A Comparative Analysis of Machine Learning Algorithms on Card-Based Financial Fraud Detection with Infusion of Sigmoid and Isotonic Functions

Ariyo Olorunmeye Omolade, Rasheed Gbenga Jimoh

Department of Computer Science, University of Ilorin, Ilorin, Nigeria

DOI: https://doi.org/10.51244/IJRSI.2023.1011027

Received: 29 October 2023; Revised: 08 November 2023; Accepted: 11 November 2023; Published: 11 December 2023

ABSTRACT

There is no doubt that the commencement of the e-revolution in the financial sector of the economy has introduced opportunity for electronic fraud in the card payment ecosystem globally. This is occasioned by factors such as increased knowledge in the fintech space, poverty, pair pressure on the perpetrators. This study was focused on comparing of several known Machine leaning Algorithms – Logistic regression, Decision trees, Random Forest, Extra-Trees, Adaboost and Gradient boosting on how they perform comparatively when applied to Fraud detection. The raw data used were obtained from The Xente Fraud Detection data set used for the development of the financial fraud detection model which includes sample of approximately 140,000 transactions categorized into Fraud and Non-Fraud. Results from the study indicated that Adaboost Model outperformed the remaining applied models thereby making Adaboost a good model for fraud detection. Further research work can be carried out by comparing the performance with other Deep Learning Algorithms.

Keywords: Deep Learning, Data Imbalance, Card Fraud, Algorithm, Adaboost

INTRODUCTION

The e-revolution occasioned by the emerging ubiquitous computing did not eliminate the financial sector which has forced all financial transactions to be online. A situation with great security challenges due to the expanded network across the internet. No doubt, such ubiquitous opportunities have provided a friendlier, result-oriented and efficient financial transaction without any constraint imposed by the geographical location and time [1]. However, these gains are not without their pains, the more critical among the pains is the need to keep such ubiquitous transactions secured from fraudsters.

Financial fraud had been known to be an intentionally deceptive action aimed at providing the perpetrator with an unlawful access to people's fund or assets. These have over the years been categorized into; tax fraud, credit card fraud, wire fraud, securities fraud, and bankruptcy fraud [2].

In 2017, a study found that a Deep Learning approach provided comparable results to prevailing fraud detection methods such as Gradient Boosted Trees and Logistic Regression [3]. Therefore, efforts in securing financial transactions should be an endless engagement.

The application of Deep Learning Algorithm (DLA) has been found useful and applicable in the aspect of fraud detection and other aspect of machine learning problems [4]. Further researches also showed that the

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

field of machine learning is observing its golden era as DLA is slowly becoming the main-stay in this field with the use of multiple layers to represent the abstractions of data for the development of powerful computational models [5].

Researchers have discovered that the application of DLA can help in overcoming the bottlenecks of earlier primitive networks that lacked efficient training and abstractions of hierarchical data [6]. In the same vein, it was discovered that among the world's leading economies and technology companies, DLA have proved to be of best proven capabilities and performance in so many areas [7].

The financial industry has evolved through many phases since the history of exchange began, from the crude old forms of transaction up to the 21st century where technological innovations have simplified every single banking operation including the easy and seamless transfer of funds from one person to another [8]. This notwithstanding, security of such seamless transactions is still of great concern.

It is also interesting as it gets through many years of evolution and technological advancements, the financial sector has also inherited numerous risks and possibilities of security breaches as people's savings and funds are everyday being defrauded through illegal activities of hackers, scammers, fraudsters and dubious social engineers [9]. The reason for this kind of greed is obvious as the global financial assets hit an all-time worth of $124 trillion dollars according to the recently released [9]. For the fact that these funds are hosted and transacted electronically, this motivated the fraudster towards their activities [10].

In 2019, the Nilson report on credit card fraud estimates a total of $28.65bn worldwide and at the end of 2020, the US alone lost $11bn to credit card fraud [9]. Such alarming rates of financial fraud calls for serious research attention.

B. Statement of the Problem

Financial frauds are criminal in nature and are increasingly becoming sophisticated in leaps and bound while detection and prevention is not a simple endeavour [11]. A lot of research resources had been deployed in the past to check financial fraud occurrences, yet the criminality perseveres [12]. Researchers have found that card-based and other financial related frauds are on the increase which has resulted in the loss of $3 billion to North American financial institutions only in 2017 [13]. It therefore implies that the challenge has a global perspective.[14] pointed out several problems about existing fraud detection methods arising from noisy data and overlapping patterns, to include highly unbalanced datasets where only a little percentage of the available dataset is seen as fraud, thereby making the training of models difficult. This has led to several false judgements on possible threats. Hence, a more radical approach is desired. Another Neural Network architecture employed in fraud detection are Parallel Granular Neural Networks (PGNNs), this method was mainly targeted at improving the speed at which the voluminous customer transaction data is mined in order to detect fraudulent flags. Though, this approach is deficient with regards to detection rate [15]. Previous Researchers have found out that the use of Machine learning techniques to detect fraud in the past have not yielded optimal result [13]. Thus, the researcher intends to apply DLA to achieve the desired security of the ubiquitous financial transactions.

C. Aim and Objectives of Study

The aim of this research is to develop an enhanced card-based financial fraud detection system. The specific objectives are to:

- Design and evaluate multiple Machine leaning models for card-based fraud detection;
- simulate the models;
- evaluate the appropriateness of the best model

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

D. What is Fraud

The term "fraud" can be defined in a variety of ways. "In the business world, fraud is defined as a willful deceit, misappropriation of a company's assets, or financial data manipulation to the perpetrator's benefit" [16]. According to the International norms on Auditing(ISA), fraud is defined as" an purposeful act by one or further individualities among operation, those charged with governance, workers, or third parties, involving the use of deception to gain an unjust or illegal advantage" by one or further individualities among operation, those charged with governance, workers, or third parties(17).Further definition by reveals that Fraud is "any illegal act characterized by deception, concealment, or breach of trust". Fraudulent transactions are the exception rather than the rule. Other abnormalities, such as discrepancies in accounting records, are the result of insufficient procedures or other internal control flaws.

According to [18], majority of financial fraud are premised on the setting of predefined thresholds and rules that are statistically motivated, these are rarely enough to track recent sophisticated frauds.

