Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 218 (2023) 2575–2584

Procedia Computer Science

www.elsevier.com/locate/procedia

International Conference on Machine Learning and Data Engineering

Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques

Palak Gupta[a], Anmol Varshney[a], Mohammad Rafeek Khan[b], Rafeeq Ahmed[b], Mohammed Shuaib[b], Shadab Alam[b]*

[a] *Department of Computer Engineering & Applications, GLA University, Mathura, UP, INDIA*
[b] *Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India*
[b] *College of Computer Science & IT, Jazan University, Jazan, Saudi Arabia*

Abstract

The number of individuals who use credit cards has increased dramatically in recent decades, as has the volume of credit card fraud transactions. Consequently, banks and credit card companies must be able to classify fraudulent credit card transactions so that clients do not have to pay for products they did not purchase. Data Science can easily tackle such challenges, and the value of Machine Learning methodologies cannot be emphasized. The study demonstrates how to model utilizing multiple classifiers and data balance using machine learning approaches to learning about Credit Card Fraud Detection. The data has been observed as an imbalanced dataset that could have inferred not much optimal performance of models. The experimentation on the imbalanced data has been done and observed that XGBoost has yielded good performance with 0.91 precision score and 0.99 accuracy score. The different sampling techniques have been carried out in procedure so as to enhance the scores in terms of precision, recall, f1-score, and accuracy. The Random Oversampling technique has come out to be the best suited technique over the imbalance data and yields 0.99 precision and 0.99 accuracy score, when applied on the best model i.e., XGBoost.
The models are then used to compare the results of all of the classifiers employed, resulting in varied conclusions and further research. While working on the study, many data balancing procedures such as oversampling, under sampling, and SMOTE are used, with XGBoost beating residual algorithms with a 99% accuracy score and precision score when Random Over-Sampling is considered. The research suggested the use of data sampling techniques to balance data over the algorithms that show best results under the imbalanced data scenarios, to conclude the best possible performance of the model for fraudulent activities classification.

© 2023 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the International Conference on Machine Learning and Data Engineering

Keywords: Credit card fraud; Logistic Regression; Decision Tree; XGBoost; Artificial Neural Network; SMOTE; UnderSampling; OverSampling

* Corresponding author.
E-mail address: s4shadab@gmail.com

1877-0509 © 2023 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the International Conference on Machine Learning and Data Engineering
10.1016/j.procs.2023.01.231

1. Introduction

Credit card fraud is currently one of the most serious issues confronting businesses and their foundations. It was discovered that around 0.05 percent of all monthly active money owed was fraudulent, implying that 5 out of every 10,000 active money owed was fake. As a result of this circumstance, fraud detection has been vital and has been used to manage the transactions that are executed, at the end facing huge losses. Credit Card Fraud is one of the most disastrous issues facing businesses today, data manipulation is the major task [1].
However, in order to properly combat this scam, it is necessary to first understand how fraud is carried out. People who commit credit card fraud use a wide range of techniques to achieve their goals. Credit card fraud occurs when someone takes the actual card or when crucial information about the card and account, such as the card's account number, becomes available to anybody at any point during a legal transaction. Card numbers, such as the Primary Account Number (PAN), are printed again on the card on a regular basis, and the information is stored in a machine-readable format on a magnetic stripe on the bottom back. All of these methods aid in the reduction of credit card theft.
Fraud detection solutions emerge on a regular basis to protect the activities of criminals from adapting their various fraudulent transactions. There are several sorts of fraud that may be classified as follows: Card theft, Account Bankruptcy, Credit Card fraud transactions, Counterfeit Fraud, Application-based fraud.

In earlier and current studies, the following strategies were often employed to detect fraud transactions [2]: Artificial Neural Networks, Decision Tree, Genetic Algorithms, Bayesian Networks, Gradient Boosting techniques, Support Vector Machines

This research will focus on the Credit Card Fraud Detection dataset, which is a classification issue that can be found on the prominent dataset repository Kaggle. The study began with a basic pre-processing of the dataset before moving on to classification with machine learning algorithms, including Decision Tree Classifier, Logistic Regression, XGBoost Classifier, and Artificial Neural Network. The findings reveal that the accuracy score for all four classifiers is more than 99 per cent showing biased performance, which suggests the data is not balanced and it is reduced from a higher-dimensional pace [3], thus the study went on to compare all classifiers using the F1- Score. As a result, XGBoost has the highest F1-Score. On the dataset, we now use three data balancing techniques: random oversampling, random under-sampling, and SMOTE. The XG Boost classifier is then utilized exclusively for subsequent investigation. The XGBoost classifier is applied independently for each data balancing strategy, and the results are observed. The conclusion is that of the three strategies, Random Oversampling produced the best results.

