Performance Analysis of Credit Card Fraud Detection using Machine Learning Techniques

Subhalakshmi C,Umashankar T ,Varsha H,
Vinitha P,Tejaswini A

Department of Information Technology
SSN College of Engineering
Kalavakkam, Chennai, India

subhalakshmi2010983@ssn.edu.in,
umashankar2010566@ssn.edu.in,
varsha2011056@ssn.edu.in,
vinitha2010465@ssn.edu.in,
tejaswini2012017@ssn.edu.in

***Abstract*—Financial fraud is an ever growing menace with far consequences in the financial industry. Data mining had played an imperative role in the detection of credit card fraud in online transactions. Credit card fraud detection, which is a data mining problem, becomes challenging due to two major reasons – first, the profiles of normal and fraudulent behaviours change constantly and secondly, credit card fraud data sets are highly skewed. The performance of fraud detection in credit card transactions is greatly affected by the sampling approach on dataset, selection of variables and detection technique(s) used. This paper investigates the performance of k-nearest neighbor and logistic regression on highly skewed credit card fraud data. Dataset of credit card transactions is sourced from European cardholders containing 284,807 transactions. A hybrid technique of under-sampling and oversampling is carried out on the skewed data. These techniques are applied on the raw and preprocessed data. The work is implemented in Python. The performance of the techniques is evaluated based on accuracy, sensitivity, specificity, precision, Matthews correlation coefficient and balanced classification rate. The results shows of optimal accuracy for k-nearest neighbor and logistic regression classifiers are 97.92%, 97.69% and 54.86% respectively. The comparative results show that k-nearest neighbour performs better than logistic regression techniques.**

I. INTRODUCTION

Financial fraud is an ever growing menace with far reaching consequences in the finance industry, corporate organizations, and government. Fraud can be defined as criminal deception with intent of acquiring financial gain. High dependence on internet technology has enjoyed increased credit card transactions. As credit card transactions become the most prevailing mode of payment for both online and offline transaction, credit card fraud rate also accelerates. Credit card fraud can come in either inner card fraud or external card fraud. Inner card fraud occurs as a result of consent between cardholders and bank by using false identity to commit fraud while the external card fraud involves the use of stolen credit card to get cash through dubious means. A lot of researches have been devoted to detection of external card fraud which accounts for majority of credit card frauds. Detecting fraudulent transactions using traditional methods of manual detection is time consuming and inefficient, thus the advent of big data has made manual methods more impractical. However, financial institutions have focused attention to recent computational methodologies to handle credit card fraud problem.

Data mining technique is one notable methods used in solving credit fraud detection problem. Credit card fraud detection is the process of identifying those transactions that are fraudulent into two classes of legitimate (genuine) and fraudulent transactions [1]. Credit card fraud detection is based on analysis of a card's spending behaviour. Many techniques have been applied to credit card fraud detection, artificial neural network [2], genetic algorithm [3, 4], support vector machine [5], frequent itemset mining [6], decision tree [7], migrating birds optimization algorithm [8], naïve bayes [9]. A comparative analysis of logistic regression is carried out in [10]. The performance of bayesian and neural network [11] is evaluated on credit card fraud data. Decision tree, neural networks and logistic regression are tested for their applicability in fraud detections [12]. This paper [13] evaluates data mining approaches, and random forests, together with logistic regression, as part of an attempt to better detect credit card fraud while logistic regression is applied on credit card fraud detection problem [14]. A number of challenges are associated with credit card detection, namely fraudulent behaviour profile are dynamic, that is fraudulent

transactions tend to look like legitimate ones; credit card transaction datasets are rarely available and highly imbalanced (or skewed); optimal feature (variables) selection for the models; suitable metric to evaluate performance of techniques on skewed credit card fraud data. Credit card fraud detection performance is greatly affected by type of sampling approach used, selection of variables and detection technique(s) used. This study investigates the effect of hybrid sampling on performance of fraud detection of k-nearest neighbour and logistic regression classifiers on highly skewed credit card fraud data.

