AI-Based Credit Card Fraud Detection System Using Machine Learning

Dr. Pushpa Ravikumar[1]; Gowrav A. S.[2];
Dr. Arpitha C. N.[3]; Dr. Anser Pasha C. A.[4]

[1]Professor & Head, Department of CS&E, Adichunchanagiri Institute of Technology, Chickmagaluru-577102
[2]PG Student, Department of CS&E, Adichunchanagiri Institute of Technology, Chickmagaluru-577102
[3]Assistant Professor, Department of CS&E, Adichunchanagiri Institute of Technology, Chickmagaluru-577102
[4]Assistant Professor, Department of CS&E, Adichunchanagiri Institute of Technology, Chickmagaluru-577102

Publication Date: 2026/07/16

Abstract: The rapid growth of digital banking, online transactions, and the electronic payment of the systems has been significantly increased the use of credit cards, results in the parallel rise in fraudulent activities. Traditional methods of detecting the fraud are often unable to handle large-scale transaction data and evolving fraud patterns efficiently. This paper presents an AI-Based Credit Card Fraud Detection System using Machine Learning to identify suspicious transactions accurately and in the real time. To identify patterns and detect potential fraud, the proposed system analyzes past transaction data containing various transaction-related attributes amount, merchant details, category, time, and customer information. Data preprocessing techniques including K-Nearest Neighbor (KNN) imputation are applied to handle missing values, followed by label encoding and Z-score normalization to improve data quality and consistency. Feature engineering is performed to extract meaningful transaction patterns. The processed data is then classified using the XGBoost algorithm, which improves prediction accuracy through sequential learning and optimized decision trees. Experimental evaluation is carried out using a credit card transaction dataset containing legitimate and fraudulent records.

Keywords: *Machine Learning, XGBoost, Credit Card Fraud Detection, K-Nearest Neighbor (KNN),Fraud Classification.*

How to Cite: Dr. Pushpa Ravikumar; Gowrav A. S.; Dr. Arpitha C. N.; Dr. Anser Pasha C. A. (2026) AI-Based Credit Card Fraud Detection System Using Machine Learning. *International Journal of Innovative Science and Research Technology,* 11(6), 3521-3528. https://doi.org/10.38124/ijisrt/26jun1943

I. INTRODUCTION

The increasing use of digital payments and online banking has increased the using the credit cards, leading to more fraudulent transactions. Existing fraud detection methods are often unable to efficiently detect modern and complex fraud patterns due to large transaction volumes and changing user behavior.Advances in AI and Machine Learning provide an effective solution by analyzing history of transaction data and identifying suspicious activities automatically. Machine learning models are improved in detecting accuracy and support real-time decision making. This paper presents an AI-Based Credit Card Fraud Detection System by Using the Machine Learning algorithms to classify the transactions as legitimate or fraudulent. The proposed system applies preprocessing techniques used such as K-Nearest Neighbor (KNN), label encoding, feature engineering, and Z-score normalization. The processed data is classified using the XGBoost algorithm is used improve the fraud detecting accuracy and reduce financial losses. The system aims to enhance transaction security, minimize false alerts, and support secure digital payment environments.

II. RELATED WORKS

The Credit card fraud detection has become an important research area due to rapid increase in digital transactions and financial cybercrime. Several researchers have been proposed to the Machine Learning and Deep Learning techniques to improve fraud detection accuracy and reduce financial losses. Lucas and Jurgovsky (2020) presented a comprehensive survey on machine learning-based fraud detection methods and discussed the challenges of handling highly imbalanced transaction datasets. Their work highlighted the importance of selecting suitable classification techniques for effective fraud identification. Gorte, Mohod, and Keole (2023) reviewed

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1943

different Machine Learning and the Deep Learning approaches and compared their performance while detecting the fraud transactions The study is showed that the advanced learning models are used to improve the prediction capability and reduce false detection rates. Ghosh Dastidar, Caelen, and Granitzer (2024) investigated recent developments in fraud detection and emphasized the advantages of ensembleing the learning methods to handle large-scale transaction data. Naik and Dahale (2024) developed a practical machine learning-based fraud detection framework focusing on real-time implementation and transaction monitoring. Verma and Dhar (2024) proposed a deep learning-based approach that demonstrated improved fraud classifies the performance to compare with the traditional methods. Kokate and Chettyi (2025) introduced an SVM-RBF-based fraud detection model and reported effective identification of suspicious transaction behavior.

