Credit Card Fraud Detection Using XGBoost Algorithm

Ahmed Qasim Abdulghani
Department of Computer Engineering / Information Technologies, Institute of Graduate Studies,
University of Altınbaş – Turkey
ahmed.qasim.ag@gmail.com

Osman Nuri UCAN
Department of Electrical and Computer Engineering, School of Science and Engineering,
University of Altınbaş – Turkey
osman.ucan@altinbas.edu.tr

Khattab M. Ali Alheeti
Department of Computer Networking Systems, College of Computer Science and Information Technology,
University of Anbar - Iraq
co.khattab.alheeti@uoanbar.edu.iq

2021 14th International Conference on Developments in eSystems Engineering (DeSE) | 978-1-6654-0888-2/21/$31.00 ©2021 IEEE | DOI: 10.1109/DESE54285.2021.9719580

***Abstract* - Credit card is one of the modern payment methods widely spread all over the world. It provides excellent facilities in purchasing as well as selling operations. However, it suffers from fraud problems, causing considerable economic losses to banks, institutions, and individuals, amounting to billions of dollars annually. That has made great interest in finding systems and means with outstanding capabilities to confront fraud, whose patterns in addition to methods are increasing dramatically. One of the most prominent techniques used by researchers in this field is Machine Learning (ML) techniques. In this paper, we proposed some of the classification ML algorithms such as Logistic regression(LR), Linear Discriminant Analysis (LDA), and Naïve Bayes(NB), additionally, the boosting algorithm XGBoost to create models capable of detecting fraud. The dataset from Kaggle. We used performance metrics such as accuracy, precision, f1, recall, AUC confusion matrix to evaluate the models' performance. The XGBoost model presented the best results compared to other models.**

Keywords– Credit Card Fraud, Fraud Detection, Machine Learning, SMOTE, XGBoost, Naïve Bayes.

I. INTRODUCTION

The credit card system is currently widely used in modern economies to facilitate business operations worldwide. Due to this ubiquity of credit cards, it has been targeted for cyberattacks besides fraud worldwide. That requires greater security to resolve violations and unauthorized users effectively. Thieves or fraudsters often perform unauthorized or illicit transactions, which usually find unethical methods to threaten credit card systems[1]. Therefore, there is an urgent need for fraud detection methods to be speedy in detection as well as to be able to keep pace with significant changes in fraud methods and their ever-changing strategies[2].

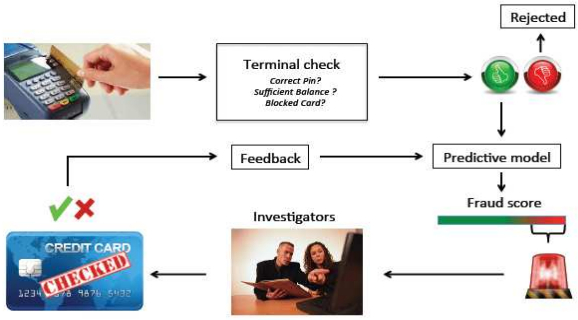

Figure .1. The Credit Card Fraud Detection Process[3]

The detection processes available and currently used depend on multiple methods and means such as artificial intelligence techniques, statistics, and data mining techniques. The detection process passes through an organized sequence, see Figure 1; first, a terminal verification is done for the card. Then, if not rejected, it gives a predictive model that raises alerts for suspicious transactions if they are not rejected. Investigators are improving the accuracy of the predictive model by providing feedback on signs [2].

An excellent solution to detect fraud should reduce fraud at high risk to the lowest level. High-risk fraud causes Losing considerable amounts. The whole credit limit is usually the most significant target when a card is stolen. Fraudsters seize the available amount in a maximum of 4-5 transactions [4]. An effective fraud detection system must have some benefits. Such as to process skewed distributions, process noise, detecting fraudulent transactions that look like legitimate transactions very similarly, being adaptable to changes in fraudulent shapes, and the method of classification used in the assessment of fraud detection must be carefully selected. So metrics such as classification accuracy is inappropriate for skewed distribution[5].

There are many types of fraud: Credit Card, Telecommunication, Computer Intrusion, Bankruptcy, Theft/Counterfeit, Application, and Behavioural Fraud[6]. Credit Card Fraud (CCF) is divided into two main types: Offline fraud and Online fraud. Offline fraud is done by stealing credit cards and taking advantage of them. Online fraud is done via the Internet through hacking operations through computers or phones and devices connected to the network and various credit card information activities.

