Credit Card Fraud Detection using XGBoost Classifier with a Threshold Value

Ayushi Maurya
Centre for Advanced Studies ,Lucknow
Arun Kumar (drarun@cas.res.in)
Centre for Advanced Studies https://orcid.org/0000-0001-5694-5861
Shiv Prakash
University of Allahabad

Research Article

Keywords: Credit card, fraud detection, XGBoost, SMOTE, threshold values

Posted Date: June 10th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1722294/v1

Abstract

Over the past years, speedy development of e-commerce techniques has been observed, making it promising for society to choose the best worthwhile product. This has made us dependent on financial institutions, where everyone deals with online banking facilities. Moreover, for payment, people are preferring credit cards over other methods which thus, have a higher risk of getting compromised. Thus, it is a big responsibility of financial institutions to upgrade their existing mechanism to prevent these fraud actions. However, it has also made it easy for scammers to exploit this big chance. Credit Card Fraud Detection helps us to identify fraudulent transactions. The proposed model in this paper detects fraud transaction using the XGBoost classifier to handle the imbalanced data. In the standard approach, the threshold value is pre-defined, which will lead to poor performance. Thus, in our proposed model, calculation and comparison of different threshold values are done to obtain the best value which gives an optimum result and high efficiency.

1. Introduction

Nowadays credit card fraud is increasing day by day. Primarily, it is because of two reasons. Firstly, looking at the COVID situations most people are preferring to use contactless approach [1], [2]. People save their card details on their phones which put them at a higher risk of getting scammed. Secondly, the culprit is often able to steal large amounts of money in a very short time online. Just by sitting in front of the computer and knowing some tips and tricks one gains a lot of money. Moreover, due to COVID-19, the economy has fallen and many people have lost their jobs during this time. So, many people lie on the thievery technique either offline or online to earn a good amount of money. The vast majority of people are utilizing credit cards for purchasing their necessities so fraud-related through is likewise rising progressively. In the current time, practically every one of the endeavours from a majority of enterprises is utilizing the credit card as a mode of payment [3]. Credit card fraud is occurring in all associations like Bank, Finance Industries, Automobile industries, etc. A variety of techniques like data mining, and AI algorithmic methodologies are applied to recognize the misrepresentation in the credit card transaction, but a significant outcome is not achieved yet. Henceforth, there is a need for successful and productive calculations to be developed that works significantly.

Recently, various researchers and analysts have shown a keen interest in analyzing and detecting fraud issues in credit cards by applying machine learning algorithms[4], [5]. In real life, it is very essential to revert in a short period to stop fraudulent transactions. As the scammers are developing new techniques every day, there is a need for frequent training for fraud detection models too. Hence, there is a need for effective and efficient algorithms to be developed that works effectively [6]. A typical approach for two-class problems is to look at observations and classify them according to probability. If the probability is let’s say 0.5 then all the probability above it will be classified as class A and below it as class B. But when the dataset is highly imbalanced, the above trial method will lead to erroneous predictions. The main disadvantage of using any model alone is, that even though it increases the accuracy of the model but the precision of detection is not detected effectively. Thus, the proposed model works on offsetting the

threshold along with using the Machine Learning model. Machine learning techniques have been widely known as a good fraud detection technique and threshold values can be calculated from the ROC curve and then used according to the differential problem. This will help in improving the predictions by giving optimal results.

The additional aspect that has to be given the utmost importance is the cost factor of misclassifying fraud detection. Classifying a non-fraud transaction as fraud is inconvenient at best, but allowing a fraudulent transaction to slip has a more dreadful effect. Thus, offsetting the threshold will help to reduce the false negatives at the cost of false positives and become a feasible plan.

Organization

The paper is organized as follows; section 2 consists of the related work. Section 3 elaborates the proposed methodology of Credit Card Fraud Detection. Section 4 consists of results and discussion. Section 5 comprises the conclusion.

2. Related Work

There has been various research done in the credit card fraud detection area. This is because providing security for the users is of utmost importance to develop trust between the users and the banks. By reviewing the related works, it can be grouped under different types like Machine Learning, Deep Learning, Ensemble, and other approaches as well, which are discussed as follows.

Machine learning approaches are used to give efficient and effective results for the real-time-based application. Various methods have been applied to get the required results. The most common methods are XGBoost, Random Forest, Logistic Regression, and Decision Tree.