Table 1: Summary of contribution in literature

Author(s)	Data Description	Method(s) Applied	Performance Metric System	Result	Strength(s)	Limitation(s)
Arafa, A., El-Fishawy, N., Badawy, M. (2023)	Breast Cancer Wisconsin (Diagnostic) Data Set (WBCD)	RN-Autoencoder, SVM-RBF, SGD-LR, KNN and LDA	Accuracy, Recall, F1, precision, Kappa, MCC and GM scores	RN-Autoencoder outperformed	Reduce the high-dimensionality of the gene expressions and then handle the class imbalance using RN-SMOTE	No time analysis of the model
Asha and Kumar (2021)	Kaggle European credit card transaction dataset	SVM, ANN and KNN	Accuracy and Precision	The ANN outperformed the other two algorithms	Comparative analysis of algorithms	Data Class Imbalance
Stojanovic, et. al. (2021)	Kaggle European credit card transaction dataset	Random forest, adaptive boosting and extreme gradient boosting	ROC	Adaptive Boosting (Adaboost) outperformed other algorithms	Comparative analysis	Dependence of results on initial configuration as algorithms are subjected to different trade-offs

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

Voican(2021)	Not specified	Neural Network	Accuracy	The neural network model has accuracy of99%	Provision of file extensions that can be integrated into mobile devices to prevent credit cardfraud	Absence of comparison with other techniques to determine how good the modelperforms vis- à-vis other algorithms
Almhalthawi, et. al. (2020)	Kaggle European credit card transaction dataset	CatBoost, Random forest, Extreme gradient boosting and Bayes minimum risk	F1-scores	Catboost and random forest outperformed other techniques while extreme gradient boosting when combined with Bayes minimum risk has better chances of saving cost	The study went beyond performance to examine savings and cost	Dataset imbalance
Nordling (2020)	Kaggle European credit card transaction dataset	Random Forest, Variational auto-encoder and LSTM auto-encoder	Accuracy, Precision, AUROC	Random forest model outperformed auto-encoder models	Comparative analysis	The auto-encoder is vulnerable to the data typology used
Misra, et. al. (2020)	Kaggle European credit card transaction dataset	Two stage auto-encoder, other variants of auto-encoder	Precision, accuracy	The two stage auto-encoder outperformed other variants of auto-encoder	Comparative analysis	The two stage auto-encoder requires retaining of model
More, et. al. (2020)	Not specified	Random forest technique, decision tree and Naïve Bayes techniques	F-score, precision, sensitivity and accuracy	Random forest technique performed better than the decision tree and the Naïve Bayes techniques	Comparative analysis	Imbalanced dataset

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

Husejinovic (2020)	Not specified	Naïve Bayesian and C4.5 decision tree algorithms	Precision, recall and PRC area rates	C4.5 decision tree algorithm performed better at 92.74% than the Bayesian technique that was adjudged to be poor performing	Comparative analysis	Imbalanced dataset
Sharma and Pote(2020)	Kaggle European credit card transaction dataset	Neural network and auto-encoder	Accuracy and precision	The neural network outclassed the auto-encoder in accuracy and precision as the former detects less counts of false negative or false positive cases	Comparative analysis	Extreme dataset imbalance
Abinayaa, et. al. (2020)	Not specified	Random forest algorithm	Accuracy and precision	There was 60% accuracy and 28% precision with the algorithm	Nil	Use of incomplete data for analysis
Sharma and Pote (2020)	Kaggle European credit card transaction dataset	Decision tree, random forest, auto-encoder and neural network algorithms	Accuracy and precision	All the algorithms had accuracy of 99% but neural network outclassed other algorithms by the yardstick of precision at 89% while the auto-encoder was the weakest with 20% precision	Comparative analysis	Data imbalance

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

Dada, et. al. (2019)	German and Australian credit card transaction datasetculled fromthe UCI data repository	K-star, Naïve Bayes andSVM techniques	Accuracy, ROC curve, MCC, F-score and precision	The K-star algorithm outclassedother algorithms	Comparative analysis	The study had incomplete conclusions as the result was only premised on the MCC without any recourse to other performance metrics
Askari and Hussain (2019)	Not Specified	Fuzzy rule based system	Accuracy	The fuzzy rule based system had 90% fraud detection accuracy	Nil	The study failed to carry comparative analysis
Sharma (2019)	Credit card transaction dataset as culled from the ULB	Random forest, Adaptive Boosting, Extreme Gradient Boosting and LightGBM algorithms	AUC score	Extreme gradient algorithm outperformed other algorithms	Comparative analysis	Also vulnerable to imbalanced dataset
Al-Shabi (2019)	European credit card transactions culled from the ULB	Auto-encoder and Logistic regression algorithms	Accuracy	The auto-encoder outperformed the logistic regression model	The auto-encoder was tested at three different thresholds for more robust results	Data imbalance
Manek, et. al. (2019)	Credit card transactions extracted from Kaggle	Logistic regression and auto-encoder neural network	Accuracy	The auto-encoder outperformed the logistic regression algorithm	Comparative analysis	Data imbalance
Jain, Tiwari, Dubey and Jain (2019)	KDD CUP 99 Intrusion dataset	SVM, ANN, Bayesian Network, KNN, Fuzzy logic rule based, decision tree and logistic regression	Precision and Accuracy	The ANN had the highest accuracy while the fuzzy logic rule based system had the lowest accuracy	Comparative study	Incomplete dataset for analysis

