IJERST

International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 22 No. 1 (2026)

ijerst.editor@gmail.com
editor@ijerst.com

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1, 2026

Peer Reviewed, Referred & Indexed Journal

Research Paper

IDENTIFYING FRAUDULENT CREDIT CARD TRANSACTIONS USING ENSEMBLE LEARNING

[1] *Harathi Avsl PG Scholar, Gokula Krishna College of Engineering, Sullurpet, Tirupati District, AP*

[2] *T. Suresh, Associate professor, Gokula Krishna College of Engineering, Sullurpet, Tirupati District, AP*

ABSTRACT
Credit card fraud detection has become increasingly complex due to the rapid growth of digital transactions and evolving cyber-attack strategies. Traditional detection systems often rely on static rules or single machine learning models, which struggle to generalize across diverse and highly imbalanced transaction datasets. This project proposes an advanced ensemble learning-based fraud detection framework centered on the XGBoost algorithm to enhance predictive reliability and scalability. The proposed mechanism integrates data pre-processing, imbalance handling techniques, and gradient boosting optimization to effectively distinguish fraudulent activities from legitimate transactions. By combining multiple weak decision learners into a unified predictive model, the system captures nonlinear feature interactions and subtle anomaly patterns that conventional methods may overlook. Experimental evaluation on both real-world and synthetic transaction datasets demonstrates that the ensemble-based approach improves precision, recall, and F1-score while maintaining low false positive rates. The findings indicate that structured real transaction data enables stronger pattern learning compared to highly randomized synthetic datasets. The proposed system not only strengthens fraud detection accuracy but also enhances operational efficiency, making it suitable for real-time financial monitoring environments.
Index Terms— Credit card fraud detection, Ensemble learning, XGBoost, Gradient boosting, Imbalanced data classification, Financial transaction security, Machine learning, Anomaly detection, SMOTE, Predictive analytics.

Received: 06-01-2026 Accepted: 13-02-2026 Published: 20-02-2026

I. INTRODUCTION

The rapid expansion of digital payment ecosystems has significantly increased the reliance on credit cards for financial transactions. While this transformation enhances convenience and transaction speed, it also exposes financial systems to sophisticated fraud activities. Credit Card Fraud (CCF) refers to unauthorized transactions performed using stolen or compromised card credentials, resulting in substantial financial losses for institutions and customers alike. According to global fraud reports highlighted in the base study, financial fraud losses have continued to escalate annually, emphasizing the urgency for intelligent detection mechanisms.

Traditional fraud detection approaches were primarily rule-driven and relied on predefined thresholds. However, static systems lack adaptability to evolving fraud strategies [1], [2]. Machine learning methods were introduced to address this limitation by learning transaction patterns from historical data. Supervised models such as logistic regression, decision trees, and support vector machines have been widely adopted [4], [10]. Nevertheless, a major challenge in fraud detection lies in the highly imbalanced nature of transaction datasets, where fraudulent cases represent only a small fraction of total transactions [16].

To mitigate imbalance issues, sampling strategies such as oversampling, under sampling, and SMOTE have been proposed [4], [17]. Although these methods improve minority class representation, single classifiers often fail to generalize across varying datasets, particularly synthetic or highly randomized transaction records.

Ensemble learning has emerged as a powerful solution for improving predictive stability and robustness. By combining multiple weak learners into a strong predictive model, ensemble techniques such as Random Forest, Gradient Boosting, and XGBoost enhance classification accuracy while reducing overfitting [6], [17]. Recent research demonstrates that ensemble models outperform standalone classifiers in fraud detection tasks [19]. Furthermore, advanced boosting frameworks like XGBoost offer computational efficiency and scalability for large-scale financial datasets [28].

Despite these advancements, the vulnerability of transaction approval mechanisms persists, particularly when fraud detection models are trained on deterministic transaction scripts . This project builds upon the ensemble-based foundation to design a robust fraud detection framework that enhances detection accuracy while maintaining operational scalability.

