© Volume 2, Issue 11, November 2026 | JATIR
e-ISSN: 2839-5786, p-ISSN: 3139-8464

Intelligent Financial Fraud Detection Using Machine Learning Techniques

[1]Sayali Gaikwad, [2]Aditya Nehare, [3]Sarthak Wagh, [4]Mahima Thakur
[5]Sanchita Gund
[1]*Assistant Professor Department of Information Technology Parvatibai Genba Moze College of Engineering, Wagholi, Pune, India*
[2,3,4,5]*Student, Department of Information Technology Parvatibai Genba Moze College of Engineering, Wagholi, Pune, India*
https://doi.org/10.64643/jatir.141233

***Abstract*—The adoption of online banking in India has shown a sharp increase in online financial transactions, and it has also created new prospects of fraudulent activities. Financial systems need to identify the cases of fraud within a short time and with high precision to protect their structure and safeguard the assets of the customers. In this study, the authors created a powerful machine learning model with the Extreme Gradient Boosting (XGBoost) algorithm to identify banking fraud using the Bank_Transaction_Fraud_Detection dataset of Kaggle. The model proved to be remarkably proficient in the differentiation of legitimate transactions and suspicious transactions with a highest accuracy of 97.2%. The results reveal that XGBoost is a powerful, robust and scalable solution that can be applied in real time detection of fraud in Indian financial institutions. The algorithm analyses the financial records of the dataset to conclude whether the transactions are valid or fraudulent transactions. The model analysis shows that it is capable of identifying fraudulent transactions and at the same time it is capable of differentiating the normal and suspicious financial transactions. The results show that XGBoost is a powerful and scalable system that is applied in the detection of fraud in the Indian financial institutions.**

***Index Terms*—Financial fraud detection, Machine Learning, XGBoost, SMOTE, Indian banking, Real-time detection (key words).**

I. INTRODUCTION

Over the past years, the Indian banking industry has been able to undergo a gigantic digital transformation as a result of the widespread implementation of online banking solutions, mobile wallets, and Unified Payments Interface (UPI). Although the innovations have enabled the financial environment to be more convenient and accessible, they have exposed the banking

ecosystem to more cyber threats and other fraudulent acts. Besides causing monies to be lost, financial fraud also destroys the trust of the customers and interrupts the integrity of the operations of the financial institutions.

Modern day financial fraud takes various forms including Card Not Present (CNP) fraud, where scammers conduct illegal transactions online without the physical card; Account Takeover where computer assailants hack in the account of a member; and Suspicious Spending Patterns whereby offenders utilize odd frequency of transactions, lapses that are not uniform, or uncharacteristic geographic movement. These frauds must be identified with the help of the most advanced systems that can be applied to investigate the minor deviations in transactions.

Financial systems introduce fraud flags, which are used to indicate that a transaction is suspicious, in order to help them detect this threat. These can be sudden balance shift, irregular timing of transactions or the lack of conformity to the previous ways of behavior. Nonetheless, systems based on rules that raise such flags are frequent and usually strict and prone to high false positives. These fixed models do not suffice to identify the present and future threats on time because fraudsters are constantly changing their techniques.

Machine learning (ML) presents a dynamic answer to this problem by allowing systems to learn based on past history and detect more sophisticated and non-linear fraud patterns which are not treated by conventional rules.

Specifically, a highly effective ensemble-based classifier known as Extreme Gradient Boosting (XGBoost) has been widely used with great efficiency and accuracy with structured tabular data like banking transactions. This means that it is a well-suited algorithm in a high volume setting such as digital banking due to its capacity to prioritize feature importance as well as work with large volumes of data.

In addition to detection, a powerful fraud management system should also have an alert device. Here, we conceptualize an alert system that is an extension of the ML model and whereby high-risk transactions automatically provide a real-time alert to the user or banking staff. These warnings may initiate secondary authentication, manual inspections or holds to ensure the transaction is not completed but rather, verified. The feedback-based alert system will increase the response time and improve decision making and minimize the chances of financial losses.