In the past few years, due to the spread of electronic commerce and its significant development. The demand for using a credit card and benefiting from the services. Its provides has increased, as it facilitates many economic activities. Despite that, its use has severe and adverse disadvantages due to various fraud and counterfeiting methods that lead to substantial financial losses for persons, institutions and banks. Figure 2 shows global economic losses resulting from the CCF for the past years and the expected losses for the coming years according to the study in[7].

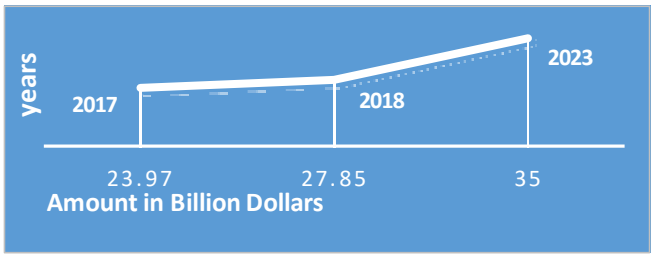

Figure 2. Statistic financial losses due to CCF[7]

This statistic showed that fraud caused substantial financial losses worldwide, as the ratio of 27.85 billion dollars in 2018 was more than the percentage in 2017, which was 23.97 billion dollars, which indicates an increase in the rate from year to year to year. And it predicted that the portion of financial losses resulting from CCF will continue to increase, reaching in the year 2023 to 35 billion dollars, and perhaps more than that[7].

To reduce the percentage of financial losses resulting from CCF, more attention must be paid to the applications of monitoring and monitoring frauds moreover, endeavouring to prevent and avoid them. Fraud detection will reduce customers' problems and complaints, thus gaining their trust. Currently, there is a heavy reliance on Machine Learning techniques in different topics such as credit card fraud detection[8], medical fields[9][10], driverless cars[11][12], etc. Machine Learning has several methods that can be used to find solutions to CCF[13], which include Supervised Learning[14], semi-supervised learning[8][15], and also unsupervised learning[15].

In this paper, we used supervised ML, specifically classification algorithms, to design a CCF detection system relying on python language. The algorithms were LR, LDA and NB, additionally the boosting algorithm XGBoost. Then evaluate the results of each classifier depending on several performance metrics, specifically confusion matrix, accuracy, f1, recall, precision and AUC.

The following sections of this paper are arranged as follows: Section 2 related works regarding credit card fraud detection. In section 3 presented the description of the dataset. In section 4, the methodology is explained. in section 5, the simulation results. Section 6 gave the discussion. Finally, in section 7, the conclusion and future works are presented.

II. RELATED STUDIES

In this section, we briefly review several previous studies that have dealt with the issue of the detection of CCF. These studies are below:

Sudha and Akila (2021) proposed to use the SVM and RF classifiers to develop the Fraud Detection System for Credit Cards depending on Operation & Transactions features. This system is used in the first step to extract users' operational features and then categorize the features into legal and suspicious by using an RF classification. The second step is to extract transaction features of users from user logs and then classify the features into legal and suspicious by the SVM classifier. The performance of the proposed system is assessed with the accuracy, precision, recall and F-1 score of the standard measures. The results indicated that a higher detection rate was achieved with good accuracy by both RF and SVM classifiers[16].

Dileep et al. (2021) tried to find out fraudulent activities in the credit card business by using algorithms that adopt machine learning techniques. Used two algorithms RF and Tree Decision. Some public data are used to determine the efficiency of the model. Then, the examination process is carried out on a set of credit card data taken from a financial institution. Also, the data samples are supplemented by some clatter to check the system's sturdiness. The meaning of the methods used in the paper is that the first method, a tree is constructed against the user's activities, and the tree scams are suspected. The second method creates a forest based on user activity, as well as attempts are made to identify the suspect. The research results show absolutely that the mainstream elective technique reaches decent levels of precision[17].