Yixuan Zhang et al. [7] worked on XGBoost classifier on the IEEE-CIS Fraud Detection Competition dataset from Kaggle. It showed a comparison of XGBoost with other methods like Support Vector Machine, Random Forest, and Logistic Regression, out of which XGBoost performance was appreciated and had an accuracy of 97.1. Along with XGBoost, some feature engineering techniques with oversampling of the data using SMOTE have been done. Amusan et al. [8] firstly tried to balance the dataset using under-sampling and then they tried to work on different classification models of the machine learning algorithm such as Logistic regression, Random Forest, KNN, and Decision tree classifiers. Random Forest showed significant performance with the highest accuracy of 95%. Even though other algorithms received accuracy above 90% but the main purpose of the research was not only to increase the accuracy alone but to detect the fraud more precisely. Kumar et al. [9] used a random forest algorithm (RFA) alongside with decision tree to differentiate the fraudulent transaction from the normal transaction. This is a supervised learning algorithm that uses a decision tree for the classification of the dataset. The performance of the model was given by accuracy which came out to be 90% for this work. Random Forest has an advantage over other methods as it can be used as Classification as well as Regression. Carcillo et al. [5] proposed the execution of a hybrid approach. This approach combines and uses

supervised learning along with unsupervised learning. This work becomes complicated when one has to track the customer's buying behaviour and the fraudster's new way of fraud patterns. Thus, making use of unsupervised outlier scores which are computed at each level of granularity combined to extend the feature set of a fraud detection classifier. This is then compared and tested on annotated CCFD dataset.

Deep Learning technique is an upcoming and flourishing area of machine learning which produces a state-ofthe-art result in many real-life applications. There is various work done on recurrent neural networks and convolutional neural networks. Mainly, the fraud detection system uses the latter group than the former as it provides context-aware solutions. In recent work, an additional concept of deep learning i.e., sequence modelling has been applied to abstract the serial pattern of the data.

Unlike other authors which used traditional methods, Forough et al. [3] proposed an ensemble model which is based on sequential modelling of data and making use of deep recurrent neural network along with a novel voting mechanism based on an artificial neural network to detect fraud transactions. The authors worked on two real-world datasets to demonstrate the proposed work. Gao et al. [10] gathered and analysed the transaction data flow which reflected customer behaviour. Instead of using the machine learning approach alone, they applied deep learning concepts along with it. The author used XGBoost along with LSTM for comparison of studies. XGBoost is widely used in financial classification and LSTM (Long-Short Term Memory) is used in time series information. LSTM algorithm gives good accuracy without feature extraction whereas XGBoost mainly depends on feature extraction.

Another technique that is popular in detecting credit card frauds is based on Ensemble learning approach. Instead of creating one model and working on it considering it the best, ensemble aims at working as a collection of models. It collaborates different learning algorithms as a group to make one model which will give the optimal result.

Alberto Rodriguez et al. [11] proposed a framework that bonds between a signal processing and pattern recognition around credit card fraud detection. The author executed the proposed model using mixture of scores, which is related to familiar likelihood ratio statistics. Moreover, Shamsolmoali et al. [12] have studied many state-of-the-art data mining approaches, with the bagging ensemble classifier which is based on a decision tree. They demonstrated that their proposed approach was time-effective and handled imbalanced datasets efficiently.

Yalong Xie [13] proposed a "Heterogeneous Ensemble Learning Model based on Data Distribution" (HELMDD) to deal with imbalanced data in CCFD. To validate the efficiency and effectiveness he worked on two different datasets by using the above method and then the comparison of the results was done.

Halvaiee and Akbari [14] have looked into fraud detection using an artificial immune structure. The author's work adds some advances to the artificial recognition structure algorithm, hence improving the precision of the model, which thus reduces the cost and the training time. Izotova et al. [15] compared different approaches used for fraud detection problems. The paper makes use of the heterogeneous as well as the homogeneous Poisson process to obtain the possibility of predicting fraud. Also, it used

classification problems using Machine Learning algorithms and ensemble methods like boosting, and finally, the conclusions were compared. Victoria Priscilla [16] proposed an OXGBoost (optimized XGBoost) approach to handle imbalanced classes in the dataset without making use of resampling techniques. He made use of the RamdomizedSearchCV optimization technique to find the optimal parameters of the OXGBoost and got an accuracy of 98%.

Research gap

After the analysis of the related work, the issue with the above-stated models is that the result is not consistent. For a particular form of dataset, they offer great results and bad or unsatisfactory results for other form of dataset. Also, there has been no work done in which XGBoost model have been combined with threshold value to detect fraud.

3. Methodology

In this section, the working of the proposed model has been explained. The credit card fraud detection method is used for the detection of fraudulent transactions from legitimate transactions [17]. The proposed fraud detector is based on the XGBoost classifier along with setting an accurate threshold. The structure of the proposed model is as follows.

