transaction is fraudulent or not. Still having many challenges and trying to overcome those problems. Fraud in any form is criminal. Credit card fraud is theft.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 1679-1685 www.ijaem.net ISSN: 2395-5252

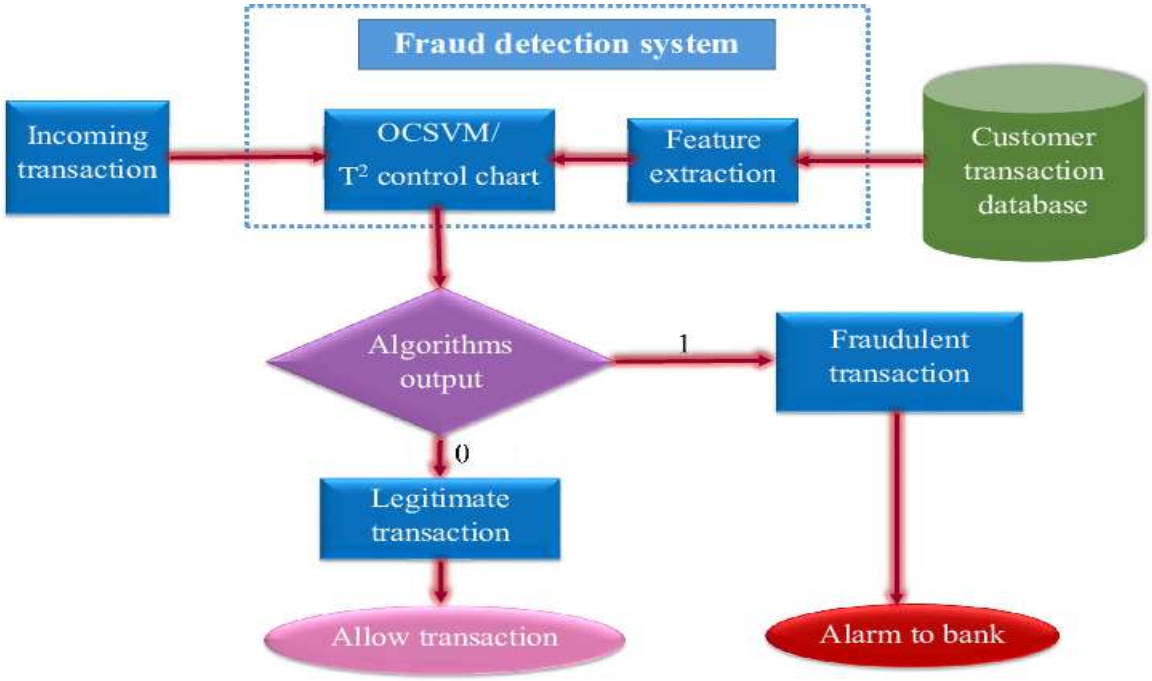


Fig.3.1: Workflow overview.

Many companies use Data Mining Techniques to find fraud by using some traditional methods, which are no longer prevalent, and this is because fraudsters have become so sophisticated that they can commit fraud even if they do not follow the rules. Therefore, using Machine Learning is the conventional method.

Additionally, machine learning comes with its own set of challenges. Kaggle data has a great deal of imbalance, which could provide us with the best algorithms for the given challenges. The algorithm is accurate to a maximum of 99.9% even if it is not good due to the heavy imbalance. Here, the oversampling is considered to provide us with good results as in , Outlier detection and removal algorithms are used to accurately predict fraudulent transactions in a credit card transaction dataset as in.

Outlier data enables the detection of anomalous activity. Fraudsters are so clever that after a large number of algorithms and mechanisms are proposed to stop fraudulent transactions, they always find new ways to make anonymous transactions, and sometimes even the proposed algorithm cannot determine whether the transaction is fraudulent or not. In order to stop these frauds, the proposed algorithm should be made to learn from past frauds so it can be used to prevent future frauds. It can even detect the fraud before it occurs.