This paper seeks to carry out comparative analysis of credit card fraud detection using k-nearest neighbor and logistic regression techniques on highly skewed data based on accuracy, sensitivity, specificity and Matthews's correlation coefficient (MCC) metrics.

The rest of this paper is organized as follows: Section II gives detailed review on credit card fraud, feature selection detection techniques and performance comparison. Section III describes the experimental setup approach including the data pre-processing and the three classifier methods on credit card fraud detection. Section IV reports the experimental results and discussion about the comparative analysis. Section V concludes the comparative study and suggests future areas of research.

II. RELATED WORKS

Classification of credit card transactions is mostly a binary classification problem. Here, credit card transaction is either as a legitimate transaction (negative class) or a fraudulent transaction (positive class). Fraud detection is generally viewed as a data mining classification problem, where the objective is to correctly classify the credit card transactions as legitimate or fraudulent [6].

A. Credit Card Fraud

Credit card frauds have been partitioned into two types: inner card fraud and external fraud [12, 15] while a broader classification have been done in three categories, that is, traditional card related frauds (application, stolen, account takeover, fake and counterfeit), merchant related frauds (merchant collusion and triangulation) and Internet frauds (site cloning, credit card generators and false merchant sites) [16]. It is reported in [17] that the total amount of fraud losses of banks and businesses around the world reached more than USD 16 billion in 2014 with an increase of nearly USD 2.5 billion in the previous year recorded losses, meaning that, each USD 100 is having 5.6 cents that was fraudulent, the report concluded.

Credit card transactions data are mainly characterized by an unusual phenomenon. Both legitimate transactions and fraudulent ones tend to share the same profile. Fraudsters learn new ways to mimic the spending behaviour of legitimate card (or cardholder). Thus, the profiles of normal and fraudulent behaviours are constantly dynamic. This inherent characteristic leads to a decrease in the number of true fraudulent cases identified in a pool of credit card transactions data leading to a highly skewed distribution towards the negative class (legitimate transactions). The credit card data investigated in [18] contains 20% of the positive cases, 0.025% positive cases [19] and below 0.005% positive cases [8]. The data used in this study has positive class (frauds) accounting for 0.172% of all transactions. A number of sampling approaches have been applied to the highly skewed credit card transactions data. A random sampling approach is used in [18, 20] and reports experimental results indicating that 50:50 artificially distribution of fraud/non-fraud training data generate classifiers with the highest true positive rate and low false positive rate. The paper [8] uses stratified sampling to under sample the legitimate records to a meaningful number. It experiment on 50:50, 10:90 and 1:99 distributions of fraud to legitimate cases reports that 10:90 distribution has the best performance (regarding the performance comparisons on the 1:99 set) as it is closest to the real distribution of frauds and legitimates. Stratified sampling is also applied in [21]. In this study, a hybrid of under-sampling the negative cases and oversampling the positive cases is carried in order to preserve valuable patterns from the data.

B. Feature (Variables) selection

The basis of credit card fraud detection lies in the analysis of cardholder's spending behaviour. This spending profile is analysed using optimal selection of variables that capture the unique behaviour of a credit card. The profile of both a legitimate and fraudulent transaction tends to be constantly changing. Thus, optimal selection of variables that greatly differentiates both profiles is needed to achieve efficient classification of credit card transaction. The variables that form the card usage profile and techniques used affect the performance of credit card fraud detection systems. These variables are derived from a combination of transaction and past transaction history of a credit card. These variables fall under five main variable types, namely all transactions statistics, regional statistics, merchant type statistics, time based amount statistics and time-based number of transactions statistics [19].