Tran and Dang (2021) proposed to use two resampling approaches of Synthetic Minority Oversampling Technique (SMOTE) and Adaptive Synthetic (ADASYN) to work on an imbalanced dataset for getting the balanced dataset. The following ML algorithms are used on balanced data: RF, KNN, LR and Decision Tree. To assess the performance of these models, comprehensive classification measures, including fundamental, combined and graphic measures, are used. Authors note that the ML algorithms show positive results for fraudulent activities after resampling the dataset[18].

Janvitha et al. (2021) worked based on the past transactions and the amount used in those transactions to determine the status of the transaction, depending on using HMM (Hidden Markov Model) and various clustering. This model takes the card holder's conduct pattern, and the model is trained to predict. Only when the probability is satisfying is the incoming transaction accepted. First, the historical transactions have to be worked out, and the hidden pattern of the cardholder's profile is analyzed. Secondly, the characteristic pattern of all the fraud and normal samples must be classified into clusters that share the common characteristics using many clustering Algorithms. Finally, this model helps to determine whether a real or fraud-related transaction is the current transaction based on the historical transaction using Hmm. The study enables to recognize which clustering algorithm integrated with Hmm helps to accurately predict the transaction status to prevent an act of fraud. In a bunch of transactions, genuine transactions are therefore never refused because they are fraud[19].

RB and KR (2021) produced a method for detecting the fraud of credit cards depending on Deep Learning. Also made a comparison between it and algorithms of ML such as SVM, K-nn and ANN to predict fraud in credit cards. And then have used the neural network, even if it is difficult to train the model suitable for the model of credit card fraud detection.

The model is best suited for CCF detection using Artificial Neural Network (ANN), which gives an accuracy of around 100 percent. It provides more exactness than unsupervised algorithms of learning. Data pre-processing, standardization, and under-sampling to overcome the problems faced by using an imbalanced dataset are carried out in this research[20].

Shaohui et al. (2021) proposed a model depending on the RF algorithm for detecting transaction fraud. The study results of the data from IEEE CIS fraud indicate that the method of this model is superior to the model benchmark, such as LR and SVM. In the end, the accuracy this model gave was 97.4%, while the score for the AUC ROC was 92.7%[21].

III. DATASET DESCRIPTION

In machine learning, datasets play a crucial role. As the efficiency of the model depends mainly on the type of data, it is working on. And because our study requires data in the field of credit card fraud, data from Kaggle[22] was used. It is not easy to form reliable data in this study. This dataset was generated from credit card transactions of European cardholders during two days of September 2013. Because the issue of confidentiality is an important matter that cannot be overlooked, it isn't easy to present and display all the essential characteristics and information of the data. Therefore, these datasets offered consist of numerical values; these are the result of the transformation of PCA. This dataset consists of 31 columns. As a result of the principle of confidentiality, the columns were given new labels. The first column is Time, and from the second column to column no.29, the labelling started from V1, V2, ..., V28, followed by the last two columns and labelled Amount and Class, respectively. Also, all the dataset values were presented as numerical values after they were converted to PCA values, except for the values of columns (Amount and Time). As for the last column, No. 31 (Class), its values were confined between (1 or 0), as these values indicate whether the transaction was genuine or fraudulent. If the value is 0, the transaction is considered original. If the value is 1, the transaction is deemed to be fraudulent. The total number of transactions is 284,807, including 492 scams.

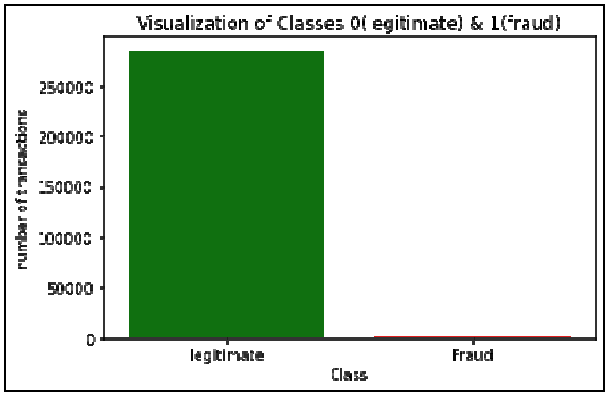

Figure.3. Dataset distribution

In Figure 3, we can see this dataset is very imbalanced, as the percentage of fraudulent transactions out of the total is only 0.173%, while the percentage of legal transactions is 99.827%. There are various techniques used to balance the dataset. In this research, we used Synthetic Minority Oversampling Technique (SMOTE).