III. METHODOLOGY

The proposed AI-Based Credit Card Fraud Detection System Using Machine Learning follows a structured workflow to identify fraudulent transactions accurately and efficiently. The methodology consists of collecting the data, preprocessing, feature engineering, model training, and performance evaluation. Initially, the credit card transactions datasets is collected from historical transaction records containing both the legitimate and fraud transactions. The datasets includes attributes such as transaction time, credit card number, merchant details, transaction category, amount, customer information, and fraud labels. Figure 1 shows architecture diagram for Credit Card Fraud Detection System Using Machine Learning.

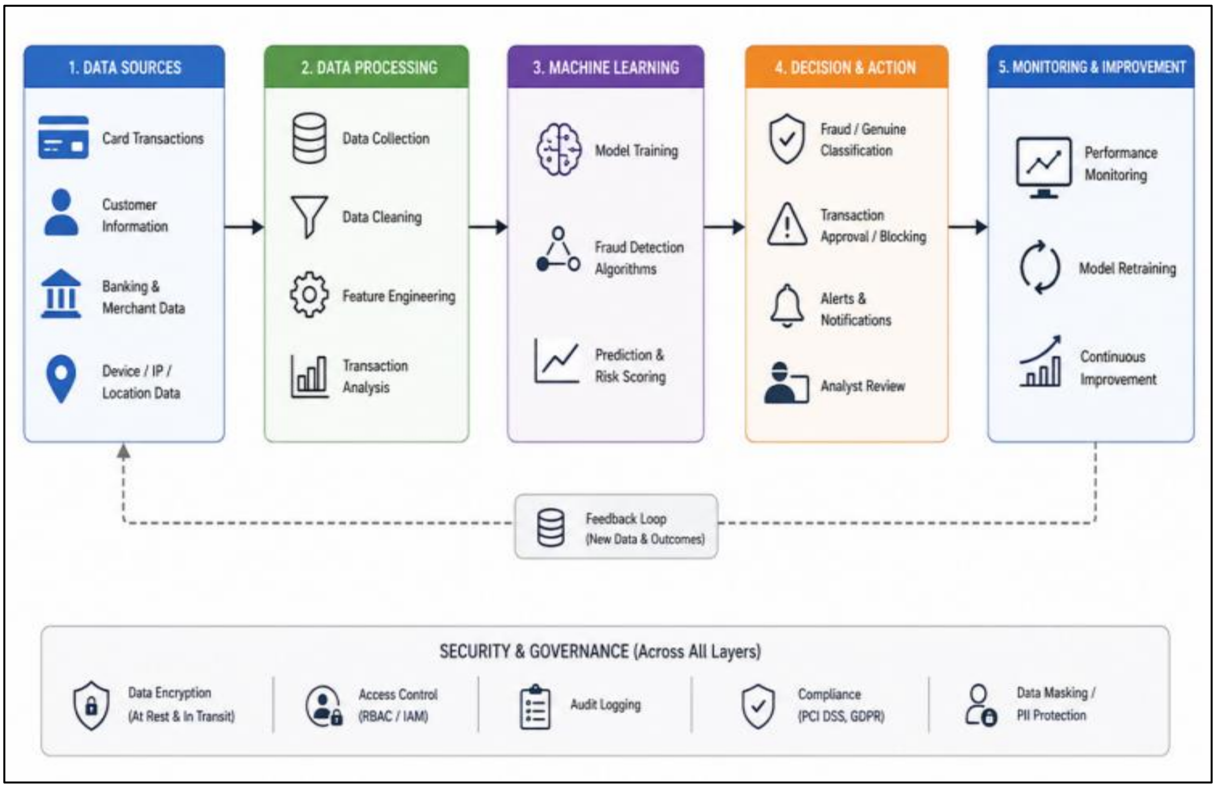

Fig 1 Architecture Diagram for Credit Card Fraud Detection System Using Machine Learning

➢ *Dataset Description*

The proposed AI-Based Credit Card Fraud Detection System Using Machine Learning uses a Credit Card Fraud Detecting Datasets collected from European cardholders' transaction records. The dataset is contained both normal (legitimate) and suspicious (fraudulent) transactions and is used to train and to evaluate the machine learning models for fraud detection.

