An Ensemble Model for Credit Card Fraudulent Transactions Detection and Classification

Folashade Auru [1*], Sunday Adewumi[2], Victoria I. Yemi-Peter[3]
1,2&3Department of Computer Science, Faculty of Sciences, Federal University Lokoja, Lokoja, Nigeria.
*Corresponding Author: mowumiauru@gmail.com

Received: September 14, 2024 Accepted: November 28, 2024

Abstract: Credit card payment is gradually becoming a most preferred mode of payments globally. Like many new innovations that invariably turns out to be a success story economically, it often passes through a difficult development stage and acceptance by users due to social and cultural reasons. Implementing Credit/Debit card payments have security challenges, a bane for low acceptance by users from social and cultural standpoints. Big data analytics is one way by which the world is solving and coping with this challenge. The rate at which fraudsters use credit/debit card to commit crimes is on the rise and this need to be curbed to the barest minimum to leverage on the benefits that technology has brought. Though, there are different models for curbing the growing trend of credit card fraud informs of identifying and isolating scenarios, but these are incapable of dealing with the trends. This paper proposes an Ensemble model (that is, Random Forest Classifier, Gradient Boosting Classifier, and CatBoost Classifier) to identify patterns and fraudulent activities in transactions made using credit cards. The dataset of credit card transaction was used to monitor the transaction behaviour of credit card owners. The ensemble model was trained on the outputs of the three individual machine learning classifier algorithms using the stacking classifier. The results showed that, the model achieved prediction accuracy of 96%, a precision score of 98% for the fraudulent transactions, and 96% for non-fraudulent transactions.

Keywords: Ensemble machine learning, Accuracy, Credit card, fraud, Random Forest Classifier, Gradient Boosting Classifier, CatBoost

Introduction

Credit card fraud is widespread due the rise in the online transactions, which has resulted in fraudulent activities [1, 2]. Detecting credit card theft has proven to be a difficult task. Banks and other financial institutions are faced with difficult problems of providing clients with secure transactions. Recently, these institutions are seeking ways to build reliable credit card fraud detection systems to curb the menace of fraud related with the credit card usage. Criminal-minded individuals continue to defraud unsuspecting owners of credit cards [3]. Lakshmi and Selvani, [4] described credit card fraud as a situation where an individual's credit card is used by a third-party without the knowledge and permission of the card holder or owner [4]. Drawing from this, it suffices that Credit card fraud is simply the use of a credit card or debit card to withdraw money, make payment for property or goods and services without the authorization or knowledge of the owner of the card. while Fraud Detection is a process of monitoring the transaction behaviour of a cardholder in order to detect whether an incoming transaction is done by the cardholder or otherwise [5]. Fraud detection is a set of checks and measures put in place to identify and prevent unauthorized or illegitimate claims of funds, property, or goods and services. In this research, we shall be demonstrating how a hybrid of machine learning algorithms can be used to identify patterns and fraudulent activities in transactions made on credit cards. The model will make use of three machine learning classifier algorithms: Random Forest Classifier [6], Gradient Boosting Classifier [7], and CatBoost Classifier [8]. To tackle the menace of credit card fraud, several policing methods involving caught-the-act approach and cyber policing approach whereby the perpetrator is tracked through the matrix, located and arrested. The more recent approach which dwells more on prevention than cure made possible through advances in machine learning or what is conterminously described as artificial intelligence (AI), whereby machines are trained to learn and positively identify potentially fraudulent transactions through a series of complex processes while it is still being initiated. Machine learning is defined [9] as the identification of patterns and structures and making decisions based on observations extracted from the data received.

One of the most effective tools to use is Artificial Intelligence (AI). AI and Machine Learning has seen great improvements in recent times; and it has proven to be applicable in almost every field of human endeavour. The need for a system that can reduce losses became critical for everyone. Hence, the need to develop a Credit Card Fraud Detection System using the Hybrid of Classification algorithms.

The remaining sections of this paper are organized as follows: Section two highlights related works. Section four presents the methodology used and general discussion. (Random Forest Classifier, Gradient Boosting Classifier, and CatBoost Classifier. Section four is the presentation of the result and the findings followed by Section five, which is the conclusion.