IV. METHODOLOGY

In this paper, we proposed a CCF detection system using several ML techniques. ML classifiers LR, LDA, NB, and the boosting algorithm XGBoost have been implemented in Python two times. The first time was on an original dataset (before applying SMOTE), and the second time after applying SMOTE. Then, we presented their results. Finally, we compared these results with other papers results.

Our methodology requires going through several steps:

- The first step: bring and collect the dataset. The lack of the credit card datasets is one of the most significant difficulties the researchers face,besides the process of our implementation, we used the data set from the Kaggle website, it was a European cardholder dataset.
- The second step: preprocessing the collected dataset. We scaled the features Amount and Time, and then the resulting values were placed in two new columns for each feature, where the values ranged between 1 and -1. As for the Time column replaced to a normalizedtime, and the Amount returned to a normalizedamount. After that, we dropped the two primary columns, Amount and Time. Another pre-processing was SMOTE to balance the classes of the dataset. The SMOTE increased the minority class “class 1” to equal the majority class “class 0”, from 492 transactions to 284315 transactions.
- The third step: splitting the dataset into test and train datasets. We split the data by 0.3, meaning that it is 30% for testing and 70% for training. The random state was 42.
- The fourth step: choosing a model according to our dataset and the type of the task. We used LR, LDA, NB and XGBoost. We used all these classifiers with default parameters without change.
- The fifth step: evaluation of the performance of the models. We used confusion matrix, accuracy, precision, recall, f1 score and AUC.

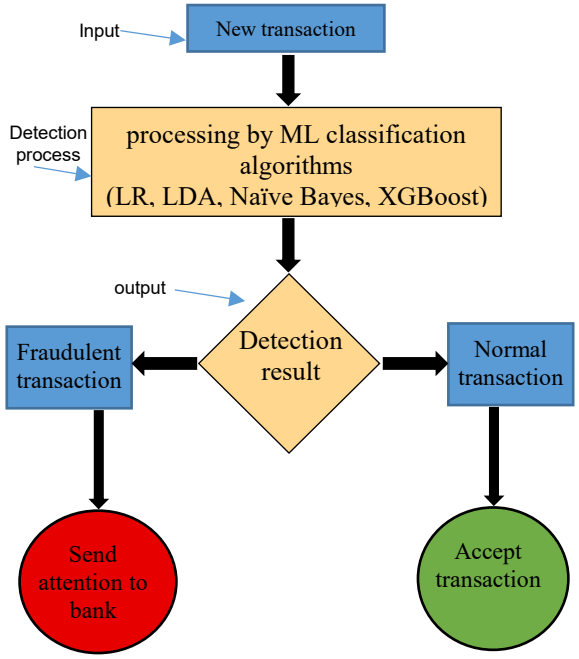

Figure.4. The proposed CCF detection system Architecture

Figure 4 illustrate the main critical stages of our proposed system. The detecting process is divided into many steps. When a new transaction occurs, the bank will store all information about the transaction in the bank dataset server. The transaction is then analyzed using ML algorithms, which identifies any fraud. If the transaction is fraudulent, the system will send attention to the bank to automatically block the card; Otherwise, the transaction will be accepted.

- LR: in classification work, LR is commonly used. LR used to forecast results based on a set of input variables. One of the classes is returned as a binary. This algorithm makes it simple to classify binary data as either 0 or 1[23].
- LDA is a technique for reducing the dimensionality of a problem and making predictions. LDA calculates the likelihood that new input is part of one of the existing classes based on Bayes' theorem. In classification problems, LDA should be used with a categorical output variable and binary or multi-class class support[24].
- NB: it is based on the Bayesian posterior probability approach[25]. It is perfect for the large dataset as it does not require iterative parameter approximation[26]. It is effective in both training and classification[27].
- XGBoost: In many situations, it is superior. An ANN (Artificial Neural Network) underpins the system. It's more efficient when dealing with a big dataset.

V. SIMULATION RESULTS

The dataset used is a high imbalance; in this case, the results will be not satisfactory because the model will not train accurately. We used SMOTE technique to balance the dataset. We evaluated the performance of each algorithm before and after applying the SMOTE. We used the following evaluation metrics to assess the algorithm's performance: Confusion Matrix, Accuracy, F1, Recall, Precision, and AUC.