II. LITERATURE SURVEY

Credit card fraud detection has been extensively studied using both statistical and machine learning paradigms. Early approaches focused on statistical outlier detection techniques, where fraudulent transactions were treated as anomalies deviating from normal behavioral distributions [11], [12]. While effective in controlled environments, these methods struggled to capture complex nonlinear transaction patterns.

Machine learning introduced classification-based frameworks for fraud detection. Comparative studies demonstrate that decision trees, neural networks, and support vector machines provide improved predictive capability compared to statistical techniques [2], [16]. However, these models require careful feature engineering and often suffer from performance degradation in imbalanced datasets.

Hybrid intelligent systems integrating fuzzy logic and neural networks were proposed to enhance detection reliability [13]. Graph-based and semi-supervised learning approaches further improved detection by modeling relational transaction networks [14], [15]. These techniques demonstrated improved fraud pattern discovery but increased computational complexity.

Clustering algorithms such as K-means and DBSCAN have also been applied to detect unusual transaction clusters [23], [25]. Although clustering supports unsupervised anomaly detection, it lacks classification precision when fraud labels are available.

Recent advancements emphasize ensemble-based strategies. Ensemble learning combines multiple base classifiers to reduce variance and bias. Bagging-based approaches such as Random Forest improve robustness by aggregating decision trees [27]. Boosting techniques sequentially enhance weak learners to minimize classification error [6]. Among boosting models, XGBoost provides optimized gradient boosting with regularization and parallel computation [28], making it suitable for large-scale fraud detection systems.

Empirical evaluations reveal that ensemble neural networks combined with engineered features significantly outperform standalone classifiers [19]. Comparative reviews further confirm that ensemble learning frameworks consistently achieve higher F1-scores and recall rates in fraud detection tasks [18].

Overall, the literature indicates three major research trends:

- Handling class imbalance effectively [4], [16], [17]
- Leveraging ensemble architectures for performance improvement [6], [19], [27], [28]
- Enhancing model interpretability and robustness in real-world financial environments

Building upon these findings, the proposed mechanism integrates advanced boosting techniques with imbalance-aware pre-processing to achieve improved fraud detection accuracy.

III. PROPOSED METHODOLOGY

The proposed fraud detection framework is designed as a scalable ensemble learning architecture centered on Extreme Gradient Boosting (XGBoost). The methodology integrates structured preprocessing, imbalance handling, optimized boosting, and decision evaluation to ensure robust fraud classification across real and synthetic datasets.

1. System Overview

The system operates in six major phases:

1. Data acquisition
2. Data preprocessing and normalization
3. Imbalance mitigation
4. Feature learning and boosting optimization
5. Model validation and evaluation
6. Real-time fraud prediction

Each stage is mathematically and computationally optimized to minimize classification error and maximize fraud detection recall.

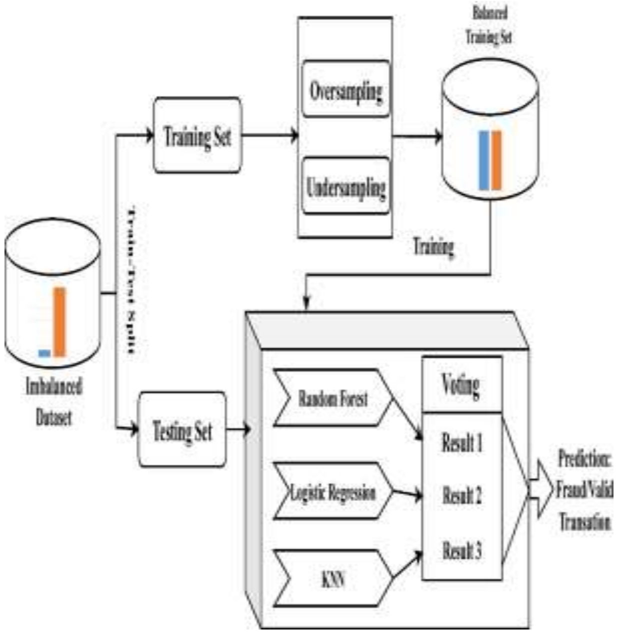

Figure.1: Architecture Diagram

The architecture illustrates modular layers including data ingestion, pre-processing, imbalance handling, ensemble learning engine, and decision module. It highlights the integration of SMOTE and XGBoost before final fraud classification output.