The variables that fall under all transactions statistics type depict the general card usage profile of the card. The variables under regional statistics type show the spending habits of the card with taken into account the geographical regions. The variables under merchant statistics type show the usage of the card in different merchant categories. The variables of time based statistics types identify the usage profile of the cards with respect to usage amounts versus time ranges or frequencies of usage versus time ranges. Most literature focused on cardholder profile rather than card profile. It is evident that a person can operate two or more credit cards for different purposes. Therefore, one can exhibit different spending profile on such cards. In this study, focus is

beamed on card rather than cardholder because one credit card can only exhibit a unique spending profile while a cardholder can exhibit multiple behaviours on different cards. A total of 30 variables are used in [18], 27 variables in [19] and 20 variables are reduced to 16 relevant ones [6]

C.Credit card Fraud Detection

As credit card becomes the most general mode of payment (both online and regular purchase), fraud rate tends to accelerate. Detecting fraudulent transactions using traditional methods of manual detection are time consuming and inaccurate, thus the advent of big data had made these manual methods more impractical. However, financial institutions have turned to intelligent techniques. These intelligent fraud techniques comprise of computational intelligence (CI)-based techniques. Statistical fraud detection methods have been divided into two broad categories: supervised and unsupervised [22]. In supervised fraud detection methods [13], models are estimated based on the samples of fraudulent and legitimate transactions to classify new transactions as fraudulent or legitimate while in unsupervised fraud detection, outliers' transactions are detected as potential instances of fraudulent transactions. A detailed discussion of supervised and unsupervised techniques is found in [23]. Quite a number of studies on a range of techniques have been carried out in solving credit card fraud detection problem. These techniques include but not limited to; neural network models (NN), Bayesian network (BN), intelligent decision engines (IDE), expert systems, meta-learning agents, machine learning, pattern recognition, rule-based systems, logic regression (LR), support vector machine (SVM), decision tree, k-nearest neighbor (kNN), meta learning strategy, adaptive learning etc. Some related works on comparative study of credit card fraud detection techniques are presented.

III. METHODOLOGY

This section describes the dataset used in the experiments and the classifiers under study, namely; k Nearest Neighbour and Logistic Regression techniques. The different stages involved in generating the classifiers include; collection of data, preprocessing of data, analysis of data, training of the classifier algorithm and testing (evaluation).During the preprocessing stage, the data is converted into useable format fit and sampled. For the analysis stage, the feature selection and reduction is already carried out on the dataset using PCA. The training stage is where the classifier algorithms are developed and fed with the processed data. The performance comparison of the classifiers is analyzed based on accuracy, sensitivity, specificity, precision, Matthews correlation coefficient and balanced classification rate.

A. DATASET

Using a dataset of financial transactions, build a machine learning model that can accurately detect instances of online payment fraud. The goal is to minimize false positives and false negatives, as both can have significant consequences for both customers and credit card companies. The model should take into account various features of the transactions, such as the amount transferred, the type of transaction, and the balances of the sending and receiving accounts. By accurately detecting fraudulent transactions, credit card companies can protect their customers from unauthorized charges and prevent financial losses due to fraud.

- Build and train a machine learning model using the provided financial transaction data that can accurately predict instances of online payment fraud.
- Evaluate the performance of the machine learning model using appropriate metrics such as accuracy, precision, recall, and F1-score.

B.Classification Algorithms :

Decision tree: It can handle both numerical and categorical features, making them suitable for analyzing the various features of financial transactions, such as transaction type, amount, and account balances.Decision tree classifiers are capable of identifying complex relationships between features, making them well-suited for detecting fraudulent transactions that may not follow obvious patterns.The interpretability of decision tree classifiers can be an advantage in this context, as it may be important for stakeholders to understand how the model is making its predictions.
Decision tree classifiers can be sensitive to noisy or irrelevant features, so feature selection or dimensionality reduction may be necessary to improve model performance.

Random forest: It can handle both numerical and categorical features, making them suitable for analyzing the various features of financial transactions, such as transaction type, amount, and account balances.Ensemble methods such as random forests can be more accurate than single decision tree classifiers, as they combine the predictions of multiple decision trees to make more robust and accurate predictions. Random forest classifiers can handle noisy or irrelevant features, as they only consider a random subset of features at each split, making them less prone to overfitting.The interpretability of the random forest classifier may be lower than that of a single decision tree, as it may be more difficult to trace the decision-making process across multiple trees.