Related Work

A Credit Card Fraud Detection System makes use of normal transaction history of the user/cardholder and also fraudulent transaction history to monitor new transactions, with these features (normal and fraudulent transaction history) the system is able to learn and then make predictions whether a transaction is normal or not. Credit card fraud can occur online and offline.

A study in [9] attempted at identifying and solving credit card fraud using advanced machine learning (ML), the deep learning (DL) technique, and deep neural networks. The study adopted a survey design approach involving reported cases of credit card related fraud perpetrated through Point of Sale (POS) and Automated Teller Machine (ATM) through theft and cloning. The authors suggested a hybrid-genetic algorithm that can

automatically detect credit card fraud. The model was able to efficiently distinguish between fraudulent and authentic credit card transactions, obtaining an accuracy of 74.00%. There is the need to improve on the accuracy realized from the model for credit card detection.

Multiple techniques were considered to detect credit card frauds using SVM, KNN, DT, XGBoost Random Forest and Logistic regression by [10]. The data was collected from EU FI dataset containing 284,808 transactions of different credit cards. The dataset used was relatively imbalance as it contains 0.172% fraud cases from the genuine transactions.

Several ML techniques were analyzed in order to judge multiple classifiers by [11]. The study wanted to improve the accuracy of fraud detection through the Synthetic-Minority-Oversampling-Technique (SMOTE) for the conventional oversampling method. Also, sampling methods such as Synthetic-Minority-Oversampling-Technique (SMOTE) with advanced boosting methods such as Isolation-Forest, SVM, and Local-Outlier-Factor (LOF) were applied for better accuracy of outcomes. The models were tested with samples of small records and the Isolation-Forest outperform the other models and achieve 99.74% accuracy, the SVM was 45.84% accurate, and the Local-Outlier-Factor (LOF) was 99.66% accurate.

In [12], the researchers used machine learning techniques to design a model that can detect card fraud, the research focused on the analysis and preprocessing of datasets, and deployment of multiple outlier's detector algorithms such as Local-Factor-Isolation-Forest algorithm on the PCA transformed Credit Card Transaction Data. The algorithm was able to achieve an accuracy of 99.6% accuracy, but was 28% precise when using tenth of dataset. However, when the whole dataset was used, the precision raised to 33%. The increase in accuracy was due to the huge difference between genuine and valid transactions.

The researchers in [13] utilized Random Forest algorithm to detect fraud in credit card. Cardholders' dataset containing 100,000 transactions was adopted by the researchers with 0.262% fraud transactions. Even though the dataset was not balanced, the imbalanced dataset was used. In training the model, the researchers used 80% of the dataset and 20% for testing the model. The evaluation of the model was carried out was based on accuracy, precision and recall. The model was able to achieve an accuracy of 0.9793. The study also performed a comparative analysis of RF, DT and NB models, but the RF out performed all other compared models.

The study in [14] adopted machine learning algorithms to detect credit card fraud. The authors considered certain ML and DL algorithms such as SVM, ANN. DT, LR and RF for detecting fraudulent activities in credit card. Credit card fraud dataset from Kaggle was used to train the models. Accuracy, precision and false alarm rate was used to evaluate the performance of the model. From the result, the ANN outperformed all other algorithms used and obtained an accuracy of 99.92%. The LR performed excellently at an accuracy of 95.55%, the RF has an accuracy of 99.21%, SVM at 95.16% accuracy and DT at 98.47% accuracy.

Another research [15] illustrated the modelling of credit card data with ML algorithms to detect credit card fraud. The researchers used several anomaly detection methods like Isolation-Forest algorithm and Local-Outlier-Factor on the PCA transformed Credit Card Transaction data. The dataset used was obtained from Kaggle. An accuracy of 99.6% was obtained by the algorithm used but they obtain a precision of 28% when considering the tenth data, but when the algorithm is feed with the entire data, the precision rise to 33%.

Some researchers believed XGBoost is an effective, system implementation algorithm based on CART [16]. The researchers used precise data containing online transaction gotten from a financial institution in detection of fraud in credit card. XGBoost and SMOTE were used to sample the dataset. The outcome showed that for best result, SMOKE needed to be used with XGBoost.