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

Maniraj and Saini (2019)	Not specified	Local outlier factor and isolation forest algorithm	Accuracy and precision	The technique performedwellat 99% accuracy especially when tenth of the data is supplied to the algorithm	Nil	Single technique analysis that gives no roomfor comparisonwith any other technique as benchmark
Fawehinmi (2018)	Not specified	Anomy detection technique through generic algorithm, the SVM and artificial neural network	Accuracy and precision	The anomy generic algorithm outperformedthe other two techniques	Compar ative analysis	Dataset imbalance
Sweers (2018)	European credit card transactions from Kaggle	The conventional and variational auto-encoder	Recall and precision	The regular auto-encoders outclassed the variational auto-encoders	Compar ative analysis	Dataset imbalance
Reshma (2018)	European transactions extracted from Kaggle	Regular auto-encoder, Variational auto-encoder, restricted Boltzmann machine and the deep belief network	ROC curve (AUC) value	The variational auto-encooder outperformed other algorithms considered in the study	Compar ative analysis	Absence of real time data as well as presence of data imbalance
Khare and Sait (2018)	European transactions from ULB	Decision tree, random forest, support vector machines and logistic regression	Accuracy	The randomforest algorithm performed better than other techniques	Compar ative analysis	Inadequate preprocessing which led to the presence of imbalanced dataset
Choi and Lee (2018)	Korean transactions extracted from the Korea IoT environment	Naïve Bayes, SVM, C4.5, random forest and neural network techniques	F-score	The neural network outclassed other techniques	Compar ative analysis	The method is slow as it takes longer time to achieve results
Pumsirirat and Yan (2018)	European, German and Australian credit card transaction dataextracted from Kaggle and the UCI machine learning repository	Auto-encoder and therestricted Boltzman machine	AUC score	The auto- encoder outperformed the Boltzman machine as measured by the AUC score	Comparati ve analysis with dataset spanning across different countries	Simulation of data which was assumed may not reflect reallife situation

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

Besenbruch (2018)	Credit card transactions as culled from Kaggle	The auto-encoder and the feed-forward algorithms	AUC score	The auto-encoder outperformed the feed forward network	Comparative analysis	Vulnerability to data imbalance
Renstrom and Holmsten (2018)	Not specified	Single, stacked and variational auto-encoder	Accuracy	The stacked auto-encoder performed better than the single and variational auto-encoder	Comparative analysis	Data imbalance
Lu (2017)	Credit card transactions from Kaggle	Logistic and neural network techniques	Recall	The logistic regression outclassed the neural network	Comparative analysis	Data imbalance
Banerjee, et. al. (2018)	Credit card transactions from the University of California, San Diego and Fair Isaac Corporation competition	Naïve Bayes, Random forest, multilayer perception, KNN, logistic regression and support vector machine algorithms	F-Scores	The SVM outclassed other algorithms	Comparative analysis	Data imbalance
Razooqi, et. al. (2016)	Not specified	Fuzzy logic rule based and ANN algorithms	Accuracy	The ANN outclassed the Fuzzy logic rule based system	Comparative analysis	Absence of real credit card transactions for analysis
Seo and Choi (2016)	Korean credit card transactions from and unspecified source	Decision tree and SVM	Accuracy and Precision	The SVM performed better than the decision tree	Comparative analysis	Data imbalance
Singh, et. al. (2012)	Not specified	SVM based radial basis function and the linear/quadratic systems offraud detection	Accuracy	The SVM based radial basis function fared better than the linear and quadratic systems of fraud detection	Comparative analysis	Dataimbalance

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

Jiang, et. al. (n.d)	Credit card transactions culled from Kaggle	Auto-encoder algorithm	Accuracy	The auto-encoder had accuracy as high as 97% with a 7 layered denoising procedure	The auto-encoder was subjected to a 7 layered denoising procedure	Data imbalance
Amany and Issa (n.d)	Data extracted from 154 individual financial transactions	Rule-based decision tree algorithm	Accuracy	The rule-based decision tree had up to 92% accuracy	Nil	Absence of comparative yardstick for analysis

Source: Author's compilation (2023)

DATA AND METHODOLOGY

This focuses on the development of an enhanced card-based financial fraud detection model. We created multiple models with varying regularizations and based on the evaluation technique applied, one with the best performance for detection accuracy is selected. Evaluation techniques used include: confusion metrics, precision, recall, F1, ROC and AUC. The concepts and the design of the methods carried out in the research are described in Figure 1.