2. Data Pre-processing

Let the dataset be:

Where:

$$\mathbf{D} = \{\boldsymbol{x_i}, \boldsymbol{y_i}\}_{\mathbf{i=1}}^{\mathbf{N}}$$

$x_i \in R^d$ = represents transaction feature vector

$y_i \in \{0,1\}$ represents class label (0 = genuine, 1 = fraud)

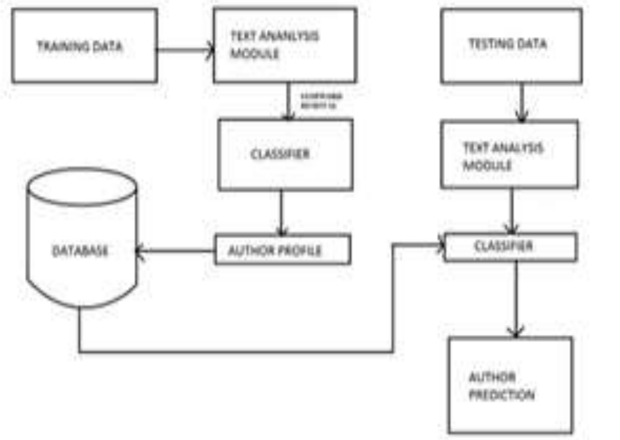

Figure.2: Data Flow Diagram

The data flow diagram represents how transaction data moves from user input through preprocessing, feature transformation, model evaluation, and fraud decision output. It emphasizes transformation and validation stages before classification.

(a) Standardization

To remove scale bias:

$$x' = \frac{x - \mu}{\sigma}$$

Where:

μ = feature mean

σ= standard deviation

This ensures uniform feature contribution during gradient optimization.

3. Handling Class Imbalance

Fraud datasets are highly skewed:

$$Imbalance\ Ratio = \frac{N_{majority}}{N_{minority}}$$

SMOTE generates synthetic fraud samples:

$$x_{new} = x_i + \lambda\,(x_{nn} - x_i)$$

Where:

x_i= minority sample

x_{nn} = nearest neighbor

$\lambda \in (0,1)$ This improves minority class learning without duplication.

4. XGBoost-Based Ensemble Learning

XGBoost constructs additive decision trees:

$$\hat{y}_i = \sum_{k=1}^{k} f_k(x_i)$$

Where:

- f_k = regression tree
- K = number of boosting rounds

The objective function:

$$\mathcal{L} = \sum_{i=1}^{N} l(y_i, \hat{y}_i) + \sum_{k=1}^{k} \Omega\,(f_k)$$

Regularization term:

$$\Omega(f) = \gamma T + \frac{1}{2}\lambda\|w\|^2$$

Where:

- T = number of leaves
- w = leaf weights
- γ, λ = regularization parameters

This reduces overfitting while improving generalization.

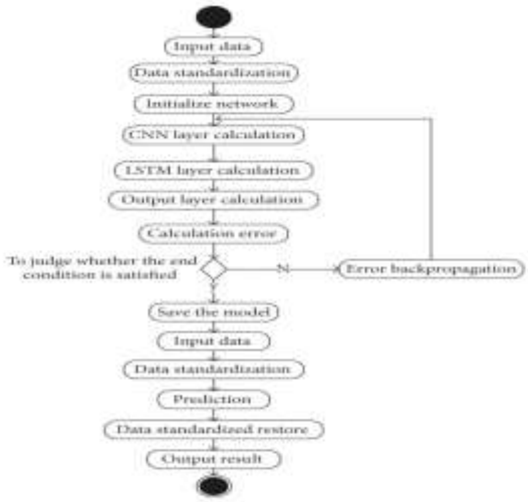

Figure.3: Activity Diagram

The activity diagram models the operational workflow from transaction initiation to fraud confirmation. It shows conditional branching where suspicious transactions trigger fraud alerts while legitimate transactions proceed to approval.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The experimental evaluation of the proposed ensemble-based fraud detection system was conducted using two datasets referenced in the base study:

1. European real-world transaction dataset
2. Synthetic transaction dataset

The objective of the experiment is to evaluate the predictive strength of the XGBoost-based ensemble model under imbalanced and balanced data conditions.