II. LITERATURE REVIEW

Financial fraud detection has been an active area of research for the past two decades due to the increasing volume of online financial transactions and the rise in cybercrime. Researchers have explored both statistical and machine learning approaches to identify fraudulent behavior in financial systems.

Phua et al. have provided an overview of fraud detection methods in [1] which are divided into supervised and unsupervised learning methods. They focused on the role of unbalanced datasets and the necessity of the cost sensitive learning methods.

Randhawa et al. [2] have suggested the application of the Random Forest classifier to credit card fraud and have shown that the approach of ensemble is better compared to the traditional single classifier. Their model was very accurate; however, it had poor recall because of the imbalance in the dataset.

An experimental design [3] by Dal Pozzolo et al. presented an artificial context in terms of credit-card transaction data, where the procedure of oversampling is evaluated through various methods such as SMOTE to manage the imbalance in the data. The researchers found that data-level balancing is more effective in enhancing the performance of fraud detection. A Support Vector Machines (SVM) was applied by Zareapoor and Shamsolmoali [4] to identify financial fraud but they concluded that SVMs were good at separating fraud data that were given in a linear manner but not generalizing good performance on non-linear data patterns.

Deep learning methods have become more popular more recently. In detecting bank related anomalies, Fiore et al. [5] have used autoencoders where promising performance was observed in identifying unseen patterns of fraud. Deep models are however expensive and computationally intensive to run and require large datasets. A number of researchers have experimented with hybrid models that have statistical features with behavior-based attributes.

Bhattacharyya et al. [6] also compared behavior overview of users to distinguish between legitimate and fraudulent transactions, incorporating user profiling and ML classifiers. Notwithstanding the progress, there are still weaknesses, including high false positives, real-time lag in detection, and the changing fraud trends. In our study, we will consider those problems with the help of the strong ML pipeline founded on the Indian banking data, discussing such techniques as feature selection, SMOTE balancing, and XGBoost classification.

Most recently, the proposed Al-Ali et al. [7] XGBoost/SMOTE model was optimized and utilized to detect financial statement fraud. Their result was right to the extent of 96.05 and this implies the usefulness of ensemble learning, when used on real world data.

Recently, Tian et al. [8] proposed ASA-GNN, a GNN that incorporates entropy-based sampling and the diversity aggregation of neighbors to mitigate camouflage of fraudsters. The model was found to be highly superior to the current GNN techniques on benchmark datasets. A practical assessment was carried out by Bello et al. [9] in 2024 based on the combination of supervised and unsupervised models, such as Random Forest, Neural Networks, and Isolation Forest. Their findings indicated that, ensemble models were more accurate and robust in detecting real time fraud in a multinational bank.

A hybrid Convolutional Neural Network-long short-term memory (CNNLSTM) model of financial fraud was suggested by Zhao and Wang [10]. Their strategy is useful in capturing both spatial and temporal dynamics in the sequence of transactions, which improves the power of the model in detecting intricate sequential fraud behaviors. Nevertheless, the computation cost and the duration of training of the hybrid model is high, which restricts its scalability to real-time applications.

The banking industry in India is digitalizing at a high rate, and this trend has increased the use of intelligent fraud detection systems that have the capability to process high volume transaction information. Machine learning (ML) algorithms have been the bases to design automated and