In Fig. 1, the credit card transaction data is first put in the transaction analyzer which contains the customer profile database. This is the database containing all the information related to credit card users. It is this part where the processing of the data will take place. After the transaction analyzer, it goes to the deviation analyzer. The deviation analyzer analyses the transaction. If the transaction shows any deviation, then it is predicted that the fraud has occurred which goes to the fraud history database and halts the transaction further from happening. And if no deviation is found means the transaction is normal and the transaction can pass further.

The transaction analyzer contains different processes as stated in Fig. 2. Firstly, dataset gathering is done. After the collection of the dataset, preprocessing of the data is done, which is followed by feature engineering and data sampling. Preprocessing the dataset is of utmost importance to check if there are any missing values or not to maintain the uniformity of the dataset [18].

In our proposed model, oversampling has been done using SMOTE technique, and finally fed into the XGBoost classifier. After completing its task in the transaction analyzer, it further moves to the Deviation analyzer. This is where the threshold value is calculated and set. The detailed architecture is given below.

The Credit Card Fraud detection system identifies and detects fraud transactions and non-fraud transactions. For the Credit card Transactions, the dataset which contains transactions made by credit cards in September 2013 by European cardholders has been chosen[19].

Table 1: Sample of the dataset

	Time	V1	V2	V3	V4	...	V26	V27	V28	Amount	Class
0	0.000	-1.360	-0.073	2.536	1.378	...	-0.189	0.134	-0.021	149.620	0
1	0.000	1.192	0.266	0.166	0.448	...	0.126	-0.009	0.015	2.690	0
2	1.000	1.358	-1.340	1.773	0.380	...	-0.139	-0.055	-0.061	378.660	0
3	1.000	0.966	-0.185	1.793	-0.863	...	-0.222	0.063	0.060	123.500	0
4	2.000	1.158	0.878	1.549	0.403	...	0.502	0.219	0.215	69.990	0

For the given dataset given in Table 1, we have four columns Time, V1-V28 features, Amount and Class. The Time attribute gives the time between each transaction and the corresponding transaction made by the user. V1V28 are attributes that consist of personal data and sensitive data of the user. The Amount column gives the amount of the transaction and Class distinguishes the transaction as 1 if found fraud else 0.

Figure 3 represents the proposed model for Credit Card Fraud Detection. The model first balances the imbalanced data, XGBoost classifier has been applied which is a boosting ensemble method, and finally offsetting the threshold by calculating the threshold value is done[21], [22]. The following stages are involved in the proposed system, including pre-processing stage, feature extraction, sampling of data, model training, and a model evaluation phase. The first is the Pre-processing phase. This is the stage where all the necessary python libraries are imported along with the given dataset. The dataset is thoroughly checked to see if there are any missing values or not, and further the class distribution of the target variable is done. For better understanding, two classes have been made where Class 0 represents genuine transactions whereas Class 1 represents fraud transactions. It is also observed that the dataset majorly contains legitimate transactions and only a small number of fraudulent transactions is present. Only 0.17% of the total dataset is fraudulent transaction. Thus, the dataset is highly imbalanced. The pre-processing phase ends by scaling the dataset in which the Principal Component Analysis (PCA) has been applied. PCA is used for the dimensionality reduction of big datasets. This is done by transforming a larger dataset into a smaller one keeping all the information intact. Since smaller datasets are better for visualization and exploration, PCA makes the data easy to understand for machine learning algorithms [23]. Thus, its main idea is to decrease the number of variables in the dataset, while preserving the information as much as possible. After studying statistics, it can be observed that the V1-V28 attributes are zero-centred, unlike column Amount and Time. To get a detailed view, histograms for the above attributes have been plotted.

There is not much to analyze from the histograms given in Fig. 4 but there is an unusual distribution of Amount and the Time attribute, thus detailed inspection of the Time column and the Amount column is done.

From the above Fig. 5, it can be inferred that the legitimate transactions fall throughout the night, but their frequency grows with the start of the working day[24]. In contrast, there is a peak of fraudulent

transactions at night around 2 a.m. that looks suspicious. In addition, the data for the fraudulent transactions looks more evenly spread.

The mean of all transaction's amounts to $88.35 while the major transaction recorded in the data set sums to $25,691.16. Yet, the division of the monetary value of all transactions is right-skewed heavily as shown in Fig. 6 [24], [25]. The huge majority of transactions are comparatively small and only a small fraction of transactions come close to the maximum [26].