III. METHODOLOGY

The dataset was obtained from Kaggle, a data analysis website that provides datasets. This dataset consists of 31 columns, 28 of which are named v1-v28 to protect sensitive data. There are also columns for Time, Amount, and Class. Immediately following a transaction is a time gap shown by time. Money transacted is amount. Valid transactions are classified into class 0, and fraudulent transactions are classified into class 1. Plotting different graphs allows us to check for inconsistencies and to comprehend the data visually:

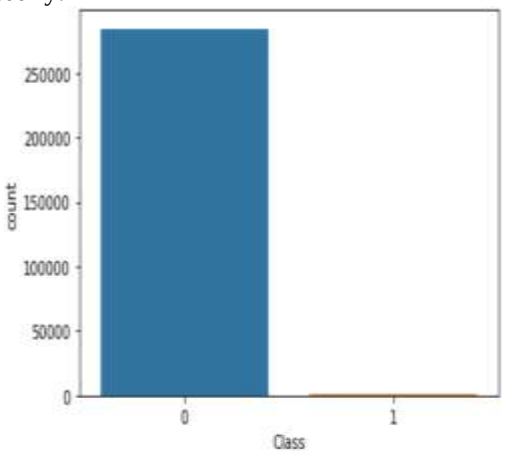


Fig.3.2: This graph shows that the number of fraudulent transactions is much lower than the legitimate ones.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 1679-1685 www.ijaem.net ISSN: 2395-5252

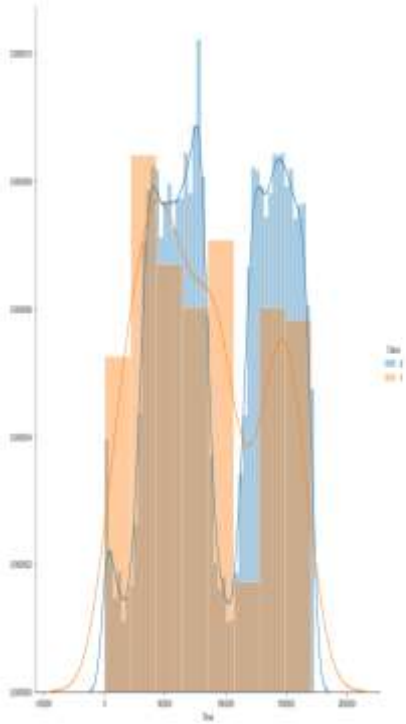
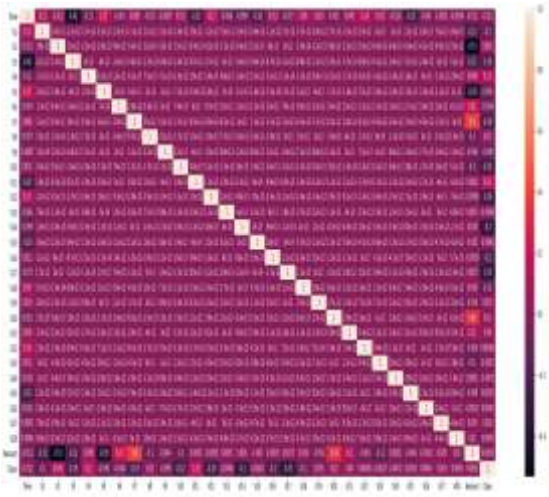


Fig.3.3:-This graph shows the times at which transactions were done within two days. It can be seen that the least number of transactions were made during night time and highest during the days.

After checking this dataset, we plot a histogram for every column. This is done to get a graphical representation of the dataset which can be used to verify that there are no missing any values in the dataset. This is done to ensure that we don't require any missing value imputation and the machine learning algorithms can process the dataset smoothly.

After this analysis, we plot a heatmap to get a colored representation of the data and to study the correlation between out predicting variables and the class variable. This heatmap is shown below:



The dataset is now formatted and processed. The time and amount column are standardized and the Class column is removed to ensure fairness of evaluation. The data is processed by a set of algorithms from modules. The following module diagram explains how these algorithms work together: This data is fit into a model and the following outlier detection modules are applied on it:

