

# A Cost Sensitive Learning Framework Using Xgboost for Financial Fraud Detection In Imbalanced Datasets

R. Arunadevi<sup>1</sup>, R.A. Amali Priyadharshini<sup>2</sup>, K. Atchaya<sup>3</sup>, B. Jema<sup>4</sup>, B. Sowmiya Navis<sup>5</sup>

<sup>1</sup>Professor, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu - 613 006, India b

Email: [aruna.ap.cse.pits@gmail.com](mailto:aruna.ap.cse.pits@gmail.com)

<sup>2</sup>UG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu - 613 006, India

Email: [amaliputhu19@gmail.com](mailto:amaliputhu19@gmail.com)

<sup>3</sup>UG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu - 613 006, India

Email: [katchaya29122003@gmail.com](mailto:katchaya29122003@gmail.com)

<sup>4</sup>UG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu - 613 006, India

Email: [susijema22@gmail.com](mailto:susijema22@gmail.com)

<sup>5</sup>UG Student, Department of Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur, Tamil Nadu - 613 006, India

Email: [sowmiyanavis@gmail.com](mailto:sowmiyanavis@gmail.com)

## Abstract:

The rapid growth of digital financial transactions has significantly increased the risk of fraudulent activities, making efficient fraud detection systems essential for modern financial institutions. Traditional Machine Learning models often struggle to accurately identify fraudulent transactions due to the class imbalance problem, where fraudulent instances are significantly fewer than legitimate ones. This paper proposes a cost-sensitive learning framework using Extreme Gradient Boosting (XGBoost) for financial fraud detection in imbalanced datasets.

The proposed system incorporates data preprocessing, feature transformation, and cost-sensitive learning techniques to improve the detection of minority fraud cases. By assigning higher misclassification costs to fraudulent transactions, the model enhances its ability to detect fraud while maintaining overall performance. The system also provides real-time prediction through a user-friendly web interface, generating classification results along with a risk score for decision support. Experimental results demonstrate that the proposed approach achieves high accuracy, improved recall, and balanced performance, making it suitable for real-world financial fraud detection applications.

Keywords—Financial Fraud Detection, XGBoost, Cost-Sensitive Learning, Imbalanced Dataset, Machine Learning, Risk Score

## I. INTRODUCTION:

The rapid growth of digital payment systems and online financial services has significantly increased the volume and velocity of financial transactions worldwide. While this transformation enhances operational efficiency and user convenience, it also exposes financial systems to sophisticated fraudulent activities, leading to substantial economic losses for

both individuals and organizations. Detecting fraudulent transactions in real time has therefore become a critical requirement for modern financial institutions. Traditional rule-based fraud detection systems, which rely on predefined patterns, are often insufficient to capture evolving and complex fraud behaviors. As a result, Machine Learning-based approaches have gained prominence due to their ability to learn hidden patterns from large-scale transaction

data and provide automated, adaptive fraud detection solutions.

A major challenge in financial fraud detection is the presence of highly imbalanced datasets, where fraudulent transactions represent only a small minority compared to legitimate ones. This imbalance causes conventional Machine Learning models to be biased toward the majority class, resulting in poor fraud detection performance, particularly in identifying rare but critical fraud instances. To overcome this limitation, advanced techniques such as cost-sensitive learning and ensemble methods have been widely adopted. In this work, a cost-sensitive learning framework based on the XGBoost algorithm is proposed to effectively address the class imbalance problem and improve detection accuracy. The system incorporates data preprocessing, feature transformation, and hyperparameter optimization to enhance model performance. Furthermore, a web-based interface is developed to enable real-time fraud prediction and risk assessment, thereby supporting efficient identification and prevention of suspicious financial transactions.

The proposed framework balances accuracy and efficiency, making it suitable for real-time applications. It also offers a scalable solution adaptable to evolving fraud patterns. Overall, this work enhances reliability in financial fraud detection systems.

## **II. RELATED WORK:**

Masad A. Alrasheedi et al [1] presented a comparative study on Machine Learning models for credit card fraud detection using transaction data. The study evaluates algorithms such as Decision Trees, Random Forest, Support Vector Machines, and Neural Networks to identify fraudulent activities. The authors highlight that ensemble methods provide better accuracy due to their ability to capture complex patterns. They also emphasize the issue of class imbalance and the importance of using appropriate evaluation metrics like precision and recall. The study concludes that model selection and imbalance handling are crucial for improving fraud detection performance.