In [17] they carried out a survey on credit detecting credit card fraud. The researchers considered different areas detecting credit card fraud which include Insurance fraud, corporate fraud and bank fraud. The researchers focused on virtual and physical transactions using Decision Tree, Logistic regression, KNN, SVM, Genetic Algorithm, NN and NB. The theoretical backgrounds explained are Regression, clustering, classification, outlier detection, visualization and prediction. Existing statistical and computational based techniques such as Artificial Immune system (AIS), Bayesian Belief Network, NN, LR, SVM, DT, Self-organizing map, Hybrid Methods were explained. The researchers arrived at a conclusion that all aforementioned machine learning techniques are capable of detecting with high accuracy.

In study [18], authors attempted to identify 100% of the fraudulent transactions with data gotten from Europe cardholders in September2013. The dataset contained 2 days transactions which includes 492 frauds from 284,807 transactions. The modeling was done using logistic model with each independent variable having its own parameter. Accuracy of 99.6% was attained while having a 28% precision when 10% of the data set was considered. In a study carried out by [16] discussed and analyzed different ML techniques used for card fraud detection including Hidden Markov Model, DT, LR, SVM, Genetic Algorithm, NN, RF, and the BBN. In addition, it discusses the strength and weaknesses associated with each of the considered approaches.

A comparative study carried out by [20] focused on three supervised machine learning algorithms to determine the most suitable for identifying credit card frauds. The authors considered CatBoost, XGBoost and Stochastic Gradient Boosting. After training and testing were carried out individually on the three models, the performances of the models were evaluated based on sensitivity, specificity, error rate and accuracy. Results showed that, CatBoost model achieved the highest accuracy. There is need for improvement by up-scaling and increasing the size of the data for better performance of the model.

In a study by [21], a system based on an artificial neural network was proposed to detect credit card transaction fraud. Performance is measured based on predictions. It also uses classification algorithms such as SVM and KNN to build models that can detect credit card fraud. Comparing the algorithms that were used for the experiment, we conclude that artificial neural networks make better predictions than systems designed with SVM and NN algorithms. The dataset that was used by the researchers consists 31attributes, 30 of which has of information such as age, name, and other information about the account.

A study carried out by [22] developed a fraud detection model for Streaming Transaction Data by the analyzing previous transactional information by extracting of the

behavioral patterns associated with such credit cards. The dataset used comprised data from the European Credit Card Fraud dataset. The dataset was divided into clusters using the Sliding-Window method, and then the Synthetic-Minority-Over-Sampling Technique (SMOTE) was used on it. Different classifiers are then used on datasets. The result showed that the Logistic Regression, Decision Tree and Random Forest algorithms performed better than the other classifiers considered in the study.

According to a study in [23], the proposition of a spectral-clustering hybrid model for the detection of credit card frauds was undertaken. The used model was trained with a modular neural network. The transactions contained in the dataset used were classified into benign and genuine credit card transactions. Results showed that, the model successfully detects benign transactions with an accuracy of 74%. 33,000 credit card transactions records within a 24 months' period of African-based bank customers were understudied.

Methodology

Model Description

The three machine learning classifier algorithms selected for the research were trained on the train data individually and their outputs were used to train the stacking classifier. Stacking is an Ensemble learning technique to combine multiple classification models through a meta-classifier [1, 2, 3, 21]. The first level classifiers are trained with the complete train dataset, which includes Random Forest, Gradient Boosting, and CatBoost Classifiers. Then, the meta-classifier is fitted based on the output of the initial first level classifiers in two ways. The first is by using the outputs of the initial first level classifiers as input or features to the meta-classifier. The second is by using the probabilities of the first level classifiers as features to the meta-classifier. This research adopted the second method in which the predictions of the individually trained classifiers are stacked and used to train the meta-classifier composed of Logistic Regression classifier. After training the meta-classifier, a final model and prediction are obtained from the model.