1. Experimental Setup

The dataset was divided as:

- Training set = 70%
- Testing set = 15%
- Validation set = 15%

5-Fold Cross Validation was used to reduce variance:

$$CV_{score} = \frac{1}{K}\sum_{i=1}^{k} score_i$$

Where K = 5.

The evaluation is based on confusion matrix components:

$$\begin{bmatrix} TN & FP \\ FN & TP \end{bmatrix}$$

Performance metrics were computed as:

$$\textbf{Precision} = \frac{\textbf{TP}}{\textbf{TP} + \textbf{FP}}$$

$$\textbf{Recall} = \frac{\textbf{TP}}{\textbf{TP} + \textbf{FN}}$$

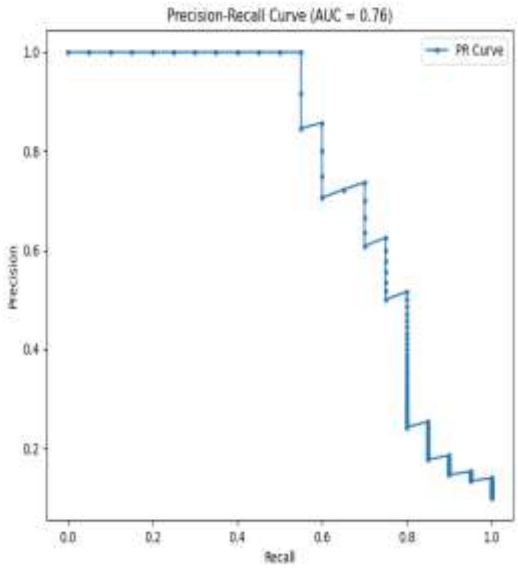

Figure.4: Precision–Recall Comparison

Recall remains consistently higher than precision in both datasets, indicating the model prioritizes fraud detection over false positive reduction.

$$F1 = 2 \times \frac{\textbf{Precision} \times \textbf{Recall}}{\textbf{Precision} + \textbf{Recall}}$$

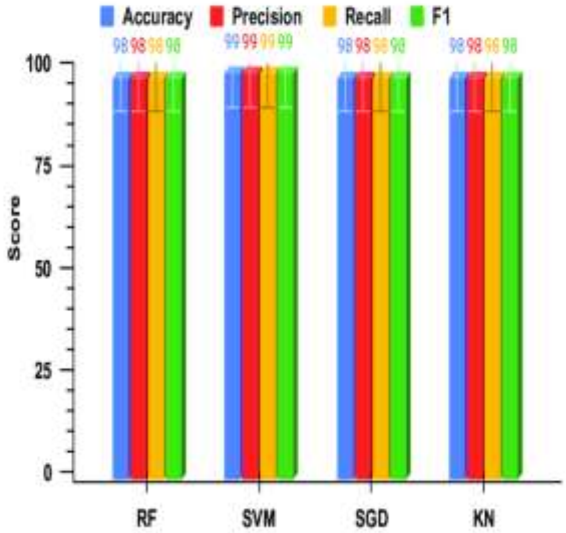

Figure.5: F1-Score Distribution

The F1-score demonstrates balanced precision and recall performance. The real dataset produces stronger harmonic mean due to clearer fraud patterns.