KNN: K-Nearest Neighbors (KNN) is a non-parametric and lazy machine learning algorithm that can be used for classification and regression tasks. KNN works by finding the k-nearest neighbors to a given test data point based on a distance metric, such as Euclidean distance, and then

assigning the test data point to the class that is most frequent among its k-nearest neighbors.For the problem of detecting online payment fraud, KNN could be a suitable algorithm, as it can handle both numerical and categorical data, and can be effective when the data has a clear separation between the classes. However, the performance of KNN can be sensitive to the choice of k and the distance metric used, and it can be computationally expensive when working with large datasets.

ADA BOOST: The ADA Boost algorithm works by combining multiple weak classifiers to create a strong classifier. By doing so, it is able to create a more robust and accurate model than any individual weak classifier. Additionally, ADA Boost is able to handle imbalanced datasets, which is often the case with fraud detection datasets where the number of fraudulent transactions is much lower than the number of legitimate transactions.Overall, the ADA Boost algorithm is a highly effective method for detecting credit card payment fraud, and can be a valuable tool for credit card companies to prevent fraudulent charges and protect their customers.

Logistic Regression: Logistic regression is a statistical method that analyzes a dataset with one or more independent variables that determine an outcome. In the context of this problem statement, logistic regression can be used to predict whether a payment transaction is fraudulent or not based on the input variables.The logistic regression algorithm works by fitting a logistic function to the training data, which outputs a probability value between 0 and 1. If the probability is greater than a certain threshold value (usually 0.5), the transaction is predicted to be fraudulent. Otherwise, it is predicted to be legitimate.

MLP:A multilayer perceptron (MLP) can be used for online fraud detection. An MLP is a type of neural network that consists of multiple layers of interconnected nodes. Each node in the MLP receives input signals from the nodes in the previous layer, processes those signals using an activation function, and then passes the output to the nodes in the next layer.

In fraud detection, an MLP can be trained on a dataset of transaction data to learn the patterns and features of fraudulent transactions. The MLP can be trained to identify these patterns and features in new transactions, and flag them as potentially fraudulent.

EDA: Exploratory Data Analysis (EDA) is an important step in the data analysis process that involves visualizing and understanding the structure and characteristics of the data. In the context of online fraud detection, EDA can help to identify patterns and trends in the data that may be indicative of fraudulent activity.

Model Evaluation: The three principal metrics utilized in the evaluation of a classifier are accuracy, precision, and recall.

Accuracy: refers to the proportion of accurate predictions given the test data. It is evaluated by the division of the total count of correct predictions and the total count of predictions.

$$\textbf{Accuracy} = (TP + TN) / (TP + TN + FP + FN),$$

Precision: Precision refers to the percentage of relevant examples (true positives) out of all examples predicted to be associated with a specific label.

$$\textbf{Precision} = \textbf{TruePositives} / (\textbf{TruePositives} + \textbf{FalsePositives})$$

Recall: The proportion of instances expected to be associated with a class divided by the aggregate number of examples that are actually associated with the class is defined as recall.

$$\textbf{Recall} = \textbf{TruePositives} / (\textbf{TruePositives} + \textbf{FalseNegatives})$$

The F1 score may be understood as a harmonic mean of accuracy and recall, with the greatest value as 1 and the lowest value as 0. Precision and recall both contribute equally to the F1 score.

C.INFERENCE

Decision Tree:The decision tree classifier with a score of 0.99973281 on the trained dataset for detecting online payment fraud shows a highly promising performance for the given problem statement. This shows that the model is able to accurately predict whether a given transaction is fraudulent or not, with a very high level of accuracy.

Random Forest:The random forest classifier with a score of 0.99973281 on the trained dataset for detecting online payment fraud shows a highly promising performance for the given problem statement. This indicates that the model is able to accurately predict whether a given transaction is fraudulent or not, with a very high level of accuracy.

In conclusion, the high score of the random forest classifier on the trained dataset suggests that it is a strong candidate for detecting online payment fraud, but further testing and validation are necessary before deploying the model.

Comparing Decision tree classifier and random tree classifier:

Both decision tree classifiers and random forest classifiers are capable of detecting online payment fraud in the given problem statement, but there are some key differences between them.

A decision tree classifier is a simple and interpretable machine learning model that uses a tree-like structure to make decisions based on the features of the input data. Decision tree classifiers are capable of handling both numerical and categorical data, and can be trained quickly on large datasets. However, decision tree classifiers are prone to overfitting, especially when the tree becomes too deep or complex, and they may not generalize well to new, unseen data.

