

Financial Fraud Detection for Credit Card Using XGBoost & SMOTE

Tufan Majumder¹, Dr. Dinesh Mishra²

1 Department of Information Technology, Mangalayatan University, Jabalpur, Madhya Pradesh, India.

Email: tufanmajumder@gmail.com

2 Department of Computer Science and Engineering, Mangalayatan University, Jabalpur, Madhya Pradesh, India.

Email: dinesh.mishra@mangalayatan.ac.in

ABSTRACT

The area of fraud detection has been traditionally correlated with data mining and text mining. Even before the "big data" phenomena started in 2008, text mining and data mining were used as instruments of fraud detection. However, the limited technological capabilities of the pre-big data technologies made it very difficult for researchers to run fraud detection algorithms on large amounts of data. This paper reviews various existing learning methods for financial fraud detection of credit card fraud across different areas and find out their strengths and weaknesses. This paper has developed a credit card fraud detection system using XGBoost (eXtreme Gradient Boosting) method. In the proposed system, data imbalance problem has also been resolved by using SMOTE. Results are evaluated and compared with many states of art methods & found that the presented method performs well in achieving more accurate results after resolving data imbalance.

Keywords: Financial fraud, Credit card fraud, Fraudster, Machine Learning, Deep Learning, Class imbalance, Boosting.

1. INTRODUCTION

In recent years, financial fraud activities such as credit card fraud, money laundering, health fraud and cyber fraud increase gradually. These activities cause the loss of personal and/or enterprises' properties. Even worse, they endanger the security of nation because the profit from fraud may go to terrorism [1]. Thus, accurately detecting financial fraud and tracing fraud are necessary and urgent. Taking money laundering as an example, money laundering is defined as the process of using trades to move money/goods with the intent of obscuring the true origin of funds. Usually, the prices, quantity or quality of goods on an invoice of money laundering are fake purposely. The misrepresentation of prices, quantity or quality of goods on an invoice merely exposes slight difference from regular basis if we use these numbers as features to generate detection policy. Under certain circumstances, this kind of detector may work well with relatively stable trading entities. Unfortunately, the real-world situation is more complicated, especially within Free Trade Zones (FTZs) where international trade involves complex procedures and exchange of information between trading entities. The fraud activities, especial money laundering, are deeper stealth. Money laundering activities may take different forms [1] such as the concealing transportation of cash using trading operations; the acquisition and sale of intangibles; and related party transactions. In contrast with other fraud activities, money laundering demonstrates special characteristic which presents high risk to financial system with obscuring the money trail, collectivization behavior and wild trading regions in FTZs. Many fraud detection models work with attribute-value data points that are generated from transactions data.

With the expansion of e-commerce and the widespread adoption of online payment methods, fraudulent activities have seen a noticeable surge. Credible reports indicate a stark and rapid increase in financial losses attributed to credit and debit card fraud between 2020 and 2022

[1]. What's particularly striking is that while unauthorized purchases and the use of counterfeit credit cards make up a relatively small portion, approximately 12-17%, of the total reported fraud cases, they account for a disproportionately large share, ranging from 75% to 80%, of the overall financial losses. In light of these critical issues, private businesses and government organizations have substantially increased their funding for research and development projects. Their primary objective is to create more resilient and effective systems for detecting fraudulent activities. Implementing automated fraud detection systems has become essential for financial institutions that oversee credit card issuance and online transaction management. These systems not only help reduce financial losses but also play a crucial role in enhancing customer faith and assurance. Innovative big data and artificial intelligence possibilities have opened up, giving intriguing potentials, particularly in utilizing powerful machine learning algorithms to combat financial crime. Modern fraud detection systems, aided by cutting-edge data analysis and advanced machine/deep learning algorithms, have demonstrated extraordinary efficacy [2]. Typically, these algorithms are trained on large datasets of labeled transactions, allowing them to differentiate between regular and fraudulent activity. The ultimate result is the development of binary classification models capable of distinguishing between valid and fraudulent transactions. Detecting fraudulent transactions using classification algorithms is a difficult task that requires constant innovation and flexibility. In the same way, innovation assures security, data availability, dependability, and resilience against cyber warfare assaults in the fight against wireless communication interference, the financial industry must continually innovate to stay ahead in the struggle against financial crime.

Financial fraud refers to the use of fraudulent and illegal methods or deceptive tactics to gain financial benefits. Fraud can be committed in different areas of finance, including banking, insurance, taxation, and corporates, and more. Fiscal fraud and evasion, including credit card fraud, tax evasion, financial statement fraud, money laundry, and other types of financial fraud, has become a growing problem. Despite efforts to eliminate financial fraud, its occurrence adversely affects business and society as hundreds of millions of dollars are lost to fraud each year. This significant financial loss has dramatically affected individuals, merchants, and banks. Nowadays, fraud attempts have increased drastically, which makes fraud detection more important than ever. The Association of Certified Fraud Examiners (ACFE) has announced that 10% of incidents concerning white-collar crime involve falsification of financial statements [3]. They classified occupational fraud into three types: asset misappropriation, corruption, and financial statement fraud. Financial statement fraud resulted in the most significant losses among them. Although the occurrence frequency of asset misappropriation and corruption is much higher than financial statement fraud, the financial implications of these latter crimes are still far less severe. In particular, as reported in a survey from EisnerAmper, which is among the prominent accounting firms in the U.S., ' ' the average median loss of financial statement fraud (\$800,000 in 2018) accounts for over three times the monetary loss of corruption (\$250,000) and seven times as much as asset misappropriation (\$114,000)' ' [4].

Financial statements are documents that describe details about a company, specifically their business activities and financial performance, including income, expenses, profits, loans, presumable concerns that may emerge later, and managerial comments on the business performance [5], [6]. All firms are obligated to announce their financial statements in a quarterly and annual manner. Financial statements can be used to indicate the performance of a company [6]. Investors, market analysts, and creditors exploit financial reports to investigate and assess the financial health and earnings potentials of a business. Financial statements consist of four sections; income statement, balance sheet, cash flow statement, and explanatory notes. Financial statement fraud involves falsifying financial statements to pretend the company more profitable than it is, increase the stock prices, avoid payment of

the taxes, or get a bank loan. Fraud triangle in auditing is a framework to demonstrate the motivation behind an individual's decision to commit fraud. It is built upon the fraud triangle theory that was proposed by [7]. The fraud triangle has three elements that increase the risk of fraud: incentive, rationalization, and opportunity, which, together, lead to fraudulent behavior. Auditing professionals have extensively used this theory to explain the motivation behind an individual's decision to commit fraud. It is indispensable to understand the fraud triangle to evaluate financial fraud.

Gupta and Singh [8] suggested that when there are incentives such as the obligation to achieve an outcome or cover losses, the potential for fraud increases. The company will encounter temptations or pressures to adopt fraudulent practices. Moreover, the lack of inspections or unsuccessful controls provides a favorable occasion for committing fraud. Rationalization happens when the fraudster aims to justify the fraudulent action, and it could be affected by the others and the conditions. Dbouk and Zaarour [7] remarked that people who perpetrate fraud incline to stay inside their moral safe zone. Therefore, the fraudster inwardly attempts to legitimize and defend the fraudulent behavior in preparation for committing the first fraud. Dbouk and Zaarour [7] indicated that rationalization occurs when the committer constructed a justification for the fraud and not desired to be deemed an offender. This situation enables fraudsters to consider their dilemma as a particular exemption rather than criminal behavior. Traditional methods of fraud detection, including manual detection, are not only costly, imprecise, and time sapping, but also impractical [9]. Activities are conducted to minimize losses resulting from fraudulent actions, but they are not too effective. Artificial intelligence, especially machine learning technologies, turned out to be one of the greatest thriving methods in fraud discovery. Data mining contributes to identify fraud and act immediately to lower overheads. Millions of statement documents can be searched through data mining techniques to spot patterns and identify fraudulent statements [10]. In most cases, prevailing fraud detection techniques have a common data mining rationale, but they may differ in many facets with specific domain knowledge. The goal of financial statement fraud detection (FSFD) is to categorize financial statements into fraudulent or non-fraudulent. Both supervised and unsupervised methods were used to predict fraudulent statements. Classification has been the most popular technique to identify fraudulent financial statements. Most FSFD practices employ supervised machine learning strategies [11], [12] that generally have a two-stage scheme. A model is trained on a dataset containing feature vectors and the class labels in the first stage. Afterward, in the next stage, test samples are classified using the trained model. The performance of machine learning/data mining (ML/DM) algorithms is directly associated with the way feature vectors are extracted from the input data and how informative they are. Selecting inappropriate features may lead to irrelevant or meaningless features and weak performance [7]. This paper presents a systematic literature review in the scope of intelligent financial statement fraud detection. The primary focus of this systematic literature review is on identifying the ML/DM techniques and datasets employed for FSFD. Furthermore, we aim to analyze the gaps and uncover the trend of research in this area (from the beginning to the most recent studies). The other recently published reviews have focused on the specific areas of finance, such as credit card fraud detection [13], fraud prediction in bank credit administration [14], online banking fraud detection [15], and payment card fraud detection [16]. The scope of our systematic literature review, however, is different from previous ones. Figure 1 shows the focus of the other review articles in the finance area.