1. **Random Forest**
2. **Logistic Regression**
3. **Logistic Regression**

These algorithms are a part of sklearn. The ensemble module in the sklearn package includes ensemble-based methods and functions for the classification, regression and outlier detection. This free and open-source Python library is built using NumPy, SciPy and matplotlib modules which provides a lot of simple and efficient tools which can be used for data analysis and machine learning. It features various classification, clustering and regression algorithms and is designed to interoperate with the numerical and scientific libraries. We've used Jupyter Notebook platform to make a program in Python to demonstrate the approach that this paper suggests. This program can also be executed on the cloud using Google Collab platform which supports all python notebook files. Detailed explanations about the modules with pseudocodes for their algorithms and output graphs are given as follows:

a. Dataset and Machine Learning Libraries

The dataset contains transactions of European credit card holders of September 2013 for two days it contains v1-v28 PCA [4] feature

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 1679-1685 www.ijaem.net ISSN: 2395-5252

because of confidentiality issues and Time, Amount, which are known features and class with 0 and 1 where 1 means fraud 0 means non fraud. The model is implemented in google collab using Python as programming language. Libraries like Panda, NumPy, Matplotlib are used for further data pre-processing.

3.2 Data Pre-processing

The dataset is the first step before any analysis. The information () and the description () methods were used. Null and missing details should be addressed. Using sklearn to handle missing values, To import simple imputer class. Override the default value of the object class to replace the missing data with the average value of the object class.

3.3 Feature Extraction

Irrelevant characteristics detract from the model's performance. Our model was improved by identifying the most relevant properties of the dataset. PCA is a dimensionality reduction technique for identifying correlations and patterns in a dataset, so as to make it easier to transform the dataset into significantly lower dimensions without sacrificing data integrity. Its main aim is to remove inconsistencies, Redundant data, highly correlated features.

3.4 Data Splitting

Data set is split in the ratio of 0.65:0.35 where the former is test data and latter is testing data.

3.5 Machine Learning Model Training

In this study, Random Forest, Logistic Regression, and Nave Bayes were used as machine learning techniques.

3.5.1 Random Forest

Random Forest is a classification algorithm in which it contains many numbers of decision trees for different subsets of the dataset and average of all decision trees accuracy and improves the total accuracy. If number of decision trees increases the accuracy of random forest also increases the random forest is same as decision tree, but it contains main of them from which a better outcome can be expected.

3.5.2Logistic Regression

It is used for both classification and regression, but it is widely used for classification. The output is a binary belonging to one of the classes. It is used to predict output with the help of dependent variables. This algorithm easily binary classification to two values 0 or 1

$$p = 1/1 + e^{-(a0+a1x1+a2x2+\cdots....+anxn)} \quad (1)$$

Eq. 1 Explains the principle and how the logistic Regression works. In above equation a0+a1x1+a2x2+⋯.... +anxn a0, a1…. an. are coefficients and x1, x2…...xn are independent variables, p is outcome.

3.5.3Naïve Bayes Classifier (NB)

A classification algorithm which uses Bayesian principle to find the output. It takes the probability of an event (feature) with that probability it calculates the probability of another output and based on it shoes whether it is fraudulent transaction or not.

$$p(c/x) = p(X\ 1/c) * p(x\ 2/c) *.. * p(xn/c) * p(c) \quad (2)$$

Eq. 2 Explains the principle of Naive Bayes and how it works. The above equation is outcome of probability events naive bias uses Bayesian principle for predicting the outcome.

Confusion matrix: By providing information about correctly and incorrectly classified classes, the confusion matrix provides us with more knowledge about how our prediction model performs.

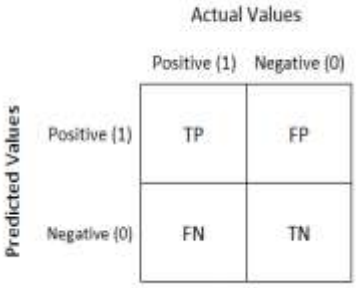


Figure3.4: Confusion Matrix Formation

Accuracy: Accuracy is the percentage of correctly predicted outputs
Precision: Number of correctly classified outputs can be used to measure the degree of precision.
Recall: the measure of our model correctly identifying True Positives
F1 score: Average of Precision and Recall.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 1679-1685 www.ijaem.net ISSN: 2395-5252

IV. EXPERIMENTS AND RESULTS

The accuracy, recall, precision scores were calculated as well as the ROU-AUC scores and the Confusion Matrix for finding the best algorithm. Our strategy will be to explain our results after analyzing the data with data mining techniques in order to determine which algorithm is most suitable for our requirements. (Class 0 means Genuine transaction and 1 means fraud transaction.).