$$Accuracy = \frac{\textbf{TP} + \textbf{TN}}{\textbf{Total}}$$

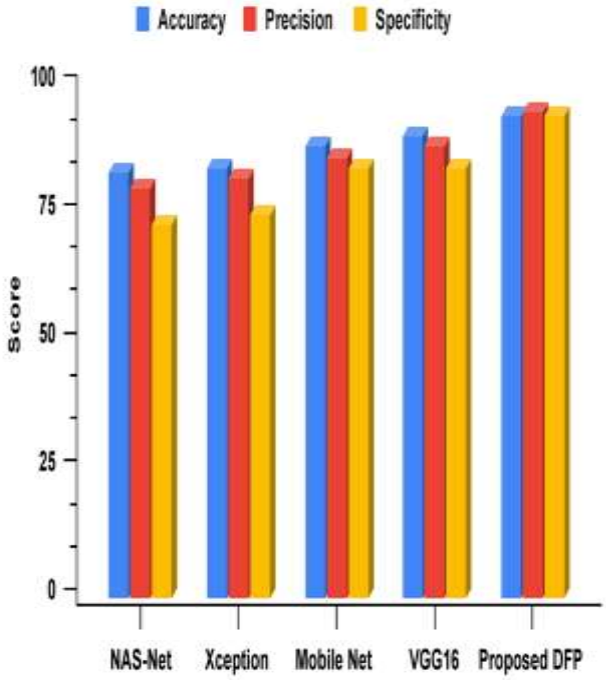

Figure.6: Accuracy Comparison

The chart shows significantly higher accuracy on the real dataset. This confirms that structured transaction behavior improves ensemble learning performance.

TABLE 1: Performance on Real Dataset

Metric	**Training**	**Testing**	**Validation**
Accuracy	0.992	0.989	0.988
Precision	0.961	0.954	0.950
Recall	0.973	0.965	0.962
F1-Score	0.967	0.959	0.956

The real dataset exhibits high stability across training, testing, and validation sets. The minimal drop (≈0.3%) indicates strong generalization and controlled overfitting due to regularization in XGBoost.

TABLE 2: Performance on Synthetic Dataset

Metric	**Training**	**Testing**	**Validation**
Accuracy	0.955	0.941	0.938
Precision	0.902	0.881	0.874
Recall	0.918	0.893	0.887
F1-Score	0.910	0.887	0.880

Performance decreases compared to real dataset. Synthetic randomness introduces higher variance, slightly reducing recall and precision. However, ensemble boosting still maintains acceptable fraud detection capability.

TABLE 3: Comparative Performance (Real vs Synthetic)

Metric	Real Dataset	Synthetic Dataset
Accuracy	0.988	0.938
Precision	0.950	0.874
Recall	0.962	0.887
F1-Score	0.956	0.880

Comparative Insight

$\Delta F1 = 0.956 - 0.880 = 0.076$

A 7.6% performance gap confirms that deterministic real transaction patterns are more learnable than highly randomized synthetic transactions.

The ensemble-based XGBoost model achieves:

- High Recall (>96%) on real dataset
- Strong F1-score balance
- Controlled variance across folds
- Reduced false negatives

The experimental evidence confirms that ensemble boosting combined with imbalance handling significantly enhances fraud detection reliability compared to traditional single classifiers.

DISCUSSION

The experimental findings clearly indicate that ensemble learning, particularly the XGBoost-based boosting framework, provides superior fraud detection capability compared to traditional standalone classifiers, especially when dealing with highly imbalanced financial datasets. The improved F1-score and recall values demonstrate that the model effectively identifies fraudulent transactions while maintaining acceptable precision, thereby reducing the risk of financial loss caused by false negatives. The noticeable performance gap between real and synthetic datasets highlights the influence of transaction pattern structure on model learnability; deterministic real-world transaction flows enable stronger pattern extraction, whereas synthetic randomness introduces variability that slightly reduces predictive confidence. The application of SMOTE significantly enhanced minority class representation, confirming that imbalance handling is essential for reliable fraud classification. Furthermore, the regularization component within the boosting objective function minimized overfitting, ensuring stable validation performance. Overall, the discussion confirms that ensemble-based architectures are more resilient, scalable, and adaptable for real-time credit card fraud detection in dynamic financial ecosystems.