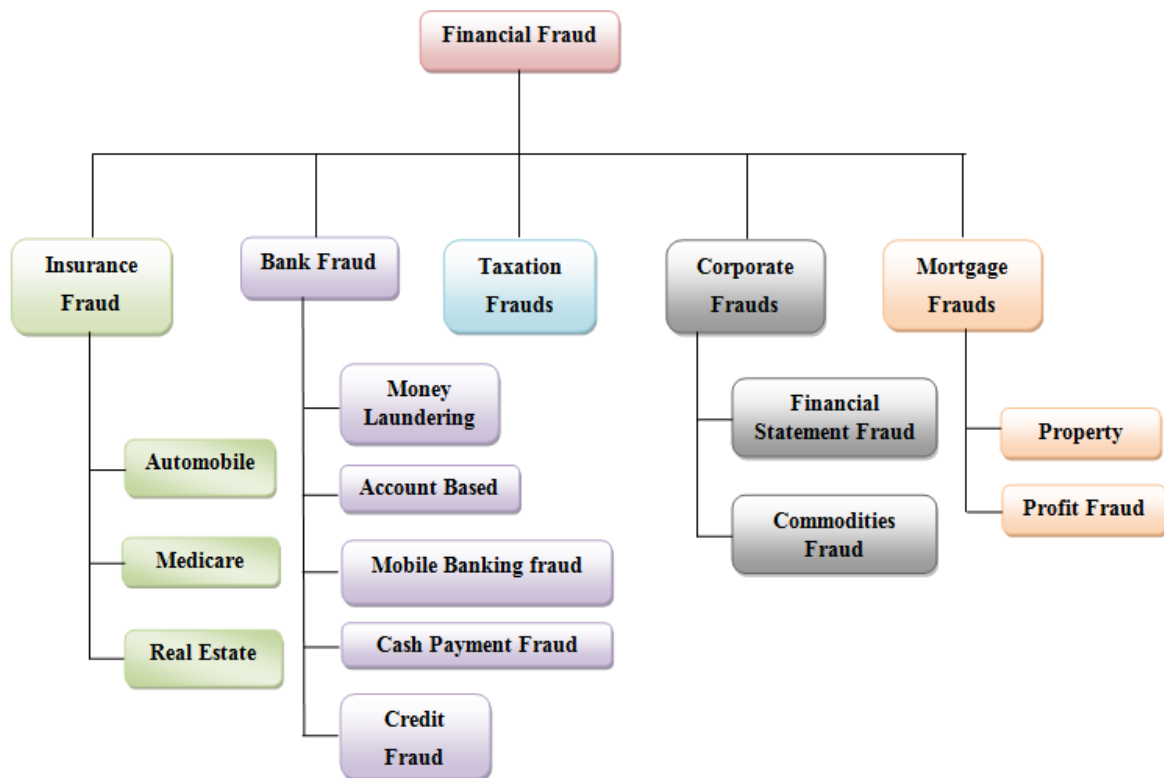


Figure 1: Financial Fraud Types.

2. LITRATURE REVIEW

A systematic literature review (SLR) is undertaken to study the current status of research in the financial fraud detection area and address the research questions. Inspired by Kitchenham, we followed the following steps to develop our SLR protocol [17].

A. Definition of the research questions: This study attempts to answer the following questions:

RQ1: What fraud detection techniques and datasets related to financial statements were employed in the literature?

RQ2: What are the gaps, trends of research, and future research directions in this area?

B. Developing search strategy: It is necessary to identify appropriate search concepts and keywords. In order to find the most related studies, we choose the below search string to obtain them in different digital libraries:

‘ ‘ fraud’ ’ AND ‘ ‘ financial fraud’ ’ AND ‘ ‘ fraud detection’ ’ OR ‘ ‘ machine learning’ ’ . We ‘ ‘ Machine Learning’ ’ to make sure that we can discover the studies that used machine learning techniques. Besides, we embedded the ‘ ‘ financial fraud’ ’ term to focus on articles that worked on the financial fraud detection. We searched the above search string in IEEE Xplore only for this review article. We only focused on the peer-reviewed journal and conference articles. The search was conducted in **July 2024**, and there was limitation for the publication year is 2022. We tried to use the abstract and make a comparison table given below:

C. Data extraction: This step entails deriving relevant data and information from the selected papers. We used the details about techniques and datasets to answer RQ1. We analyzed this information to group similar studies together, in terms of their datasets and techniques. Extracting the objective and the conclusion of each study will help us recognize the trends of the works, analyze the gaps, and determine future research (RQ2).

D. Meta-analysis: This section demonstrates the primary investigation results of the selected articles using a statistical approach to combine the outcomes from multiple studies. We answer the defined research questions based on the ultimately determined papers (47 papers) in the Results section. The publication years of the selected papers that met our criteria are varied between 2022 and 2024, while it suggests a rising interest in this area of research over the last four years, namely from 2020 to 2024. It is worth to mention that since our study was concluded in July 2024, papers published after that date were not included in our study.

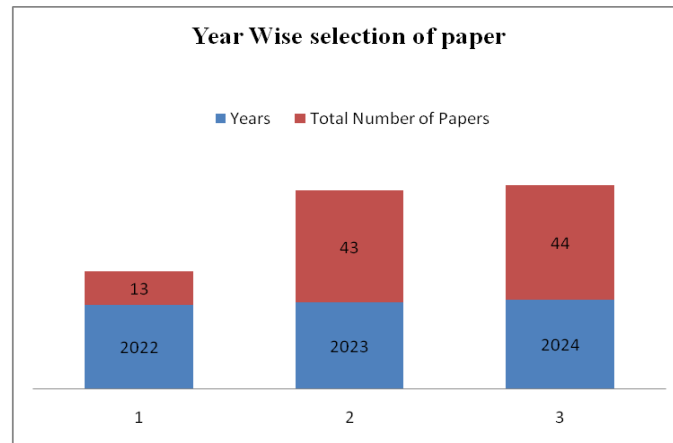


Figure 2: Selection of paper.

2.1 Fraud Types used in this study

In our study, we have done two types of studies with algorithms used and result parameters. Table 2 includes the study of credit card fraud transaction and Table 3 includes the description of the dataset used for analysis.

Table 2. Credit Card Fraud Transaction.