1.1 Contribution-

- ✓ We proposed a framework to evaluate how unbalanced data influences machine learning models, resulting in bias towards a specific category, may help organizations survive in their technological transformation and transformations.
- ✓ Data-driven choices utilizing machine learning algorithms will encompass procedures, culture, and technology.
- ✓ It will assist decide which data sampling approach to utilize for better algorithm outcomes.
- ✓ This paper has its contribution in terms of the accuracy, during the experimentation phase when machine learning models are applied to the dataset directly then the results given by the model were too biased, in other words only one class was shown as outcome.
- ✓ But further experimentation improved the accuracy as the implementation of the machine learning algorithms was conducted along with the oversampling technique which proved to be the boon for the credit card fraud detection dataset.

1.2 Organization

The rest of the paper is organized as follows: Section 2 discusses the related work. Section 3 discusses the machine learning concepts used in the manuscript. In section 4, we have discussed the Data Balancing Techniques;

then in section 5, we have shown the experimental procedure for our datasets and in Section 6 we have shown the results and discussed the findings; and finally, we have concluded in the last section.

2. Related Work

Ongoing fraudulent activities are leaving drastic impacts on the industry as well as their economy. To prevent this, various studies have been taken into consideration where so many researchers have contributed their proposed methods for detecting fraudulent transactions. Researchers highlighted how neural network methods are utilized for categorization in one of the studies [4]. In these papers [5-9], several machine learning algorithms for the detection of credit card fraud are examined, and various predictions and conclusions are drawn. For the identification of credit card fraud, the paper applied both classification and ensemble learning methodologies. Some researchers investigated the usefulness of a HOBA analysis in conjunction with their suggested fraud detection approach based on deep learning architecture [10]. A variety of functions have been used to pick amongst nodes one by one in order to reduce classification error [11].

Several reviews have been conducted over the previous research for the analysis of machine learning applications in identifying the credit card fraudulent activities with novel and stacked architectures [12-15]. The researches have been conducted widely over different data mining techniques out of which approximately 23% of the studies have done on the SVM technique followed by both naïve bayes and Random forest techniques that contributed 13% of the overall research studies as per the reviews [16-20]. The studies have gone so far and mainly focused on the data. The researchers have analyzed the data to be imbalanced, probably the reason for the degraded performance of models, therefore applied under sampling and oversampling and got better results by under-sampling technique on logistic regression [21]. An Artificial neural network works well when it comes to complex data, therefore experimented well by the researchers for fraud detection [22]. Further analysis has been shown in this paper to study more frequently used techniques that could outperform the previous results. The top three algorithms are selected for usage in the second step, when 19 resampling approaches are applied to each.

The All K-Nearest Neighbors under sampling strategy in conjunction with CatBoost is regarded as the best recommended model based on 330 evaluation metric values that required about a month to acquire. Consequently, the KNN-CatBoost model is compared to similar research. With an AUC value of 97.94%, a Recall value of 95.91%, and an F1-Score value of 87.40%, the findings suggest that the proposed model surpasses earlier models [23]. This study proposes a Deep Convolution Neural Network (DCNN) technique for detecting financial fraud using a deep learning algorithm. This approach can improve the detection accuracy when a big volume of data is involved. Using a real-time credit card fraud dataset, the current machine learning models, auto-encoder model, and other deep learning models are compared to the proposed model in order to evaluate its performance. Using the suggested model, it was possible to achieve 0.99 percent detection accuracy for a timeframe of 45 seconds, as demonstrated in the experimental findings [24]. Furthermore, the strategies the being used by the researchers to enhance result so as this paper has contributed by using simple techniques with best result over complex techniques with less results.