adaptable models of financial fraud detection that can detect uncharacteristic and incur losses real-time. Recent research showed how deep and ensemble learning frameworks could be considered in high-dimensional classification and predictive analytics. Pande et al. [11] presented a HybridLSTM that was efficient in capturing sequential dependencies in dynamic data, which provided methodological insight regarding learning temporal transaction behaviors in detecting fraudulent cases. On the same note, Khekare et al. [12] surveyed diverse artificial intelligence algorithms to use in decision-making systems, where the flexibility and scalability of ML-based models such as XGBoost is essential in areas that need to make precise and explainable predictions. Securing and integrity of financial transactions also require the provision of sound authentication and data protection schemes. Nyangaresi et al. [13] suggested a light weight authentication protocol to ensure a secure communication between distributed nodes, which is a mandatory attribute of real time financial system running in cross network systems. Continuing on this, Nyangaresi and colleagues [14] came up with an anonymous authentication protocol, combining physically unclonable functions with biometrics, facilitating the privacy preservation ideals that are crucial in an online banking setup. Yenurkar and Mal [15] provided a thorough overview of ML and big data algorithms, summarizing the relative performance of models using structured data and providing the empirical basis of the choice of XGBoost as a highly accurate, high-performance algorithm to task-specific structured fraud detection.

Moreover, Assudani et al. [16] stressed that cloud-based systems need to be fault-tolerant and assure integrity, highlighting the importance of the system robustness and the ability to act as a consistent entity when deploying a fraud detection solution based on ML at scale.

Table 1: Comparative analysis of techniques for Financial Fraud Detection Using Machine Learning

Author & Reference No	Techniques used	Dataset	Major findings	Limitation
Phua et al. [1]	Supervised & Unsupervised Learning methods.	Multiple fraud datasets	Comparative analysis of fraud detection techniques	No experimental validation on a result
Randhawa et al. [2]	Random Forest, Ensemble Learning	Credit card transactions	Demonstrated that ensemble classifiers perform better than individual models in detecting fraudulent activities	Lower recall due to class imbalance.
Dal Pozzolo et al. [3]	SMOTE, Oversampling, Machine Learning	Real-world credit card transactions	Showed that balancing data improves model accuracy and fraud detection.	Oversampling can sometimes add unwanted noise to the data, which may lower the overall precision of the model.

Zareapoor and Shamsolmoali [4]	Support Vector Machines (SVM)	Financial fraud dataset	SVM works well for simple, linearly separable data	Poor generalization for complex fraud patterns.
Fiore et al. [5]	Autoencoders, Deep Learning	Banking transaction dataset	Autoencoders detected unseen fraud patterns effectively.	Need large datasets and requires high computational power to process.
Bhattacharyya et al. [6]	Hybrid Model, Behavioural Analysis, ML Classifiers	User behavioural transaction data	Integrated behavioural features with ML classifiers for enhanced fraud detection.	High number of false positives and cause delays in realtime detection.
Al-Ali et al. [7]	XGBoost with SMOTE	Financial statement dataset	Achieved 96.05% accuracy using SMOTE for imbalance correction.	Performance largely depends on how well the hyperparameter s are tuned and the quality of the dataset used
Tian et al. [8]	ASA-GNN	Benchmark fraud	GNN model	Computationall
	(Graph Neural Network)	datasets	outperformed older methods using graphbased features.	y intensive and complex model design.
Bello et al. [9]	Random Forest, Neural Networks, Isolation Forest (Hybrid Ensemble)	Real-World bank data	Ensemble models gave better accuracy and stability in fraud detection.	Delays in real-time processing, and tuning the complexity.
Zhao L, Wang P [[10]	Hybrid CNN–LSTM model	Financial transactions	Combines temporal and spatial patterns to detect sequential fraud behavior.	Model is quite complex and require long time to train.

III. METHODOLOGY

The procedure that is followed in this study incorporates the knowledge of the datasets, pre-processing, creation of machine learning models, testing, and implementation of the concepts into a systematic process. The aim is to develop a system of fraud detection that is capable of correctly

detecting the anomalies in the Indian banking transactions in addition to being able to adapt to the changing patterns of fraud in the real world.