➢ *Model Training (XGBoost)*

The Model Training phase uses the XGBoost (Extreme Gradient Boosting) algorithm to classify the credit card transactions are normal or fraudulent. After preprocessing the dataset through data cleaning process, label encoding, feature engineering, and normalization, selected features such as Amount, Amount_norm, Category_enc, and Gender_enc are provided as input to the model. XGBoost trains by building the multiple decision trees sequentially, they form each new tree corrects the errors made by previous trees using gradient and hessian calculations. The model starts with an initial prediction value and continuously updates predictions using leaf weights and gain calculations to improve classification performance. Finally, transactions with prediction values greater than 0.5 are classified as Fraud (1) and values less than 0.5 are classified as Normal (0), enabling accurate and efficient fraud detection.

➢ *Detection and Prediction*

The Detection and Prediction process identifies whether a credit card transaction is normal or fraudulent using Machine Learning. After preprocessing the transaction data using KNN,

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1943

label encoding, feature engineering, and Z-score normalization, the datas are given to the XGBoost model for analysis. The model evaluates transaction patterns and predicts fraud probability. If the prediction value is greater than 0.5, the transaction is classified as Fraud (1); otherwise, it is classified as Normal (0).

➢ *Data Pre-Processing*

The Data Pre-processing stage prepares the credit card transaction datasets before training machine learning model. Initially, the missing values are handled by using the KNN (K-Nearest Neighbors) imputation technique to improve data quality. Then, categorical attributes such as Gender and Transaction Category are converted to the numerical values using Label Encoding. After encoding, Feature Engineering is applied to extract useful fraud-related information from transaction patterns. Finally, Z-score Normalization is performed to scale numerical values such as transaction amount into a common range, which will improves the model performance and prediction accuracy. The processed datasets are used as input for the XGBoost model to detect the fraud transactions efficiently.

➢ *Model Performance Evaluation*

The Model Performance Evaluation phase measures how effectively the XGBoost model detects fraudulent credit card transactions.

- *Model is Evaluated with:*

✓ Accuracy: It Measures overall correctness of predictions.

$$Accuracy = \frac{TP}{TP+TN+FP+FN} \tag{1}$$

✓ Precision: Measures how many transactions predicted as fraud were actually fraudulent.

$$Precision = \frac{TP}{TP+FP} \tag{2}$$

✓ Recall: Measures how many actual fraudulent transactions are correctly used to identify the model.

$$Recall = \frac{TP}{TP+FN} \tag{3}$$

✓ F1-Score: Measures the balance between the Precision and the Recall to evaluate the overall fraud detection performance of the model.

$$F1 - Score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \tag{4}$$

IV. RESULTS

The proposed AI-Based Credit Card Fraud Detecting System using XGBoost successfully identified fraudulent and normal credit card transactions with good classification performance. After applying the data preprocessing techniques such as KNN imputation, label encoding, feature engineering, and Z-score normalization, the trained model analyzed transaction patterns and generated prediction results.

➢ *Quantitative Performance Evaluation*

The Quantitative Performance Evaluation measures the main effectiveness of the proposed XGBoost-based Credit Card Fraud Detecting System using standard classification metrics.