3. Training Algorithms and Techniques

Classification is referred to as the prediction issue in the field of machine learning. This problem involves classifying independent variables (input data) into groups, and there can be anywhere from two to many groupings. Both structured and unstructured data may be classified using several strategies that can be used for both types of data. An algorithm that is used to translate incoming data into a certain class or category is what is meant to be understood by the term "classifier." There are three distinct types of classification: binary classification, multi-label classification, as well as multi-class classification. Binary classification is the simplest form of classification [25-26].The following is a list of classifiers that are utilized in the process of determining whether or not a credit card transaction is fraudulent:

3.1 Logistic Regression

It is one of the supervised algorithms that is utilized for the purpose of classifying the dataset into distinct categories. The value of a categorical or numerical variable, dependent on each other, may be predicted with the help of this classifier. Logistic Regression is the method that has the capacity to categorize fresh data by making use of both continuous and discrete datasets at the same time. This ability is what gives the algorithm its name. Due to the fact that it possesses this quality, it is considered to be one of the essential machine learning algorithms. This classifier's primary function is to provide predictions on the probability associated with a variety of scenarios.

3.2 Decision Tree Classifier

This classifier can be utilized for classification-based difficulties as well as regression-based issues; nevertheless, for the most part, it is recommended for classification applications. The structure of this classifier resembles a tree, with the core nodes representing the attributes of the dataset, the branches representing the decision rules, and the leaf nodes of the tree representing the final outputs. Therefore, we can also say that this classifier gives a graphical method for finding all of the potential answers to a specific problem based on the conditions that have been provided. When the size of the tree increases, it also indicates that the tree is becoming deeper, which means that more conventional decision rules and models will fit more precisely.

3.3 XGBoost Classifier

Gradient Boosting is used to create this classifier. In many contests, the model generated after using this classifier is a clear winner. Weights play an important part in the XGBoost algorithm. A decision tree is created. Weights are assigned to certain independent factors, which are then input into the decision tree, which predicts the outcomes.
XG Boost provides a number of advantages, including the reduction of overfitting, which is why it is frequently referred to as a regularized boosting strategy. XGBoost also accommodates missed values in the data with ease, and it features a built-in cross-validation mechanism that executes at each step.

4. Data Balancing Techniques

The following are examples of strategies that may be used to counterbalance the dataset in order to optimize the results:

4.1 Random over Sampling

The random oversampling technique compositely comprises randomly selecting certain samples from minority groups, along with their alternative, and then introducing them to the testing set. This is done in order to get a more equitable distribution of data.

4.2 Random under-sampling

Using this approach, let it first remove certain instances from the training data, and then we will randomly choose some entries from the category that contains the bulk of the items. As a consequence of this, we can state that individuals of the class that has the most individuals are eliminated by a stochastic function until the values become balanced.

4.3 SMOTE

The SMOTE approach maintains equilibrium by performing the following steps:
First, do an investigation on the characteristics of the underrepresented group. After that, choose the numbers that are closest to the one being considered (k). After that, it should create a line connecting any of the minority points to any of the spots that are nearby. Repeat the previous procedure for all of the points that belong to the minority and each of their varied k neighbours until the data are balanced.

5. Experimental Procedure

Data exploration: It is the process of discovering data insights via the use of various visualization approaches. It is the initial phase in the data analysis process. Pre-processing stage is a crucial stage in machine learning since it enhances the quality of the data, allowing us to extract relevant knowledge from big data with greater ease. Additionally, data becomes enough for modelling purposes.

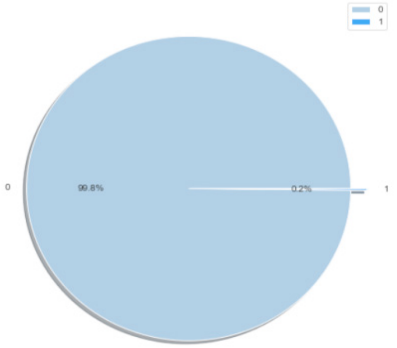


Fig. 1: Pie representation of target class

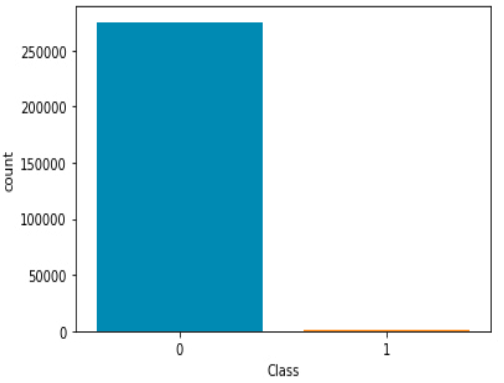


Fig. 2: Count of both classes

It is the initial phase in developing or deploying a machine learning model. Data pre-processing cleans and organizes data that is partial, erroneous, missing certain values, or inconsistent. Moving on with this stage, the target characteristic has been assessed, and it can be seen that the proportion of class 1 is far lower than the rest of class 2; as a result, the data is extremely unbalanced and may produce biased outcomes.
The pie chart shown in Fig 1, represents the percentage ratio in which the categories are distributed in the data.
The bar chart shown in Fig 2, represents the count of each class category distributed in the data. It can be seen that data seems to be imbalanced, hence the knowledge of ultimate balancing techniques needs to be applied.