The next phase is feature extraction. This is the stage where the necessary features are selected, transformed to the required form, and then extracted to be used. As the dataset is highly imbalanced, thus, oversampling the data using SMOTE technique is done. Oversampling helps to decrease the class count discrepancy and SMOTE oversamples the marginal class data by creating new synthetic examples. The following phase is Model training in which the oversampled data is then trained using XGBoost classifier and cross-validation using 3-fold in Stratified k-fold has been applied. The resulting phase is the Model evaluation in which Metrics are evaluated on the ROC AUC by calculating the True Positives & False Positive rates. After evaluation, the function prints the parameters that yield the highest AUC score. Finally, finding a threshold value by looking at the ROC to compare if this value is apt for work or not. By finding the highest accuracy from the confusion matrix, the appropriate threshold is then selected. If the accuracy is not as required then again moving to the feature engineering phase to extract more features to give us a higher accuracy of the program.

In most of the work, it is observed that the threshold value, if any taken has been fixed beforehand. For example, let's take into consideration the binary classification problem. The threshold is fixed at 0.5, and if the probability is below 0.5 then it will be classified as Class A and if the probability is above 0.5, it will be classified as Class B. This hypothesis might be true for binary classification, but for real-time data which is highly imbalanced, it might lead to poor predictions. Threshold moving i.e., setting the threshold according to our requirement is the new method of improving the prediction. In the proposed model, calculation of threshold value is done by analysing the ROC curve which is used to analyse the performance of model at all classification thresholds. Thus, choosing the highest threshold which gives us the best optimum result.

When it comes to fraud detection, one major issue is the cost of misclassifying a transaction. Classifying a normal transaction as fraud is still endurable, but letting a fraud transaction slip away has major consequences. Thus, offsetting the threshold will help us reduce the number of false negatives at the cost of false positives becomes a feasible approach.

4. Results And Discussion

In Fig. 7, it can be seen that the AUC curve for XGBoost is given to be pretty high. When we move towards the peak of the curve, i.e., towards the right along the curve, we get more True Positives (TP) but also acquire False Positives (FP). So, this leads to getting more fraud transactions and also flagging more normal transactions as fraud. In the graph above, the calculated AUC is given as 0.99.

The confusion matrix provides the experimental values of the Threshold as shown in Fig. 8. For Credit Card Fraud Detection using the XGBoost classifier, the empirical value of the threshold comes out to be 0.80 in this case. The false positives, as well as false negatives both, are low. If the threshold value is increased it leads to missing more fraudulent transactions and if the threshold value is lowered, it doubles the rate of several false positives.

5 Conclusion

Nowadays several approaches are available for identifying credit card fraud, but not a single approach can identify it completely before it happens. Generally, it recognizes after the fraud has occurred, when it is difficult for the banks to halt the transaction. This problem has affected the banks adversely.

The main goal of this paper is to detect fraudulent transactions with good accuracy and with good precision.

XGBoost classifier has been applied in the proposed model because it works well with the imbalanced dataset. Also, XGBoost is a boosting ensemble method that has a higher prediction level and it is cost-effective. And, so it will detect the fraud in an effective manner. The concept of offsetting threshold has been applied to the model as well. In this regard, the threshold value is set by looking at the ROC curve. For the proposed model, the threshold value calculated is 0.8. Increasing the threshold value led to skipping fraud transactions and lowering the value led to doubling the rate of false positives.

Declarations

- **Funding:-** No Funding
- **Data Availability:** Available on reasonable request.
- **Conflict of Interest**- Authors have no conflict of interest

References

1. Y. Lucas and J. Jurgovsky, “Credit card fraud detection using machine learning: A survey,” Oct. 2020, [Online]. Available: http://arxiv.org/abs/2010.06479
2. Univerzitet u Istočnom Sarajevu. Faculty of Electrical Engineering, IEEE Industry Applications Society, Institute of Electrical and Electronics Engineers. Bosnia and Herzegovina Section, Institute of Electrical and Electronics Engineers. Serbia and Montenegro Section, and Institute of Electrical and Electronics Engineers, *2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH) : proceedings : March 20-21, 2019, Jahorina, East Sarajevo, Republic of Srpska, Bosnia and Herzegovina*.
3. J. Forough and S. Momtazi, “Ensemble of deep sequential models for credit card fraud detection,” *Applied Soft Computing*, vol. 99, Feb. 2021, doi: 10.1016/j.asoc.2020.106883.