References	Algorithm	Result parameters
[1]	XGBoost, Artificial Neural Networks (ANN), and Relational Graph Convolutional Networks (R-GCN)	Accuracy
[2]	KNN	Accuracy
[3]	NA	Accuracy
[8]	SVM, LR	AUC Score
[11]	CNN	Accuracy, Precision, Recall
[12]	KNN, LR and Random Forest	Precision and Recall.
[13]	Optimization algorithm	Accuracy
[14]	RF, GB, CatBoost.	Accuracy
[16]	Decision Trees, Random Forest, Extra Trees Classifier, and XGBoost Classifier, Ensemble Classifier.	Accuracy, precision, and recall
[18]	GNN	Accuracy
[19]	RF, DT, LR, XGBoost.	f1-score, precision, and AUC
[20]	LR	Accuracy
[21]	DT, RF	Accuracy
[22]	XGBoost	Accuracy, Precision, Recall, Specificity, FPR, AUC, MCC, G-mean
[23]	Naive Bayes	Accuracy

[24]	RF, LR, DT, XGBoost	Accuracy
[26]	GBM	Accuracy, precision, recall, and F1-score
[28]	Gradient Boosting	Accuracy
[29]	SVM, RF, 1D-CNN, XGBoost, LR, AdaBoost.	Accuracy
[30]	RF	Accuracy, precision, recall, and F1-Score
[31]	Long Short-Term Memory	recall and accuracy
[32]	XGBoost, CatBoost and LightGBM.	ROC-AUC
[33]	Gradient Boosting	Accuracy Score.
[35]	LR	Accuracy Score.
[36]	RF	Accuracy Score
[40]	K-means, RF, DT, KNN and Naive Bayes.	Accuracy Score
[42]	Hybrid of LR, DT and RF	Accuracy Score
[43]	DT, LR, RF and SVM	Accuracy Score
[46]	AdaBoost, LR and RF.	Accuracy Score
[47]	LR, SVM and KNN.	Accuracy, precision, recall, and F1-Score
[50]	FCM-SVMSMOTE-CNN	Accuracy Score
[51]	RF and KNN	Accuracy, precision, recall, and F1-Score and Cost.
[52]	ML and DL.	Accuracy, precision, recall, and F1-Score
[53]	CNN, LSTM and Ensemble.	Area Under the Curve
[55]	CNN, LSTM, and DNN.	Accuracy, precision, recall, and F1-Score
[57]	LR, KNN, DT, RF, AdaBoost, CatBoost and LightGBM.	AUC and F1-Score.
[61]	Random Forest	Accuracy
[62]	LR, RF, GBM and XGBoost	AUPRC and AUC-ROC.
[64]	DT, LR, SVM, NB, RF, XGBoost, Gradient Boosting, AdaBoost and Stacking.	precision and F1-score
[65]	SVM, ANN and CNN.	Accuracy, precision, F1 score and recall
[67]	RF	F1 Score
[70]	DT, NN and Clustering.	Accuracy Score.
[71]	DT, CatBoost and XGBoost.	AUC and AUPRC
[72]	CNN, LSTM and MLP.	Accuracy Score.
[73]	Random-Tree-Based Random Forest (RTBRF), SVM.	Recall, Precision, detection rate
[75]	LR, RF, KNN and XGBoost.	Accuracy Score.
[76]	KNN	Accuracy Score.
[77]	RF, CatBoost, DT and Isolation Forest	Accuracy Score.
[78]	XGB, DT, LR and RF.	Accuracy, Sensitivity.
[79]	LR, DT, RF.	Accuracy Score.
[80]	XGBoost.	Accuracy, Efficiency.
[82]	RF	Accuracy Score.
[83]	GAN	Recall, F1-score,

		Accuracy, and Precision.
[84]	LR, DT, XGBoost, NB and RF.	Accuracy Score
[85]	ET, GB, DT, RF, AdaBoost.	Accuracy, Recall, Precision and F1-score
[87]	PSO and K-means.	Accuracy, Precision, and Recall
[88]	DT, RF, ANN and LR.	Accuracy
[89]	DT, RF, LR and XGBoost.	Accuracy
[90]	LSTM and CNN	Accuracy
[91]	LightGBM	Accuracy
[92]	CNN	accuracy, precision, and recall
[93]	Catboost	accuracy
[97]	Generative Adversarial Networks (GANs)	accuracy, precision, and recall
[99]	GNN and DNN.	accuracy

Table 3: Dataset Used

Ref	Dataset Name
[13]	European Cardholders.
[14]	European Cardholder Data.
[17]	Real world transaction dataset
[19]	European card benchmark dataset
[20]	Real credit card transaction dataset
[21]	Kaggle dataset
[24]	A variety of real and fraudulent credit card transaction datasets
[27]	Banksim dataset from Kaggle
[38]	UCI Machine Learning Repository, GitHub, Kaggle,
[45]	Real and synthetic bank dataset
[51]	European card holders 2013
[55]	European cardholder dataset.

2.2 Machine learning algorithm analysis for Financial Fraud Detection:

Table 4: Algorithm used for financial fraud detection from 2022 to 2024.

Algorithm Name	References	Total
SVM	[6], [19], [29], [34], [38], [43], [44], [47], [50], [59], [60], [64], [65], [69], [73], [94], [98].	17
DECISION TREE	[6], [16], [19], [21], [24], [38], [40], [42], [43], [49], [57], [59], [60], [63], [64], [70], [71], [77], [79], [84], [86], [88], [89], [94], [98].	25
RANDOM FOREST	[16], [17], [19], [21], [24], [29], [30], [36], [37], [38], [40], [42], [43], [47], [49], [51], [57], [59], [60], [61], [62], [63], [64], [66], [67], [73], [77], [78], [79], [81], [82], [84], [88], [89], [94], [95].	36
KNN	[2], [34], [38], [39], [40], [47], [49], [51], [57], [59], [63], [76], [86], [94].	14
LOGISTIC REGRESSION	[2], [17], [19], [20], [24], [29], [35], [38], [42], [43], [46], [47], [49], [57], [59], [60], [63], [64], [78], [79], [81], [84], [88], [89], [94], [98].	26
AdaBoost	[29], [46], [57], [64], [94], [95].	6

XGBoost	[1], [7], [15], [16], [17], [19], [22], [24], [29], [37], [49], [62], [64], [66], [71], [78], [80], [81], [84], [86], [89], [94].	22
CatBoost	[32], [38], [57], [71], [77].	5
Extra Tree Classifier	[16].	1
Ensemble Classifier	[16], [25], [45], [53].	4
Clustering	[40], [50], [70], [82].	4
CNN	[27], [29], [38], [50], [53], [55], [65], [73], [90].	9
LightGBM	[10], [15], [17], [26], [28], [32], [33], [57], [62], [66], [91].	11
NN	[1], [6], [18], [25], [34], [54], [69], [70], [98],	9
LSTM	[1], [31], [53], [55], [68], [73], [90],	7
RNN	[38], [68],	2
DNN	[55], [99]	2
ANN	[65], [88],	2
MLP	[73]	1

The analysis chart based on algorithm used for credit card fraud transaction is shown below.

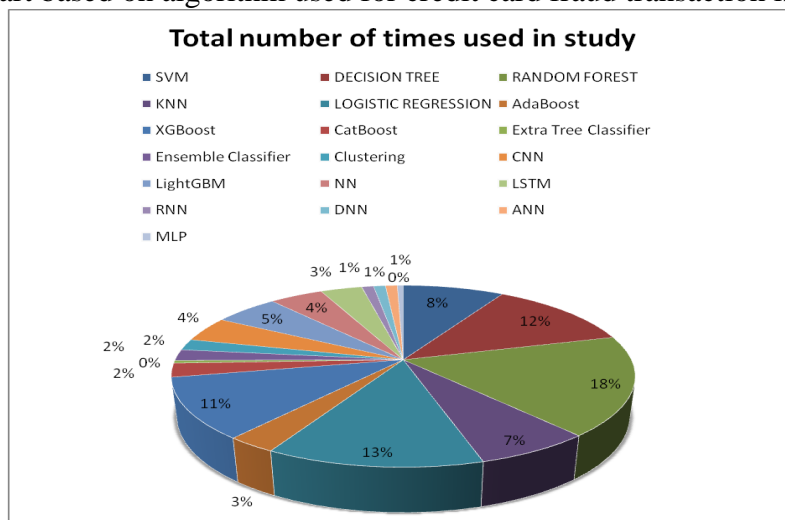


Figure 3: Machine Learning algorithm used analysis chart for credit card fraud transaction.

3. METHODOLOGY

From the study, we conclude that credit card fraud detection is the major problem found in fraud transaction detection. So to get insight into the details, we have implemented the creditcard fraud model using machine learning and deep learning algorithms. The dataset that used is European Cardholder Data as mentioned in table 3.