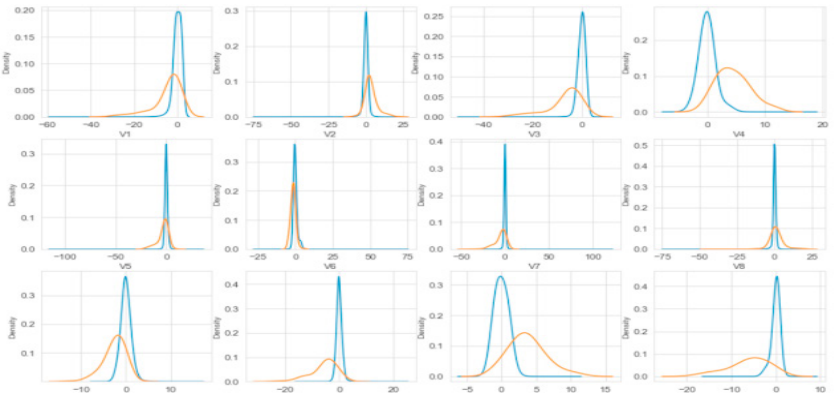


Fig. 3: Imbalance data distribution

In Fig. 3, the data appear to be very unbalanced, which might lead to biased results and poor model performance, since class 0 comprises more than 90 per cent of the distribution in data and is, therefore, the majority class. Following the application of the sampling approach, the data may be moulded into a balanced format. Class 1 was therefore oversampled using a random oversampling approach, as seen in the following figure.

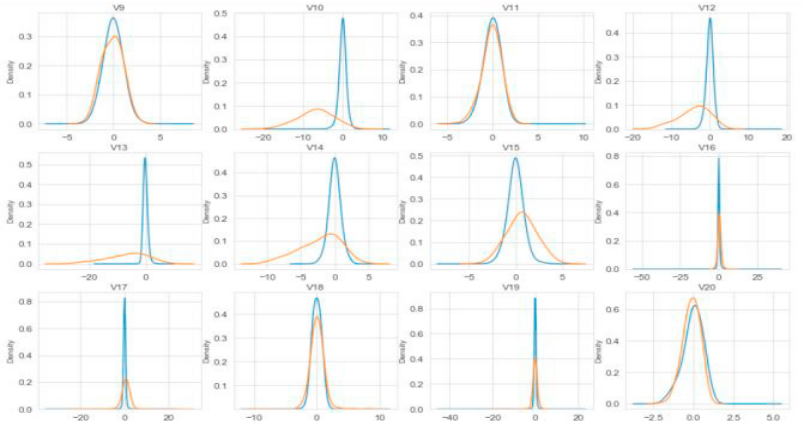


Fig. 4: Distribution of data after Random Oversampling

5.1 Feature selection:

An example of this is the elimination of independent variables and just utilizing relevant data to train a model. As a result, data may be compressed more efficiently thanks to this method. For such machine learning algorithms, the most essential characteristic is automatically picked. Our model gets more efficient as a result of this approach. There are several ways to enhance the model, but both data preparation and feature engineering play a significant role.

5.2 Data Pre-processing:

We have 31 characteristics in our dataset, therefore certain attributes may be beneficial to our model while others may be detrimental. Pre-processing began by removing characteristics that were unnecessary. With PCA's best quality features having already been extracted, the 'time' property no longer appears to be useful and has been removed from the data. In addition, the data has indeed been cleaned up by deleting any samples that are identical. Removed was the duplicated row in its entirety.

As a result of the variance in estimation, the values are normalized in the best feasible manner. Algorithm modelling is depicted here in a simplified architecture/workflow.

