

An intelligent approach to detect and predict online fraud transaction using XGBoost algorithm

Bala Santhosh Kumar, Pasupula Praveen Yadav, Mogathala Raghavendra Reddy

Department of Computer Science and Engineering, G. Pulla Reddy Engineering College, Kurnool, India

Article Info

Article history:

Received Jan 13, 2024

Revised Apr 20, 2024

Accepted May 7, 2024

Keywords:

Credit card

Extreme gradient boosting

Fraud

Machine learning

Prediction

Transactions

ABSTRACT

The most popular payment method in recent years is the credit card. Due to the E-commerce industry's explosive growth, the usage of credit cards for online purchases have been greatly increased as a result frauds has increased. Banks have been facing challenges to detect the credit card system fraud in recent years. Credit card fraud happens when the card was stolen for any unauthorized purposes or if the fraudster utilizes the credit card information for his own use. In order to prevent credit card fraud, it is essential to build detection measures. While detecting credit card theft with machine learning (ML), the features of credit card frauds play an important and they must be carefully selected. A fraud detection algorithm must be created in order to correctly locate and stop fraudulent activity as technology advances along with the amount of fraud cases. ML methods are essential for identifying fraudulent transactions. The implementation of fraud detection models is particularly difficult because of the sensitive nature of the data, the unbalanced class distributions, and the lack of data. In this work, an intelligent approach to detect and predict online fraud transaction using extreme gradient boosting (XGBoost) algorithm is described. The XGBoost model predicts whether a transaction is fraud or not. This model will achieve better performance interarm of recall, precision, accuracy and F1-score for credit card fraud detection.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Bala Santhosh Kumar

Department of Computer Science and Engineering, G. Pulla Reddy Engineering College

Kurnool, Andhra Pradesh, India

Email: balasanthoshkumar3@gmail.com

1. INTRODUCTION

Online shopping is becoming more and more popular as mobile devices become more widely used. Criminals have access to risky technologies like Trojan and false base-stations, the internet environment is open, and online purchasing platforms include bugs. All of factors contribute to a significant increase in cases of credit card frauds. Criminals can use a cardholder credit card to make transactions when they steal or cheats the cardholder's credit card details [1].

Currently, one of the most popular methods of payment is mobile. Every day, the online trading platform processes thousands of transactions. A few criminals have the potential to commit crimes thanks to the widespread use of network transactions. The risk of theft is happened when personal property is present in a complex network environment, consumer interests and has a negative impact on the growth of the network economy. In order to address the issue of network transaction fraud, transaction fraud detection is one of the most important technologies [2].

For certain online payment options, all that is needed is the card number, card verification value (CVV) and expiration date; yet, in some cases, this data can lost without our understanding. When fraudsters

use phishing techniques to obtain personal information, they don't know that our information has been compromised when they conduct online transactions. Some people who have been impacted might not even be aware that their credit card information has been compromised because all he needs to conduct fraud is the card information for a few small purchases. It is essential to keep the card details confidential. However, there are situations when they have no control over the information. Information may be leaked as a result of phishing sites, and sometimes the cards themselves may be lost or stolen [3].

Credit cards and online payments have made by gathering credit card information from users and utilizing it for illegal transactions, fraudsters can take advantage of consumers more easily. As a result, there are a significant number of fraudulent transactions made every day. These fraudulent transactions are being searched out by banks and e-commerce companies in an effort to prevent them from occurring again. The technique of analysing cardholder transaction behaviour to determine if a transaction is genuine is known as fraud detection [4].

Abuse of a profit-making organization's system is referred to as fraud, even if it is not always associated with specific legal issues. Fraud is an action that occurs everywhere when someone or anything is deceived into giving up their financial benefits. The process of recognising fraudulent transactions and dividing them into two classes: both lawful and fake transactions are included in the identification of credit card fraud. Traditional card-related frauds, online frauds, and other types of fraud are the three basic categories into which these types of fraud may be classified. Whenever the top-level management committed fraud, it is also known as internal fraud or management fraud. This fraud performed by people exterior of the organization is referred to as customer fraud or external fraud. Because fraud detection is a component of extensive fraud prevention, it automates and reduces the human screening process steps [5].