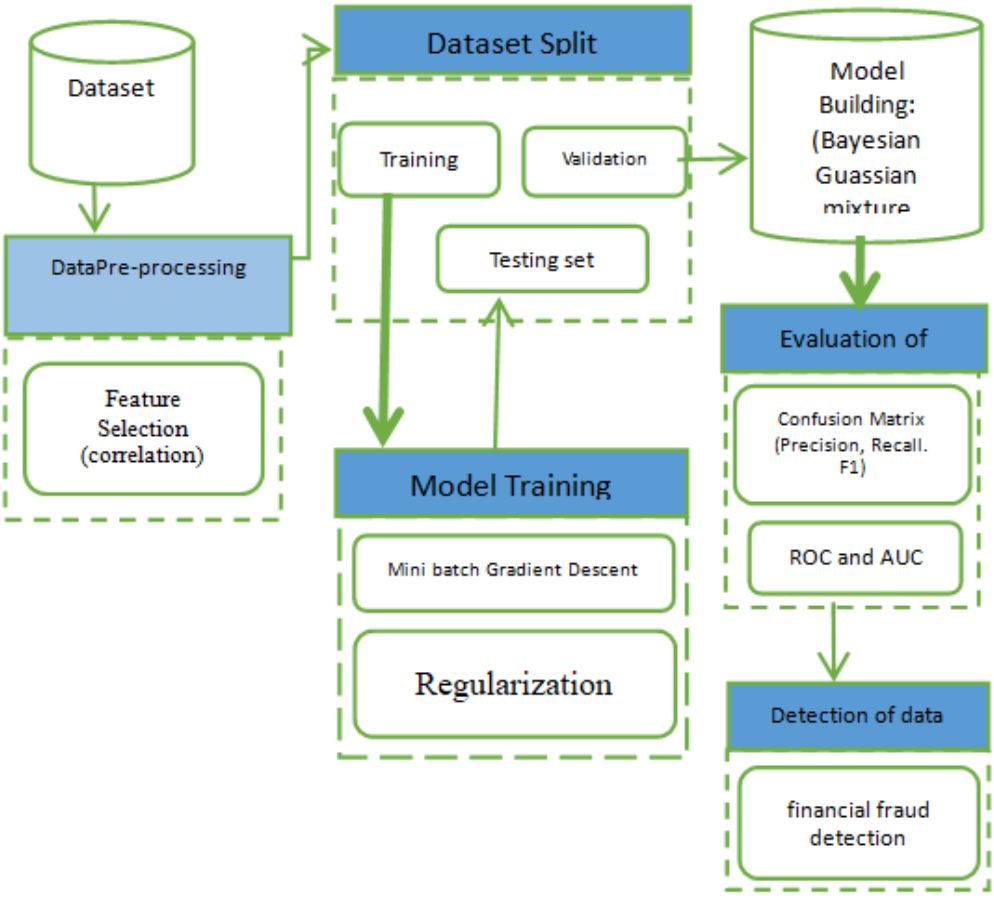

Figure 1: showing the Design method

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

DATA SOURCE AND DESCRIPTION

The Xente Fraud Detection data set used in this research for the development of the financial fraud detection model includes a sample of approximately 95,662 transactions that came about between 15 November 2018 and 15 March 2019. It was collected by Xente Fraud Detection Challenge platform via xente: an e-commerce and financial service app serving 10,000+ customers in Uganda.. In the datasets, we have a Training.csv file: for Transactions from 15 November 2018 to 13 February 2019, including whether or not each transaction is fraudulent which will be used to train the model. Also there is the Test.csv file: for Transactions from 13 February 2019 to 14 March 2019, not including whether or not each transaction is fraudulent.

CORRELATION METHOD

Carrying out Feature Selection in model building is a very important step, to achieve an efficient model. This aids in the reduction of the input feature set, allowing for the removal of unnecessary features and the retention of only the important features from the original feature set [19]. Correlation is a feature selection technique that determines the relationship between input features in a sample data set. It is a measure of the relationship used to evaluate different features. The correlation coefficient is ±1. When the two properties are linearly dependent; otherwise, the correlation coefficient is 0. Correlated variables develop into broader pairings of coefficients that can reveal more about the data, as well as reveal any features that are uninformative or redundant, in line with its strength/weakness [20]. The linear correlation coefficient 'r' for a pair of features

(x, y), given by

$$r = \frac{Covariance(x,y)}{Standarddeviation(x).Standarddeviation(y)}$$

$$r = \frac{n\sum(xy) - \sum(x)\sum(y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]}}$$

Where n= number of pairs of score, $\sum(xy)$= sum of the products of paired scores, $\sum x$ = sum of x scores, $\sum y$ = sum of y scores, $\sum x^2$= sum of squared x scores, $\sum y^2$= sum of squared y scores, if r is equal to or greater that 0.5 the we can say there is positive correlation.

Feature Engineering (Deriving New Features)

We observed through careful analysis of the data, that it was possible to create new independent features from all the identifiers. It was observed that some of the identifiers had numerical details that could possibly be explored and reverse engineered to form a representation and pattern for each user. So, in total, we were able to re-engineer 7 new features from all the 7 identifier features. A new categorical feature was also engineered by performing ordinal encoding which isa type frequency encoding on categorical features to distinguish if a transaction was either a debit or a credit so as to do away with or drop the 'Amount' feature leaving only the absolute feature, 'value'. The feature 'value' is exactly the same as the 'Amount' and the only thing that differentiate the two is the fact that 'Value' is the absolute value of the 'Amount' which has negative values. Hence the reason we are dropping it. New features were also created by grouping each transaction by the product category, pricing strategy, transaction type (debit or credit) and all 7 identifier features which include:

– Batch Id

– Channel Id

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

– Product Id

– Subscription Id

– Account Id

– Customer Id and

– Provider Id

DATA ANALYSIS AND VISUALIZATION

Our first instance of statistical analysis was to consider how much skewness and kurtosis from the mean our features were, including the newly created features. The skewness and kurtosis simply helped us to find where most of the data is concentrated in each feature as shown below, figure 2, shows the histogram plot of some of the numerical features and how skewed they are.