Nurafni Damanik, Chuan-Ming Liu *et al.* [2] proposed an advanced fraud detection approach using K-SMOTEENN and stacking ensemble techniques to address class imbalance. The study shows that combining resampling methods with ensemble learning improves the detection of minority fraud cases and enhances overall model performance and reliability. Additionally, the authors emphasized that K-SMOTEENN effectively removes noise while generating synthetic samples, leading to better class separation. The stacking ensemble further integrates multiple base learners to capture diverse patterns in transaction data, resulting in improved generalization and reduced overfitting in fraud detection models.

Alamin Talukder *et al.* [3] proposed a multistage ensemble Machine Learning model for detecting fraudulent transactions. The approach combines multiple models in different stages to improve detection accuracy and robustness. The study demonstrates that ensemble strategies enhance the identification of complex fraud patterns and improve performance in imbalanced datasets compared to single-model approaches. Furthermore, the multistage design allows progressive refinement of predictions, where initial models filter obvious cases and subsequent models focus on difficult instances, thereby increasing overall detection efficiency and reducing false positives.

S. S. Suganya *et al.* [4] explored ensemble learning approaches for financial fraud detection, showing that combining multiple models improves accuracy and detection performance compared to individual algorithms. The study highlights the effectiveness of ensemble methods in identifying complex fraud patterns. In addition, the authors discussed the importance of model diversity in ensemble design, where different classifiers contribute unique decision boundaries. This diversity helps in improving robustness and stability, making the system more reliable in real-time financial environments. The results emphasize the importance of advanced learning techniques for reliable fraud detection.

Ebenezer Esenogho *et al.* [5] presented an ensemble of neural network models combined with feature engineering techniques to enhance fraud detection performance. The study shows that extracting meaningful features improves model accuracy and detection capability. It also highlights that ensemble neural networks can better capture complex transaction patterns compared to traditional models. Moreover, the authors emphasized the role of feature selection and transformation in reducing dimensionality and noise, which significantly contributes to improved learning efficiency and faster model convergence. The results demonstrate improved performance in identifying fraudulent transactions compared to traditional approaches.

M. Alojail, S. Bhatia *et al.* [6] proposed an ensemble learning approach for analyzing user behavior in e-commerce systems. The study demonstrates that combining multiple algorithms improves the detection of anomalous and potentially fraudulent activities. It highlights the importance of behavioral patterns in identifying suspicious transactions. Additionally, the authors focused on temporal and sequential user activity analysis, which helps in detecting deviations from normal behavior patterns. This approach improves early fraud detection and enhances system adaptability to evolving user behavior. The results show enhanced accuracy and reliability compared to single-model approaches.

K. H. Ahmed [7] proposed an ensemble-based fraud detection model that combines multiple Machine Learning classifiers to improve the accuracy and reliability of fraud detection. The study introduced a hybrid data sampling technique integrating both oversampling and undersampling methods to effectively handle class imbalance. By balancing the dataset, the proposed approach enhances the detection of

minority fraudulent transactions while maintaining overall performance. Furthermore, the study highlights that hybrid sampling reduces bias toward the majority class and improves recall for fraud cases, while the ensemble model ensures better stability and consistency across different datasets.

K. G. Dastidar [8] presented a comprehensive survey of Machine Learning techniques used in credit card fraud detection, including supervised, unsupervised, and ensemble methods. The author analyzed key challenges such as class imbalance, feature selection, and evolving fraud patterns, and highlighted that ensemble learning and cost-sensitive approaches provide better performance in detecting fraudulent transactions. Furthermore, the study emphasized that traditional models often fail to generalize well on highly skewed datasets, necessitating the use of advanced sampling and adaptive learning techniques. The paper also discussed the importance of real-time fraud detection systems and the integration of data-driven approaches for continuous model improvement. In addition, the author suggested that hybrid models combining multiple techniques can significantly enhance detection accuracy, scalability, and robustness in dynamic financial environments.