Fraud is characterised as criminal or wrongful deception used to produce financial or personal benefit. The illegal use of credit card information for both physical or digital manner purchases is referred to as credit card fraud. Since cardholders often submit their card number, expiration date, and card verification number over the phone or website, fraud can occur during digital transactions. Credit card fraud is the illegal utilisation of credit card information to complete a transaction [6].

When doing a purchase in person, a credit card is required, but a digital transaction is carried out over the phone or the Internet and requires the collection of certain types of information, including the verification number, expiration date, and card's number. The main difficulty in advancing e-commerce is an increase of fraud cases in the transaction, which also result in significant economic losses. So, while doing transactions online, fraud detection is essential [7].

Credit cards have improved the convenience and accessibility of online transactions. A significant amount of capital is lost each year due to fraud transactions, and this loss may get higher in the upcoming year. In addition, a manual process to an algorithm with competence for automatically identifying fraud might make up the system for its detection. All previous types of fraud transactions that have happened can be represented as the basis for the automated operation. Various fraud investigators evaluate the manual technique by examining each transaction separately and producing binary feedback for each transaction [8]. Fraudulent transactions should be quickly and accurately identified by an effective fraud detection system. The ability of genuine consumers to use the payments system must not be compromised, even while it is essential to stop bad actors from carrying out fraudulent transactions [9]. Researchers are trying to come up with a way to identify and avoid frauds by the significant loss that fraudulent activities are causing. Several approaches have previously been developed and examined.

For companies, uses of machine learning (ML) and artificial intelligence (AI) in the finance sector can result in excellent results including increased productivity, decreased operating costs, and higher satisfaction with customers. In order to find credit card fraud, several ML-based methods have been created [10]. AI systems may learn and automatically improve based on experience due to ML, and is an application of AI. Computers may learn from previous performance (data) using ML, a type of AI, and increase their capacity for predicting without explicit programming [11].

The main objective of ML is to create computer programs that can access data and utilise it to learn for themselves. Among the hottest topics of this year is ML, which is a subset of AI. A growing number of businesses are looking to invest in ML to enhance their services [12]. To enable the computer to carry out tasks without hard coding, ML combines a number of computer techniques with statistical modelling. The "training data" would be used to train the generated model. From the experience information that has been stored, predictions may be made or actions can be taken [13].

The extremely skewed structure of credit card fraud datasets makes it difficult for existing models for credit card fraud detection to overcome their low detection accuracy. In order to effectively identify credit card fraud, it is crucial to create ML models that have an excellent score for accuracy [14]. To obtain better accuracy, an intelligent approach to detect and predict online fraud transaction using extreme gradient boosting (XGBoost) algorithm is presented. The main objective is to detect whether the transaction is

fraudulent or not. The novel contribution of this work is achieving accurate results for credit card fraud prediction and detection.

The long short-term memory (LSTM) is used as a base learner in Adaptive boost (AdaBoost) technique to obtain an ensemble classifier. In this analysis, publicly available real world credit card dataset is used to validate the performance. The performance of this approach is compared with multi-layer perceptron (MLP), support vector machine (SVM), decision tree (DT) and traditional LSTM and AdaBoost. The results showed that this ensemble classifier outperformed other classifiers in terms of sensitivity and specificity [15].

A wide range of deep learning and ML methods are used to identify credit card fraud. random forest, Naive Bayes, K-nearest neighbour (KNN), logistic regression, and sequential convolutional neural network (CNN) are just a few of the approaches utilized to train the abnormal and additional transactional features. The model's accuracy is evaluated using publicly accessible data. The comparative study showed that when compared to other approaches, the KNN algorithm gives better results. Compared to the sequential pattern of previously detected data on fraud detection, this analysis indicates the differences between online and offline transactions [16].