Accuracy in terms of true and false binary representation is:

$$\textbf{Accuracy} = \frac{\textbf{True Positives} + \textbf{True Negatives}}{\textbf{Total number of samples}}$$

Recall can be calculated through obtained true and false positives as follows:

$$\textbf{Recall} = \frac{\textbf{True Positives}}{\textbf{True Positives} + \textbf{False Negatives}}$$

Precision is identified as follows:

$$\textbf{Precision} = \frac{\textbf{True Positives}}{\textbf{True Positives} + \textbf{False Positives}}$$

The F-measure is calculated through precision and recall as follows:

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

4.1 Random Forest Classifier:

The accuracy score, confusion Matrix, precision, recall, f1-score is shown in figure below :

```
********** Model Test Results **********

=== RandomForest Classifier ===
Model Accuracy:  99.9%

Confusion Matrix:
 [[99486    18]
 [   41   138]]

Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     99504
           1       0.88      0.77      0.82       179

    accuracy                           1.00     99683
   macro avg       0.94      0.88      0.91     99683
weighted avg       1.00      1.00      1.00     99683
```

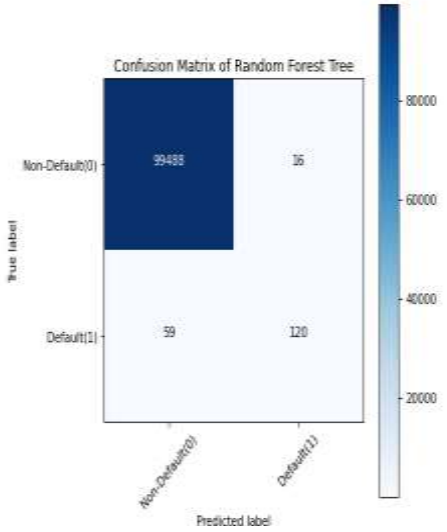


Figure 4.1:Shows Accuracy, confusion Matrix and Classification Report of RF Classifier

4.2 Logistic Regression:

The accuracy score, confusion Matrix, precision, recall, f1-score is shown in figure below:

```
=== LogisticRegression ===
Model Accuracy:  91.0%

Confusion Matrix:
 [[90607  8997]
 [   10   169]]

Classification Report:
              precision    recall  f1-score   support

           0       1.00      0.91      0.95     99504
           1       0.02      0.94      0.04       179

    accuracy                           0.91     99683
   macro avg       0.51      0.93      0.49     99683
weighted avg       1.00      0.91      0.95     99683
```

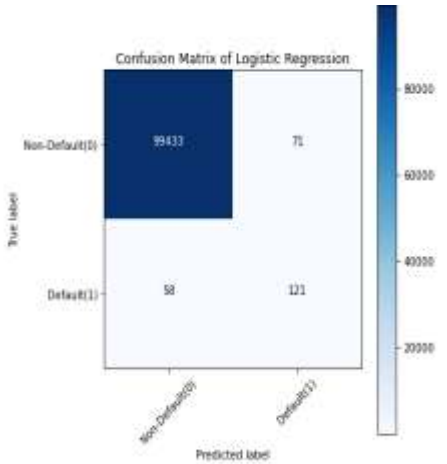


Figure 4.2: Shows Accuracy, confusion Matrix and Classification Report of logistic Regression.

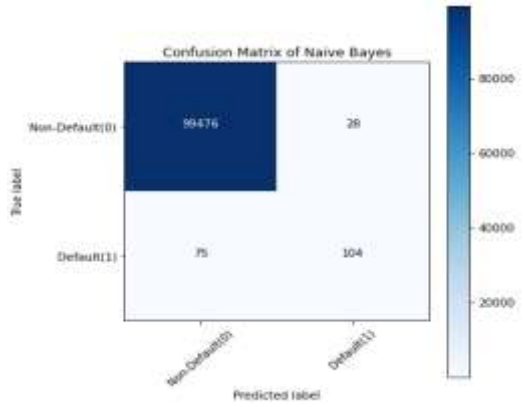
International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 1679-1685 www.ijaem.net ISSN: 2395-5252