The confusion matrix is one of the easiest and best methods used to evaluate performance. The use of a confusion matrix shows the number of classified data instances correctly. The table1 shows the confusion matrix details[28].

Table 1. Confusion matrix

Predicted class	Actual class	
	Positive(0)	Negative(1)
Positive(0)	True positive (TP)	False positive (FP)
Negative(1)	False negative (FN)	True negative (TN)

For the confusion matrix, the model is more accurate when the higher value of TP and TN. The values of all classifiers confusion matrix before and after SMOTE are shown in Figure 5, which explains the number of TP, TN, FN and FP for each classifier.

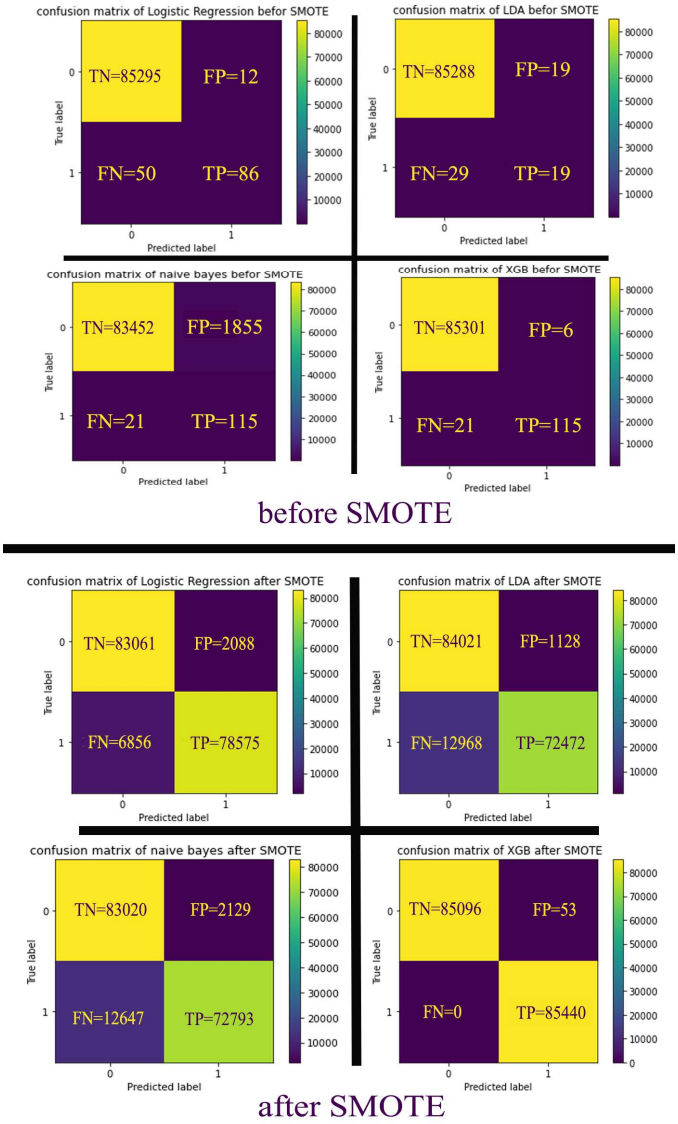

Figure 5. all classifiers confusion matrix

TP values = an actual class of the data that matches the predicted class of the data.
FP= the actual class of the data was 1, but the model predicted it to be 0.
FN= the actual value of the class was 0, but the model predicted it to be 1.
TN=the actual value was 1, and the model predicted it to be 1.

AUC (area under the ROC curve): it represents a model's classifying ability.

For the other performance metrics, we can calculate them by the following equations[28]:

$$\text{Accuracy} = (TP + TN)/ (TP+ FP+ TN+ FN) \quad (1)$$
$$\text{Precision} = TP/(TP+FP) \quad (2)$$
$$\text{Recall} = TP/(TP+FN) \quad (3)$$
$$F1 = 2*\text{precision} * \text{recall} / (\text{Precision} + \text{recall}) \quad (4)$$

The results of each classifier before SMOTE are listed in table 2.