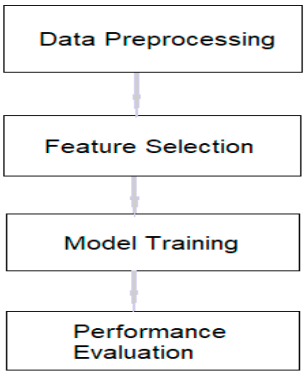


Fig. 5: Experimental workflow without balancing data

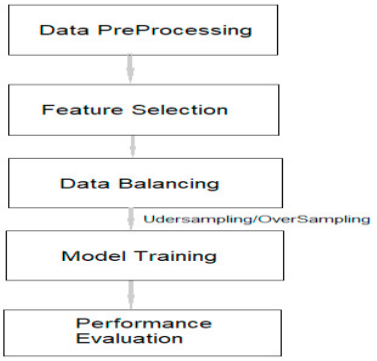


Fig. 6: Experimental workflow with balancing data

After completing all of the analytic and preparation stages, we used four distinct machine learning algorithms and then examined the outcomes. This research employs the Regression Model, Decision Tree Classification algorithm, XGBoost Classification algorithm, and ANN. In order to compare the findings, metrics' scores have been calculated

for each classifier such as Precision score, Accuracy, Recall score, and F1 Score.
After implementing these four models to the data, it is determined that the XGBoost Classifier yielded the best results but the results are found to be more biased towards one side of the class that suggested the effect of imbalance dataset analysed during exploratory data analysis phase. The distribution of data among the classes is not found to be balanced to produce unbiased effective results for the fraudulent classification. For each of the four classifiers, the accuracy is greater than 99 percent, which suggests that the data is imbalanced and, as a consequence, producing biased results out of which the best performance model is considered for further experimentation. Therefore, the data sampling techniques are opted to either filter out data or to add on more samples in order to balance the data that could result in more optimal performance of models.

5.3 Proposed Methodology:

In the previous stage, the imbalanced dataset has been splitted into training and testing sets in order to apply the machine learning classification algorithms for training the complete model. The model that attained better results, no matter if biased, is taken into consideration for its better algorithm and estimation function. Further experimentation has been carried out on three modified datasets produced by applying Random Under Sampling, Random Over Sampling, and Synthetic Minority Random Oversampling Technique (SMOTE). The selected model is trained on the modified datasets, to produce different analytical performances, with the same splitting ratio for training and testing sets. The aim is to analyze the performance of the algorithm over imbalanced and balanced datasets and so for the effect of sampling techniques. The workflow of the process has been drafted below in the form of a flow chart. The additional phase of the proposed framework is the data sampling phase in order to balance the dataset using different techniques that work on minority and majority class samples.
The study balances the data using three methods: Data oversampling, Data under-sampling, and SMOTE. Then, we employ the XGBoost prediction model for each of the data balancing strategies and examine the outcomes. In order to compare outcomes in terms of all assessing methodologies, i.e. Accuracy Scores, precision scores, recall scores, and F1 Scores, the findings of all prior and upgraded results have been documented.

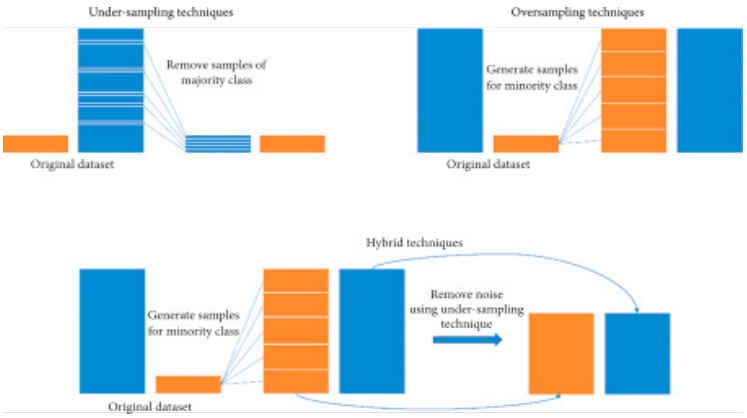


Fig. 7: Undersampling and oversampling visulaization[27]

6. Results

The research employed four distinct classifiers to determine whether or not a transaction is malicious. The classifiers are incorporated in the beginning over the dataset that was taken initially for the study i.e. imbalanced as the analysis suggests. The algorithms such as Logistic Regression, Decision Tree, XGBoost, and Artificial Neural Network have been carried out to build models on the pre-processed dataset. The findings are displayed in TABLE 1 below.