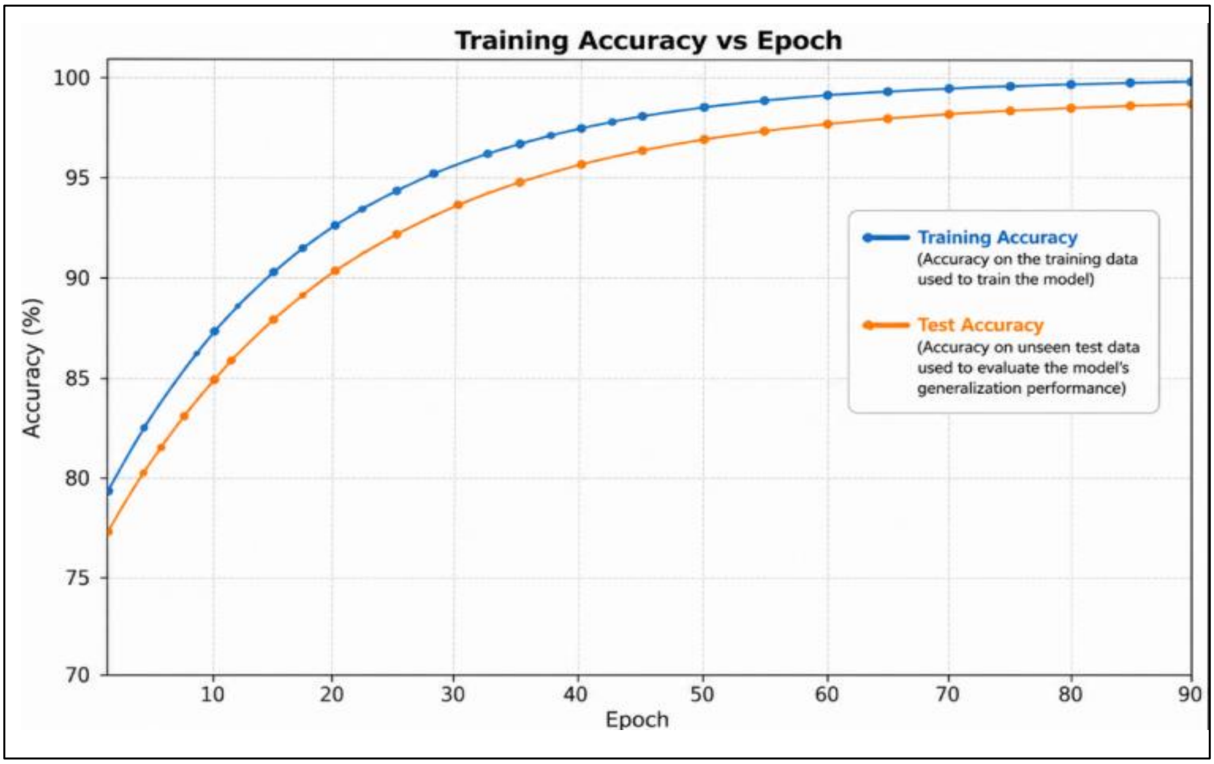

Fig 2 Accuracy Curve

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1943

The Figure 2 shows the training and test accuracy across different epochs for the Credit Card Fraud Detecting model. The blue line will represents the training accuracy, while the orange line represents test accuracy on unseen data. Since both lines increase and remain close to each other, it indicates high model performance (99.74%) with good generalization and minimal overfitting.