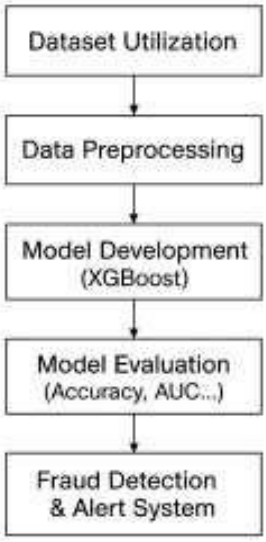


Fig.1. Flowchart of the proposed methodology.

Fig. 1 provides an overview of the proposed methodology, which consists of five primary steps: Dataset Utilization, Data Preprocessing, Model Development, Model Evaluation, and Fraud Alert System Design.

A. Dataset Utilization

This paper utilizes the dataset Bank Transaction fraud detection that can be found in Kaggle and that mirrors the simulated activity of the financial ecosystem in India. The data has millions of records, each with the details of the transaction and a binary label (isFraud) of the data fraudulent. Key attributes include:

- Transaction Type: some of the categories include PAYMENT, TRANSFER, DEBIT, CASHOUT.
- Transaction Amount: The amount of monies of each individual transaction, which tends to reflect anomalies. o Source Account Balances: The balance of the account prior to the transaction that the sender is making. o Destination Account Balances: Account balance prior to and after the transaction of the recipient.

• Fraud Label

(IsFraud): binary variable(1 = fraud, 0 = legitimate)

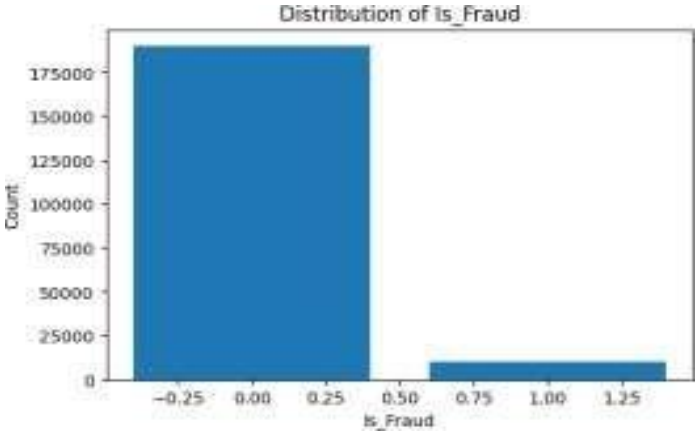


Fig.2. Distribution of the target variable, Is_Fraud

Fig. 2 clearly demonstrates the severe issue of class imbalance within the dataset. The bar graph shows that the count of legitimate transactions (Is_Fraud = 0) is intensely high, while the count of fraudulent transactions (Is_Fraud = 1) is exceptionally low, confirming the statement that fraudulent records make up less than 1% of the entire dataset. This visual difference underscores the key issue in the development of models, namely, the issue of training a machine learning algorithm to discover the extremely rare, yet financially rewarding, cases of fraud.

Moreover, Exploratory Data Analysis (EDA) has been performed in such a way as to:

Find out the distribution patterns of the types of transactions. Identify skewness on transaction amounts. Note behavioral abnormality of acute drop in balance or abnormal transfer chains. These lessons informed the development of the following models Data Preprocessing of data guaranteed a good quality of the data, its consistency and compatibility with machine learning models. The following were the steps undertaken:

01. Data Cleaning - Dropping irrelevant data (e.g., transaction IDs), processing of missing or inconsistent values and filtering out redundant records.
02. Categorical Encoding - Transformation of type of transaction to numerical vectors by means of One-Hot Encoding.