TABLE 1: Results before applying Data Balancing

MODELS	Precision	Recall	F1 Score	Accuracy Score
Logistic Regression	0.901	0.618	0.733	0.999
Decision Tree Classifies	0.881	0.754	0.813	0.999
XGBoost Classifier	0.913	0.805	0.856	0.999
Artificial Neural Network	0.875	0.830	0.852	0.999

From TABLE 1, it can be determined that the XGBoost Classification algorithm has the best outcomes based upon the various performance measures such as Precision, Recall, F1 Score, and Accuracy score as 91%, 80%, 86%, and 99% respectively that infers biased nature of algorithms while validating, suggesting the imbalanced nature of data. Thus, data balancing techniques are opted to apply on the algorithm that comes out to be the greatest with best results, no matter biased, i.e. the XGBoost Classification model.

TABLE 2: XGBoost Classifier Results after Data Balancing

Data Balancing Techniques	Precision	Recall	F1 Score	Accuracy Score
Random Over Sampling	0.997	1.0	0.998	0.998
Random Under Sampling	0.958	0.902	0.929	0.926
SMOTE	0.993	0.989	0.991	0.991

Based on TABLE 2, it can be inferred that, Random Over Sampling yields the best results among the other sampling techniques when applied on Boosting model i.e. XGBoost.

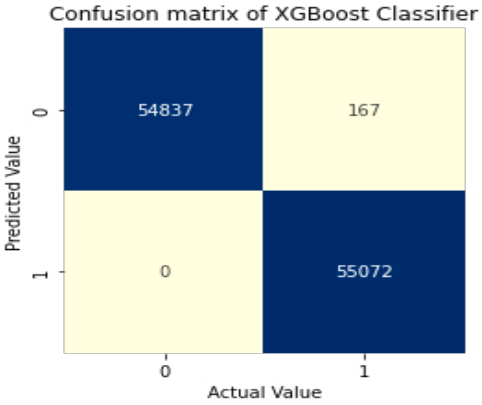


Fig. 8: Confusion matrix of XGBoost Classifier after Applying Random oversampling

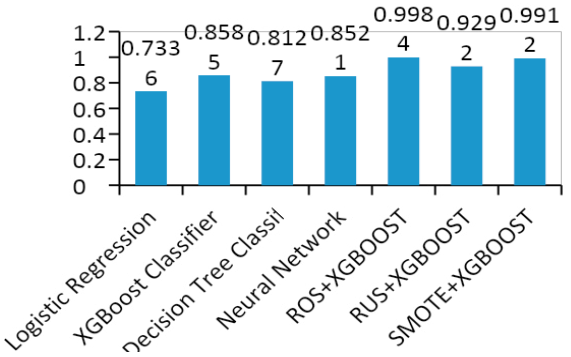


Fig.9: Comparison of all models using F1-Score

After using the random oversampling method, the confusion matrix of such an XGBoost classifier is shown in Figure 7. It can be seen that the impact of oversampling technique has affected the model's result positively. The model has given better classification results as shown above. It is that founded that only 167 wrong classification done by the model on the unseen validation data. This is because the results that we are receiving on these two variables are the best overall.

The comparison of all of the models that were made with F1-Score is displayed in the figure that can be seen above in Fig 8. It is clear that the ROS+XGBoost Classifier is producing the highest quality results of all of the methods with around 99% accuracy which is an unbiased performance. Observing the results shown by various classifiers used in this study, the XGBoost classifiers outperformed others when trained and tested on randomly oversampled data. The features that have been used in these scenarios have shown their own importance as seen in Fig 8.

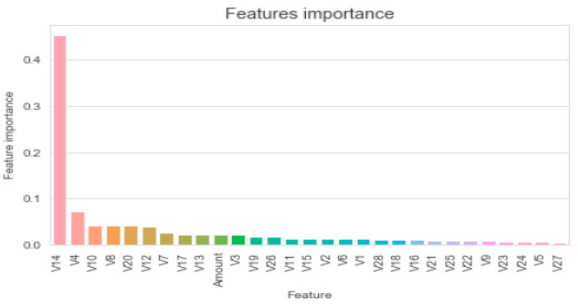


Fig. 10: Features importance of features used in XGBoost with ROS

6.1 Discussion

The research utilized the Fraudulent Transactions Detection data for the categorization, in which we determine if the transaction is fraudulent or not by assigning a value of 1 or 0 to indicate whether or not it is fraudulent. The dataset comprises a total number of 31 variables and 284807 entries in its entirety. The rows represent the total number of transactions that took place. In our data collection, we have a total of 284315 legitimate transactions and just 492 illegitimate or fraudulent ones. Therefore, 0.17% of all transactions include some form of illegal transactions.