Table 2. Classifiers result before SMOTE

Classifier	accuracy %	precision %	Recall%	F1%	AUC%
LR	99.926	87.755	78.676	81.679	81.611
LDA	99.944	84.921	84.559	10.921	89.327
NB	97.804	5.838	85	10	91.192
XGBoost	99.968	95.041	84.559	89.494	92.276

Because the dataset suffered from a high imbalance between its two classes, all classifiers presented high accuracy in table 2. That means these classifiers are trained and tested on the largest class of the dataset only. The largest class represents 99.827% of the dataset. So to get actual accuracy, we balanced the dataset by applying SMOTE. Then we re-implemented for all classifiers. The results of each classifier after SMOTE are listed in Table.3.

Table 3. Classifiers result after SMOTE

Classifier	accuracy %	precision %	Recall%	F1%	AUC%
LR	94.752	97.411	91.965	94.61	94.756
LDA	91.737	98.467	84.822	91.137	91.749
NB	91.338	97.158	85.198	90.786	91.349
XGBoost	99.969	99.938	100	99.969	99.969

After applying the SMOTE to the dataset, we noticed the best classifier performance was in the following order XGBoost, LR, LDA and NB. The accuracy rates from the best to the last were 99.969%, 94.752%, 91.737%, then 91.338%.

VI. DISCUSSION

The results that we obtained from all classifiers before applying the SMOTE Technique aren't satisfactory. They are not convincing because the dataset has a very high imbalance problem, as the percentage of fraud data is 0.173% of the total data set. That means that the models we used will be trained and tested only on the largest data set type (non-fraud class). Figure 5 shows the Confusion Matrix for all models, as the number of TN in each model before SMOTE is significantly greater than the rest. By seeing the results in Table 2, which presents the results of the classifiers before applying the SMOTE, we noted that the lowest accuracy value was 98%.

In contrast, other values such as precision, f1 and recall are weak compared to accuracy. This indicates that the model's training was poor.

After applying SMOTE that balances the two classes of the dataset by increasing the little class (fraud class) data, by seeing table 3, which presents the results of the classifiers after applying the SMOTE, we note the result for all classifiers were good. For LR, LDA and NB results, no significant differences can be observed except in the recall values of LDA and NB, which was significantly lower than the other metrics values. XGBoost gave the highest results among all models, where the values for accuracy, f1 and AUC were 99.969%, precision 99.938% and recall were 100%.

We compared the results of the best two classifiers in our work, XGBoost and LR, with the results of the best two classifiers in[29] and [30] by using accuracy, AUC and precision, as shown in table 4. With the same dataset.

Table 4. A comparison between the results of the best two classifiers in our work with other works

author	Classifier	accuracy	Precision	AUC
[29]	XGBoost	95.1%	88%	98%
[29]	Gradient boosting	0.947%	0.87%	0.92%
[30]	XGBoost	99.962%		
[30]	Random Forest	99.957%		
our paper	XGBoost	99.969%	99.938%	99.969%
our paper	LR	94.752%	97.411%	94.756%

A comparison results in table 4 showed that the XGBoost results of our work are higher than the results presented in [29] and [30], using the same dataset.

VII. CONCLUSION AND FUTURE WORKS

In this paper, we used the following ML classification algorithms: LR, LDA, NB and the boosting algorithm XGB on the credit card dataset and trained using this dataset to detect fraud. The dataset was very high imbalanced, as the percentage of fraud data from the total dataset is 0.173% only, so a balance was done for the dataset using the SMOTE technique. We split the data set after that by 30% for testing and 70% for training. Then we evaluated the performance Algorithms. The value of the results was good for most models, but the best performance was for the XGBoost model, accuracy was

99.969%, Precision 99.938%, recall 100%, F1 99.969% and AUC 99.969%.

The performance of all models was good after performing the balancing process for the dataset, as shown in table 3. But if the data set used was more natural and more significant, the performance presented would have increased much better.

In the future, to increase the performance, we need to get a larger and more real dataset from banks and also, we need to use more ML techniques, specifically more boosting algorithms. And also suggest using the fuzzy membership function.

REFERENCES

[1] B. Al Smadi and M. Min, "A Critical review of Credit Card Fraud Detection Techniques," *2020 11th IEEE Annu. Ubiquitous Comput. Electron. Mob. Commun. Conf. UEMCON 2020*, pp. 0732–0736, 2020, doi: 10.1109/UEMCON51285.2020.9298075.