4. V. Chadda and H. Jain, “Credit Card Fraud Detection,” *International Journal of Advanced Science and Technology*, vol. 29, no. 6, pp. 2201–2215, 2020.
5. F. Carcillo, Y. A. le Borgne, O. Caelen, Y. Kessaci, F. Oblé, and G. Bontempi, “Combining unsupervised and supervised learning in credit card fraud detection,” *Information Sciences*, vol. 557, pp. 317–331, May 2021, doi: 10.1016/j.ins.2019.05.042.
6. IEEE Staff and IEEE Staff, *2011 International Conference on Computer, Communication and Electrical Technology*.
7. Y. Zhang, J. Tong, Z. Wang, and F. Gao, “Customer Transaction Fraud Detection Using Xgboost Model,” in *Proceedings - 2020 International Conference on Computer Engineering and Application, ICCEA 2020*, Mar. 2020, pp. 554–558. doi: 10.1109/ICCEA50009.2020.00122.
8. E. A. Amusan, O. M. Alade, J. O. Emuoyibofarhe, and O. D. Fenwa, “Credit Card Fraud Detection on Skewed Data using Machine Learning Techniques,” LAUJCI, 2021. [Online]. Available: www.laujci.lautech.edu.ng
9. E. A. M.Suresh Kumar, V.Soundarya , S.Kavitha , E.S.Keerthika, *CREDIT CARD FRAUD DETECTION USING RANDOM FOREST ALGORITHM*. 2019.
10. J. Gao, W. Sun, and X. Sui, “Research on Default Prediction for Credit Card Users Based on XGBoostLSTM Model,” *Discrete Dynamics in Nature and Society*, vol. 2021, pp. 1–13, Dec. 2021, doi: 10.1155/2021/5080472.
11. S. G. Salazar Addisson, Rodriguez Alberto, and Vergara Luis, *Combination of Multiple Detectors for Credit Card Fraud Detection*.
12. M. Zareapoor and P. Shamsolmoali, “Application of credit card fraud detection: Based on bagging ensemble classifier,” in *Procedia Computer Science*, 2015, vol. 48, no. C, pp. 679–685. doi: 10.1016/j.procs.2015.04.201.
13. Y. Xie, A. Li, L. Gao, and Z. Liu, “A Heterogeneous Ensemble Learning Model Based on Data Distribution for Credit Card Fraud Detection,” *Wireless Communications and Mobile Computing*, vol. 2021, 2021, doi: 10.1155/2021/2531210.
14. N. Soltani Halvaiee and M. K. Akbari, “A novel model for credit card fraud detection using Artificial Immune Systems,” *Applied Soft Computing Journal*, vol. 24, pp. 40–49, 2014, doi: 10.1016/J.ASOC.2014.06.042.
15. A. Izotova and A. Valiullin, “Comparison of Poisson process and machine learning algorithms approach for credit card fraud detection,” in *Procedia Computer Science*, 2021, vol. 186, pp. 721–726. doi: 10.1016/j.procs.2021.04.214.
16. C. V. Priscilla and D. P. Prabha, “Influence of optimizing xgboost to handle class imbalance in credit card fraud detection,” in *Proceedings of the 3rd International Conference on Smart Systems and Inventive Technology, ICSSIT 2020*, Aug. 2020, pp. 1309–1315. doi: 10.1109/ICSSIT48917.2020.9214206.
17. John O. Awoyemi, Adebayo O. Adetunmbi, and Samuel A. Oluwadare, *Credit card fraud detection using Machine Learning Techniques: A Comparative Analysis*.

18. D. Prusti, S. S. Harshini Padmanabhuni, and S. Kumar Rath, “Credit Card Fraud Detection by Implementing Machine Learning techniques.”
19. Y. A. Rodríguez *et al.*, *Fraud Detection in Big Data using Supervised and Semi-supervised Learning Techniques*.
20. Dilip Singh Sisodia, Nerella Keerthana Reddy, and Shivangi Bhandari, *Performance Evaluation of Class Balancing Techniques for Credit Card Fraud Detection*.
21. S. Lei, K. Xu, Y. Huang, and X. Sha, “An xgboost based system for financial fraud detection,” in *E3S Web of Conferences*, Dec. 2020, vol. 214. doi: 10.1051/e3sconf/202021402042.
22. C. Meng, L. Zhou, and B. Liu, “A case study in credit fraud detection with SMOTE and XGboost,” in *Journal of Physics: Conference Series*, Aug. 2020, vol. 1601, no. 5. doi: 10.1088/17426596/1601/5/052016.
23. V. V. Madhav and K. A. Kumari, “Analysis of Credit Card Fraud Data using PCA,” 2020. [Online]. Available: www.iosrjen.org
24. S. Ounacer, S. Ardchir, Z. Rachad, and M. Azouazi, “A Proposed Architecture for Real Time Credit Card Fraud Detection,” 2018. [Online]. Available: www.sciencepubco.com/index.php/IJET
25. C. Meng, L. Zhou, and B. Liu, “A case study in credit fraud detection with SMOTE and XGboost,” in *Journal of Physics: Conference Series*, Aug. 2020, vol. 1601, no. 5. doi: 10.1088/17426596/1601/5/052016.
26. V. Shah, “Data Balancing for Credit Card Fraud Detection using Complementary Neural Networks and SMOTE Algorithm,” 2020.