### III. PROPOSED METHODOLOGY

The proposed model is a cost-sensitive Machine Learning framework designed to detect fraudulent financial transactions in highly imbalanced datasets. It utilizes the XGBoost algorithm as the core classifier due to its ability to handle large-scale data and capture complex patterns. The model incorporates a cost-sensitive learning approach, where higher misclassification costs are assigned to fraudulent transactions to improve the detection of minority class instances. The framework follows a structured pipeline including data acquisition, preprocessing, feature transformation, dataset partitioning, class imbalance analysis, and model training. Hyperparameter tuning is applied to optimize the XGBoost model for better performance. Finally, the model is evaluated using metrics such as precision, recall, F1-score, and ROC-AUC to ensure effective fraud detection with reduced false negatives. This approach enhances the system's ability to accurately identify fraudulent transactions in real-world financial environments

#### a. System Overview

The proposed system is an end-to-end financial fraud detection framework that uses a cost-sensitive XGBoost model to handle imbalanced transaction data. It begins with data acquisition through manual entry or CSV upload, followed by preprocessing and feature transformation to prepare the dataset. The data is then split using a stratified approach, and the model is trained with cost-sensitive learning and optimized using hyperparameter tuning. The trained model generates probability-based predictions, which are evaluated using metrics such as precision, recall, F1-score, ROC-AUC, and confusion matrix. Finally, the system provides fraud classification results, performance metrics, and reporting support through an integrated web interface, enabling efficient and real-time fraud detection.

#### b. Data Acquisition

Data acquisition is the initial stage of the proposed system, where the financial transaction dataset is collected and loaded for analysis. The dataset includes features such as transaction amount, transaction time, and class labels indicating fraudulent or legitimate transactions. In this project, the data is imported using appropriate processing libraries and subjected to validation checks to ensure consistency, completeness, and correctness. Missing or inconsistent values are identified and handled to maintain data quality. Additionally, the dataset is analyzed to understand the distribution of transactions, particularly the class imbalance between fraudulent and legitimate cases. This step ensures a clean and reliable dataset, forming the foundation for effective model training and fraud detection.

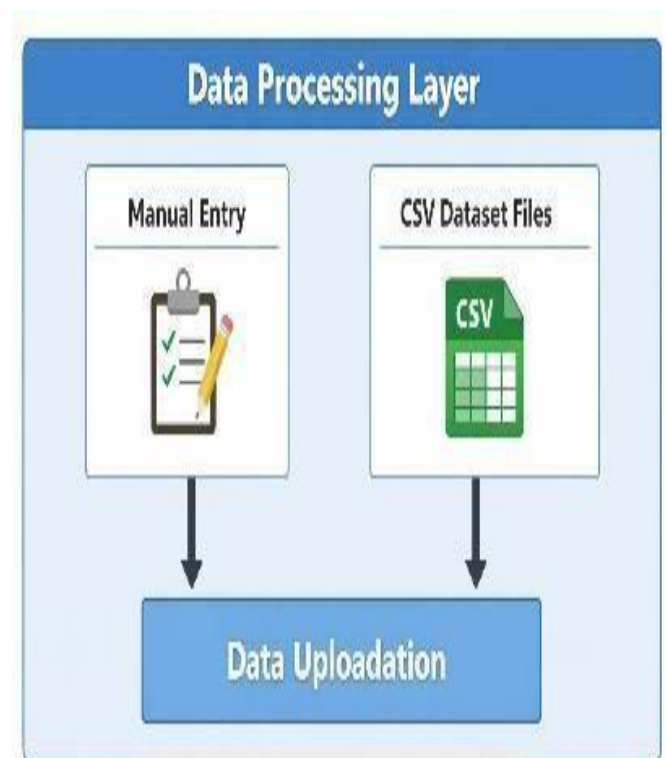


Fig 1. Data Processing Layer

### c. Data Preprocessing Layer

The data preprocessing layer transforms raw transactional data into a clean and structured format suitable for Machine Learning. In this project, essential preprocessing steps such as handling missing values through imputation or removal, eliminating duplicate records, and filtering noisy data are performed to improve data quality. Normalization techniques are applied to ensure uniform feature scaling, and consistency checks are conducted to maintain data integrity across all attributes. These operations reduce data irregularities and prevent bias during model training. Additionally, this stage prepares the dataset for subsequent processes such as class imbalance handling and feature transformation, thereby enhancing the overall reliability and performance of the fraud detection system.