In this study, it is observed that most of the work already has been implemented on the European Card holder dataset. This dataset has total of 2, 84,807 transactions. Out of a total, only 492 were fraudulent. This dataset is highly unbalanced with positive class contribution of 0.172 % only.

To check the model performance on this dataset, we will use Cross-validation with Repeated K-fold and Stratified K-fold. Random Over sampler is used with Stratified K-fold cross validation. Finally SMOTE will used with ADASYN and results are compared.

All the techniques will be used with machine learning algorithms like Logistic Regression, Random Forest, Support Vector Machine, XGBoost, AdaBoost, Extra Tree Classifier and also some deep learning algorithms.

For Building the model, the dataset is divided into Training set and Testing set. The training set is used to train the model. Once the models are trained, they will be tested by Testing set. The Extended version of Train-Test model is called “ Train-Test-Validation dataset” in Machine Learning. In this version, the Training Set is further divided into “ Training set”

and “ Validation set” . Once the training of the models is over, the validation set is used to check the performance of the models. If the performance of the model is satisfactory, then the testing will be done. If the performance is not satisfactory, the model is tuned with different hyperparameters.

When a model is being trained, test and validated by using “ Train-test-validation” model, then there is a “ Bias” in this model because the model is not trained or tested with the entire dataset. Due to this the model may go to a problem called “ Overfitting” . The idea of cross-validation arises because of the problem with “ Train-test-validation” model. In cross-validation methods, the models are trained and tested with the entire datasets. In this credit-card implementation work, two cross-validation techniques called K-fold and Stratified K-folds are used. In K-fold cross-validation all the entire datasets elements are used for training and testing. But it has some challenges of some class elements in entire iterations. Due to that we also compare it with Stratified K-fold where each iteration has all the representation of classes which minimizes the overfitting problem.

General working of proposed system is shown below:

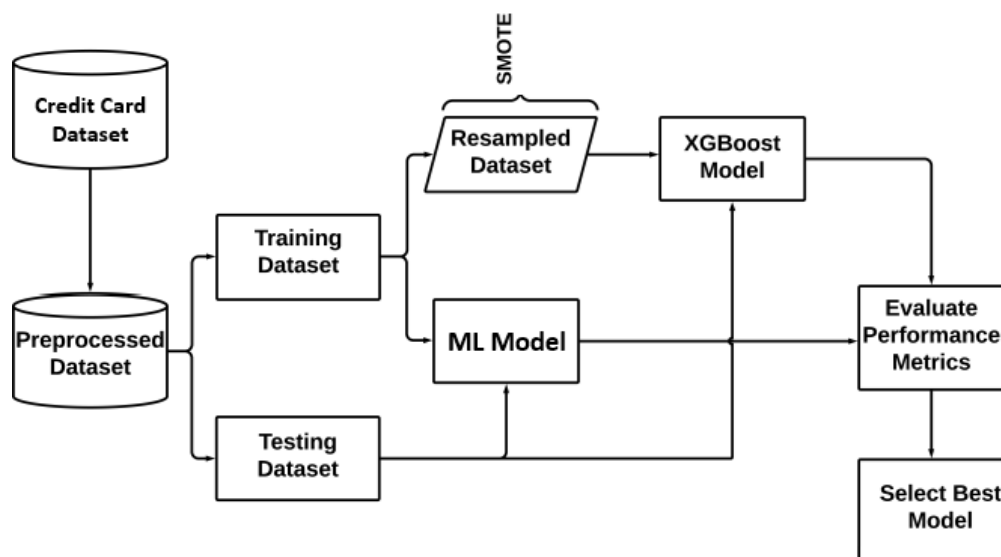


Figure 4: Architecture of the system

4. RESULT AND PERFORMANCE EVALUATION

The presented model has been implemented with many machine learning techniques- logistic regression, K-nearest neighbour, decision tree, extra tree & extreme gradient tree. Data imbalance has been implemented with random under sampling, random oversampling and SMOTE techniques. Performance of the methods has been compared with accuracy, precision and recall. Figure below represents the comparison of different methods.

	Methodology		Model	Accuracy	Precision	Recall
0	LR	Logistic Regression with L1 Regularisation		0.500000	0.000000	0.000000
1	LR	Logistic Regression with L1 Regularisation		0.500000	0.000000	0.000000
2	LR	Logistic Regression with L1 Regularisation		0.500000	0.000000	0.000000
3	KNN		KNN	0.876502	0.999052	0.753719
4	KNN		KNN	0.887324	0.943548	0.823944
5	KNN with SMOTE		KNN	0.917944	0.995593	0.839603
6	DT with Random Undersampling	Tree Model with gini criteria		0.869718	0.894737	0.838028
7	DT with Random Undersampling	Tree Model with entropy criteria		0.890845	0.911111	0.866197
8	Random Undersampling		XGBoost	0.929577	0.955224	0.901408
9	Random Oversampling		XGBoost	0.901496	0.999781	0.803168
10	Random Oversampling		XGBoost	0.901496	0.999781	0.803168
11	XGBOOST With SMOTE		XGBoost	0.938459	0.999693	0.877188
12	Random Undersampling		EXT	0.908451	0.975410	0.838028
13	Random Oversampling		EXT	0.862792	0.999903	0.725654

Figure 4: Performance parameters of various implemented algorithms

A chart for comparing accuracy is shown below:

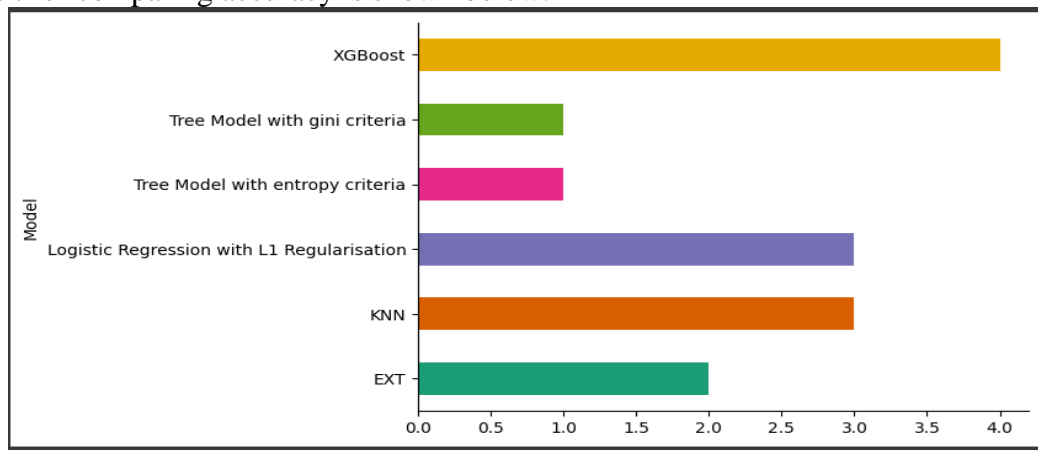


Figure 5: Comparison of accuracy

The result shows that XGBoost method with SMOTE provide accuracy 93.84%, precision 99.9% and recall 87.7% which is better than all other implemented solutions.

5. CONCLUSION

Financial fraud detection is a developing area in which it is advantageous to outrun the fraudsters. Besides, there are still aspects of intelligent financial fraud detection that have not been investigated thoroughly. In this study, we applied XGBoost (Extreme Gradient Boosting) and SMOTE (Synthetic Minority Over-sampling Technique) to tackle the problem of credit card fraud detection. The primary objective was to improve the model's ability to predict fraudulent transactions, which are inherently imbalanced in most datasets, with fraud cases being much fewer than legitimate ones. The credit card fraud dataset often suffers from class imbalance, where fraudulent transactions (minority class) are significantly fewer than legitimate ones (majority class). The application of SMOTE significantly improved model performance. Further improvements could include experimenting with other advanced sampling techniques. Incorporating additional features (e.g., transaction history, behavioural data) could also enhance model performance, particularly for detecting new or sophisticated types of fraud. It may be beneficial to explore hybrid approaches, combining XGBoost with

other models like Neural Networks or Random Forests to further improve the robustness of the fraud detection system.