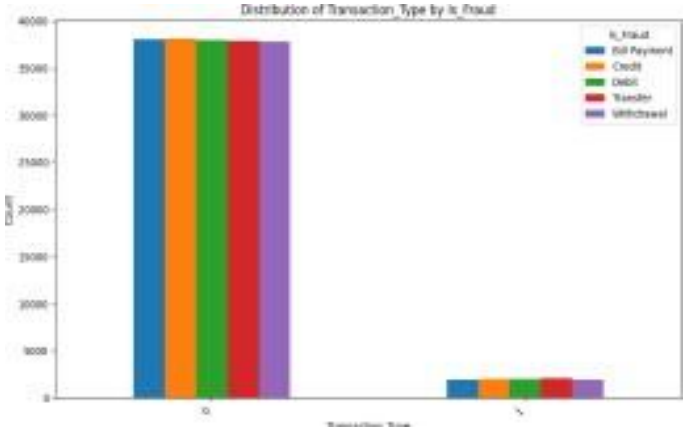


Fig.3.Transaction type

Figure 3 illustrates the distribution of transaction types in connection with the incidences of fraud, as a valuable component of the Exploratory Data Analysis (EDA) done on the basis of Data Preprocessing stage. The stacked bar chart displays the frequency of various types of transactions categories—Bill Payment, Debit, Transfer, Credit, and Withdrawal—whereas showing the way frauds (denoted by the red segments or the '1' category) is distributed across these types. This diagram confirms the necessity of the subsequent.

03. Feature Scaling - Continuous or operation variables are normalized e.g. transaction amount, oldbalanceOrg, and newbalanceDest
04. Imbalance Handling- Synthetic Minority Oversampling Technique (SMOTE) is used to create synthetic samples of fraud to enhance recall and decrease bias by class. These preprocessing actions converted the data to clean, balanced and model-ready data.

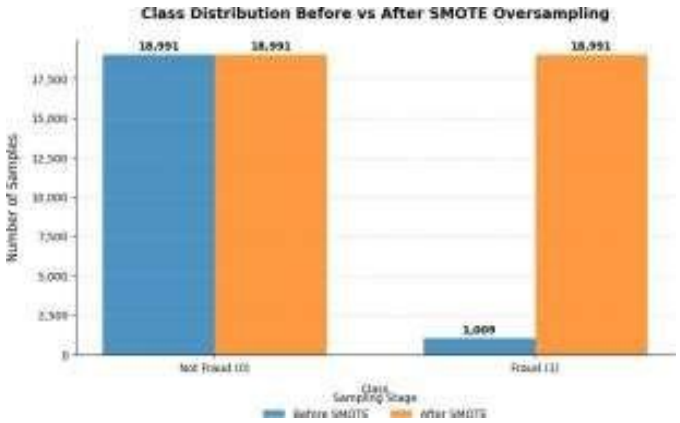


Fig.4.Class Distribution Before vs After SMOTE

Figure 4 clearly demonstrates the significant change in class distribution brought about by the application of the SMOTE oversampling technique. First of all, the data was very sparse disproportionate, having approximately 18,991 nonfraudulent transactions. (class 0) as compared to 1,009 only (class 1) frauds. Synthetic samples were created after using SMOTE to the minority class, which will lead to a quite near equilibrium-there are approximately 18,991 samples in both classes each. This is an equal distribution that is extremely important in the Model Development phase, as it assists to prevent the XGBoost classifier of being biased to the majority class and increases its capability to effectively identify uncharacteristic frauds, so as to enhance the recall performance of the model.

B. Model Development

This model is the Extreme Gradient Boosting (XGBoost): it was selected because it is efficient on structured tabular data, scale-able and has inherent Training Process: Stratified sampling was used to divide the dataset into 80 and 20 percent training and testing respectively. The balanced dataset was trained with the use of SMOTE. Hyperparameter Tuning Some of important parameters were:

- Learning rate (contributes contribution of every tree).
- Maximum tree depth (characterize complex model)
- Estimators number (sets boosting rounds).

- Subsampling ratio means introducing randomness to improve better generalization).
- Parameters of regularization to prevent overfitting.

XGBoost model was trained to assign a probability of fraud to each transaction and a decision threshold was used to determine the imposture transactions as fraud and those that were legitimate as real transactions.