On the other hand, a random forest classifier is an ensemble learning method that combines multiple decision tree classifiers to make more accurate predictions. Random forests can reduce the risk of overfitting and can handle noisy or irrelevant features in the data. Random forests are also capable of handling large datasets with high-dimensional features. However, random forests can be computationally expensive to train and may require more tuning of hyperparameters compared to a single decision tree.

When comparing the scores of the decision tree classifier and the random forest classifier for detecting online payment fraud, we can see that the random forest classifier and decision tree classifier have the same score of 0.99973281. This suggests that both the classifiers may be suited for this problem statement, as both them were able to achieve higher accuracy in making predictions.

KNN: Based on the score of 0.9995803615491732, it appears that the KNN algorithm was able to accurately classify the majority of the samples in the given dataset. However, it is important to note that the score may not be indicative of the algorithm's performance on unseen data, and further testing and validation may be necessary.

Comparing KNN

Based on the scores mentioned above using the columns of the dataset, we can compare the performance of KNN, Random Forest Classifier, and Decision Tree Classifier as follows:

- Decision Tree Classifier: This model has the highest score of 0.99973281, indicating that it performs the best among the three models. However, it may be prone to overfitting and may not generalize well to new data.
- Random Forest Classifier: This model has a score of 0.99973281, which is equal to the score of the Decision Tree Classifier. However, it has the advantage of being less prone to overfitting than the Decision Tree Classifier, and can therefore be more robust and reliable.
- KNN: This model has a score of 0.9995803615491732, which is slightly lower than the scores of the other two models. KNN can perform well if the number of neighbors is chosen carefully and the data is scaled appropriately. However, it may not perform well if the dataset is very large or has many features.

Overall, the Decision Tree Classifier and Random Forest Classifier appear to be the best-performing models for this problem, based on their higher scores.

ADA Boost: The ADA Boost model was trained on the credit card payment fraud dataset using the features 'step', 'type', 'amount', 'nameOrig', 'oldbalanceOrg', 'newbalanceOrig', 'nameDest', 'oldbalanceDest', and 'newbalanceDest'. After training, the model achieved an accuracy score of 0.9989501180331373, which indicates that it is a highly accurate method for detecting fraudulent credit card transactions.

Comparing Ada boost with knn, random tree classifier and decision tree classifier

- Decision Tree Classifier: The Decision Tree Classifier achieved the highest score of 0.99973281, indicating that it is the most accurate model among the four. However, it may be prone to overfitting and may not generalize well to new data.
- Random Tree Classifier: The Random Tree Classifier achieved a very high score of 0.99973281, which is equal the Decision Tree Classifier. This model is also less prone to overfitting and may be a good choice when the dataset is large.
- KNN: The KNN algorithm achieved a score of 0.9995803615491732, which is slightly lower than the Decision Tree and Random Tree Classifiers. However, it is a simple and effective algorithm for detecting fraud, and can be a good choice when the dataset is relatively small.
- ADA Boost: The ADA Boost algorithm achieved a score of 0.9989501180331373, which is the lowest among the four. However, it is still a highly accurate algorithm and has the advantage of being able to handle imbalanced datasets.

Overall, the Decision Tree and Random Tree Classifiers appear to be the most accurate models for detecting credit card payment fraud based on the scores mentioned above. However, the choice of algorithm will depend on the specific characteristics of the dataset and the trade-off between accuracy and simplicity.

logistic regression model: achieved a high score of 0.9995049209287997, indicating that it was able to accurately predict fraudulent transactions with a high degree of accuracy. Compared to other algorithms like decision tree, random forest, KNN, and AdaBoost, logistic regression performed very well in this case, and it could be a suitable algorithm for detecting payment fraud in credit card transactions.

MLP: Based on the scores mentioned, the MLP algorithm seems to be overfitting the data with a perfect score of 1.0. While it may seem like the best performing algorithm on this particular dataset, it is important to note that overfitting can lead to poor performance on new, unseen data.