REFERENCES

- [1] N. R. Shanbhog, K. S. Totad, A. R. Hanchinal and A. P. Bidargaddi, "Fraud Detection in Financial Transactions Using Deep Learning Approach: A Comparative Study," 2024 5th International Conference for Emerging Technology (INCET), Belgaum, India, 2024, pp. 1-7, doi: 10.1109/INCET61516.2024.10593486.
- [2] K. N, P. B, T. Rao and A. Kodipalli, "Analysis of Fraud Detection in Online Transactions Using Computational Models," 2024 5th International Conference for Emerging Technology (INCET), Belgaum, India, 2024, pp. 1-4, doi: 10.1109/INCET61516.2024.10593071.
- [3] R. Gupta, R. Goyal, K. Malik and I. Sahu, "AI-Enhanced Data Mining for Fraud Detection in Financial Transactions," 2024 3rd International Conference on Sentiment Analysis and Deep Learning (ICSADL), Bhimdatta, Nepal, 2024, pp. 244-249, doi: 10.1109/ICSADL61749.2024.00045.
- [4] G. Manoharan, S. D. N. H. Ali, D. M. Sathe, A. Karthik, A. Nagpal and A. Sidana, "Fraud Detection in E-commerce Transactions: A Machine Learning Perspective," 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2024, pp. 1-5, doi: 10.1109/ACCAI61061.2024.10601813.
- [5] K. Balaji, N. Saxena, N. R. Behera, M. Kiran Kumar, H. K. Prasad and P. R. Gedamkar, "Improved Fraud Detection in Banking Systems through Machine Learning and Big Data Analytics with Management Key Components," 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2024, pp. 1-6, doi: 10.1109/ACCAI61061.2024.10601803.
- [6] G. Manoharan, A. Dharmaraj, S. C. Sheela, K. Naidu, M. Chavva and J. K. Chaudhary, "Machine Learning-Based Real-Time Fraud Detection in Financial Transactions," 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), Chennai, India, 2024, pp. 1-6, doi: 10.1109/ACCAI61061.2024.10602350.
- [7] K. Pundir, N. Kaur, A. Kumar, N. Kumar and C. Das, "Detect Legitimate and Illicit Transactions Using Machine Learning," 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), Gautam Buddha Nagar, India, 2024, pp. 418-423, doi: 10.1109/IC3SE62002.2024.10592946.
- [8] S. Sharma, N. Kavitha, N. Dhaliwal, B. Rajalakshmi, I. Sumalatha and R. Kavitha, "Fraud Identification in Financial Transactions: Machine Learning-Based Anomaly Detection Method," 2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE), Gautam Buddha Nagar, India, 2024, pp. 1564-1569, doi: 10.1109/IC3SE62002.2024.10593528.
- [9] T. Porkodi, R. Rajkumar, R. Sathiya and M. S. Raja, "An Automatic ATM Card Fraud Detection Using Advanced Security Model Based on AOA-CNN-XGBoost Approach," 2024 International Conference on Electronics, Computing, Communication and Control Technology (ICECCC), Bengaluru, India, 2024, pp. 1-7, doi: 10.1109/ICECCC61767.2024.10593851.
- [10] X. Zhao, Q. Zhang and C. Zhang, "Enhancing Transaction Fraud Detection with a Hybrid Machine Learning Model," 2024 IEEE 4th International Conference on Electronic Technology, Communication and Information (ICETCI), Changchun, China, 2024, pp. 427-432, doi: 10.1109/ICETCI61221.2024.10594463.
- [11] B. R. Gudivaka, M. Almusawi, M. S. Priyanka, M. R. Dhanda and M. Thanjaivadivel, "An Improved Variational Autoencoder Generative Adversarial Network with Convolutional

Neural Network for Fraud Financial Transaction Detection," 2024 Second International Conference on Data Science and Information System (ICDSIS), Hassan, India, 2024, pp. 1-4, doi: 10.1109/ICDSIS61070.2024.10594271.

[12] R. Raman, V. Kumar, B. G. Pillai, D. Rabadiya, R. Divekar and H. Vachharajani, "Detecting Credit Card Fraud: A Comparative Analysis of KNN, Random Forest, and Logistic Regression Methods," 2024 Second International Conference on Data Science and Information System (ICDSIS), Hassan, India, 2024, pp. 1-5, doi: 10.1109/ICDSIS61070.2024.10594698.

[13] P. K. Pareek, B. R. Mohan, E. V. Vidya, P. Zanke and K. S. Navyashree, "DBROA based Convolutional Auto Encoder for European Credit Card Fraud Detection," 2024 Second International Conference on Data Science and Information System (ICDSIS), Hassan, India, 2024, pp. 1-7, doi: 10.1109/ICDSIS61070.2024.10594444.

[14] S. Chaurasia, S. Kesharwani, S. Sharma, S. Sharma and B. Chugh, "Analysis of Ensemble Machine Learning Models for Fraud Detection," 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS), Gurugram, India, 2024, pp. 1-6, doi: 10.1109/ISCS61804.2024.10581076.

[15] A. Rezaei, M. Yazdinejad and M. Sookhak, "Credit Card Fraud Detection Using Tree-Based Algorithms For Highly Imbalanced Data," 2024 IEEE 3rd International Conference on Computing and Machine Intelligence (ICMI), Mt Pleasant, MI, USA, 2024, pp. 1-6, doi: 10.1109/ICMI60790.2024.10586088.

[16] S. S. Chakravarthi, B. R. S. Balaji, M. N. C. S. Chowdhary and S. Sountharajan, "Ensembled Learning for Detecting Fraudulent Online Transactions," 2024 5th International Conference on Innovative Trends in Information Technology (ICITIIT), Kottayam, India, 2024, pp. 1-6, doi: 10.1109/ICITIIT61487.2024.10580283.

[17] S. Patel, M. Pandey and R. D., "Fraud Detection in Financial Transactions: A Machine Learning Approach," 2024 Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 2024, pp. 1-8, doi: 10.1109/ICONSTEM60960.2024.10568903.

[18] M. Thilagavathi, R. Saranyadevi, N. Vijayakumar, K. Selvi, L. Anitha and K. Sudharson, "AI-Driven Fraud Detection in Financial Transactions with Graph Neural Networks and Anomaly Detection," 2024 International Conference on Science Technology Engineering and Management (ICSTEM), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICSTEM61137.2024.10560838.

[19] M. A. Islam, A. T. M. Asif Imran, M. H. Rahman, M. A. H. Pabel, B. K. Mishra and K. Basu, "Analysis and Performance Evaluation of Credit Card Fraud by Multi-model ML," 2024 3rd International Conference on Advancement in Electrical and Electronic Engineering (ICAEEE), Gazipur, Bangladesh, 2024, pp. 1-7, doi: 10.1109/ICAEEE62219.2024.10561719.

[20] B. A. Smadi, W. B. Glisson, M. Tahat, H. Alamleh and A. A. S. AlQahtani, "Credit Card Transactions Fraud Detection for Multiple Consumer Behaviors," 2024 International Conference on Computing, Networking and Communications (ICNC), Big Island, HI, USA, 2024, pp. 26-32, doi: 10.1109/ICNC59896.2024.10556040.

[21] B. Vihurskyi, "Credit Card Fraud Detection with XAI: Improving Interpretability and Trust," 2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE), Ballari, India, 2024, pp. 1-6, doi: 10.1109/ICDCECE60827.2024.10548159.

[22] S. K. Jain and S. Asha, "Credit Card Fraud Detection System using SMOTEENN and Adaptive XGBoost and comparing the result with state-of-art-technique," 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), Pune, India, 2024, pp. 1-7, doi: 10.1109/I2CT61223.2024.10543887.