Random Forest Classifier: It is the Bagging or Bootstrap Aggregating Ensemble Method by creating multiple decision trees. The more the trees in the forest produce more robust the prediction, more accuracy, stable predictions and the overall outcomes even without hyper-parameter tuning. It is a Supervised ML algorithm capable of solving regression and classification problems. Also, RF operates on large dataset with high dimensionality. RF performs object classification using their attributes from different DT like votes. Thereafter, the RF selects the classification with the highest votes. Random Forest builds a group of decision trees trained with the bagging method. The idea behind the bagging method is to combine a set of weak learning models for optimizing the overall accuracy and stability of the model as well as variance reduction.

Gradient Boosting Classifier: It reduces bias error of the model during classification and regression problems. Gradient Boosting operates well for heterogeneous data, small data using dissimilar architecture from the RF algorithm. It is an iterative algorithm based on decision trees that reduces bias error (that is, error from wrong assumption). Gradient boosting minimizes the prediction error, and increases correct categories prediction.

Cat Boosting Classifier: It is based on the Gradient Boosting Classifier, which uses gradient boosting on decision trees. CatBoost used full binary trees and symmetric which lessen possibility of overfitting; and more reliable to parameter changes. It produces faster predictor for numerical and categorical data. It is built on Gradient Boosting Decision Tree (GBDT) for the purpose of improving and enhancing the predictive outcome of a model through an iterative learning process. CatBoost produce great results even without hyper-parameter tuning as its default parameters are a better starting point against other GBDT. CatBoost added a permutation-driven substitute to the classic algorithm, and an innovative algorithm for processing categorical features, this innovation is called Ordered Boosting.

The paper combines three machine learning classifier algorithms using the Stacking ensemble technique to detect fraud in credit card transactions. The block diagram of the proposed Ensemble model is represented in Figure 1.