[2] M. Puh and L. Brkić, "Detecting credit card fraud using selected machine learning algorithms," in *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2019 - Proceedings*, May 2019, pp. 1250–1255, doi: 10.23919/MIPRO.2019.8757212.

[3] A. Dal Pozzolo, "Adaptive Machine Learning for Credit Card Fraud Detection Declaration of Authorship," PhD Thesis, Department of Computer Science, Université Libre de Bruxelles, 2015.

[4] E. Duman and M. H. Ozcelik, "Detecting credit card fraud by genetic algorithm and scatter search," *Expert Syst. Appl.*, vol. 38, no. 10, pp. 13057–13063, Sep. 2011, doi: 10.1016/j.eswa.2011.04.110.

[5] A. O. Adewumi and A. A. Akinyelu, "A survey of machine-learning and nature-inspired based credit card fraud detection techniques," *Int. J. Syst. Assur. Eng. Manag.*, vol. 8, no. 2, pp. 937–953, Nov. 2017, doi: 10.1007/s13198-016-0551-y.

[6] K. Chaudhary, J. Yadav, and B. Mallick, "A review of Fraud Detection Techniques: Credit Card," in *International Journal of Computer Applications*, 2012, vol. 45, no. 1, pp. 39--44.

[7] The Nilson Report, "Nilson Report – Card Fraud Losses Reach $27.85 Billion." 2019, Accessed: Mar. 22, 2021. [Online]. Available: https://nilsonreport.com/mention/407/1link/.

[8] A. Salazar, G. Safont, and L. Vergara, "Semi-Supervised Learning for Imbalanced Classification of Credit Card Transaction," *Proc. Int. Jt. Conf. Neural Networks*, vol. 2018-July, pp. 1–7, 2018, doi: 10.1109/IJCNN.2018.8489755.

[9] H. F. Dheyab, O. N. Ucan, M. Khalaf, and A. H. Mohammed, "Implementation a Various Types of Machine Learning Approaches for Biomedical Datasets based on Sickle Cell Disorder," in *4th International Symposium on Multidisciplinary Studies and Innovative Technologies, ISMSIT 2020 - Proceedings*, Oct. 2020, doi: 10.1109/ISMSIT50672.2020.9254994.

[10] A. Alzahrani, K. M Ali Alheeti, S. Salah Thabit, D. Al_Dosary, and M. Shaban Al-Ani, "Intelligent Mobile Coronavirus Recognition Centre Based on IEEE 802.15.4," *Int. J. Interact. Mob. Technol.*, vol. 15, no. 16, p. 4, Aug. 2021, doi: 10.3991/ijim.v15i16.24193.

[11] K. M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "An intrusion detection system against malicious attacks on the communication network of driverless cars," *2015 12th Annu. IEEE Consum. Commun. Netw. Conf. CCNC 2015*, pp. 916–921, Jul. 2015, doi: 10.1109/CCNC.2015.7158098.

[12] N. Abd, K. M. A. Alheeti, and S. S. Al-Rawi, "Intelligent Intrusion Detection System in Internal Communication Systems for Driverless Cars," *Webology*, vol. 17, no. 2, pp. 376–393, 2020, doi: 10.14704/WEB/V17I2/WEB17039.

[13] J. Gao, Z. Zhou, J. Ai, B. Xia, and S. Coggeshall, "Predicting Credit Card Transaction Fraud Using Machine Learning Algorithms," *J. Intell. Learn. Syst. Appl.*, vol. 11, no. 03, pp. 33–63, Aug. 2019, doi: 10.4236/jilsa.2019.113003.

[14] A. Roy, J. Sun, R. Mahoney, L. Alonzi, S. Adams, and P. Beling, "Deep learning detecting fraud in credit card transactions," *2018 Syst. Inf. Eng. Des. Symp. SIEDS 2018*, pp. 129–134, 2018, doi: 10.1109/SIEDS.2018.8374722.

[15] F. Carcillo, Y. A. Le Borgne, O. Caelen, and G. Bontempi, "Streaming active learning strategies for real-life credit card fraud detection: assessment and visualization," *Int. J. Data Sci. Anal.*, vol. 5, no. 4, pp. 285–300, 2018, doi: 10.1007/s41060-018-0116-z.