[23] G. S. Chaitanya, K. Deepika, G. S. Prabhav, R. B. Patil and M. A. Jabbar, "Credit Card Fraud Detection using Hidden Naive Bayes and Bayesian Belief Network," 2024 IEEE

- 9th International Conference for Convergence in Technology (I2CT), Pune, India, 2024, pp. 1-6, doi: 10.1109/I2CT61223.2024.10544328.
- [24] N. Ahirwar, D. Singh and K. Maheshwar, "Efficient Credit Card Fraud Detection Based on Multiple ML Algorithms," 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), Pune, India, 2024, pp. 1-7, doi: 10.1109/I2CT61223.2024.10544195.
- [25] A. C. Hiremath, A. Arya, L. Sriranga, K. V. S. R. Reddy and M. Nikhil, "Ensemble of Graph Neural Networks for Enhanced Financial Fraud Detection," 2024 IEEE 9th International Conference for Convergence in Technology (I2CT), Pune, India, 2024, pp. 1-8, doi: 10.1109/I2CT61223.2024.10543898.
- [26] N. N. Jose, A. K. Arigela, G. Vivekanandan, R. Sethuraman, S. B. T. Naganathan and N. Venu, "Optimizing Payment Transaction Security: Utilizing Gradient Boosting Machines for Fraud Detection", 2024 10th International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 2024, pp. 720-725, doi: 10.1109/ICCSP60870.2024.10543774.
- [27] S. R. Banu, T. N. Gongada, K. Santosh, H. Chowdhary, R. Sabareesh and S. Muthuperumal, "Financial Fraud Detection Using Hybrid Convolutional and Recurrent Neural Networks: An Analysis of Unstructured Data in Banking," 2024 10th International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 2024, pp. 1027-1031, doi: 10.1109/ICCSP60870.2024.10543545.
- [28] N. Deshai, A. K. Arigela, S. Ashwini, N. N. Jose, V. Palanivel and N. Venu, "Secure Swipe Enhancing Card Transactions Through Gradient Boosted Fraud Detection," 2024 10th International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 2024, pp. 394-399, doi: 10.1109/ICCSP60870.2024.10544369.
- [29] B. Paulraj, "Machine Learning Approaches for Credit Card Fraud Detection: A Comparative Analysis and the Promise of 1D Convolutional Neural Networks," 2024 7th International Conference on Information and Computer Technologies (ICICT), Honolulu, HI, USA, 2024, pp. 82-92, doi: 10.1109/ICICT62343.2024.00020.
- [30] S. -I. Mihali and Ş. -L. Niță, "Credit Card Fraud Detection based on Random Forest Model," 2024 International Conference on Development and Application Systems (DAS), Suceava, Romania, 2024, pp. 111-114, doi: 10.1109/DAS61944.2024.10541240.
- [31] S. Jhansi Ida, K. Balasubadra, S. R R and L. N. T, "Enhancing Credit Card Fraud Detection through LSTM-Based Sequential Analysis with Early Stopping," 2024 2nd International Conference on Networking and Communications (ICNWC), Chennai, India, 2024, pp. 1-6, doi: 10.1109/ICNWC60771.2024.10537550.
- [32] R. P, M. A. Guptha and A. H. Kumar, "Optimal Weight-Tuning for Unbalanced Data in Credit Card Fraud Detection," 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS), Chennai, India, 2024, pp. 1-6, doi: 10.1109/ADICS58448.2024.10533545.
- [33] K. W. Thar and T. T. Wai, "Machine Learning Based Predictive Modelling for Fraud Detection in Digital Banking," 2024 IEEE Conference on Computer Applications (ICCA), Yangon, Myanmar, 2024, pp. 1-5, doi: 10.1109/ICCA62361.2024.10532788.
- [34] S. Khosravi, M. Kargari, B. Teimourpour, M. Talebi, A. Eshghi and A. Aliabdi, "GHM: An Ensemble Approach to Fraud Detection with a Graph-Based HMM Method," 2024 10th International Conference on Web Research (ICWR), Tehran, Iran, Islamic Republic of, 2024, pp. 99-104, doi: 10.1109/ICWR61162.2024.10533348.
- [35] S. Banka, B. Kanchanapalli, N. K. Shaik, K. Dasari, D. Poojitha and A. Nalla, "Securing Fintech: A Machine Learning Approach for Credit Card Fraud Detection," 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS), Coimbatore, India, 2024, pp. 814-821, doi: 10.1109/ICC-ROBINS60238.2024.10533901.
- [36] S. Tanapanichkan, S. Kosolsombat and T. Luangwiriya, "Credit Card Fraud Detection Using Machine Learning," 2024 IEEE International Conference on Cybernetics and

- Innovations (ICCI), Chonburi, Thailand, 2024, pp. 1-5, doi: 10.1109/ICCI60780.2024.10532670.
- [37] Tamanna, S. Kamboj, L. Singh and T. Kaur, "Automated Fraud Detection in Financial Transactions using Machine Learning: An Ensemble Perspective," 2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA), Namakkal, India, 2024, pp. 1-6, doi: 10.1109/AIMLA59606.2024.10531422.
- [38] P. Kumari and S. Mittal, "Fraud Detection System for Financial System Using Machine Learning Techniques: A Review," 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, 2024, pp. 1-6, doi: 10.1109/ICRITO61523.2024.10522197.
- [39] H. Aldosari, "Garra Rufa Fish Optimization-based K-Nearest Neighbor for Credit Card Fraud Detection," 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT), Bengaluru, India, 2024, pp. 1-5, doi: 10.1109/ICDCOT61034.2024.10516188.
- [40] K. Sreekala, R. Sridivya, N. K. K. Rao, R. K. Mandal, G. J. Moses and A. Lakshmanarao, "A hybrid Kmeans and ML Classification Approach for Credit Card Fraud Detection," 2024 3rd International Conference for Innovation in Technology (INOCON), Bangalore, India, 2024, pp. 1-5, doi: 10.1109/INOCON60754.2024.10511603.
- [41] B. Kumar, S. K. Gupta and M. Patnaik, "Machine Learning-Powered Fraud Detection & Prevention: A Comprehensive Implementation," 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2024, pp. 1-6, doi: 10.1109/IDCIoT59759.2024.10467714.
- [42] D. Jahnavi, M. A. S. Pulata, S. Sami, B. Vakamullu and B. Mohan G, "Robust Hybrid Machine Learning Model for Financial Fraud Detection in Credit Card Transactions," 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2024, pp. 680-686, doi: 10.1109/IDCIoT59759.2024.10467340.
- [43] V. R. Adhegaonkar, A. R. Thakur and N. Varghese, "Advancing Credit Card Fraud Detection Through Explainable Machine Learning Methods," 2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT), Bengaluru, India, 2024, pp. 792-796, doi: 10.1109/IDCIoT59759.2024.10467999.
- [44] A. Khanum, C. K S, B. Singh and C. Gomathi, "Fraud Detection in Financial Transactions: A Machine Learning Approach vs. Rule-Based Systems," 2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bangalore, India, 2024, pp. 1-5, doi: 10.1109/IITCEE59897.2024.10467759.
- [45] S. Kishan and K. Alluru, "Fraud Detection in Banking Transactions Using Ensemble Learning," 2023 IEEE Fifth International Conference on Advances in Electronics, Computers and Communications (ICAEECC), Bengaluru, India, 2023, pp. 1-9, doi: 10.1109/ICAEECC59324.2023.10560116.
- [46] A. -A. Al-Maari and M. Abdulnabi, "Credit Card Fraud Transaction Detection Using a Hybrid Machine Learning Model," 2023 IEEE 21st Student Conference on Research and Development (SCORED), Kuala Lumpur, Malaysia, 2023, pp. 119-123, doi: 10.1109/SCORED60679.2023.10563915.
- [47] Rinku, A. K. Dubey, S. K. Narang and N. Kishore, "Enhancing Credit Card Fraud Detection: Analyzing Time and Amount Distributions with Computational Intelligence Algorithms," 2023 Third International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Gobichettipalayam, India, 2023, pp. 331-337, doi: 10.1109/ICUIS60567.2023.00061.