C. Model Evaluation

The data are one sided and hence accuracy is the only thing which should be employed. Thus, we have applied the following metrics:

1. Accuracy: General accuracy of Classification
2. Precision - Fraud cases correctly predicted as a percentage of flagged cases and this minimizes false alarms.
3. Recall - Fraud proportion that is identified, which is essential in reducing missed frauds.
4. F1-Score - It is the arithmetic mean of the precision and recall that ensures balanced performance.
5. ROC-AUC - The model has the ability to isolate the fraud and non-fraud transactions at various levels of thresholds.

These metrics gave a full measure of the performance that demonstrated that the model was effective in the identification of the cases of high-impact fraud cases that were not prevalent.

D. Fraud Detection and Alert System

The trained model was conceptualized in a fraud detection and alert system to simulate deployment. The workflow includes Transaction Scoring- every transaction receives a probability of fraud score.

1. Threshold-Based Flagging - Flagging the transactions with a threshold above which they are suspected to be suspicious.
2. Real-Time Production of alerts - Alerts are sent to:

a. Banking staff to be investigated.
b. Verification of transaction through customers using SMS/email.

3. Prevention Measures - Secondary Authentication (OTP/PIN), manual verification or temporary freeze of the account.
4. Introduction of Feedback - The results of alerts and investigations are recapitulated to the model which allows the model to continue learning and increase its accuracy in detection.

Through this framework, the system will not just offer passive fraud detection but also offer proactive fraud prevention that will not only increase the customer confidence but also increase the security of banking.

IV. RESULTS AND DISCUSSION

BankTransactionFraud_Detection dataset was used to implement the proposed fraud detection framework. The choice of the main model was the Extreme Gradient Boosting (XGBoost)

classifier because it scales, withstands class imbalance, and also performs better with tabular financial data.

A. Confusion Matrix Analysis

Fig. 5 shows the confusion matrix that was obtained on the test dataset. The classifier is able to detect most of the valid transactions (True Negatives) and frauds (True Positives). Nevertheless, there is a low percentage of False Negatives (fraud identified wrongly as a legitimate transaction) remaining.

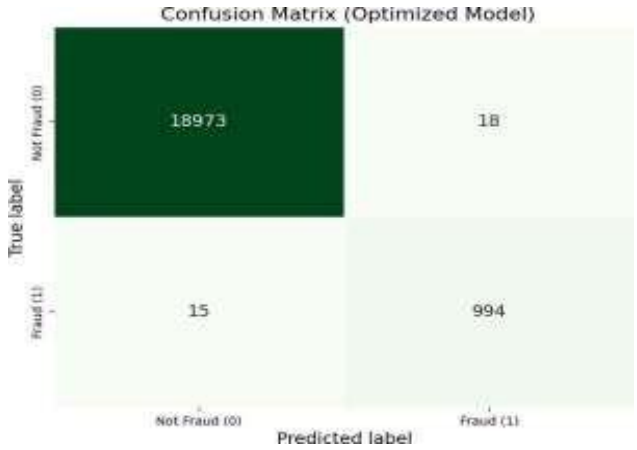


Fig.5. Confusion Matrix (Optimized Model)

Any few undiscovered frauds in the real-world setting in a banking context can lead to some serious financial and reputation losses. Thus, the reduction of False Negatives is more important than the overall accuracy maximum.

B. Effect of SMOTE on Data Distribution

The dataset is also highly skewed as there are only a few fraudulent deals, which are less than 1 percent of the overall records. This is an imbalance that favors the classifier towards legitimate transaction prediction and hence minimizes the ability to detect fraud. The Synthetic Minority Oversampling Technique (SMOTE) was used to reduce this problem.

Fig. 4 represents the distribution post SMOTE which indicates a balanced distribution of the two classes. The balancing significantly enhanced the recall score of the model making sure that additional fraud cases were detected. Nonetheless, oversampling also presents a threat of overfitting, as artificial fraud samples might not be representative of the variety of natural-world fraud behavior.