[16] C. Sudha and D. Akila, "Credit card fraud detection system based on operational transaction features using SVM and random forest classifiers," in *Proceedings of 2nd International Conference on Computation, Automation and Knowledge Management, ICCAKM 2021*, Jan. 2021, pp. 133–138, doi: 10.1109/ICCAKM50778.2021.9357709.

[17] M. R. Dileep, A. V Navaneeth, and M. Abhishek, "A Novel Approach for Credit Card Fraud Detection using Decision Tree and Random Forest Algorithms," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, Feb. 2021, pp. 1025–1028, doi: 10.1109/ICICV50876.2021.9388431.

[18] T. C. Tran and T. K. Dang, "Machine Learning for Prediction of Imbalanced Data: Credit Fraud Detection," in *Proceedings of the 2021 15th International Conference on Ubiquitous Information Management and Communication, IMCOM 2021*, Jan. 2021, pp. 1–7, doi: 10.1109/IMCOM51814.2021.9377352.

[19] K. Janvitha, C. R. S. Vasavi, A. Sruthi, K. Praharshitha, and D. K. Anguraj, "Survey on Detection of Credit Card Frauds using Hmm and various Clustering Approaches," in *Proceedings of the 6th International Conference on Inventive Computation Technologies, ICICT 2021*, Jan. 2021, pp. 101–107, doi: 10.1109/ICICT50816.2021.9358773.

[20] A. RB and S. K. KR, "Credit Card Fraud Detection Using Artificial Neural Network," *Glob. Transitions Proc.*, Jan. 2021, doi: 10.1016/j.gltp.2021.01.006.

[21] D. Shaohui, G. W. Qiu, H. Mai, and H. Yu, "Customer Transaction Fraud Detection Using Random Forest," in *2021 IEEE International Conference on Consumer Electronics and Computer Engineering, ICCECE 2021*, Jan. 2021, pp. 144–147, doi: 10.1109/ICCECE51280.2021.9342259.

[22] A. D. Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Calibrating probability with undersampling for unbalanced classification," in *Proceedings - 2015 IEEE Symposium Series on Computational Intelligence, SSCI 2015*, 2015, pp. 159–166, doi: 10.1109/SSCI.2015.33.

[23] D. Tanouz, R. R. Subramanian, D. Eswar, G. V. P. Reddy, A. R. Kumar, and C. H. V. N. M. Praneeth, "Credit card fraud detection using machine learning," in *Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021*, May 2021, pp. 967–972, doi: 10.1109/ICICCS51141.2021.9432308.

[24] T. Saranya, S. Sridevi, C. Deisy, T. D. Chung, and M. K. A. A. Khan, "Performance Analysis of Machine Learning Algorithms in Intrusion Detection System: A Review," in *Procedia Computer Science*, Jan. 2020, vol. 171, pp. 1251–1260, doi: 10.1016/j.procs.2020.04.133.

[25] M. A. Hambali, Y. K. Saheed, T. O. Oladele, and M. D. Gbolagade, "Adaboost Ensemble Algorithms for Breast Cancer Classification," *J. Adv. Comput. Res. Q.*, vol. 10, no. 2, pp. 1–10, May 2019.

[26] K. Suresh and R. Dillibabu, "Designing a Machine Learning Based Software Risk Assessment Model Using Naïve Bayes Algorithm," *TAGA J.*, vol. 14, pp. 3141–3147, 2018.

[27] I. D. Dinov, "Probabilistic Learning: Classification Using Naive Bayes," in *Data Science and Predictive Analytics*, Springer, Cham, 2018, pp. 289–305.

[28] M. Hossin, Mohammad Sulaiman, "A review on evaluation metrics for data classification evaluations," *Int. J. Data Min. \& Knowl. Manag. Process*, vol. 5, 2015.

[29] H. Feng, "Ensemble learning in credit card fraud detection using boosting methods," *Proc. - 2021 2nd Int. Conf. Comput. Data Sci. CDS 2021*, pp. 7–11, Jan. 2021, doi: 10.1109/CDS52072.2021.00009.

[30] V. Jain, M. Agrawal, and A. Kumar, "Performance Analysis of Machine Learning Algorithms in Credit Cards Fraud Detection," *ICRITO 2020 - IEEE 8th Int. Conf. Reliab. Infocom Technol. Optim. (Trends Futur. Dir.*, pp. 86–88, 2020, doi: 10.1109/ICRITO48877.2020.9197762.