In real-world transactions, this system focuses on four common fraud occasions. A number of ML models are used to address each scam with the best method being determined through evaluations. This evaluation provides extensive guidance for selecting the optimal algorithm with relation to the different fraud types, and to demonstrate the evaluation, they offer an acceptable performance measure. The real-time credit card fraud detection is a significant critical topic that they focus on in this project. To evaluate that a particular transaction is legitimate or fraudulent, with integrated ML models and an application programming interface (API) module, they conduct predictive analytics. They also evaluate a state-of-the-art strategy that successfully addresses the skewed distribution of data. A secret disclosure agreement manages the source of the data utilised in the experiments; this was sent by a financial institution [17].

Several ML techniques, including random forest, SVM, and KNN, as well as deep learning techniques, including restricted boltzmann machines (RBM), CNN, autoencoders, and deep belief networks (DBN), are all being evaluated in this analysis. The German, Australian, and European (EU) databases will all be utilised. The three measures for evaluation would be Matthew's correlation coefficient (MCC), area under the ROC curve (AUC), and cost of failure [18].

Considering the concept of assessing previous customer transaction data and extracting behavioural patterns, the main objective of the analysis is to develop and generate a unique fraud detection algorithm for streaming transaction data. Whereby cardholders are placed into several categories according to the size of their transactions. Then, in order to extract the distinct behavioural patterns of the groupings, the sliding window approach is utilised to aggregate the transactions done by cards from various groups. The groupings are later trained separately with various classifiers. Then, one of the best techniques for predicting frauds can be selected based on the classifier with the higher rating score [19].

A 3D convolution network is provided with learnt tensor representations on top of the spatial-temporal attention is utilized. With 3D convolution and detection networks, the attentional weights are jointly learnt from beginning to end. Then, using the dataset of real-world card transactions, they do extensive experiments. In terms of both AUC and precision-recall curves, spatial-temporal attention-based graph network (STAGN) performs better than other state-of-the-art baselines, according to the results. Additionally, they conduct empirical research on the proposed approach for fraud detection and knowledge discovery with domain experts; these results show its excellence in locating suspicious transactions, mining temporal, spatial fraud hotspots, and recognizing fraud patterns. It is also shown that this method is beneficial in other user behavior-based activities [20].

The aggregation of the transactions in each group is explained using a window-sliding technique. Utilize the aggregating transactions and previous transactions of the cardholder, then, for each cardholder, they identify a wide range of behaviour patterns. Then, developing on all of the behaviour patterns, for each group, they train a set of classifiers. The classifier set is then utilized to determine if a new transaction is fraudulent and to detect online fraud, the detection procedure integrates a feedback mechanism to handle the concept drift issue. The experiment results demonstrate the advantages of this approach over other methods [21].

The objective is to identify all fraudulent transactions while reducing incorrect fraud categories. An example of a classification sample is the detection of credit card fraud. In this process, they have focused on data analysis, data pre-processing, and the use of various anomaly detection techniques, on the principal component analysis (PCA) changed credit card transaction data, using algorithms like the local outlier factor and isolation forest. Even while the algorithm achieves above 95% accuracy, it only has a 28% precision when only a tenth of the data set is used [22].

Processing alerts generated by a fraud detection system is allowed researchers to evaluate a group of deep neural networks capacity to identify false positives. It is given and explained the way every neural network setting is performed. The most optimal option allowed for 35.16% less alerts while still capturing 91.79% of all fraud instances. As a result of the neural network's classification of false positive alerts as

such, the cost of human inspection would significantly decrease as a result of the obtained alert reduction rate [23]. A variational automated encoding (VAE) oversampling approach is used in conjunction with classic deep learning methods. In a data set with imbalances, a large number of different minority group cases are generated using the VAE technique, and these instances are then utilised to train the classification network. To examine the proposed approach, transactions done by European cardholders over two days in September 2013 are included in a credit card fraud dataset. On measures like precision, F-measure, accuracy, and specificity, the VAE model performs well after being given the expanded dataset for training. The results of this experiment indicate that imbalanced classification problems can be successfully addressed by the VAE-based oversampling approach [24].

A new approach is described to develop individual behaviours that can improve low-frequency user behaviour by transferring the behaviour of the current transaction group and transaction state. In order to create the user's own transaction behaviour benchmark, they first consider the user's only previous transactions and the best method to determining risk thresholds. A multi-behavior detection model based on new transaction behaviour can be proposed on this basis. The Naive Bayes model is used to compute the chance that the current transaction is fraudulent and then to decide, depending on the outcome of each behaviour. Experiments show that the approach proposed in this study can benefit low-frequency users, who can detect fraud transactions with high accuracy and make fraud transactions when evaluating normal transactions [25].