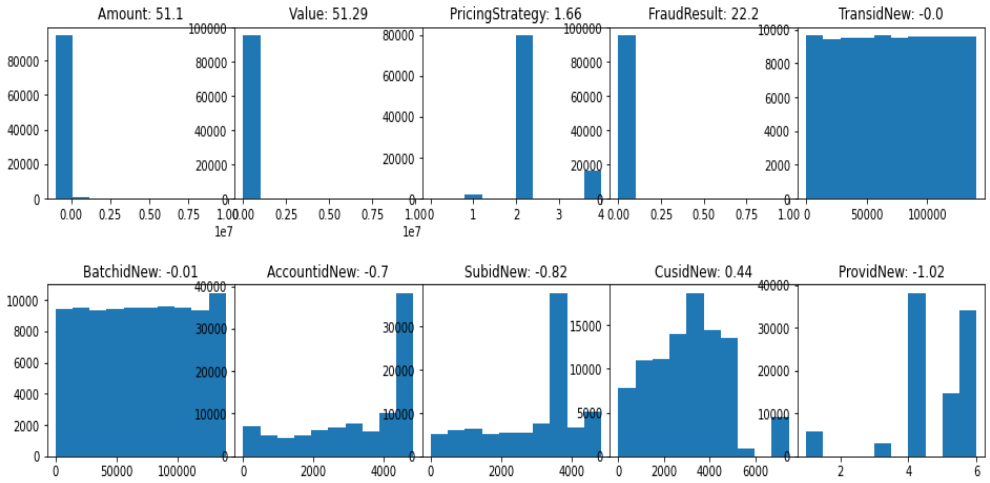

Figure 2: Histogram plot of numerical features of the Xente dataset

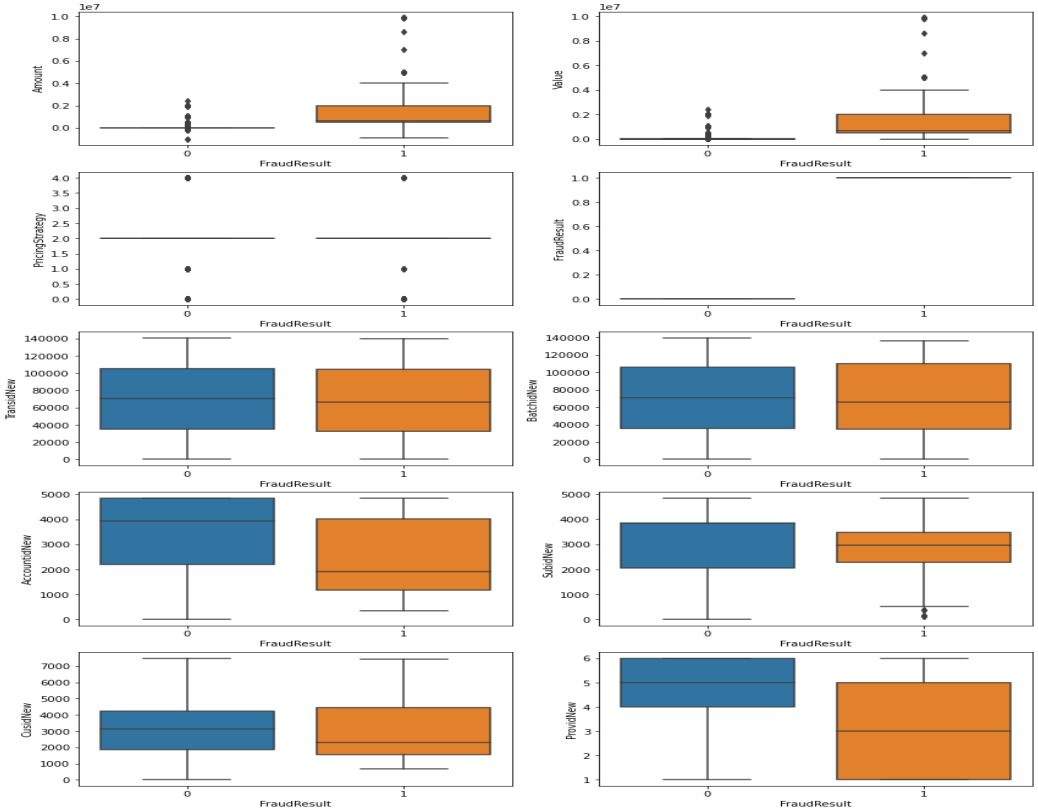

Figure 3: shows a box plot that examines the extent of outlier content in the numerical features.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

CORRELATION, COVARIANCE AND VARIABLE RELATIONSHIPS

In a bid to understand the relationship between each of the independent variables and the dependent variable (Fraud Result), and the relationship/covariance between each independent variables, we explored the Spearman, Kendall and Pearson's correlation methods but we chose to use the Pearson's correlation coefficient due to the fact that we have mostly continuous data. Hence checking for extent of linearity within each variable could give some sense of importance each variable brings to the machine learning modelling. The Spearman's coefficient would have be best for ordinal, normal scale or categorical variables which we would also examine for proper understanding. Below in figure 4 shows the Pearson's correlation coefficient and co-linearity for the numerical features.

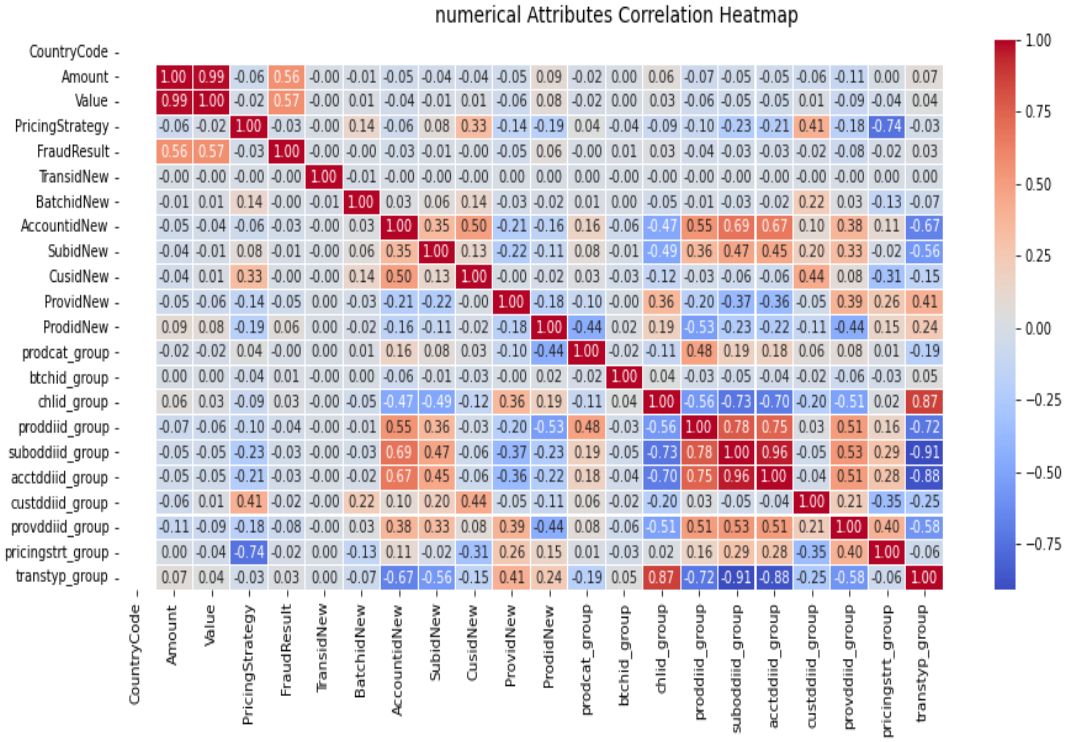

Figure 4: showing the Pearson's correlation coefficient and co-linearity for the numerical features

Dimensionality Reduction and Feature selection

Here we applied the recursive feature engineering methodology to select features that are important and as well reduce the dimension of the dataset so as to avoid clogging the model with redundant features that reduces the accuracy of the model. The first grouped identity features were first trained in within baseline models which include the: Random forest, decision trees, Logistics regression and the ada boost classifier as baseline classifiers for broader inference. But firstly we used the stratified shuffle split approach to segment our dataset into a training and validation set. This is because our dataset is an imbalanced dataset that has far greater representation of one class than the other class. So, in such cases, the stratified shuffle split approach is the best approach because it helps split data in a specified number of bags with a near equal representation of the smaller class in all the bags. In the table showing the representation of each class in the dataset and it can be seen that the fraudulent cases have far greater representation which we would try to solve later using 2 approaches.

Class	Count
0 (non-Fraud)	95,469
1 (Fraud)	193

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

Dealing with Class Imbalance

The xente dataset has a very wide imbalance in the dataset (see table above) and to solve this problem we deployed two techniques: Resampling and Ensemble method.