Figures

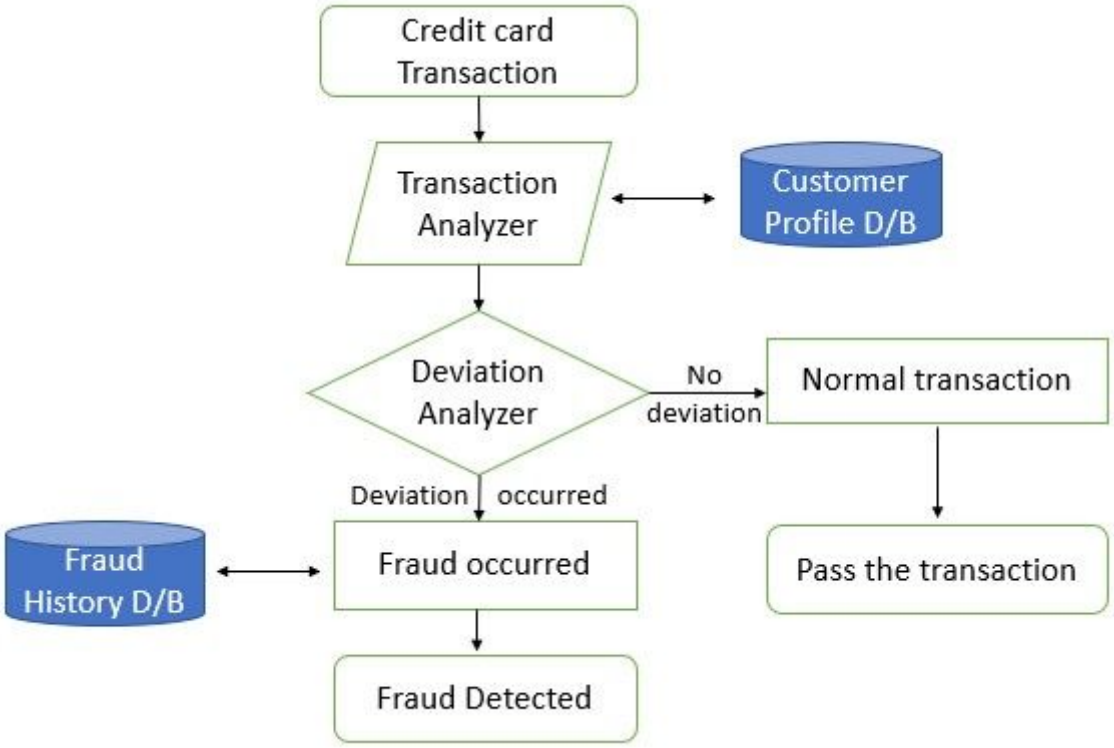

Figure 1

Research Framework of our proposed model

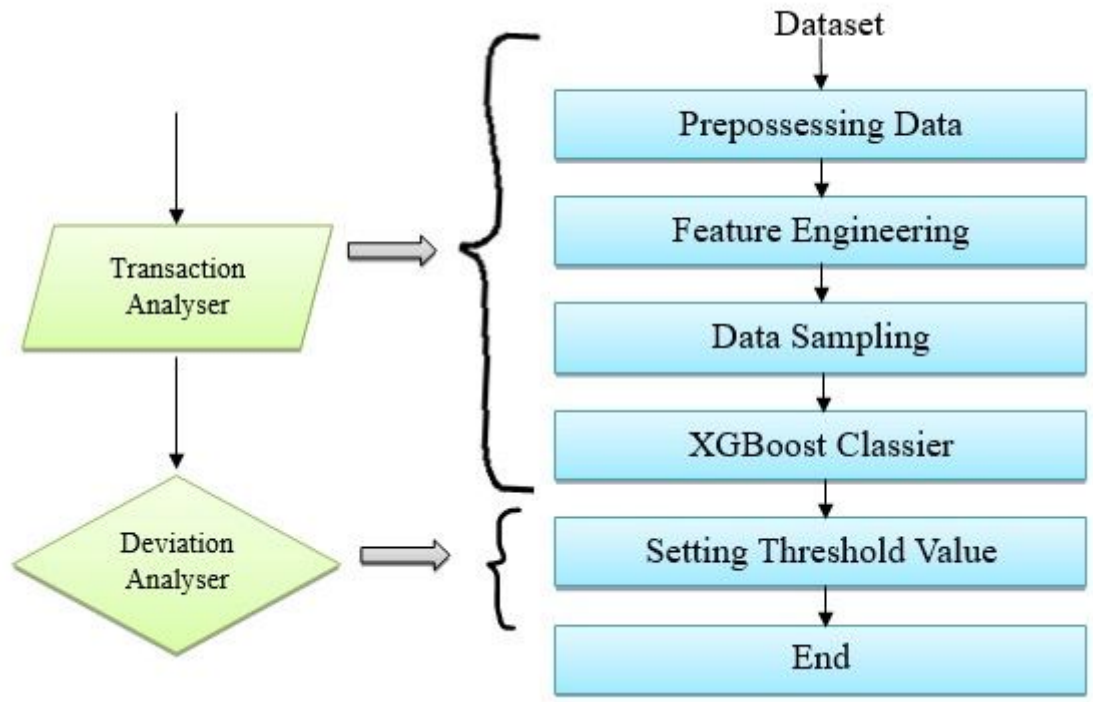

Figure 2

Flowchart for our proposed model

Figure 3