6.2 Limitations

The idea of using the sampling techniques all over the way has impressed the research with good results in the objective of classifying the credit card fraudulent activity based on different features as instance. The data sampling techniques are the way to overcome the negative effect of imbalanced data on the training and validation of models resulting in biased results that seem higher in terms of scores but produce negative impact when tested on unseen random data. As far as the data is analysed the technique works positively. The limitation can arise when the sampling technique would be chosen to apply on extremely jumbled data with no normal distribution. The ROS works for credit card continuous nature data that was observed to be normally distributed and noise free after analysis and cleaning. The study may not guarantee the same performance of models over the data that is of different nature or un-cleaned. To overcome the effect of poor results the research suggests analyzing and pre-processing the unseen data so as to gain the benefit of this study and model.

7. Conclusion and Future Work

Before using any method for balancing the data, the XGBoost Classifier has produced the best possible results among the four classification algorithms that were used for modelling. This was before we used any method for balancing the data. The fact that the overall accuracy is more than 99 per cent indicates that the data are not balanced, thus we compare classifiers using the F1 score instead. The XGBoost Classification model has an F1-score of 0.856, precision score as 0.913, recall as 0.805, and an accuracy score of 0.99 as mentioned in the result section in Table 1.

The study is extended to improve the overall performance of classifiers are expected to be effective if three different Data Balancing approaches could be used on the best selected model i.e. XGBoost Classifier, which is currently producing the best results in terms of precision, f1 score, and accuracy as compared to all of the other classifiers that were tried. Therefore, out of the three methods for balancing the data, Random Over Sampling is producing the best results on the chosen algorithm. This is in contrast to Random Under-Sampling as well as the SMOTE method. Because of this, Random Over-Sampling with the XGBoost Classifier is providing us with the greatest outcomes in the case of all Accuracy scores, as well as Precision scores, Recall scores, and F1 Scores as 0.998, 0.997, 1.0, and 0.998 respectively. The visible increase in the performance of the model can be observed and concluded as the best optimal proposed approach with unbiased results.

In the future, effort might be made to look for approaches and strategies that are more effective than those now being used and could help overcome the limitations of this study. The repetitive use of sampling and testing that is carried out repeatedly may be left in the past as new algorithms can be built that have the potential to immediately

infer behaviour that is comparable to what this study performs.

References

[1] Ahmed R, Ahmad N, (2012). Knowledge representation by concept mining & fuzzy relation from unstructured data. Published in international journal of research review in engineering science and technology (ISSN 2278-6643) Volume-1 Issue-2.

[2] Chahar, Ravindra Kumar and Prasad, S.V.A.V. and Ahmad, Rafeeq, (March 11, 2019). A Novel Application for Optimization Utility in Smart Grid using Machine Learning Technique, (2019). Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE).

[3] Singh, Bharat and Kumar, Kundan and Mohan, Sudhir and Ahmad, Rafeeq, (February 8, 2019). Ensemble of Clustering Approaches for Feature Selection of High Dimensional Data. Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE) 2019.

[4] Simon Haykin,(1999). "Neural Networks: A Comprehensive Foundation," 2nd Edition, pp.842.

[5] Tej Paul Bhatla, Vikram Prabhu & Amit Dua (2003). "Understanding Credit Card Frauds,".

[6] Sadgali, N. Sael, and F. Benabbou,-Detection and prevention of credit card fraud: State of art, MCCSIS (2018). Multi Conf. Comput. Sci. Inf. Syst. Proc. Int. Conf. Big Data Anal. Data Min. Comput. Intell. 2018, Theory Pract. Mod. Comput. 2018 Connect. Sma, no. March 2019, pp. 129–136.

[7] R. R. Popat and J. Chaudhary(2018). A Survey on Credit Card Fraud Detection Using Machine Learning,‖ Proc. 2nd Int. Conf. Trends Electron. Informatics, ICOEI vol. 25, no. 01, pp. 1120–1125.