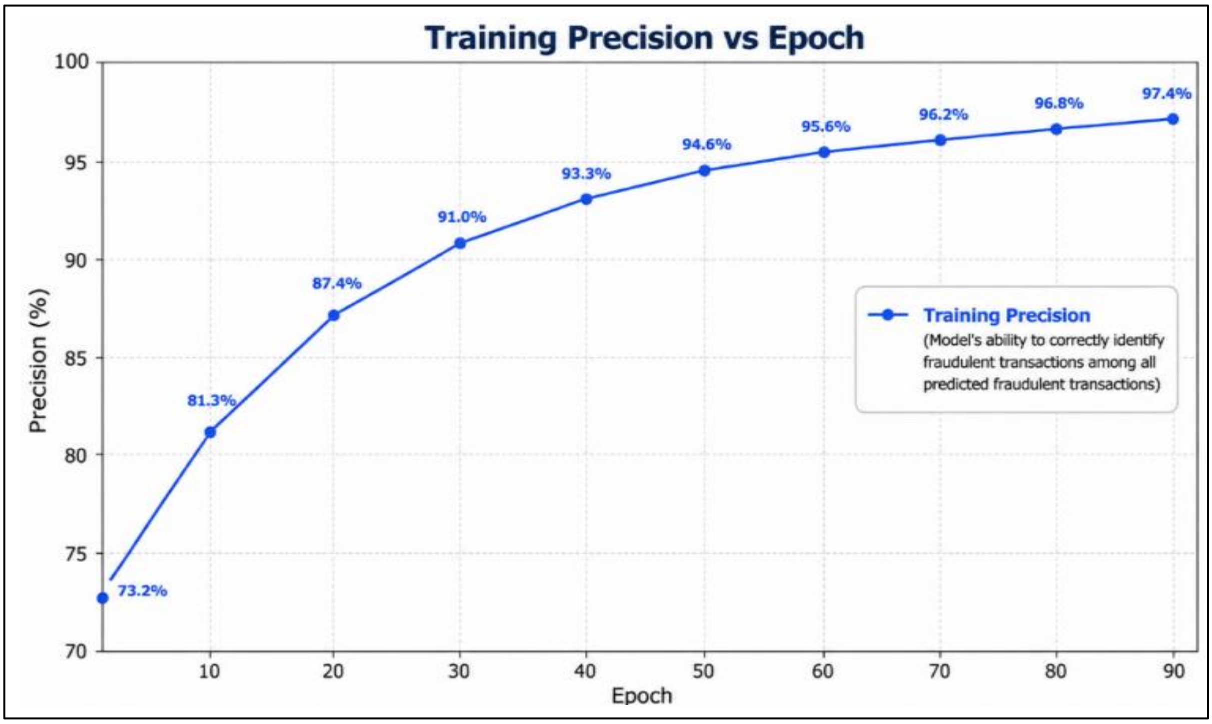

Fig 3 Precision Curve

The Figure 3 shows the training precision improving across 90 epochs, indicating that the model becomes more accurate in identifying fraudulent transactions over time. Precision gradually increases and stabilizes near 97.4%, showing the model producing the fewer false positive and achieves reliable fraud detection performance.

The Figure 4 shows how the model's ability is used to correctly identify fraudulent transactions improves during training over 90 boosting rounds (epochs). The Training Recall (solid red line) increases steadily and reaches a higher value than the Validation Recall (dashed red line), indicating better learning on training data.