To express the logical relation of transaction record attribute, a logical graph of behavior profiles (LGBP), a complete order-based model is used. They can determine the possibility of a path-based transition from one attribute to another using the LGBP and users' transaction records. In order to describe a user's wide range of transaction behaviours, they develop an information entropy-based diversity coefficient simultaneously. They also create a state transition probability matrix to record the temporal characteristics of a user's transactions. In order to determine whether an incoming transaction is fraudulent or not, they can create a BP for each user. The tests using real data sets show that described method is outperforms three other state-of-the-art ones [26].

The organization of the work is organized as follows: The literature survey is discussed after the introduction. The section 2 describes the proposed methodology. The section 3 evaluates the results and discussion. The section 4 presents the conclusion.

2. AN INTELLIGENT APPROACH TO DETECT AND PREDICT ONLINE FRAUD TRANSACTION

In this section, an intelligent approach to detect and predict online fraud transaction using XGBoost algorithm is presented. The block diagram of presented approach is shown in Figure 1. The dataset is collected from Kaggle and is credit card fraud detection. transactions made in September 2013 using credit cards by European cardholders are included in the dataset. They have 492 frauds out of 284,807 transactions in the dataset, which shows transactions that happened within the past two days. Since frauds make up 0.172% of all transactions, the dataset is extremely unbalanced. Only numerical input variables from a PCA transformation are present. They simply cannot offer the original features and additional context for the information due to privacy issues. Only the features "Time" and "Amount" have not been changed by PCA. The primary components obtained using PCA are features V1, V2, ...V28. The variable "Time" contains the seconds that passed between each transaction and the dataset's initial transaction. The "Amount" feature refers to the transaction amount and may be used for example-dependent, cost-sensitive learning. Feature "Class," the response variable, if fraud has occurred, it has a value of 1, else it has a value of 0.

To extract, transform, normalise, and scale new features that will be utilised in the ML algorithm process, preprocessing is performed. Since data loading and integration are handled with at the dataset stage. They concentrated on memory optimisation of the dataset and removal of highly correlated columns. A model's generalisation and interpretability can both be enhanced by removing collinear features. These collinear characteristics are eliminated if the correlation coefficient increases beyond the removed. To turn unprocessed data into high-quality data, pre-processing is performed. PCA, which has the properties of extraction, transformation, normalisation, and scaling, is used for preprocessing in this analysis. Testing and training make advantage of frequency encoding. Since label encoding and one hot encoding are unsuitable for nominal categorical data, frequency encoding is the best option for this data.

Exploratory data analysis (EDA) is required to analyse the data and, if necessary, execute feature modification. Analyse the data to see whether it is skewed in any way. Making exploratory process into data to search for patterns is an important step in EDA, graphical representations and summary statistics are can be used to check assumptions, discover anomalies, and test hypotheses. Understanding the information first and attempting to gather as many insights from it as possible are effective practises. Before getting dirty with the data, the EDA has to make sense of the information that is currently accessible.

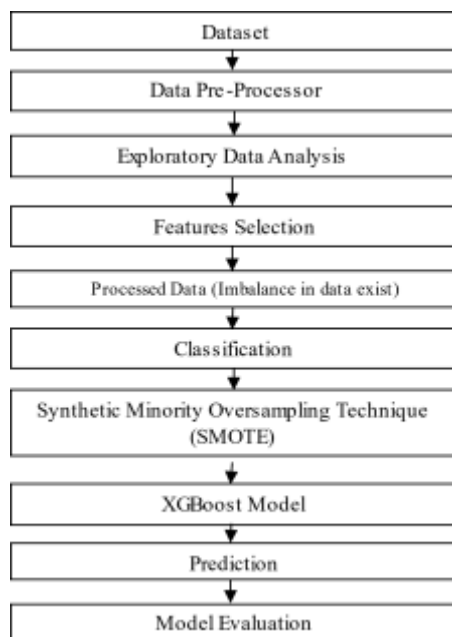


Figure 1. Block diagram of an intelligent approach to detect and predict online fraud transaction using XGBoost algorithm

When there are many characteristics, choosing important and relevant ones is essential for the efficient detection of credit card fraud. A fundamental method called feature selection chooses the variables in a dataset that are most important. Reducing overfitting, increasing accuracy, and reducing training time may all be achieved by carefully selecting the right characteristics and eliminating those that are less important.