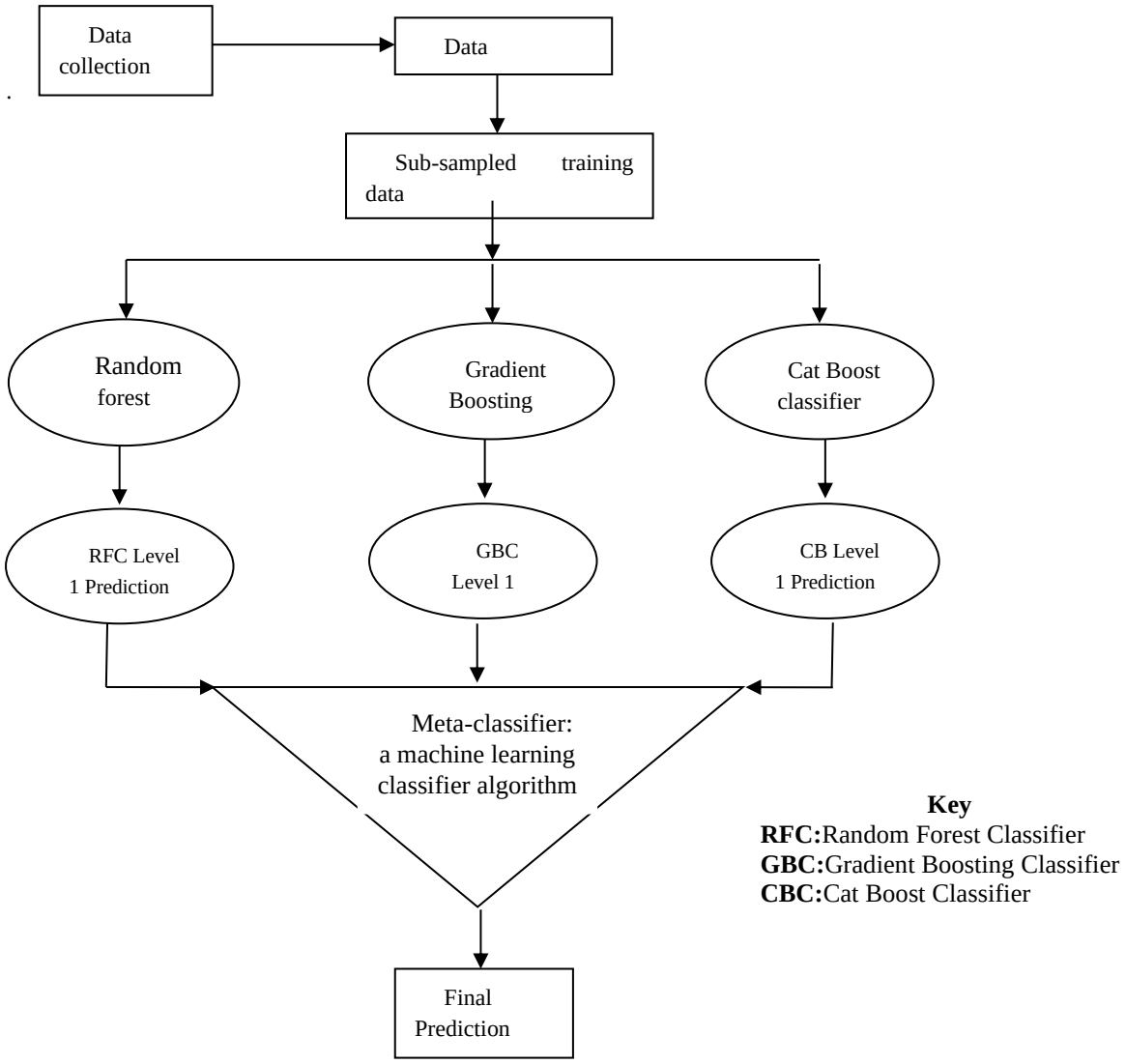

Figure 1: Credit card fraud detection model block diagram

Data Collection and Description: The dataset used in this research contains two days' transaction of credit card holders in September 2013 and the European cardholders containing a total of 284,807 transactions. The dataset is highly unbalanced and had to undergo preprocessing. Random Under-Sampling was applied on the dataset to enable the model to learn well from the data and prevent it from making biased predictions because of the biased nature of the dataset. Also, the fraudulent transactions were made to be equal to the number of non-fraudulent transactions for the target variable (Class) and enable unbiased predictions of the model. The numerical variables are contained in the dataset were realized through a PCA (Principal Component Analysis) transformation.

Evaluation parameters: The train data consists of 90% of the sub-sampled dataset and 10% for testing. The Classification Report, Accuracy Score, F1 score [1, 2, 3].

Results and Discussion

The dataset is biased, so we carried out Random Under-Sample on the data to make the number of fraudulent transactions equal to the number of non-fraudulent transactions considering the target variable (Class), to enable the model make unbiased predictions. Visualization and Exploratory Data

At the end of the implementation phase, two different set results were obtained. The first is training outcomes of the three models (Random Forest Classifier, Gradient Boosting Classifier and CatBoost Classifier) that were

trained individually. For the Random Forest Classifier, the Test accuracy was 0.98989898989899 approximately 99% while the Train accuracy was 0.9966101694915255 approximately 100%. The ROC_AUC_Score (Receiver Operator Characteristic Area Under Curve) was 0.9897959183673469 and the F1 Score was 0.9896907216494846. The Precision on Class 0 was 98% while the Precision on Class 1 was 100%.

For the Gradient Boosting, the Test accuracy was 0.9797979797979798 approximately 98% while the Train accuracy was 0.9966101694915255 approximately 100%. The ROC_AUC_Score (Receiver Operator Characteristic_Area Under Curve) was 0.9797959183673469 approximately 98% while the F1 Score was 0.9795918367346939 approximately 98%. The Precision on Class 0 was 98% while the Precision on Class 1 was 98%.

For the CatBoost Classifier, the Test accuracy was 0.9696969696969697 approximately 97% while the Train accuracy was 1.0 which is 100%. The ROC_AUC_Score (Receiver Operator Characteristic_Area Under Curve) was 0.9697959183673469 approximately 97% while the F1 Score was 0.9696969696969697 approximately 97%. The Precision on Class 0 was 98% while the Precision on Class 1 was 96%.