Key operations:

- Missing value imputation or removal
- Duplicate record elimination
- Noise filtering and normalization
- Data consistency verification

This stage reduces data irregularities and enhances model reliability. Preprocessing also prepares the dataset for imbalance handling and feature transformation.

### d. Feature Transformation

The feature engineering and transformation stage improves the quality of the dataset by refining how features are represented. In this project, the process is divided into feature engineering and feature scaling. Feature engineering involves creating meaningful attributes from transaction data to capture behavioral patterns and enhance fraud detection capability. Feature scaling is applied to bring all features into a uniform range using normalization or standardization, ensuring balanced contribution during model training. This step is essential for improving the performance, stability, and convergence of algorithms such as XGBoost. Feature transformation improves the representational power of the dataset by generating meaningful attributes.

Includes:

- Behavioral feature extraction (transaction frequency, spending patterns)

- Feature scaling (standardization / normalization)
- Dimensional consistency

### e. Data Partitioning Strategy

The dataset is divided into training and testing sets in an 80:20 ratio to enable effective model development and evaluation. In this project, a stratified sampling approach is employed to preserve the original class distribution of fraudulent and legitimate transactions in both subsets. This is particularly important for imbalanced datasets, as it prevents bias and ensures that the model learns from a representative distribution of data. The training set is used to build and optimize the model, while the testing set is reserved for evaluating its performance on unseen data. This strategy helps in assessing the model's generalization capability, avoiding overfitting, and ensuring reliable and unbiased performance metrics for fraud detection.

A stratified sampling approach is applied to preserve the original class distribution in both subsets. This is essential for imbalanced datasets, as improper splitting can lead to biased evaluation.

### f. Class Imbalance Analysis

Fraud detection datasets typically exhibit extreme class imbalance, where fraudulent transactions constitute less than 1% of the total data. In this stage, statistical analysis is performed to examine the distribution of classes, along with visualization techniques to clearly represent the imbalance and compute the ratio between fraudulent and legitimate transactions. This analysis helps in understanding the severity of skewness in the dataset. Class imbalance significantly affects classifier performance, as most Machine Learning models tend to be biased toward the majority class, leading to poor detection of minority fraud cases. As the imbalance increases, model performance, particularly in terms of recall and precision for fraudulent transactions, deteriorates. Therefore, this step is essential for identifying the need for advanced techniques such as cost-sensitive learning and resampling methods to improve fraud detection effectiveness.

This stage involves:

- Statistical distribution analysis
- Visualization of class imbalance
- Ratio computation

Imbalance severely affects classifier performance because models tend to favor the majority class.

### g. Cost-Sensitive Learning Mechanism

To overcome imbalance limitations, the proposed model incorporates a cost-sensitive learning strategy, where misclassification costs are explicitly modeled.

Key concept:

- False Negative (fraud missed) → High cost
- False Positive → Lower cost

This is implemented using:

- Class weight calculation:

This parameter adjusts the loss function, forcing the model to focus more on minority fraud cases.

- Research shows that cost-sensitive approaches significantly reduce fraud-related financial losses compared to traditional methods.

#### h. Model Initialization

In this stage, the XGBoost classifier is initialized with appropriate configuration settings to effectively handle the fraud detection problem. The objective function is defined as binary logistic to perform binary classification between fraudulent and legitimate transactions. The evaluation metric is set to ROC-AUC, which provides a reliable measure of model performance, especially for imbalanced datasets. Additionally, a cost-sensitive parameter, *scale\_pos\_weight*, is incorporated to assign higher importance to the minority (fraud) class, thereby improving the model's ability to detect fraudulent transactions.

It is typically calculated as:

$$\text{scale\_pos\_weight} = \frac{\text{Number of Negative Samples}}{\text{Number of Positive Samples}}$$

This weighting mechanism ensures that misclassification of fraudulent transactions is penalized more heavily during training, thereby improving detection performance.

This configuration ensures that the model is properly tuned to address class imbalance and achieve better predictive performance.