Hyperparameter Turning to avoid Overfitting

In this research, because we are dealing with imbalance data, Grid search and lasso regularization technique was employed to prevent overfitting. We could have also tried to inject more data as a way of also preventing overfitting but because of the limitation of not having more data, we sticked to 10-fold cross validation.

RESULTS AND DISCUSSION

Considering the imbalance existing between both classes, we needed to come up with a strategy to deal with this problem else we would be having a biased result. After the application of the recursive feature selection approach for feature selection and appropriate regularization, we adopted the stratified shuffling approach for establishing our train, test and validation set in a ratio of 70% : 15% :15% for the holdout set.

Data Presentation

Algorithms	F1-score	Training Accuracy	Validation accuracy
Logistic regression	0.394	0.998	0.998
Decision trees	0.866	1.0	0.999
Random forest	0.875	1.0	0.999
Extra-Trees	0.827	1.0	0.999
Adaboost	0.915	0.999	0.999
Gradient boosting	0.400	0.998	0.998

Table showing the baseline performance of 6 Algorithms across 2 metrics

Taking a closer look at the Adaboost's performance because it has a higher F1-score when compared to others which is an indicator that it recall and precision were both high. We printed the confusion metrics and discovered how sensitive the model was in detecting fraudulent cases. See the matrix below.

TN: 19093	FP: 1
FN: 6	TP: 33

Table showing the confusion Matrix of Adaboost Algorithm in fraudulence cases

Each row in the confusion matrix represents an actual class while each column represents a predicted class. The first row of the matrix considers non-fraudulent transactions (True Negative class: 19093), while the remaining 1 was wrongly classified as Fraud (False Positive). The second row 6 as the False Negatives class (False Negatives) while the remaining 33 were correctly classified as Fraud (True Positives)

We went ahead to apply some isotonic $f(x) = \max(x, 0)$ and sigmoid $f(x) = 1 / (1 + \exp(-x))$ functions to some of the classifiers to check for some improvement in the models performance and the result is shown in the table below.

Algorithms	Precision	Recall	F1 score	AUC
random forest	1.000	0.865	0.928	0.932

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

bagging classifier	0.941	0.865	0.901	0.932
bagging classifier + Isotonic	0.971	0.892	0.930	0.946
bagging classifier + Sigmoid	0.968	0.811	0.882	0.905
Adaboost classifier	0.868	0.892	0.880	0.973
Adaboost classifier + Isotonic	0.794	0.730	0.761	0.865
Adaboost classifier + Sigmoid	0.929	0.703	0.800	0.851
decision tree	0.850	0.919	0.883	0.959
descision tree + Isotonic	1.000	0.811	0.896	0.905
descision tree + Sigmoid	1.000	0.811	0.896	0.905

Table showing the experimentation with sigmoid and isotonic functions

As observed from the table above, the Adaboost classifiers alone without any of the functions or transformations outperformed every other algorithm or function combination. The AUC metric informed our decision since with a value of 0.973 (AUC is a robust metric that is not affected by the class distribution or the classification threshold. This makes it a valuable tool for evaluating and comparing machine learning models) and this also proves that AUC is particularly great for evaluating the performance of binary classification models. The average accuracy remains very close for AdaBoost classifier model accuracy. Hence, we can conclude that our model generalizes well on unseen data as seen in the calibration plots below.