Secondly, the final_estimator for the stack model was the Logistic Regression algorithm while the estimator consist of the three algorithms stacked (Random Forest Classifier, Gradient Boosting Classifier and CatBoost Classifier). The results obtained after fitting of the stacked model are provided as follows:

Stack model performance on the Training set

stack_model_train_accuracy: 1.0

stack_model_train_score: 1.0

stack_model_train_f1_score 1.0

Stack model performance on the testing set

stack_model_test_accuracy: 0.9697

stack_model_test_score: 0.9696

stack_model_test_f1_score 0.9691

	precision	recall	f1-score	support
0	0.96	0.98	0.97	49
1	0.98	0.96	0.97	50
accuracy			0.97	99
macro avg	0.97	0.97	0.97	99
weighted avg	0.97	0.97	0.97	99

Figure 2: Classification report of the stack model

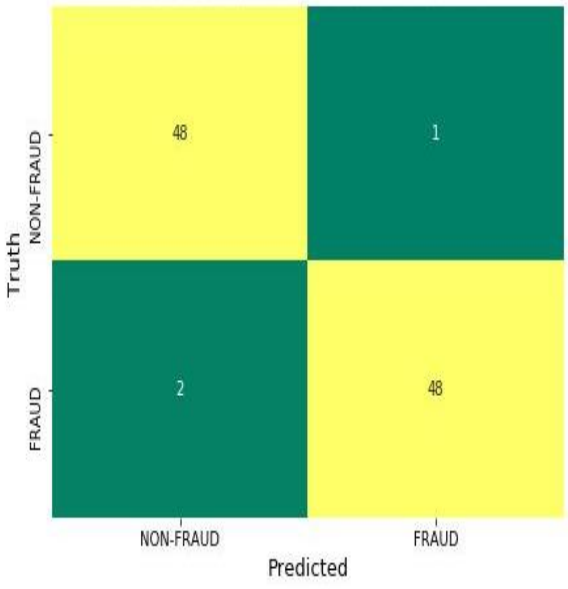

Figure 3: Confuson matrix of the stack model.

From Figures 2 and 3, the paper evaluated the proposed technique for detecting credit card fraud using a hybrid of machine learning models, which builds a more efficient and robust model capable of detecting credit card fraud at a high speed and high accuracy. From the result obtained, the model developed achieved an accuracy of 96%, a precision score of 98% for the fraudulent transactions and 96% for non-fraudulent transactions. This model assists in reducing the steady annual loss of funds and properties attributed to credit card.

Conclusion

This paper developed a credit card detection fraud model capable of detecting anomalies in credit card transactions alone in order to assist e-commerce sector and businesses. The proposed model prevents fraud incidences from happening, and in the long run saves money. Also, it detects and classifies credit card fraud based on the transaction details using a labeled dataset. The outcomes of implementing the model produced an accuracy of 96%. The model can be trained using dataset that has not undergone principal component analysis (PCA) which can be deployed into real-life system, web app and application software. In future works, the research can be extended to predicting upcoming occurrences of credit card fraud.

References

[1] Bin Sulaiman, R., Schetinin, V., & Sant, P. "Review of machine learning approach on credit card fraud detection." Human-Centric Intelligent Systems, Vol. 2, No. 1-2, pp. 55-68, 2022.

[2] Xie, Y., Liu, G., Yan, C., Jiang, C., Zhou, M., & Li, M. "Learning transactional behavioral representations for credit card fraud detection." IEEE Transactions on Neural Networks and Learning Systems, 2022.

[3] Alfaiz, N. S., & Fati, S. M. Enhanced credit card fraud detection model using machine learning. *Electronics*, Vol. 11, No. 4, pp. 662, 2022.

[4] Lakshmi, S. V. S. S., Selvani, D. K., Gao, Y., Zhang, S., Lu, J., Gao, Y., Zhang, S., & Lu, J. "Machine Learning for credit card fraud detection", *ACM*

International conference proceeding series, Vol.13, Issue., 24, pp. 213–219, 2018.

[5] Shamshida, S., Basthikodi, M., Zohara, F., Thameeza, & Mumthaz, M. "Evaluation of Credit Card Fraud Detection Using SVM and ANN", *Journal of Emerging Technologies and Innovative Research (JETIR)*, Vol.6, Issue, 5, pp.100–103, 2019.