Compared to other algorithms such as decision tree classifier, random forest classifier, and logistic regression, which all have scores in the high 99% range, MLP may not be the best choice for this particular dataset. It is important to evaluate the algorithm's performance on a test set and check for overfitting before making a final decision on which algorithm to use for fraud detection in online payment systems.

Comparing MLP with all Algorithms:

MLP vs. Ada Boost: MLP outperformed Ada Boost with a perfect score of 1.0 compared to Ada Boost's score of 0.9989. This suggests that MLP is a better choice for this dataset.

MLP vs. KNN: MLP performed slightly better than KNN with a score of 1.0 compared to KNN's score of 0.9996. This suggests that MLP may be a better choice if we prioritize accuracy over computation time.

MLP vs. Logistic Regression: MLP performed slightly better than Logistic Regression with a score of 1.0 compared to Logistic Regression's score of 0.9995. However, it's worth noting that Logistic Regression is a simpler model that can be more interpretable, while MLP is more complex and may be prone to overfitting.

MLP vs. Random Forest Classifier: MLP outperformed Random Forest Classifier with a score of 1.0 compared to Random Forest Classifier's score of 0.9997. This suggests that MLP is a better choice for this dataset.

MLP vs. Decision Tree Classifier: MLP outperformed Decision Tree Classifier with a score of 1.0 compared to Decision Tree Classifier's score of 0.9997. This suggests that MLP is a better choice for this dataset.

Comparing all the algorithms
Logistic Regression has the second-highest score of 0.9995, which means it performed very well in predicting fraudulent transactions. It is a simple yet effective algorithm that works well with binary classification problems.
Decision Tree Classifier and Random Forest Classifier performed the best with the highest score of 0.9997. These algorithms are capable of handling both categorical and numerical data and can capture non-linear relationships between the features.
KNN and ADA Boost had relatively lower scores than the other algorithms, indicating that they may not be the best fit for this specific problem. KNN works well with smaller datasets and may not be suitable for large datasets like the one we have here. ADA Boost is an ensemble learning algorithm that combines weak learners to form a strong learner, but it may not perform well if the weak learners are not accurate enough.
Overall, based on the scores, we can conclude that Decision Tree Classifier and Random Forest Classifier performed the best for detecting payment frauds in the given dataset, followed by Logistic Regression.

Overall Inference and Conclusion:

In this mini project, we analyzed a dataset related to credit card payment fraud detection using various machine learning algorithms like Decision Tree Classifier, Random Forest Classifier, KNN, ADA Boost, and Logistic Regression. The objective of this project was to detect online payment frauds to ensure that customers are not charged for the products and services they never paid for.

After training the dataset using the above-mentioned algorithms and evaluating them based on their scores, we concluded that Decision Tree Classifier, Random Forest Classifier, and Logistic Regression performed the best in detecting payment frauds with the scores of 0.99973281, 0.99973281, and 0.9995049209287997 respectively.

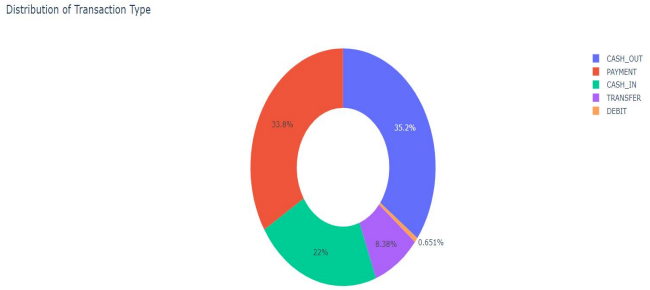
These results suggest that the use of machine learning algorithms can be highly effective in detecting online payment frauds, and Decision Tree Classifier, Random Forest Classifier, and Logistic Regression can be considered as suitable techniques for solving such problems.