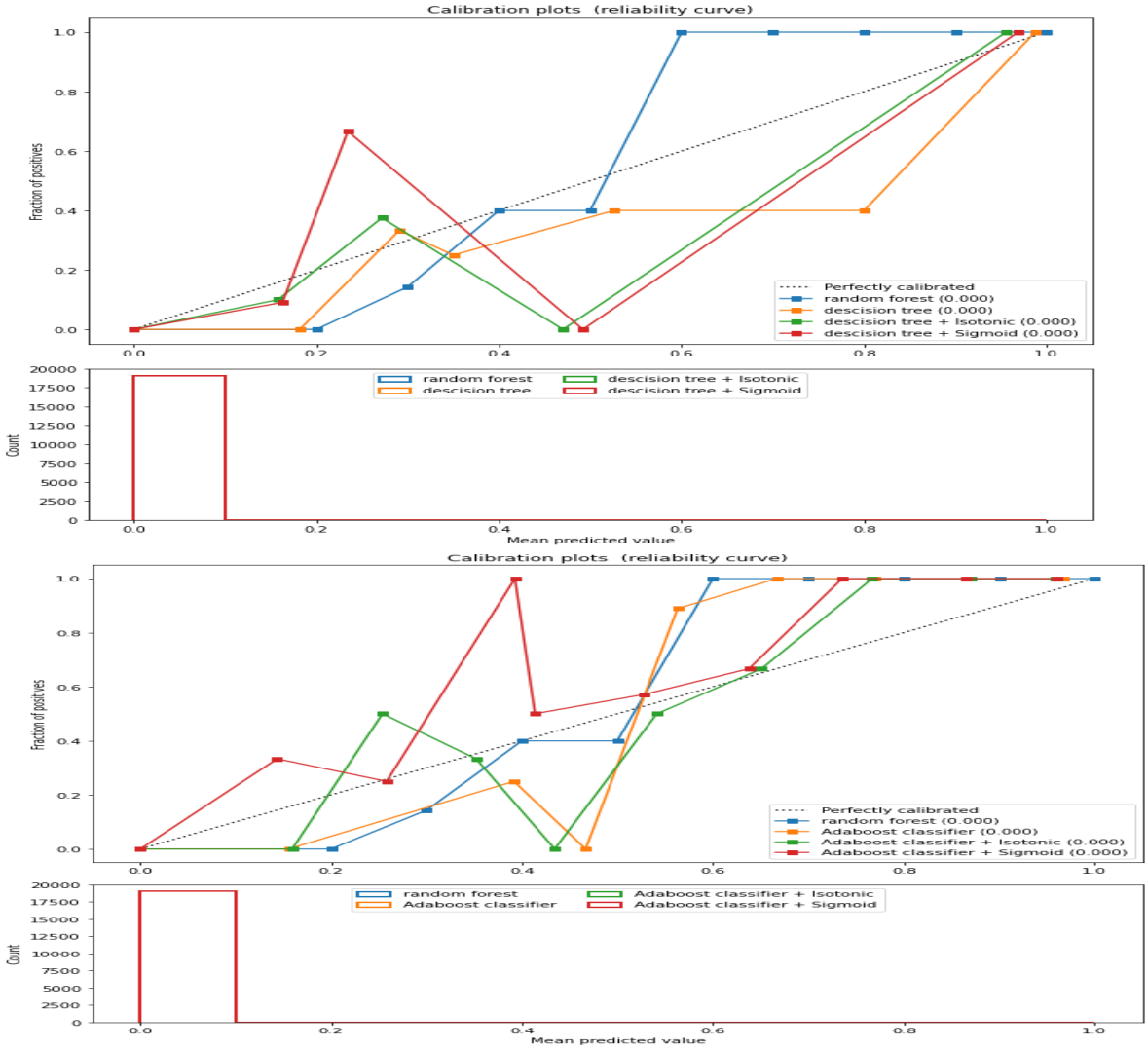

Figure 5 showing the reliability curve (the observed fraction of positives against the predicted fraction of

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

positives) of all algorithm and their functions

CONCLUSION

The study examined the comparative strength of several Algorithms using the Xente dataset for fraud detection. From the result of the study, it can be deduced that the Adaboost Algorithm outperformed the rest of the chosen algorithms when it comes to card fraud detection as seen from the AUC when no Isotonic or Sigmoid function was applied. The outcome shows that Adaboost Algorithm/model was more appropriate for Binary classification problems and by extension Card Fraud detection systems. There is no doubt that this will go along way to help financial institutions to cub card related frauds. Effort should be concerted in future studies to also compare Adaboost with other Deep learning Algorithms to see how it will perform.

REFERENCES

1. Franciska, A.M. & Sahayaselvi, S., (2017). An Overview on Digital Payments. International Journal of Research e-ISSN: 2348-6848 p-ISSN: 2348-795X Volume 04 Issue 13.
2. Doig, A. (2021). What is fraud? In Fraud (pp. 37–59). London: Willan https://doi.org/10.4324/9781843926115.
3. Roy, A., Sun, J., Mahoney, R., Alonzi, L., Adams, S., & Beling, P. (2018). Deep learning detecting fraud in credit card transactions. Systems and Information Engineering Design Symposium, SIEDS 2018
4. Marshall H. (2021). Deep Learning. Retrieved April 26, 2021, from https://www.investopedia.com/terms/d/deep-learning.asp#:~:text=Deep%20learning%20is%20a%20subset,learning%20or%20deep%20neural%20network.
5. Samira, P., Saad, S., Yilin, Y., Haiman, T., Yudong, T., Maria, P. R., Mei-Ling, S., Shu-Ching, C., Iyengar, S. S., (2018). A Survey on Deep Learning: Algorithms, Techniques, and Applications ACM Journals; ACM Computing Surveys 51, No. 5 Article No.: 92
6. Ajay S. & Ausif M. (2019). Review of Deep Learning Algorithms and Architectures. IEEE Access volume 7Retrieved Jan 19, 2021, from: https://www.readcube.com/articles/10.1109%2Faccess.2019.2912200. Digital Object Identifier 10.1109/ACCESS.2019.2912200
7. Andrew, Ng (2018) Machine learning yearning: Technical strategy for AI engineers in the era of deep learning, Tech. Rep., 2019 Retrieved April 27, 2021, from Deeplearning.ai database.
8. Abu N. (2013) Technological implementation and online banking have increased customer service, satisfaction but reduced costs in the Banking sector of Bangladesh. A Master's Thesis in Business Administration, submitted in partial fulfilment of the requirements for Masters in Business Administration Programme, Blekinge Institute of Technology 2013.
9. Business Insider Article, (2021). The digital trends disrupting the banking industry in 2021. Retrieved Jan 15, 2021, from:https://www.businessinsider.com/banking-industry-trends?IR=T
10. Hitachi Solutions Article, (2021). Top ten banking industry challenges and how you can overcome them. Retrieved April 10, 2021, fromhttps://global.hitachi-solutions.com/blog/top-10-challenges-banking-financial-organizations-can-overcome
11. Coderre, D. (2009). Computer-aided fraud prevention and detection. New Jersey: John Wiley and Sons Inc.
12. Nigrini, M. (2011). Forensic Analytics: Methods and techniques for forensic accounting investigations. Hoboken, NJ: John Wiley & Sons, Inc.
13. Nguyen, T. T., Tahir, H., Abdelrazek, M., & Babar, A. (2020). Deep learning methods for credit card fraud detection. Unpublished Paper.
14. Pradheepan R. & Neamat E. G., (2019). Fraud detection using machine learning and deep learning. International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)