[6] Petkovic, D., Altman, R., Wong, M., & Vigil, A. "Improving the explainability of Random Forest classifier–user centered approach", *In 2018 Proceedings of the Pacific Symposium*, pp. 204-215, 2018.

[7] Bentéjac, C., Csörgő, A., & Martínez-Muñoz, G. "A comparative analysis of gradient boosting algorithms", *Artificial Intelligence Review*, Vol. 54, Issue 3, pp.1937-1967, 2021.

[8] Jha, A. CatBoost – A new game of Machine Learning. Affine. https://affine.ai/catboost-a-new-game-of-machine-learning/ 2020

[9] Voican, O. "Credit card fraud detection using deep learning techniques," *Informatica Economica*, Vol. 25 Issue 1, pp.70–85. 2021,

[10] Parmar, J., Patel, A. & Savsani, M. Credit Card Fraud Detection Framework – "A Machine Learning Perspective", *International Journal of Scientific Research in Science and Technology*, pp.431-435, 2020.

[11] Warghade, S., Desai, S. & Patil, V. "Credit card fraud detection from imbalanced dataset using machine learning algorithm", *International Journal of Computer Trends and Technoloyg*, Vol.68, pp.22-28, 2020.

[12] Maniraj, S. P., Saini, A., Ahmed, S., & Sarkar, S. "Credit card fraud detection using machine learning and data science". *International Journal of Engineering Research and Technology*, Vol.8, Issue 9, pp.110-115, 2019.

[13] More, R. S., Awati, C. J., Shirgave, S. K., Deshmukh, R. J., & Patil, S. S. "Credit card fraud detection using supervised learning approach". *International Journal of Scientific & Technology Research*, Vol. 9, Issue 10, pp.216-219, 2021.

[14] Sadineni, P. K. "Detection of fraudulent transactions in credit card using machine learning algorithms". In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), pp.659-660.

[15] Aditya, S., Swarna, D. S., & Shadab, A. "Credit card fraud detection using machine learning," *International Journal of Engineering Research & Technology (IJERT)*, pp.110-115, 2019.

[16] Meng, C., Zhou, L. & Liu, B. "A case study in credit fraud detection with SMOTE and XGBoost. 2021 Journal of Physics: Conference Series. 1601. 052016. 10.1088/1742-6596/1601/5/052016.

[17] Rimpal, P. R., & Jayesh, C. "A Survey on Credit Card Fraud Detection Using Machine Learning." *2018 2nd International Conference on Trends in Electronics and Informatics* (ICOEI). (2019)

[18] Shashank, S., & Meeenu, G. (2021). Credit card fraud detection system. International Journal of Creative Research Thoughts (IJCRT), 312-316.

[19] Tiwari, P., Mehta, S., Sakhuja, N., Kumar, J., & Singh, A. K. (2021). Credit card fraud detection using Machine Learning: A Study. Retrieved from https://arxiv.org/abs/2108.10005v1

[20] Gamini, P., Tejasri Yerramsetti, S., Devi Darapu, G., Kaladhar Pentakoti, V., Prudhvi Raju, V., & Professor, A. "Detection of credit card fraudulent transactions using Boosting Algorithms," *Journal of Emerging Technologies and Innovative Research*, Vol. 8, Issue 2, pp.2031–2036, 2021.

[21] Asha, A., & Suresh Kumar, K. R. "Credit card fraud detection using artificial neural network", *Global Transitions Proceedings*, Vol.2, Issue 1, pp.35–41, 2021

[22] Dornadula, V. N., & Geetha, S. "Credit card fraud detection using machine learning algorithms," *2019 Procedia Computer Science*, 165, pp. 631–641, 2019.

[23] Ojugo, A. A., & Nwankwo, O. (2021). "Spectral-Cluster solution for credit-card fraud detection using a genetic algorithm trained modular deep learning neural network," *Journal of Information and Visualization*, Vol. 2, Issue 1, pp.15–24, 2021

[24] Ceballos, F. Stacking classifiers for higher predictive performance. Towards data science. https://towardsdatascience.com/stacking-classifiers-for-higher-predictive-performance-566f963e4840 2019.