To address the issue of the uneven class system, two different approaches are used. The primary approach uses a pre-processing method for the data to manage the classes, such as under-sampling and over-sampling. On generating new information, the second strategy is based. Data points from the main class are undersampled to ensure that both classes are equally represented. In order to enhance the amount of data points for the minor class, oversampling is used. This system basically classifies the transaction in only two states that are either fraud or legitimate transactions.

Synthetic minority oversampling technique (SMOTE) will be a method of oversampling used to increase the size and balance of a dataset by carefully producing data points from the minority class. Using a random point from the minority class, this technique performs, through first defining a restricted area inside the minority class, data points may then be produced. They might be sure that these extra instances won't compromised the dataset's integrity in this way. To enhance its size, inside a constrained region, SMOTE synthetically generates new data points in the minor class.

Recently, the technique XGBoost has dominated Kaggle contests and applied ML challenges using structured or tabular data. Speed and effectiveness were taken into consideration when developing the gradient boosted DT implementation known as XGBoost. The foundation of the XGBoost algorithm is gradient-boosted DTs. Great generalization, high expandability, and speedy processing speed are all advantages of the XGBoost model. The XGBoost algorithm is made up of a number of basis classifiers. The accessible base classifiers include DTs, KNN, SVM, logistic regression, and other methods. With the help of these algorithms, it classified the data as fraud or not. As it is based on a DT, it can give us pretty good accuracy and also efficiency. This algorithm has some key features which are optimal results and high speed. The XG boost module predicts the frauds in a transaction. The system can provide consumers with an accurate prediction of network transaction fraud probability. In the real world, the detection system may be integrated directly into the online transaction interface and predict the transaction before the user pays, this allowing for preventive detection of fraudulent behaviour.

A technique that may be used to evaluate categorization performance is the confusion matrix. False positive and false negative (FP and FN) represent the number of positive and negative classes that are incorrectly categorized, respectively. True positive (TP) and true negative (TN) represent the number of positive and negative classes that are correctly classified. Performance measures including accuracy, precision, recall, and F-measure have been chosen based on the performance criteria and the confusion matrix.

3. RESULT ANALYSIS

In this analysis, an intelligent approach to detect and predict online fraud transaction using XGBoost algorithm is presented. The provided technique’s effectiveness is evaluated interms of precision, accuracy, F1-score, and recall. Accuracy: the percentage of instances that are correctly categorized is called accuracy. One of the most used performance measures for categorization is this one. Precision: precision is the proportion of positive cases that are actually categorized as positive or fraudulent. This recall is a measure that measures the proportion of truly accurate positive predictions produced out of all possible positive predictions. The ratio of true positives to both false positives and false negatives is used to determine recall. F1-score: the F1-score is computed by averaging precision and recall over all samples. As a result, both false positives and false negatives are considered in this score. The Table 1 shows the performance evaluation. The XGBoost algorithm has obtained better performance than DT algorithm. The Figure 2 shows the recall and precision comparison graphs. The Figure 2(a) demonstrates the recall performance and Figure 2(b) demonstrates the precision comparison.