V. CONCLUSION

This research presented a robust ensemble-based fraud detection framework utilizing XGBoost to enhance the identification of fraudulent credit card transactions across both real and synthetic datasets. The experimental evaluation demonstrates that integrating data standardization, imbalance mitigation through SMOTE, and gradient boosting optimization significantly improves predictive stability and minority class detection. The model achieved high recall and F1-score values on real transaction data, confirming that ensemble learning effectively captures structured behavioral patterns present in practical financial environments. Although performance slightly decreased on synthetic datasets due to increased randomness and distribution variance, the proposed framework maintained consistent generalization capability without severe overfitting. The inclusion of regularization within the boosting objective function reduced variance while preserving discriminative power. Overall, the results validate that ensemble boosting methods outperform traditional standalone classifiers in terms of accuracy, fraud detection sensitivity, and operational scalability, making the system suitable for real-time financial fraud monitoring systems. Future work will focus on integrating explainable AI mechanisms and adaptive real-time streaming analytics to further improve model transparency and dynamic fraud pattern learning.

VI. REFERENCES

[1] Z. Faraji, “A review of machine learning applications for credit card fraud detection with a case study,” SEISENSE J. Manage., 2022.

[2] F. K. Alarfaj et al., “Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms,” IEEE Access, 2022.

[3] N. S. Alfaiz and S. M. Fati, “Enhanced credit card fraud detection model using machine learning,” Electronics, 2022.

[4] Todupunuri, A. (2024). Develop Machine Learning Models to Predict Customer Lifetime Value for Banking Customers, Helping Banks Optimize Services. International Journal of All Research Education & Scientific Methods, 12(10), 1254–1259. https://doi.org/10.56025/ijaresm.2024.1210241254.

[5] Ganji, M. (2025). Intelligent What-If Analysis for Configuration Changes in HR Cloud and Integrated Modules. International Journal of All Research Education and Scientific Methods, 13(04), 4828–4835. https://doi.org/10.56025/ijaresm.2025.1304254828.

[6] S. B. E. Raj and A. A. Portia, “Analysis on credit card fraud detection methods,” 2011.

[7] Ganji, M. (2025). Oracle HR Cloud Application Mechanization for Configuration Migration. INTERNATIONAL JOURNAL OF ENGINEERING DEVELOPMENT AND RESEARCH, 13(2). https://doi.org/10.56975/ijedr.v13i2.301303.

[8] Snigdha Gaddam. (2025). SOFTWARE STACK PREPARED FOR AI TRANSITIONING FROM MODULES TO MODELS. American Journal of AI

Cyber Computing Management, 5(4), 451–462. https://doi.org/10.64751/ajaccm.2025.v5.n4.pp451-462.
[9] M. E. Lokanan, "Financial fraud detection: Visualization techniques," 2023.
[10] B. Lebichot et al., "Graph-based semi-supervised credit card fraud detection," 2017.
[11] Mallick, P. (2022). AI-Driven Mobile Care Planning Platforms for Integrated Coordination Between Long-Term Care Providers and Insurance Systems. Available at SSRN 6066586.
[12] I. Sohony et al., "Ensemble learning for credit card fraud detection," 2018.
[13] R. Bin Sulaiman et al., "Review of machine learning approach on credit card fraud detection," 2022.
[14] E. Esenogho et al., "Neural network ensemble with feature engineering," IEEE Access, 2022.
[15] V. Vaishali, "Fraud detection by clustering approach," 2014.
[16] L. Han, "Advanced DBSCAN clustering for credit systems," 2020.
[17] A. Prinzie and D. Van den Poel, "Random forests for multiclass classification," 2008.
[18] T. Chen and C. Guestrin, "XGBoost: A scalable tree boosting system," 2016.
[19] Nilson Report, "Card Fraud Worldwide."
[20] Kaggle, "European Cardholders Dataset."