- [48] C. P. Shan, T. A. Leng, M. Ahmad, Y. Malik and F. Jaffar, "Overcoming Imbalanced Datasets and Feature Complexity in Fraud Transaction Detection Through Down-Sampling and Dimension Reduction," 2023 17th International Conference on Open Source Systems and Technologies (ICOSST), Lahore, Pakistan, 2023, pp. 1-11, doi: 10.1109/ICOSST60641.2023.10505068.
- [49] M. A. Islam, A. Nag, S. Chowdhury, S. F. A. Fahim, A. Ghosh and N. Mumtaj, "Utilization of Encoding, Early Stopping, Hyper Parameter Tuning, and Machine Learning Models for Bank Fraud Detection," 2023 IEEE 9th International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE), Thiruvananthapuram, India, 2023, pp. 321-327, doi: 10.1109/WIECON-ECE60392.2023.10456503.
- [50] Z. Xu and Y. -C. Chang, "Credit Card Fraud Detection Based on Fcm-Svmsmote-Cnn," 2023 International Conference on Computer Science and Automation Technology (CSAT), Shanghai, China, 2023, pp. 169-174, doi: 10.1109/CSAT61646.2023.00056.
- [51] S. Bharadwaj, "Credit Card Fraud Detection Using Machine Learning," 2023 16th International Conference on Developments in eSystems engineering (DeSE), Istanbul, Turkiye, 2023, pp. 168-172, doi: 10.1109/DeSE60595.2023.10469583.
- [52] T. Baabdullah, D. B. Rawat, C. Liu, A. Alzahrani and A. Almotairi, "Analysis of Cardholder Spending Behavior and Transaction Authentication to Enhance Credit Card Fraud Detection," 2023 International Conference on Machine Learning and Applications (ICMLA), Jacksonville, FL, USA, 2023, pp. 1144-1149, doi: 10.1109/ICMLA58977.2023.00171.
- [53] Z. Chen, S. Wang, D. Yan and Y. Li, "Research and Implementation of Bank Credit Card Fraud Detection System Based on Reinforcement Learning and LSTM," 2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, India, 2023, pp. 1-8, doi: 10.1109/ICMNWC60182.2023.10435890.
- [54] I. Jahan and M. Kumar, "Genetic Algorithm Based Neural Network Framework for Fraudulent Transaction Detection," 2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 2023, pp. 631-635, doi: 10.1109/ICCCIS60361.2023.10425407.
- [55] J. Geng and B. Zhang, "Credit Card Fraud Detection Using Adversarial Learning," 2023 International Conference on Image Processing, Computer Vision and Machine Learning (ICICML), Chengdu, China, 2023, pp. 891-894, doi: 10.1109/ICICML60161.2023.10424872.
- [56] S. S. Rawat and A. Kumar Mishra, "The Best ML Classifier(s): An empirical study on the learning of imbalanced and resampled credit card data," 2023 Second International Conference on Informatics (ICI), Noida, India, 2023, pp. 1-6, doi: 10.1109/ICI60088.2023.10421691.
- [57] A. Hanae, G. Youssef and E. Saida, "Analysis of Banking Fraud Detection Methods through Machine Learning Strategies in the Era of Digital Transactions," 2023 7th IEEE Congress on Information Science and Technology (CiSt), Agadir - Essaouira, Morocco, 2023, pp. 105-110, doi: 10.1109/CiSt56084.2023.10409974.
- [58] S. S. Suganya, S. Nishanth and D. Mohanadevi, "Ensemble Learning Approaches for Fraud Detection in Financial Transactions," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 805-810, doi: 10.1109/ICACRS58579.2023.10404382.
- [59] S. Maurya, K. Sharma, A. P. Singh, N. P. Tiwari, A. Sharma and H. Pant, "Credit Card Financial Fraudster Discovery with Machine Learning Classifiers," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, 2023, pp. 2206-2211, doi: 10.1109/IC3I59117.2023.10398009.
- [60] P. Shukla, M. Aggarwal, P. Jain, P. Khanna and M. K. Rana, "Financial Fraud Detection and Comparison Using Different Machine Learning Techniques," 2023 3rd International Conference on Technological Advancements in Computational Sciences

- (ICTACS), Tashkent, Uzbekistan, 2023, pp. 1205-1210, doi: 10.1109/ICTACS59847.2023.10390165.
- [61] Z. Bawany and A. D. Shanbhag, "Using Machine Learning To Detect Credit Card Fraud," 2023 International Conference on Electrical, Computer and Energy Technologies (ICECET), Cape Town, South Africa, 2023, pp. 1-7, doi: 10.1109/ICECET58911.2023.10389421.
- [62] P. Murkute, C. Dhule, P. Lipte, R. Agrawal and N. Chavhan, "Credit Card Fraud Detection Using Machine Learning Techniques," 2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI), Tiruchengode, India, 2023, pp. 1-8, doi: 10.1109/ICAEECI58247.2023.10370832.
- [63] P. Saha, S. Aanand, P. Shah, R. Khatwani, P. K. Mitra and R. Sekhar, "Comparative Analysis of ML Algorithms for Fraud Detection in Financial Transactions," 2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI), Tiruchengode, India, 2023, pp. 1-6, doi: 10.1109/ICAEECI58247.2023.10370930.
- [64] S. S. Bhakta, S. Ghosh and B. Sadhukhan, "Credit Card Fraud Detection Using Machine Learning: A Comparative Study of Ensemble Learning Algorithms," 2023 9th International Conference on Smart Computing and Communications (ICSCC), Kochi, Kerala, India, 2023, pp. 296-301, doi: 10.1109/ICSCC59169.2023.10335075.
- [65] S. M. Gopavaram and P. Vinothiyalakshmi, "Cloud Based Credit Card Fraud Detection System in Banking Using Machine Learning and Deep Learning algorithms," 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), Delhi, India, 2023, pp. 1-4, doi: 10.1109/ICCCNT56998.2023.10307070.
- [66] E. Begen, İ. U. Sayan, A. Tuğrul Bayrak and O. T. Yıldız, "Point of Sale Fraud Detection Methods via Machine Learning," 2023 International Conference on Innovations in Intelligent Systems and Applications (INISTA), Hammamet, Tunisia, 2023, pp. 1-5, doi: 10.1109/INISTA59065.2023.10310515.
- [67] R. K. Chanda, P. Kumar Pagadala, C. K. Edukulla, S. Sai Archana, S. Gurram and S. R. Maram, "Enhancing Credit Card Fraud Prediction using Decision Trees, SMOTE, and Hyper-Tuned Random Forests: A Comprehensive Approach," 2023 7th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2023, pp. 794-799, doi: 10.1109/I-SMAC58438.2023.10290611.
- [68] C. Iscan and F. P. Akbulut, "Fraud Detection using Recurrent Neural Networks for Digital Wallet Security," 2023 8th International Conference on Computer Science and Engineering (UBMK), Burdur, Turkiye, 2023, pp. 538-542, doi: 10.1109/UBMK59864.2023.10286651.
- [69] M. N. Ashtiani and B. Raahemi, "An Efficient Resampling Technique for Financial Statements Fraud Detection: A Comparative Study," 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Tenerife, Canary Islands, Spain, 2023, pp. 1-7, doi: 10.1109/ICECCME57830.2023.10253185.
- [70] A. Yadav, A. Adhikary, A. Kainth and R. Kumar, "Performance Evaluation of Machine Learning Methods for Detecting Credit Card Fraud," 2023 World Conference on Communication & Computing (WCONF), RAIPUR, India, 2023, pp. 1-7, doi: 10.1109/WCONF58270.2023.10235116.
- [71] H. Wang, Q. Liang, J. T. Hancock and T. M. Khoshgoftaar, "Enhancing Credit Card Fraud Detection Through a Novel Ensemble Feature Selection Technique," 2023 IEEE 24th International Conference on Information Reuse and Integration for Data Science (IRI), Bellevue, WA, USA, 2023, pp. 121-126, doi: 10.1109/IRI58017.2023.00028.
- [72] N. F. Aurna, M. D. Hossain, Y. Taenaka and Y. Kadobayashi, "Federated Learning-Based Credit Card Fraud Detection: Performance Analysis with Sampling Methods and Deep