Proposed Methodology Architecture

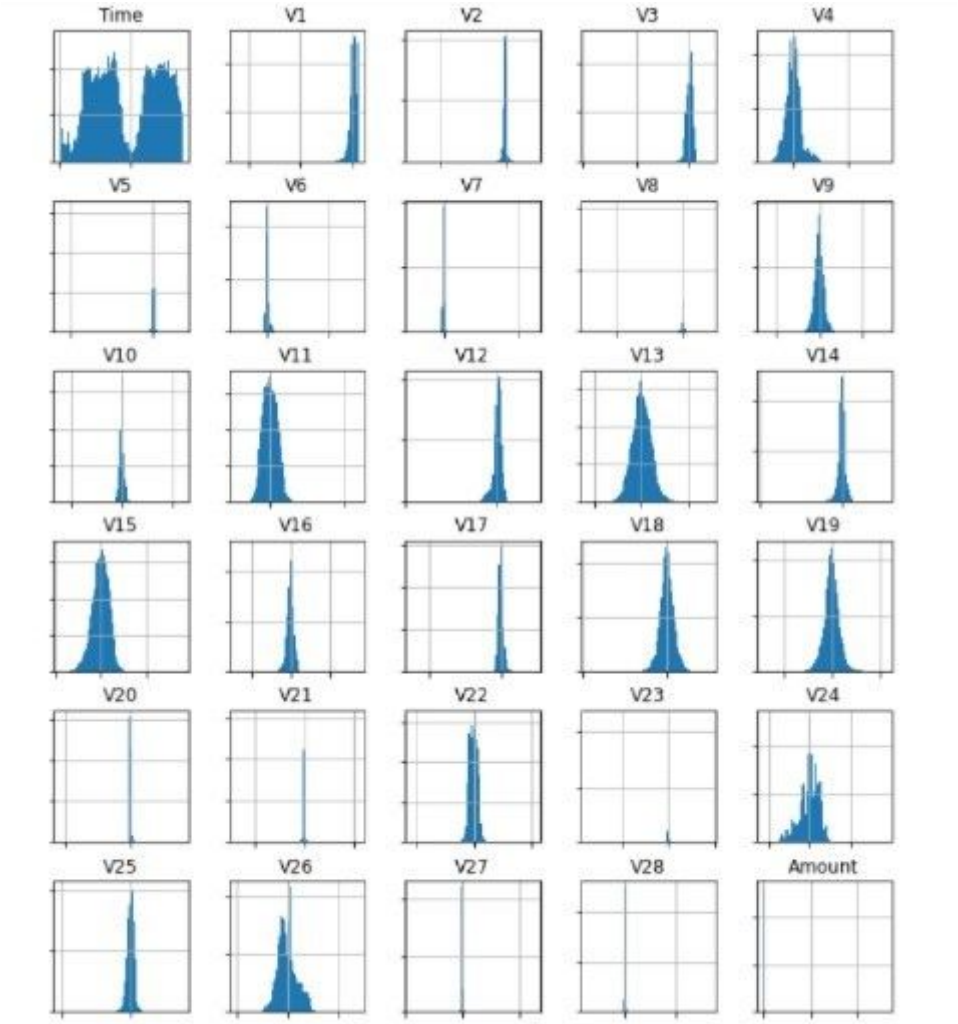

Figure 4

PCA of all the columns of the dataset

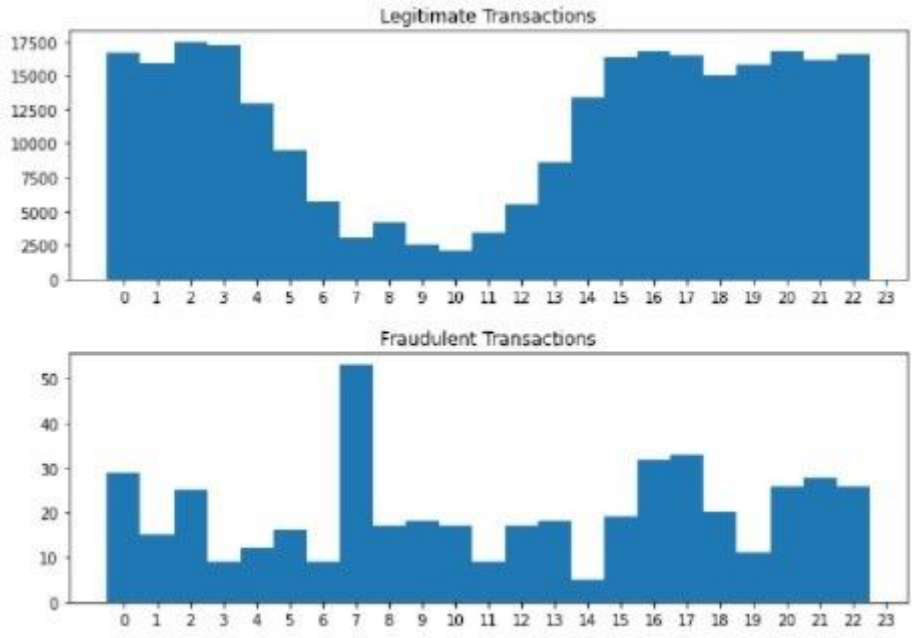

Figure 5

Statistics for the Time attribute