[8] A. Mishra and C. Ghorpade,(2018). Credit Card Fraud Detection on the Skewed Data Using Various Classification and Ensemble Techniques,‖ 2018 IEEE Int. Students' Conf. Electr. Electron. Comput. Sci. SCEECS 2018, pp. 1–5.

[9] Mittal and S. Tyagi, (2019). Performance evaluation of machine learning algorithms for credit card fraud detection,‖ Proc. 9th Int. Conf. Cloud Comput. Data Sci. Eng. Conflu. 2019, pp. 320–324.

[10] Zhang, X., Han, Y., Xu, W., & Wang, Q. (2019). HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture. Information Sciences.

[11] Haoxiang, Wang, and S. Smys, (2021). "Overview of Configuring Adaptive Activation Functions for Deep Neural Networks-A Comparative Study." Journal of Ubiquitous Computing and Communication Technologies (UCCT) 3, no. 01.

[12] Faraji, Z. (2022). A Review of Machine Learning Applications for Credit Card Fraud Detection with A Case study. *SEISENSE Journal of Management.*

[13] Al Rubaie, E. M. (2021). Improvement in credit card fraud detection using ensemble classification technique and user data. International Journal of Nonlinear Analysis and Applications, 12(2), 1255-1265.

[14] Alkhatib, K. I.-A. (2021). Credit Card Fraud Detection Based on Deep Neural Network Approach. 12th International Conference on Information and Communication Systems (ICICS) (pp. 153-156).

[15] Faraji, Z. (2020). The Causal Analysis of Financial Distress Risk and Performance. American International Journal of Business Management, 3(5), 5.

[16] Khaled Gubran Al-Hashedi, Pritheega Magalingam, (2019). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019, Computer Science Review, Volume 40, 2021, 100402, ISSN 1574-0137.

[17] Rahmani, M. K. I., Shuaib, M., Alam, S., Siddiqui, S. T., Ahmad, S., Bhatia, S., & Mashat, A. (2022). Blockchain-Based Trust Management Framework for Cloud Computing-Based Internet of Medical Things (IoMT): A Systematic Review. *Computational Intelligence and Neuroscience*, *2022*.

[18] Shuaib, M., Hassan, N. H., Usman, S., Alam, S., Bhatia, S., Agarwal, P., & Idrees, S. M. (2022). Land Registry Framework Based on Self-Sovereign Identity (SSI) for Environmental Sustainability. *Sustainability*, *14*(9), 5400.

[19] Shuaib, M., Hassan, N. H., Usman, S., Alam, S., Bhatia, S., Mashat, A., ... & Kumar, M. (2022). Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison. *Mobile Information Systems*, *2022*.

[20] Shuaib, Mohammed, Shadab Alam, Salwani Mohd Daud, and Sadaf Ahmad. "Blockchain-Based Initiatives in Social Security Sector." (2021).

[21] Itoo, F., Meenakshi & Singh, S. Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. *Int. j. inf. tecnol.* 13, 1503–1511 (2021).

[22] Sharma, Pratyush, Souradeep Banerjee, Devyanshi Tiwari, and Jagdish Chandra Patni. "Machine Learning Model for Credit Card Fraud Detection-A Comparative Analysis." *The International Arab Journal of Information Technology* 18, no. 6 (2021).

[23] Alfaiz, N.S.; Fati, S.M. (2022). Enhanced Credit Card Fraud Detection Model Using Machine Learning. *Electronics* , *11*, 662. https://doi.org/10.3390/electronics11040662

[24] [1] Bin Sulaiman, R., Schetinin, V. & Sant, P. (2022). Review of Machine Learning Approach on Credit Card Fraud Detection. Hum-Cent Intell Syst 2, 55–68 https://doi.org/10.1007/s44230-022-00004-0

[25] Bhatia, S., Alam, S., Shuaib, M., Alhameed, M. H., Jeribi, F., & Alsuwailem, R. I. (2022). Retinal Vessel Extraction via Assisted Multi-Channel Feature Map and U-Net. Frontiers in Public Health, 10.

[26] Khan, Z. A., Khubrani, M. M., Alam, S., Hui, S. J., & Wang, Y. (2021). Method for Measuring the Similarity of Multiple Metrological Sequences in the Key Phenological Phase of Rice-based on Dynamic Time.

[27] https://static-02.hindawi.com/articles/complexity/volume-2019/8460934/figures/8460934.fig.001.svgz