Table 1. Performance metrics evaluation

Metrics/ methods	DT algorithm	XGBoost algorithm
Precision (%)	92	97.2
Recall (%)	88	96.8
Accuracy (%)	90	97
F1-score (%)	91.2	97.4

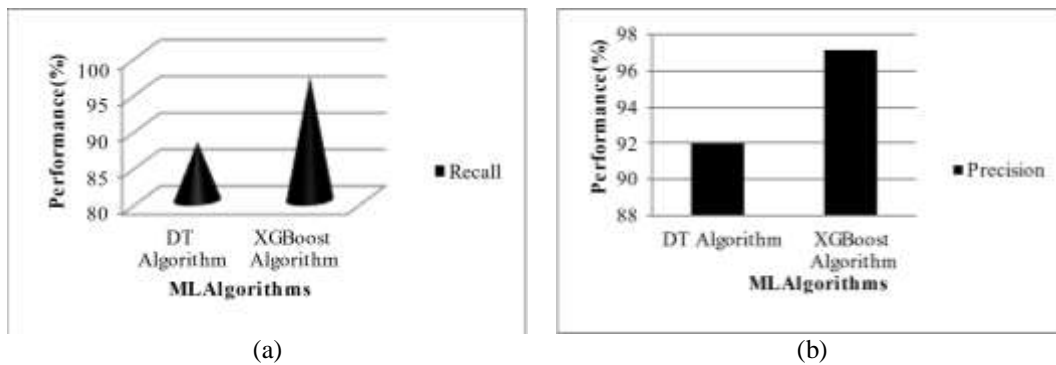


Figure 2. Performance comparison (a) recall and (b) precision

The Figure 3 shows the accuracy and F1-score comparison graphs. The Figure 3(a) demonstrates accuracy and Figure 3(b) shows F1-score performance comparison. Compared to DT algorithm, XGBoost has higher accuracy for credit card fraud detection. The XGBoost has high F1-score than DT algorithm. From the results, it is clear that, the XGBoost has higher precision, accuracy, recall and F1-score than earlier algorithms. Therefore, this approach will be useful for real time fraud detection and prediction.

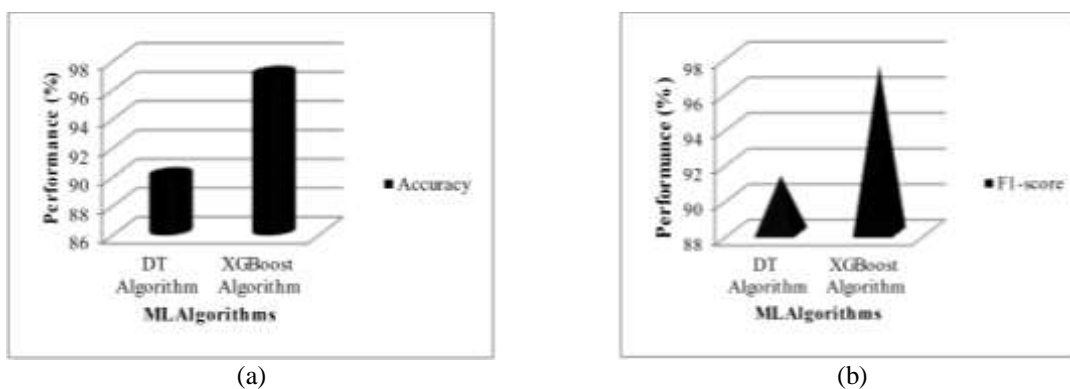


Figure 3. Performance evaluation (a) accuracy and (b) F1-score

4. CONCLUSION

Theft of credit cards has significantly developed in recent years. One of the primary objectives for increasing the level of risk management for merchants in an automated and effective manner is the development of an accurate and easy to use credit card risk monitoring system. Hence to solve these issues, an intelligent approach to detect and predict online fraud transaction using XGBoost algorithm is presented. This analysis primary goal is to develop algorithms that produce suitable results, and can be adopted by credit card businesses for more precise real-time fraud detection. The credit card fraud detection dataset from Kaggle is utilized in this method. New features are extracted, transformed, normalised, and scaled using pre-processing. EDA is performed to analyze the data also performed feature transformation. SMOTE, this method is used to deal with the imbalance in the data issue. The fraud transactions are predicted using the XGBoost algorithm. Accuracy, F1-score, precision, and recall are used to determine that the presented method performed. The XGBoost has obtained higher F1-score, accuracy, precision and accurate recall compared to earlier methods. Hence this approach will be useful for fraud transaction prediction in real time with better accuracy. Design and implementation of credit card fraud detection and prevention using hybrid ML will be implemented as a future work.