Figure 6

Statistics for Amount attribute

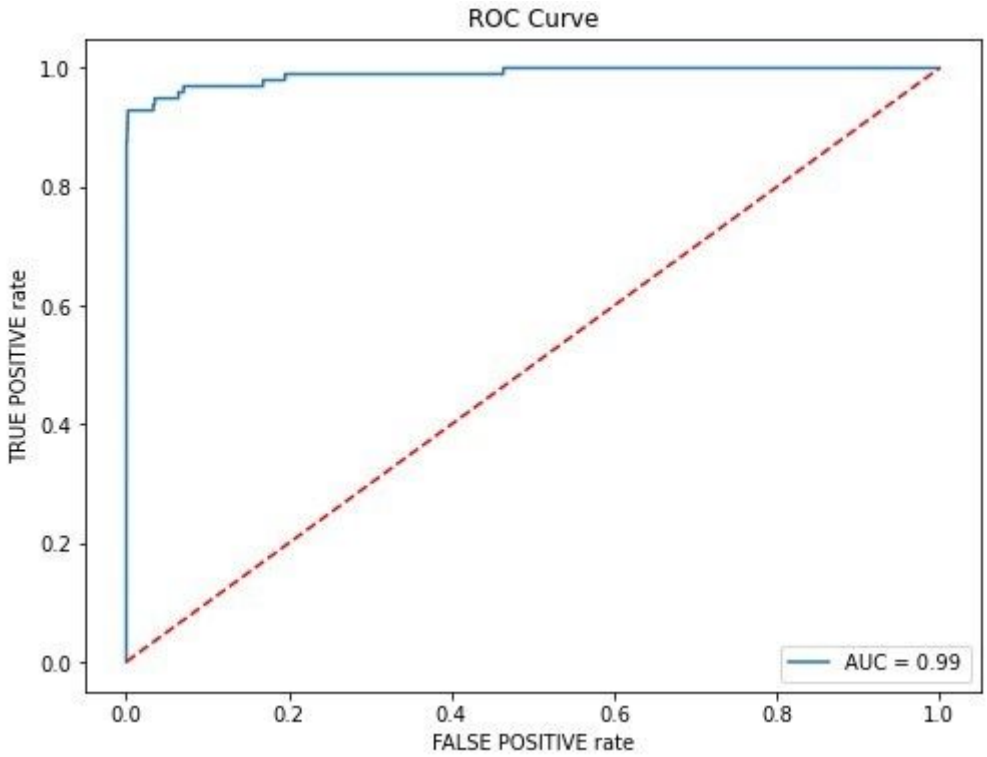

Figure 7

ROC curve for XGBoost classifier

Figure 8

Impact of Threshold adjustment on the error matrix