- Learning Algorithms," 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy, 2023, pp. 180-186, doi: 10.1109/CSR57506.2023.10224978.
- [73] K. Murugan, A. Felicia, B. Gomathy, P. T. Saravana kumar, S. M. Ramesh and E. Sakthivel, "A Credit Card Fraud Identification Technique Using Support Vector Machine," 2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC), Dharwad, India, 2023, pp. 1-7, doi: 10.1109/ICAISC58445.2023.10199684.
- [74] N. M. Reddy, K. A. Sharada, D. Pilli, R. N. Paranthaman, K. S. Reddy and A. Chauhan, "CNN-Bidirectional LSTM based Approach for Financial Fraud Detection and Prevention System," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 541-546, doi: 10.1109/ICSCSS57650.2023.10169800.
- [75] A. Jessica, F. V. Raj and J. Sankaran, "Credit Card Fraud Detection Using Machine Learning Techniques," 2023 2nd International Conference on Vision Towards Emerging Trends in Communication and Networking Technologies (ViTECoN), Vellore, India, 2023, pp. 1-6, doi: 10.1109/ViTECoN58111.2023.10157162.
- [76] A. Singhai, S. Aanjankumar and S. Poonkuntran, "A Novel Methodology for Credit Card Fraud Detection using KNN Dependent Machine Learning Methodology," 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2023, pp. 878-884, doi: 10.1109/ICAAIC56838.2023.10141427.
- [77] A. H. Ali Mohamed and S. Subramanian, "Fraud Classification In Financial Statements Using Machine Learning Techniques," 2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD), Manama, Bahrain, 2023, pp. 1-4, doi: 10.1109/ITIKD56332.2023.10100257.
- [78] I. Dawar, N. Kumar, G. Kaur, S. Chaturvedi, A. Bhardwaj and M. Rana, "Supervised Learning Methods for Identifying Credit Card Fraud," 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA), Uttarakhand, India, 2023, pp. 791-796, doi: 10.1109/ICIDCA56705.2023.10100266.
- [79] K. G. Krishna, P. Kulkarni and N. A. Natraj, "Use of Big Data Technologies for Credit Card Fraud Prediction," 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2023, pp. 1408-1413, doi: 10.1109/ICSCDS56580.2023.10104977.
- [80] A. Mahajan, V. S. Baghel and R. Jayaraman, "Credit Card Fraud Detection using Logistic Regression with Imbalanced Dataset," 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2023, pp. 339-342.
- [81] S. Khosravi, M. Kargari, B. Teimourpour, A. Eshghi and A. Aliabdi, "Using Supervised Machine Learning Approaches To Detect Fraud In The Banking Transaction Network," 2023 9th International Conference on Web Research (ICWR), Tehran, Iran, Islamic Republic of, 2023, pp. 115-119, doi: 10.1109/ICWR57742.2023.10139083.
- [82] S. Rama Krishna, V. Agarwal, D. E. Rao, V. U. Kakde, S. Kumari and P. Shankar Vadar, "Machine Learning based Data Mining for Detection of Credit Card Frauds," 2023 International Conference on Inventive Computation Technologies (ICICT), Lalitpur, Nepal, 2023, pp. 72-77, doi: 10.1109/ICICT57646.2023.10134015.
- [83] E. Strelcenia and S. Prakoonwit, "A New GAN-based data augmentation method for Handling Class Imbalance in Credit Card Fraud detection," 2023 10th International Conference on Signal Processing and Integrated Networks (SPIN), Noida, India, 2023, pp. 627-634, doi: 10.1109/SPIN57001.2023.10116543.
- [84] S. S. Velicheti, A. S. H. Pavan, B. T. Reddy, N. V. Srikala, R. Pranay and S. K. Kannaiah, "The Hustlee Credit Card Fraud Detection using Machine Learning," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 139-144, doi: 10.1109/ICCMC56507.2023.10084063.

- [85] S. Jose, D. Devassy and A. M. Antony, "Detection of Credit Card Fraud Using Resampling and Boosting Technique," 2023 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA), Ernakulam, India, 2023, pp. 1-8, doi: 10.1109/ACCTHPA57160.2023.10083376.
- [86] N. Pathak and S. Singhal, "Fraud Detection in Financial Domain using Machine Learning," 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), Greater Noida, India, 2023, pp. 1449-1452, doi: 10.1109/AISC56616.2023.10085181.
- [87] N. Sharma and V. Ranjan, "Credit Card Fraud Detection: A Hybrid of PSO and K-Means Clustering Unsupervised Approach," 2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, 2023, pp. 445-450, doi: 10.1109/Confluence56041.2023.10048876.
- [88] N. J. Nishi, F. Akter Sunny and S. C. Bakchy, "Fraud Detection of Credit Card using Data Mining Techniques," 2022 4th International Conference on Sustainable Technologies for Industry 4.0 (STI), Dhaka, Bangladesh, 2022, pp. 1-6, doi: 10.1109/STI56238.2022.10103292.
- [89] S. Mugundhan and P. Venkataramanan, "Data Characteristic Stability Based Random Forest Implementation of Credit Card Fraud Detection," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1100-1104, doi: 10.1109/IC3I56241.2022.10073027.
- [90] R. Saxena, D. Singh, M. Rakhra, S. N. Dwivedi and A. Singh, "Deep learning for the detection of fraudulent credit card activity," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1061-1067, doi: 10.1109/IC3I56241.2022.10072543.
- [91] M. Guan, R. Xue, Z. Wu, H. Yang, D. Song and Z. Zhang, "A high performance fraud detection strategy prediction model," 2022 2nd International Conference on Computer Science and Blockchain (CCSB), Wuhan, China, 2022, pp. 107-110, doi: 10.1109/CCSB58128.2022.00026.
- [92] M. L. Gambo, A. Zainal and M. N. Kassim, "A Convolutional Neural Network Model for Credit Card Fraud Detection," 2022 International Conference on Data Science and Its Applications (ICoDSA), Bandung, Indonesia, 2022, pp. 198-202, doi: 10.1109/ICoDSA55874.2022.9862930.
- [93] A. Singh, A. Singh, A. Aggarwal and A. Chauhan, "Design and Implementation of Different Machine Learning Algorithms for Credit Card Fraud Detection," 2022 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Maldives, Maldives, 2022, pp. 1-6, doi: 10.1109/ICECCME55909.2022.9988588.
- [94] T. S. Reddy, G. Nookaraju, K. Vikas, S. N. Mohanty, J. Anagandula and M. S. Ahmed, "An Analysis of Various Algorithmic Behaviors in Detecting a Financial Fraud," 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2022, pp. 1-6, doi: 10.1109/ICCCNT54827.2022.9984399.
- [95] E. Hytis, V. Nastos, C. Gogos and A. Dimitsas, "Automated identification of fraudulent financial statements by analyzing data traces," 2022 7th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), Ioannina, Greece, 2022, pp. 1-7, doi: 10.1109/SEEDA-CECNSM57760.2022.9932910.
- [96] J. Wang and C. Yang, "Financial Fraud Detection Based on Ensemble Machine Learning," 2022 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCCom/CyberSciTech), Falerna, Italy, 2022, pp. 1-6, doi: 10.1109/DASC/PiCom/CBDCCom/Cy55231.2022.9928001.

- [97] E. Strelcenia and S. Prakoonwit, "Comparative Analysis of Machine Learning Algorithms using GANs through Credit Card Fraud Detection," 2022 International Conference on Computing, Networking, Telecommunications & Engineering Sciences Applications (CoNTESA), Skopje, North Macedonia, 2022, pp. 1-5, doi: 10.1109/CoNTESA57046.2022.10011268.
- [98] A. Biswas, R. S. Deol, B. K. Jha, G. Jakka, M. R. Suguna and B. I. Thomson, "Automated Banking Fraud Detection for Identification and Restriction of Unauthorised Access in Financial Sector," 2022 3rd International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2022, pp. 809-814, doi: 10.1109/ICOSEC54921.2022.9951931.
- [99] D. Mu, "Credit Card Fraud Intelligent Detection Based on Machine Learning," 2022 IEEE International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), Changchun, China, 2022, pp. 1112-1117, doi: 10.1109/EEBDA53927.2022.9744875.
- [100] A. Fitriyani, W. Priatna, T. S. Lestari, D. Handayani, T. A. Munandar and Amri, "Data Balance Optimization of Fraud Classification for E-Commerce Transaction," 2022 Seventh International Conference on Informatics and Computing (ICIC), Denpasar, Bali, Indonesia, 2022, pp. 1-4, doi: 10.1109/ICIC56845.2022.10007028.