15. Yogesh, M., Sushill, K., (2015). A review on credit card fraud detection using BLAST-SSAHA method. International Journal of Advanced Research in Computer and Communications Engineering, 4(11), 425-433.
16. Hall, J. A., (2007). the Auditor's responsibilities relating to fraud in an audit of financial statements, Accounting Information Systems. Fifth Edition. Cincinnati: Thomson South-Western College Publishing, The International Auditing Standards Board, 2009. International Standard on Auditing No.240: The Institute of Internal Auditors, 2009. Internal Auditing and Fraud. IPPF – Practice Guide. IIA.
17. IASB (2021). Fraud and going concern in an Audit of Financial Statements: Exploring the Differences Between Public Perceptions About the Role of the Auditor and the Auditor's Responsibilities in a Financial Statement Audit. Discussion paper Retrieved January 10, 2022, from https://www.iaasb.org/publications/fraud-and-going-concern-audit-financial-statements
18. Khac, N. L. & Kechadi, M. (2010). Appliction of Data minning for anti-money laundary detection: A case study. In IEEE international conferenceon data mining workshops proceeding, 577-584.
19. Blessie EC & Karthikeyan E. (2012) Sigmis: A Feature Selection Algorithm Using Correlation Based Method. Journal of Algorithms & Computational Technology. 2012;6(3):385-394. doi:10.1260/1748-3018.6.3.385
20. Martin O. (2016), Bayesian Analysis with Python, Unleash the power and flexibility of the Bayesian framework, Copyright © Packt Publishing
21. Asha, R. B., & Kumar, K. R. (2021). Credit card fraud detection using artificial neural network. Global Transitions Proceedings, 2(1), 35-41.
22. Stojanovic, B., Bozic, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., Sundaram, M., Jordan, E., & Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in Fintech applications. Sensors, 21(1), 1-43.
23. Voican, O. (2021). Credit card fraud detection using deep learning techniques. Informatica Economica, 25(1), 70-85.
24. Almhalthawi, D., Jafar, A., & Aljnidi, M. (2020). Example-dependent cost-sensitive credit cards fraud detection using SMOTE and Bayes minimum risk. SN Applied Sciences, 2(1574), 1-12.
25. Abinayaa, S., Sangeetha, H., Karthikeyan, R. A., Sriram, K. S., & Piyush, D. (2020). Credit card fraud detection and prevention using machine learning. International Journal of Engineering and Advanced Technology, 9(4), 1199-1201.
26. Al-Shabi, M. A. (2019). Credit card fraud detection using autoencoder model in unbalanced datasets. Journal of Advances in Mathematics and Computer Science, 33(5), 1-16.
27. Askari, S., & Hussain, A. (2019). E-transactional fraud detection using fuzzy association rule mining. Paper Presented at International Conference on Information Systems and Management Science.
28. Dada, E. G., Mapayi, T., Olaifa, O. M., & Owolawi, P. A. (2019). Credit card fraud detection using K-star machine learning algorithm. 3rd Biennial International Conference on Transition from Observation to Knowledge to Intelligence (TOKI).
29. Fawehinmi, O. A. (2018). Hubrid credit card fraud detection using anomaly detection and genetic algorithm. (M.Sc. Thesis). Covenant University, Nigeria.
30. Husejinovic, A. (2020). Credit card fraud detection using naïve Bayesian and C4.5 decision tree classifiers. Periodicals of Engineering and Natural Sciences, 8(1), 1-5.
31. Jain, Y., Tiwari, N., Dubey, S., & Jain, S. (2019). A comparative analysis of various credit card fraud detection techniques. International Journal of Recent Technology and Engineering, 7(2), 402-407.
32. Manek, H., Jain, S., Kataria, N., & Bhole, C. (2019). Credit card fraud detection using machine learning. International Journal of Innovative Research in Science, Engineering and Technology, 8(4), 4507-4515.
33. Maniraj, S. P., & Saini, A. (2019). Credit card fraud detection using machine learning and data science. International Journal of Engineering Research and Technology, 8(9), 110-115.
34. Misra, S., Thakur, S., Ghosh, M., & Saha, S. K. (2020). An autoencoder based model for detecting

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume X Issue XI November 2023

fraudulent credit card transaction. Procedia Computer Science, 167(1), 254-262.
35. More, R. S., Awati, C. J., Shirgave, S. K., Rashmi, J., & Patil, S. (2020). Credit card fraud detection using supervised learning approach. International Journal of Scientific and Technology Research, 9(10), 216-219.
36. Nordling, C. (2020). Anomaly detection in credit card transactions using auto encoders. (B.Sc. Thesis). KTH University of Technology, Sweden.
37. Sharma, P., & Pote, S. (2020). Credit card fraud detection using different machine learning models. International Journal of Creative Research Thoughts (IJCRT), 8(4), 1306-1311.
38. Sharma, P., & Pote, S. (2020). Credit card fraud detection using deep learning based on neural network and auto-encoder. International Journal of Engineering And Advanced Technology, 9(5), 1140-1143.
39. Amany, A., & Issa, T. (n.d). Unsupervised identity application fraud detection using rule-based decision tree. Unpublished Paper. University of Victoria, Canada.
40. Banerjee, R., Bourla, G., Chen, S., Kashyap, M., Purohit, S., & Battipaglia, J. (2018). Comparative analysis of machine learning algorithms through credit card fraud detection. Research Paper Series. New Jersey's Governor's School of Engineering and Technology.
41. Besenbruch, J. (2018). Fraud detection using machine learning techniques. Research Paper Business Analytics, Vrije Universiteit, Amsterdam.
42. Choi, D., & Lee, K. (2018). An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation. Security and Communication Networks, 2018(1), 1-16.
43. Jiang, P., Zhang, J., & Zou, J. (n.d.). Credit card fraud detection using autoencoder neural network. Unpublished Paper.
44. Khare, N., & Sait, Y. (2018). Credit card fraud detection using machine learning models and collating machine learning models. International Journal of Pure and Applied Mathematics, 118(20), 825-838.
45. Lu, Y. (2017). Deep neural networks and fraud detection. (B.Sc. Thesis). Uppsala University.
46. Pumsirirat, A., Yan, L. (2018). Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine. International Journal of Advanced Computer Science and Applications, 9(1), 18-25.
47. Razooqi, T., Raahemifar, K., Khurana, P., & Abhari, A. (2016). Credit card fraud detection using fuzzy logic and neural network. Paper Presented at the Society for Modeling and Simulation International
48. Renstrom, M., & Holmsten, T. (2018). Fraud detection on unlabeled data with unsupervised machine learning. (B.Sc. Thesis). KTH University of Technology, Sweden.
49. Reshma, R. S. (2018). Deep learning enabled fraud detection in credit card transactions. International Journal of Research and Scientific Innovation, 5(7), 111-115.
50. Seo, J., & Choi, D. (2016). Feature selection for chargeback fraud detection based on machine learning algorithms. International Journal of Applied Engineering Research, 11(22), 10960-10966.
51. Singh, G., Gupta, R., Rastogi, A., Chandel, M. D., & Riyaz, A. (2012). A machine learning approach for detection of fraud based on SVM. International Journal of Scientific Engineering and Technology, 1(3), 194-198.
52. Sweers, T. (2018). Autoencoding credit card fraud. (B.Sc. Thesis). Radboud University.
53. Arafa, A., El-Fishawy, N., Badawy, M. et al. RN-Autoencoder: Reduced Noise Autoencoder for classifying imbalanced cancer genomic data. J Biol Eng 17, 7 (2023). https://doi.org/10.1186/s13036-022-00319-3