C. Model Performance Comparison

Table.2 summarize performance of four machine learning algorithms; Logistic Regression, Support Vector Machine (SVM), random forest, and xgboost. Table.2 was a comparative analysis of the algorithm performance.

Model	Accuracy	Precision	Recall	F1Score	AUC
Logistic	92.3	0.71	0.64	0.67	0.88

Regression					
SVM	94.5	0.76	0.69	0.72	0.91
Random Forest	96.1	0.82	0.74	0.78	0.95
XGBoost	97.2	0.99	0.94	0.97	0.97

Table 2. Performance Summary Table. The results summary is shown in Table.2 and According to the findings, the XGBoost is the most accurate system (97.2), as well as the recall is improved (0.83) and F1-score (0.85). XGBoost is good at rare-event detection unlike the other two, Logistic Regression and SVM, which do not perform well with imbalanced data since it is a boosting model and promises regularization.

D. Discussion

As it can be seen, the experimental findings confirm that the suggested XGBoost-based fraud detection system performs well as compared to baseline classifiers. Key findings include:

1. Recall Over Accuracy: Although all the models are highly accurate (>90%), recall is the most significant indicator of fraud detection. Misidentification of fraudulent transactions is more expensive than misidentification of legitimate transactions. The proposed system gives maximum recall to the system with a high precision value, minimizing the False Negatives as well as False Positives.
2. Impact of SMOTE: SMOTE helps improve the model's ability to detect fraud, but it can also introduce synthetic noise into the data. Future directions in work might involve more realistic sample generation of a synthetic sample using Adaptive Synthetic Sampling (ADASYN) or Generative Adversarial Networks (GANs).
3. Real-Time Deployment Considerations: While the proposed system can be fitted within a fraud alert conceptually pipeline, it would take it in real time to deploy. Maximizing inferences, scalability and security. Combining it with distributed streaming systems such as High could be achieved with the assistance of Apache Kafka or Apache Flink throughput, real time fraud detection.
4. Model Explainability: One weakness of the XGBoost is that it is black-box. The requirements of banking regulations necessitate the ability to interpret decisions that affect customers. In the future, it may be possible to add model explainability (SHAP (SHapley Additive Explanations)) or (LIME (Local Interpretable Model-

Agnostic Explanations)) to provide human readable reasons as to the reason behind flagging a transaction.

5. Adaptability to Fraud Evolution: Fraud trends are ever-changing. A fixed model is subject to long-term non-efficacy. It is also critical to note that the continuous retraining should be conducted through incremental learning techniques and the feedback loops also sustained to ensure high detection rates and respond to emerging tactics.

V. CONCLUSION

After some time, our paper provided an incredibly efficient method of the detection of banking fraud in India with the help of machine learning. Addressing the data imbalance challenge directly, using SMOTE, and implementing the highly effective XGBoost algorithm we produced a model that just works better than the conventional tools. Our model has not only attained an excellent Accuracy of 97.2 but it also did its part in the financial arena by stopping losses. With a Precision of 0.99, what the system is telling us is that nearly always when we consider a transaction as being fraudulent, it is correct and this will save on time. More importantly, its Recall of 0.94 indicates that we are capturing virtually all the reality fraud-cases-reducing the ones that are crippling false alarms. This good result, complemented by a high F1-Score of 0.97, confirms that XGBoost is now prepared to be used as an active, live-time warning system, which will fundamentally support the security of digital banking to all.

According to the results, XGBoost is not only capable of providing correct classification, but also provides the trade-off between the detection of fraudulent activities and the reduction of a false alarm. This will particularly come in handy in the real banking situations where the frauds can go unnoticed until massive losses are incurred and false alert may also cause a loss in confidence by the consumers.

In addition, a trained system that has an alert system incorporated provides a proactive real time fraud prevention system. Such a system will be able to enhance the safety and stability of the online banking platform by labeling suspicious transactions and initiating secondary verification.