XGBoost is selected due to:

1. High scalability
2. Ability to handle structured/tabular data
3. Strong performance in fraud detection tasks

#### i. Hyperparameter Optimization

In this stage, the XGBoost model is fine-tuned to achieve optimal performance by selecting the best combination of hyperparameters. In this project, GridSearchCV with k-fold cross-validation is employed to systematically evaluate multiple parameter combinations and identify the most effective configuration. Key parameters are tuned to control model complexity and learning behavior. The cross-validation process ensures that the model is evaluated on different subsets of the data, improving reliability and reducing variance. This optimization process enhances model robustness, minimizes overfitting, and ensures better generalization when applied to unseen transaction data, thereby improving overall fraud detection performance.

The model is fine-tuned using GridSearchCV with cross-validation, optimizing parameters such as:

- *max\_depth*
- *learning\_rate*

- *n\_estimators*
- *subsample*, *colsample\_bytree*
- regularization parameters

Hyperparameter tuning improves model robustness and prevents overfitting, ensuring better generalization to unseen data.

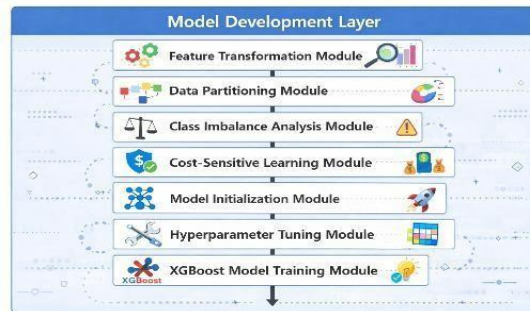


Fig2. Model Development Layer

#### j. Model Training

In this stage, the XGBoost model is trained using the optimized hyperparameters to learn patterns from the transaction dataset. The algorithm employs a gradient boosting framework, where multiple decision trees are built sequentially to improve prediction accuracy. Each iteration focuses on minimizing the loss function by correcting the errors made by previous trees. In this project, cost-sensitive learning is incorporated during training, allowing the model to assign higher importance to fraudulent transactions. This approach enables the model to effectively capture complex and nonlinear relationships within the data, resulting in improved fraud detection performance.

Key Aspects:

- Sequential construction of decision trees using gradient boosting
- Iterative minimization of the loss function to reduce prediction errors
- Incorporation of cost-sensitive weights to handle class imbalance
- Ability to model complex nonlinear patterns in transaction data.

#### k. Prediction Mechanism

In the prediction stage, the trained XGBoost model generates a probability score indicating the likelihood of a transaction being fraudulent. Based on this probability, a decision threshold is applied to classify the transaction. In this project, a threshold value of 0.35 is selected to improve the detection of fraudulent cases. If the predicted probability is greater than or equal to 0.35, the transaction is classified as fraudulent; otherwise, it is classified as legitimate. This threshold is intentionally set lower than the default value to increase the sensitivity of fraud detection, as missing fraudulent transactions can lead to significant financial loss.

**Decision Logic:**

- If probability  $\geq 0.35 \rightarrow$  Fraudulent transaction
- If probability  $< 0.35 \rightarrow$  Legitimate transaction

Threshold tuning plays a crucial role in balancing precision and recall, allowing the model to effectively trade off between false positives and false negatives.

**1. Model Evaluation Metrics**

In this stage, the performance of the trained model is evaluated using metrics that are suitable for imbalanced datasets. Since accuracy can be misleading in fraud detection, multiple evaluation measures are used to provide a comprehensive analysis of model effectiveness. In this project, recall is given higher priority to ensure that fraudulent transactions are correctly identified, thereby reducing financial risk.