REFERENCES

- [1] M. Joitson, P. Prasad, R. Joseph, and B. Jayakrishnan, "Credit card fraud detection using machine learning," *International Journal of Engineering Research & Technology (IJERT)*, vol. 11, no. 1, pp. 861–864, 2023, doi: 10.17577/IJERT2K23-230.
- [2] A. Batool and Y.-C. Byun, "An ensemble architecture based on deep learning model for click fraud detection in pay-per-click advertisement campaign," *IEEE Access*, vol. 10, pp. 113410–113426, 2022, doi: 10.1109/ACCESS.2022.3211528.
- [3] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms," *IEEE Access*, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.
- [4] H. Wang, W. Wang, Y. Liu, and B. Alidaee, "Integrating machine learning algorithms with quantum annealing solvers for online fraud detection," *IEEE Access*, vol. 10, pp. 75908–75917, 2022, doi: 10.1109/ACCESS.2022.3190897.
- [5] A. A. Basori and N. H. M. Ariffin, "The adoption factors of two-factors authentication in blockchain technology for banking and financial institutions," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 26, no. 3, pp. 1758–1764, Jun. 2022, doi: 10.11591/ijeecs.v26.i3.pp1758-1764.
- [6] S. K. Hashemi, S. L. Mirtaheri, and S. Greco, "Fraud detection in banking data by machine learning techniques," *IEEE Access*, vol. 11, pp. 3034–3043, 2023, doi: 10.1109/ACCESS.2022.3232287.
- [7] Y. Ding, W. Kang, J. Feng, B. Peng, and A. Yang, "Credit card fraud detection based on improved variational autoencoder generative adversarial network," *IEEE Access*, vol. 11, pp. 83680–83691, 2023, doi: 10.1109/ACCESS.2023.3302339.
- [8] I. D. Mienye and Y. Sun, "A deep learning ensemble with data resampling for credit card fraud detection," *IEEE Access*, vol. 11, pp. 30628–30638, 2023, doi: 10.1109/ACCESS.2023.3262020.
- [9] R. Cao, G. Liu, Y. Xie, and C. Jiang, "Two-level attention model of representation learning for fraud detection," *IEEE Transactions on Computational Social Systems*, vol. 8, no. 6, pp. 1291–1301, Dec. 2021, doi: 10.1109/TCSS.2021.3074175.
- [10] E. Ileberi, Y. Sun, and Z. Wang, "Performance evaluation of machine learning methods for credit card fraud detection using SMOTE and AdaBoost," *IEEE Access*, vol. 9, pp. 165286–165294, 2021, doi: 10.1109/ACCESS.2021.3134330.
- [11] M. Thirunavukkarasu, A. Nimisha, and A. Jyothsna, "Credit card fraud detection using machine learning," *International Journal of Computer Science and Mobile Computing*, vol. 10, no. 4, pp. 71–79, Apr. 2021, doi: 10.47760/ijcsmc.2021.v10i04.011.
- [12] B. Kasasbeh, B. Aldabaybah, and H. Ahmad, "Multilayer perceptron artificial neural networks-based model for credit card fraud detection," *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, vol. 26, no. 1, pp. 362–373, Apr. 2022, doi: 10.11591/ijeecs.v26.i1.pp362-373.
- [13] E. Ileberi, Y. Sun, and Z. Wang, "A machine learning based credit card fraud detection using the GA algorithm for feature selection," *Journal of Big Data*, vol. 9, no. 1, p. 24, Dec. 2022, doi: 10.1186/s40537-022-00573-8.
- [14] V. Viswanatha, A. Ramachandra, V. Deeksha, and R. Ranjitha, "Online fraud detection using machine learning approach," *International Journal of Engineering and Management Research*, vol. 13, no. 4, pp. 45–57, 2023, doi: 10.31033/ijemr.13.4.6.
- [15] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, "A neural network ensemble with feature engineering for improved credit card fraud detection," *IEEE Access*, vol. 10, pp. 16400–16407, 2022, doi: 10.1109/ACCESS.2022.3148298.
- [16] A. Mehbodniya *et al.*, "Financial fraud detection in healthcare using machine learning and deep learning techniques," *Security and Communication Networks*, vol. 2021, pp. 1–8, Sep. 2021, doi: 10.1155/2021/9293877.
- [17] A. Thennakoon, C. Bhagyani, S. Premadasa, S. Mihiranga, and N. Kuruwitaarachchi, "Real-time credit card fraud detection using machine learning," in *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Jan. 2019, pp. 488–493, doi: 10.1109/CONFLUENCE.2019.8776942.
- [18] P. Raghavan and N. El Gayar, "Fraud detection using machine learning and deep learning," in *Proceedings of 2019 International Conference on Computational Intelligence and Knowledge Economy, ICCIKE 2019*, 2019, pp. 334–339, doi: 10.1109/ICCIKE47802.2019.9004231.
- [19] V. N. Dornadula and S. Geetha, "Credit card fraud detection using machine learning algorithms," *Procedia Computer Science*, vol. 165, pp. 631–641, 2019, doi: 10.1016/j.procs.2020.01.057.
- [20] D. Cheng, X. Wang, Y. Zhang, and L. Zhang, "Graph neural network for fraud detection via spatial-temporal attention," *IEEE Transactions on Knowledge and Data Engineering*, vol. 34, no. 8, pp. 3800–3813, Aug. 2022, doi: 10.1109/TKDE.2020.3025588.
- [21] C. Jiang, J. Song, G. Liu, L. Zheng, and W. Luan, "Credit card fraud detection: a novel approach using aggregation strategy and feedback mechanism," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3637–3647, Oct. 2018, doi: 10.1109/JIOT.2018.2816007.
- [22] S P Maniraj, A. Saini, S. Ahmed, and A. D. Sarkar, "Credit card fraud detection using machine learning and data science," *International Journal of Engineering Research and*, vol. 08, no. 09, Sep. 2019, doi: 10.17577/IJERTV8IS090031.
- [23] R. S. M. Carrasco and M. A. Sicilia-Urban, "Evaluation of deep neural networks for reduction of credit card fraud alerts," *IEEE Access*, vol. 8, pp. 186421–186432, 2020, doi: 10.1109/ACCESS.2020.3026222.