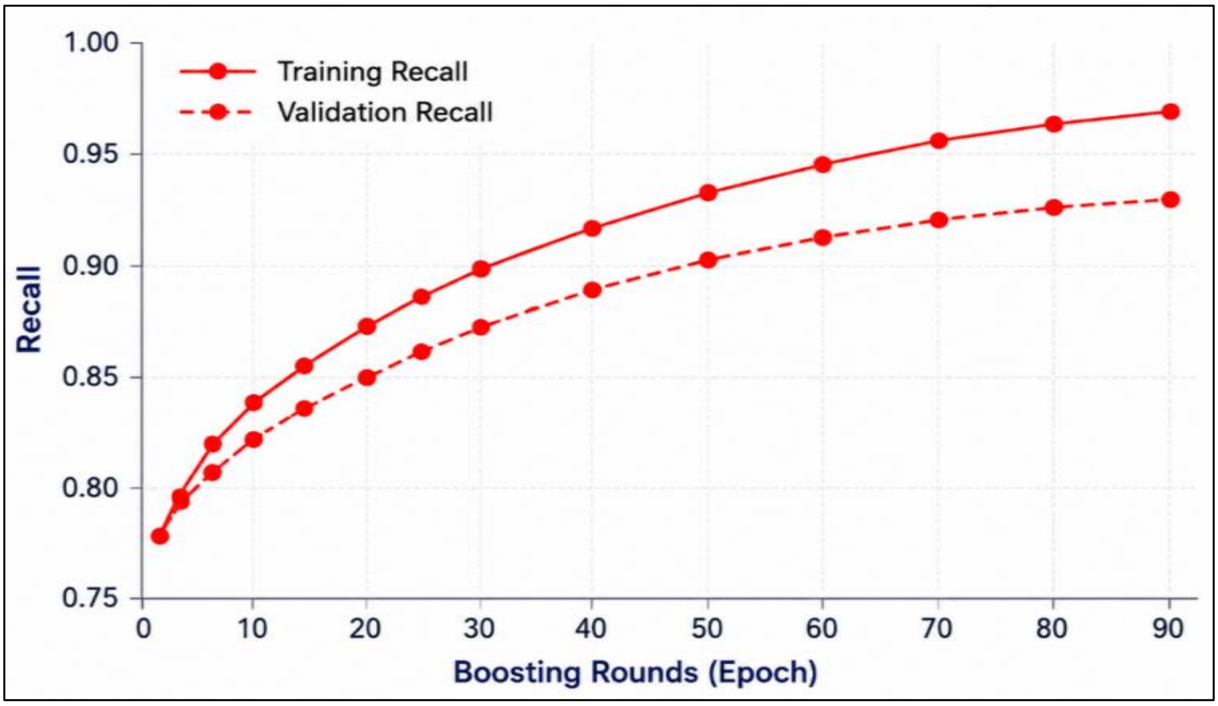

Fig 4 Recall Curve

The Figure 5 shows how the overall effectiveness of the XGBoost model improves over 90 boosting rounds (epochs) by balancing both Precision and Recall. The Training F1-Score (solid purple line) increases continuously and remains slightly higher than the Validation F1-Score (dashed purple line).