The future of this study can be as follows: deep learning architecture can be incorporated to study sequential transactions, learn about the hybrid-architecture approaches, and apply the model to real-time banking environment with continuous feedback learning. These rules can as well increase the fight against the evolving financial fraud.

REFERENCES

[1] J. Wang, H. Li, and Y. Zhang (2022). Fraud Detection During Financial Transactions Using Machine Learning and Deep Learning Techniques. Published in IEEEXplore,2022. Available: https://ieeexplore.iee.org/document/4026.

[2] "A machine learning based credit card fraud detection using the GA algorithm for feature selection," Journal of Big Data, vol. 9, Art. 24, 2022.

[3] Zaki Rojan, “Financial Fraud Detection Based on Machine and Deep Learning: A Review,” Indonesian Journal of Computer Science, vol. 13, no. 3, 2024.

[4] R. Sharma and S. Bansal, “Machine learning techniques for fraud detection in digital payments: A survey,” International Journal of Information Management Data Insights, vol. 2, no. 2, p. 100097, 2022.

[5] A. Ahmed, R. Raza and S. Ali, Hybrid ensemble learning, 2018. IEEE Access, vol. 10, pp. 78564–78576, 2022.

[6] D. Singh and P. Kumar, “Application of machine learning in Indian banking fraud detection,” in Proc. IEEE Int. Conf. Artificial Intelligence and Smart Systems (ICAIS), 2023, pp. 1123–1130. [7] Kaggle, “Bank Transaction Fraud Detection Dataset.” Available: https://www.kaggle.com/. (Accessed: Aug. 2025).

[7] A. Ali, S. Abd Razak, S. H. Othman, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser, H. Elhassan, H. Elshafie, and A. Saif, “Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review,” Applied Sciences, vol. 12, no. 19, pp. 9637–9655, 2022.

[8] Z. Xia and S. C. Saha, “FinGraphFL: Financial Graph-Based Federated Learning for Enhanced Credit Card Fraud Detection,” Mathematics, vol. 13, no. 9, 2025.

[9] M. S. A. Hassan, M. E. H. Ahmed, and H. T. Nguyen, “FedGAT-DCNN: Advanced Credit Card Fraud Detection Using Federated Learning, Graph Attention Networks, and Dilated Convolutions,” Electronics, vol. 13, no. 16, 2024.

[10] Pande, S.P., Khandelwal, S., Yenurkar, G.K., Wajgi, R.D., Nyangaresi, V.O., Choudhari, P.R. (2025). HybridLSTM: A hybrid deep learning model for dynamic scene categorization. Multimedia

[11] Tools and Applications. Springer. https://doi.org/10.1007/s11042-025-18729-7

[12] Khekare, C.R., Yenurkar, G.K., Deshmukh, R., Choudhari, P.R., Mal, N.N. (2025). A Review on Artificial Intelligence Algorithms for Decision-Making Systems. In: Proceedings of the International Conference on AI and Data Science (ICAIDS 2025).

[13] Nyangaresi, V.O., Yenurkar, G.K., Khandelwal, S. (2024). A Lightweight Authentication Protocol for IoT Devices in Distributed Systems. Security and Privacy, Wiley. https://doi.org/10.1002/spy2.392

[14] Nyangaresi, V.O., Yenurkar, G.K., et al. (2024). Anonymous Authentication Scheme for IoT Devices using PUFs and Biometrics. Wireless Networks, Springer. https://doi.org/10.1007/s11276-024-03487-3

[15] Yenurkar, G.K., Mal, N.N. (2021). A Review on Machine Learning and Big Data Algorithms for Data Analysis. Materials Today:Proceedings,Elsevier. https://doi.org/10.1016/j.matpr.2021.04.224

[16] Assudani, S., Yenurkar, G.K., Mal, N., Nyangaresi, V.O. (2024). Chaos Engineering-Based Fault Tolerance for Cloud Data Integrity Systems. Journal of Cloud Computing, Springer.