**Evaluation Metrics with Formulas:**

- **Precision:** Measures the correctness of predicted fraud cases

$$\text{Precision} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Positives}}$$

- **Recall (Sensitivity):** Measures the ability to detect actual fraud cases

$$\text{Recall} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}}$$

- **F1-Score:** Harmonic mean of precision and recall

$$\text{F1-Score} = \frac{2 \times (\text{Precision} \times \text{Recall})}{\text{Precision} + \text{Recall}}$$

- **ROC-AUC:** Represents the area under the Receiver Operating Characteristic curve, which plots True Positive Rate (TPR) against False Positive Rate (FPR)

$$\text{TPR} = \frac{\text{True Positives}}{\text{True Positives} + \text{False Negatives}}, \text{FPR} = \frac{\text{False Positives}}{\text{False Positives} + \text{True Negatives}}$$

- **Confusion Matrix:** Represents classification outcomes in terms of:
  - **TP (True Positive):** Fraud correctly identified
  - **TN (True Negative):** Legitimate correctly identified
  - **FP (False Positive):** Legitimate classified as fraud
  - **FN (False Negative):** Fraud classified as legitimate

This evaluation framework ensures a detailed and reliable assessment of the model, with a strong emphasis on maximizing fraud detection performance while controlling false alarms.

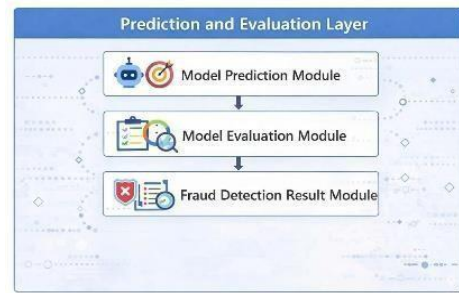


Fig3. Prediction and Evaluation Layer

**m. Result And Deployment**

In the final stage, the trained and evaluated XGBoost model is deployed to generate predictions on new transaction data. The system produces outputs including the classification of transactions as fraudulent or legitimate, along with a corresponding probability score that indicates the risk level of each transaction. Additionally, performance metrics obtained during evaluation are utilized to validate the effectiveness and reliability of the model. In this project, the deployed system is integrated into a web-based interface, enabling users to input transaction details and receive instant predictions.

**System Outputs:**

- Fraud classification (Fraud / Legitimate)
- Probability score indicating fraud risk
- Model performance metrics for validation

**Application Outcomes:**

- Supports real-time fraud detection for incoming transactions
- Enables alert generation for high-risk transactions based on threshold values
- Assists financial institutions in making informed and timely decisions

This deployment ensures that the proposed framework is not only accurate but also practical for real-world financial applications, providing an efficient and scalable solution for fraud detection.

**The final system outputs:**

- Fraud classification
- Probability score
- Performance metrics

**This enables:**

- Real-time fraud detection
- Alert generation
- Decision support for financial institutions

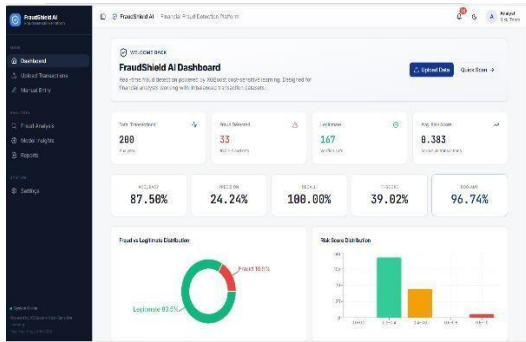


Fig4. Result

#### IV. CONCLUSION

This work presented a financial fraud detection system based on a cost-sensitive XGBoost model to effectively address the class imbalance problem in transaction datasets. The proposed framework incorporates data preprocessing and feature transformation techniques to enhance data quality, followed by model training using cost-sensitive learning to improve the detection of minority fraudulent transactions. By assigning higher importance to fraud instances and optimizing hyperparameters, the model achieves improved recall and balanced classification performance compared to traditional approaches that do not consider data imbalance. Additionally, the use of an optimized decision threshold further enhances the model's ability to detect fraud while maintaining a balance between false positives and false negatives.

The system is implemented using a FastAPI-based backend, enabling real-time fraud prediction through a web-based interface. Comprehensive evaluation using metrics such as precision, recall, F1-score, and ROC-AUC demonstrates the effectiveness and reliability of the proposed approach. Overall, the framework provides a scalable and practical solution for detecting fraudulent activities in imbalanced financial datasets, supporting efficient decision-making in real-world applications. Future enhancements can include integration of advanced models, real-time data streaming, and adaptive learning techniques to further improve system performance and robustness.

#### ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to their project guide and faculty members of the Department of Computer Science and Engineering for their continuous support, valuable guidance, and encouragement throughout this research work.

The authors also extend their thanks to their external guide, Mr. Boopathy Pandi, from Monzha Research Labs-Cochin for providing valuable insights, technical guidance and necessary resources that contributed to the successful completion of this work.

Additionally, the authors acknowledge the use of publicly available datasets and tools that supported the development and evaluation of the proposed system.

#### REFERENCES

- [1] M. A. Alrasheedi, —Enhancing Fraud Detection in Credit Card Transactions: A Comparative Study of Machine Learning Models, *Computational Economics*, pp. 1–20, 2025.
- [2] N. Damanik and C.-M. Liu, —Advanced Fraud Detection: Leveraging K-SMOTEENN and Stacking Ensemble, *IEEE Access*, vol. 13, pp. 10358–10365, 2025.
- [3] Md. Alamin Talukder, Majdi Khalid, and Md. Ashraf Uddin, —An Integrated Multistage Ensemble Machine Learning Model for Fraudulent Transaction Detection, *Journal of Big Data*, vol. 11, Article 168, pp. 1–25, 2024.
- [4] S. S. Suganya *et al.*, —Ensemble Learning Approaches for Fraud Detection in Financial Transactions, *Proceedings of the IEEE International Conference*, pp. 1–6, 2023.
- [5] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, —A Neural Network Ensemble With Feature Engineering for Improved Credit Card Fraud Detection, *IEEE Access*, vol. 10, pp. 16400–16407, 2022.
- [6] M. Alojail and S. Bhatia, —Novel Technique for Behavioral Analytics Using Ensemble Learning Algorithms in E-Commerce, *IEEE Access*, vol. 8, pp. 150072–150080, 2020.
- [7] K. H. Ahmed, S. Axelsson, Y. Li, and A. M. Sagheer, —A credit card fraud detection approach based on ensemble Machine Learning classifier with hybrid data sampling, *Machine Learning with Applications*, vol. 20, pp. 100675, 2025.
- [8] K. G. Dastidar, O. Caelen and M. Granitzer, —Machine Learning Methods for Credit Card Fraud Detection: A Survey, *IEEE Access*, vol. 12, pp. 158939–158951, 2024.
- [9] D. Mienye, Y. Sun and Z. Wang, —Improved Credit Card Fraud Detection Based on Ensemble Learning, *IEEE Access*, vol. 8, pp. 142048–142058, 2020.
- [10] R. Bin Sulaiman, V. Schetinin, and P. Sant, —Review of Machine Learning Approach on Credit Card Fraud Detection, *Human-Centric Intelligent Systems*, vol. 2, no. 1–2, pp. 55–68, 2022
- [11] E. Ileberi, Y. Sun, and Z. Wang, —A Machine Learning Based Credit Card Fraud Detection using Genetic Algorithm, *Journal of Big Data*, vol. 9, Article 73, pp. 1–21, 2022.
- [12] R. Sailusha, V. Gnaneswar, R. Ramesh, and G. R. Rao, —Credit Card Fraud Detection Using Machine Learning, *Proceedings of the International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 1264–1270, 2020
- [13] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, —Credit Card Fraud Detection – Machine Learning Methods, *Proceedings of the 18th International Symposium INFOTEH-JAHORINA*, IEEE, pp. 1–6, 2019.
- [14] A. K. Singh, R. Kumar, and S. K. Singh, —Fraud Detection in Banking Transactions Using Machine Learning, *Proceedings of the International Conference on*

Data Science and Engineering, Springer, pp. 210–220, 2022

[15] J. Jemai, A. Zarrad and A. Daud, —Identifying Fraudulent Credit Card Transactions Using Ensemble Learning,| IEEE Access, vol. 12, pp. 1–15, 2024.

[16] R. Chhabra, S. Goswami and R. K. Ranjan, —A voting ensemble machine learning based credit card fraud detection using highly imbalanced data,| Multimedia Tools and Applications, vol. 83, no. 18, pp. 54729–54753, 2024.

[17] X. Feng and S.-K. Kim, —Novel Machine Learning Based Credit Card Fraud Detection Systems,| Mathematics, vol. 12, no. 12, pp. 1–20, 2024.