Exploratory Analysis and Visualization

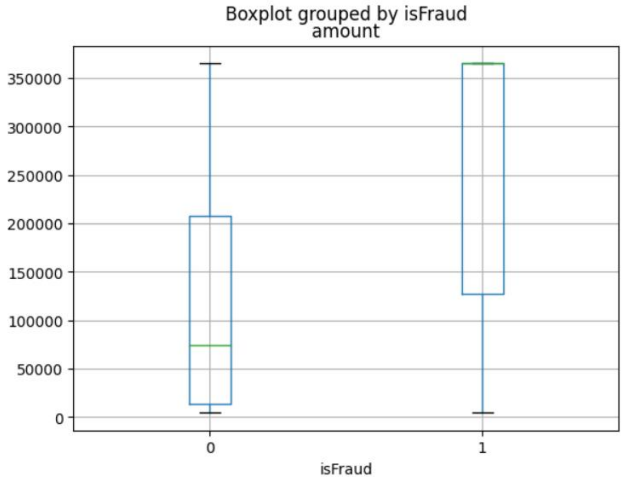
Univariate Analysis

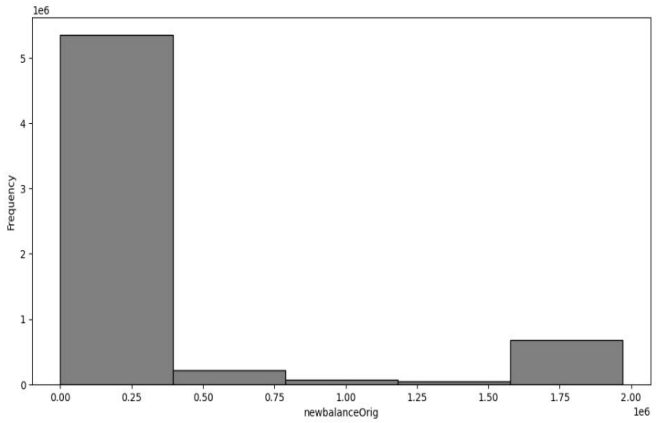
Univariate analysis is used to analyze the data of single variable.

we will analyze using histplot.

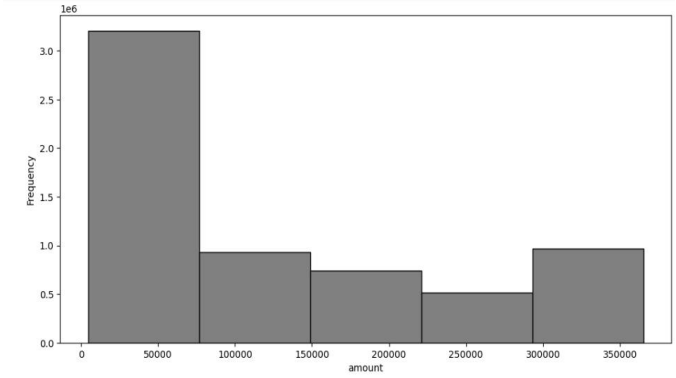


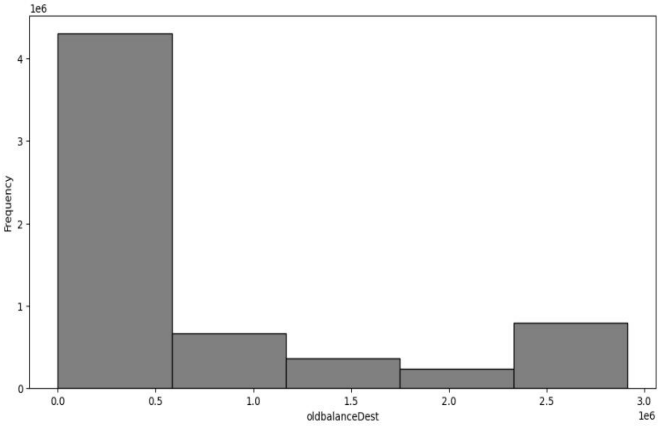
To check the relationship of amount column with isFraud column