4.3 Naïve Bayes Classifier:

The accuracy score, confusion Matrix, precision, recall, f1-score is shown in figure below:

```
=== Naive Baiye Classifier ===
Model Accuracy:  89.4%

Confusion Matrix:
 [[88962 10542]
 [   14   165]]

Classification Report:
              precision    recall  f1-score   support

           0       1.00      0.89      0.94     99504
           1       0.02      0.92      0.03       179

    accuracy                           0.89     99683
   macro avg       0.51      0.91      0.49     99683
weighted avg       1.00      0.89      0.94     99683
```

Figure 4.3: Shows Accuracy, confusion Matrix and Classification Report of logistic Regression.



V. CONCLUSION AND FUTURE SCOPE

In this paper , the algorithms decision Random Forest, logistic regression, naive bayes classification [5] machine learning algorithms, results show that Random Forest classifier performs best with having 99.1% accuracy, 100% precision, 91.1111% recall, 95.3488% f1 scores and 95.5555 ROU-AUC score. By using oversampling technique and applying algorithms, random forest was identified as the most effective algorithm. However, there are differences between all three algorithms depending on whether the decision is fraud-related or not, or by making a particular feature the root and gaining information from all trees.

All algorithms performed almost the same, but if some more real-world data is added, then the accuracy should increase [1]. To achieve 100% accuracy is not possible. The model accuracy can be further enhanced by utilizing multiple sampling techniques. Various techniques can be used for this purpose. The use of more refined algorithms with higher predictability can be supported by imbalanced datasets. Using a genetic algorithm and more data can help us train the model to yield better results.

REFERENCES

[1] R. R. Subramanian, R. Ramar, “Design of Offline and Online Writer Inference Technique”, International Journal of Innovative Technology and Exploring Engineering, vol. 9, no. 2S2, Dec. 2019, ISSN: 2278-3075

[2] Subramanian R.R., Seshadri K. (2019) Design and Evaluation of a Hybrid Hierarchical Feature Tree Based Authorship Inference Technique. In: Kolhe M., Trivedi M., Tiwari S., Singh V. (eds) Advances in Data and Information Sciences. Lecture Notes in Networks and Systems, vol 39. Springer, Singapore

[3] Joshva Devadas T., Raja Subramanian R. (2020) Paradigms for Intelligent IOT Architecture. In: Peng SL., Pal S., Huang L. (eds) Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm. Intelligent Systems Reference Library, vol 174. Springer, Cham

[4] R. R. Subramanian, B. R. Babu, K. Mamta and K. Manogna, "Design and Evaluation of a Hybrid Feature Descriptor based Handwritten Character Inference Technique," 2019 IEEE International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), Tamilnadu, India, 2019, pp. 1-5.

[5] Andrew. Y. Ng, Michael. I. Jordan, "On discriminative vs. generative classifiers: A comparison of logistic regression and naive bayes", Advances in neural information processing systems, vol. 2, pp. 841-848,2002

[6] John Richard D. Kho, Larry A. Vea “Credit Card Fraud Detection Based on Transaction Behaviour” published by Proc. of the 2017 IEEE Region 10 Conference (TENCON), Malaysia, November 5-8, 2017.

[7] 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”

[8] Learning Robert A. Sowah, Moses A. Agebure, Godfrey A. Mills, Koudjo M.

Kaumudi, "New Cluster Undersampling Technique for Class Imbalance "of 2016 IJMLC

[9] Baraneetharan, E. "Role of Machine Learning Algorithms Intrusion Detection in WSNs: A Survey." Journal of Information Technology 2, no. 03 (2020): 161-173

[10] Mitra, Ayushi. "Sentiment Analysis Using Machine Learning Approaches (Lexicon based on movie review dataset)." Journal of Ubiquitous Computing and Communication Technologies (UCCT) 2, no. 03 (2020): 145-152.

[11] Mohamed Jaward Bah, Mohamed Hammad "Progress in Outlier Detection Techniques: A Survey" Hongzhi Wang, of the 2019 IEEE