- [24] H. Tingfei, C. Guangquan, and H. Kuihua, "Using variational auto encoding in credit card fraud detection," *IEEE Access*, vol. 8, pp. 149841–149853, 2020, doi: 10.1109/ACCESS.2020.3015600.
- [25] Z. Zhang, L. Chen, Q. Liu, and P. Wang, "A fraud detection method for low-frequency transaction," *IEEE Access*, vol. 8, pp. 25210–25220, 2020, doi: 10.1109/ACCESS.2020.2970614.
- [26] L. Zheng, G. Liu, C. Yan, and C. Jiang, "Transaction fraud detection based on total order relation and behavior diversity," *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 796–806, Sep. 2018, doi: 10.1109/TCSS.2018.2856910.

BIOGRAPHIES OF AUTHORS







Bala Santhosh Kumar     completed B.Tech. at RGM College of Engineering and Ph.D. at Pondicherry University. He has 14 years of teaching experience. At present he is working as associate professor at G. Pulla Reddy Engineering College, Kurnool, A.P. His area of interest is machine learning, deep learning, and cloud computing. He can be contacted at email: santhoshkumar.bala@gmail.com.



Pasupula Praveen Yadav     completed B.Tech. at KTM College of Engineering and M.Tech. at JNTUA College of Engineering, city. He has 17 years of teaching experience. At present he is working as Assistant professor at G. Pulla Reddy Engineering College, Kurnool, A.P. His area of interest is machine learning, AI, and data science. He can be contacted at email: praveenyadav.p@gmail.com.



Mogathala Raghavendra Reddy     completed B.Tech. at St. John's College of Engineering and Technology and M.Tech. at St. Mary's College of Engineering and Technology, city. He has 13 years of teaching experience. At present he is working as Assistant professor at G. Pulla Reddy Engineering College, Kurnool, A.P. His area of interest is machine learning, AI, and data science. He can be contacted at email: raghureddy224@gmail.com.