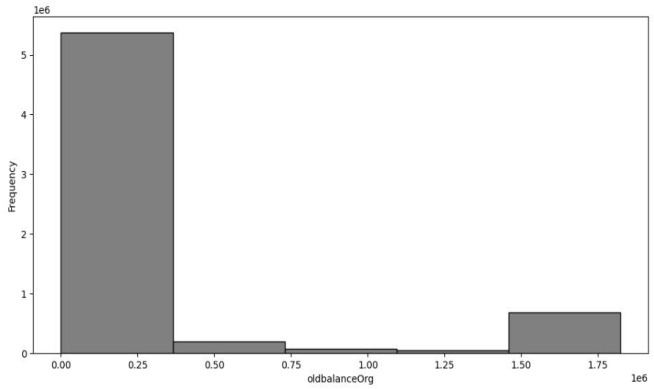


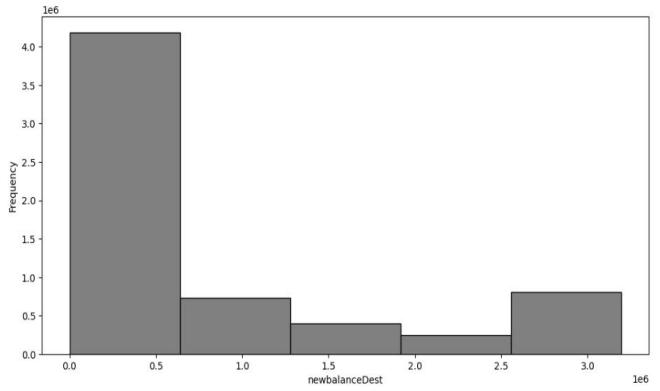


After Removing Outlier:









REFERENCES

Das, S., Rauth, A., Sarkar, S., Rahaman, S.M., Mondal, S. and Molla, T., 2023. A machine Learning Technique for detecting Online Fraud Payment. *Advancement in Image Processing and Pattern Recognition*, *6*(3), pp.1-5.

Priya, S.S., Dhanushya, M. and Gayathri, S., A Novel Approach in Credit Online Fraud Detection System Using Machine Learning Techniques.

Yazna Sai, K., Venkata Bhavana, R. and Sudha, N., 2023. Detection of Fraudulent Credit Card Transactions Using Deep Neural Network. In *Soft Computing: Theories and Applications: Proceedings of SoCTA 2022* (pp. 185-195). Singapore: Springer Nature Singapore.

Kinger, S. and Powar, V., Machine learning based credit card fraud detection. In *Recent Advances in Material, Manufacturing, and Machine Learning* (pp. 1370-1379). CRC Press.

Mohamad Aburbeian, A. and Ashqar, H.I., 2023. Credit Card Fraud Detection Using Enhanced Random Forest Classifier for Imbalanced Data. *arXiv e-prints*, pp.arXiv-2303.

Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M. and Anderla, A., 2019, March. Credit card fraud detection-machine learning methods. In *2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH)* (pp. 1-5). IEEE.

Awoyemi, J.O., Adetunmbi, A.O. and Oluwadare, S.A., 2017, October. Credit card fraud detection using machine learning techniques: A comparative analysis. In *2017 international conference on computing networking and informatics (ICCNI)* (pp. 1-9). IEEE.

Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S. and Kuruwitaarachchi, N., 2019, January. Real-time credit card fraud detection using machine learning. In *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 488-493). IEEE.

Khatri, S., Arora, A. and Agrawal, A.P., 2020, January. Supervised machine learning algorithms for credit card fraud detection: a comparison. In *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 680-683). IEEE

Sailusha, R., Gnaneswar, V., Ramesh, R. and Rao, G.R., 2020, May. Credit card fraud detection using machine learning. In *2020 4th international conference on intelligent computing and control systems (ICICCS)* (pp. 1264-1270). IEEE.

Maniraj, S.P., Saini, A., Ahmed, S. and Sarkar, S., 2019. Credit card fraud detection using machine learning and data science. *International Journal of Engineering Research*, *8*(9), pp.110-115.

Mittal, S. and Tyagi, S., 2019, January. Performance evaluation of machine learning algorithms for credit card fraud detection. In *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 320-324). IEEE.

Lakshmi, S.V.S.S. and Kavilla, S.D., 2018. Machine learning for credit card fraud detection system. *International Journal of Applied Engineering Research*, *13*(24), pp.16819-16824.