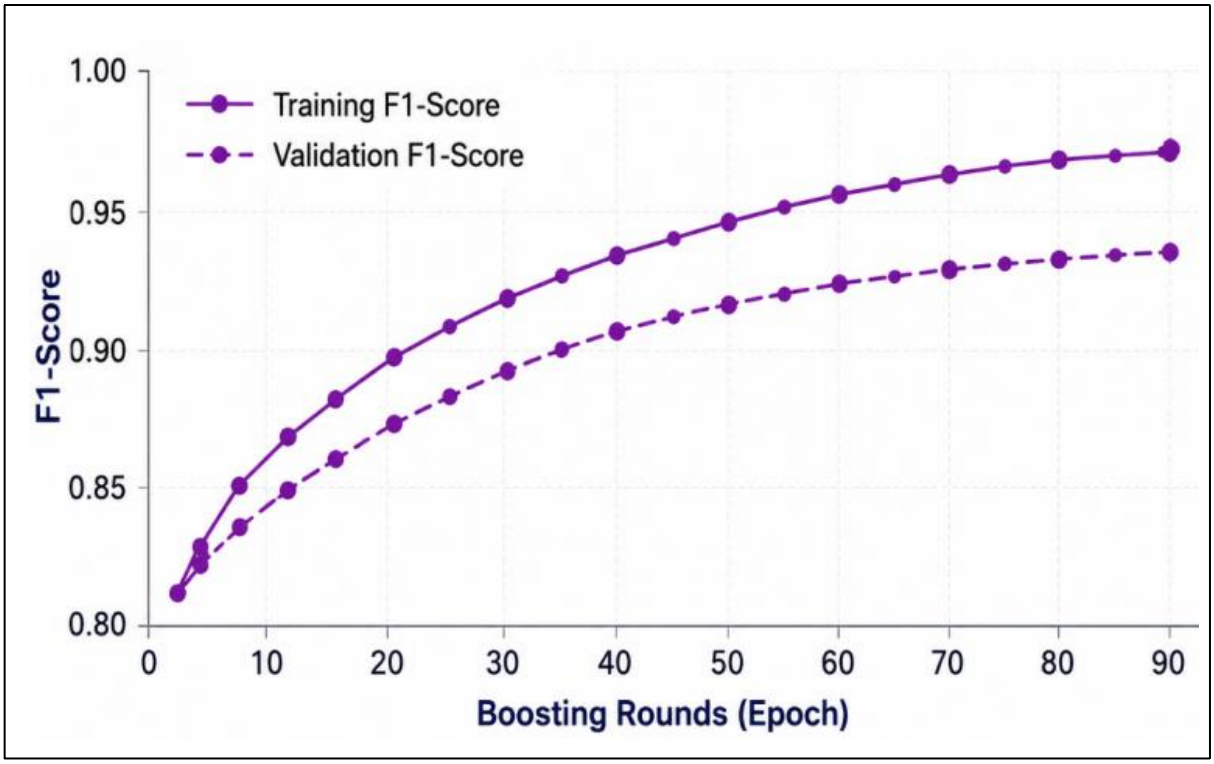

Fig 5 F1-Score curve

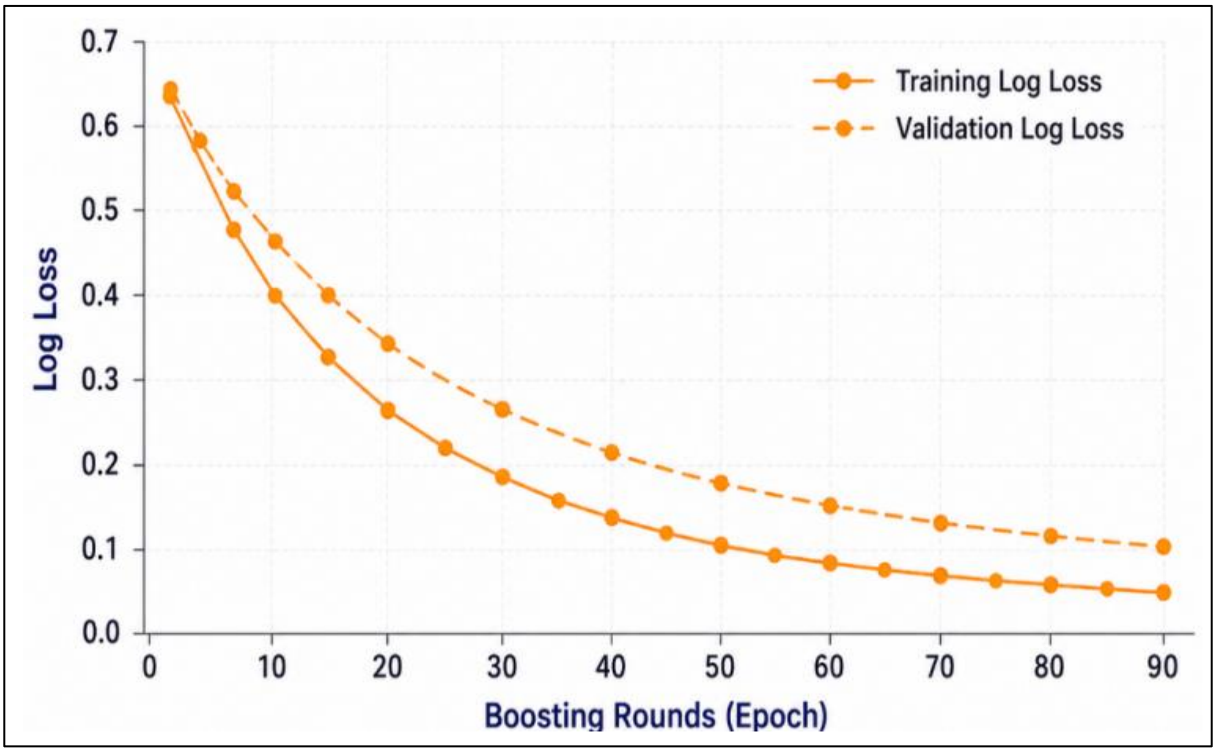

Fig 6 Loss Curve

The Figure 6 shows how the model error decreases as training progresses over 90 boosting rounds (epochs). Both Training Log Loss (solid orange line) and Validation Log Loss (dashed orange line) continuously decrease, indicates the XGBoost model will learn effectively.

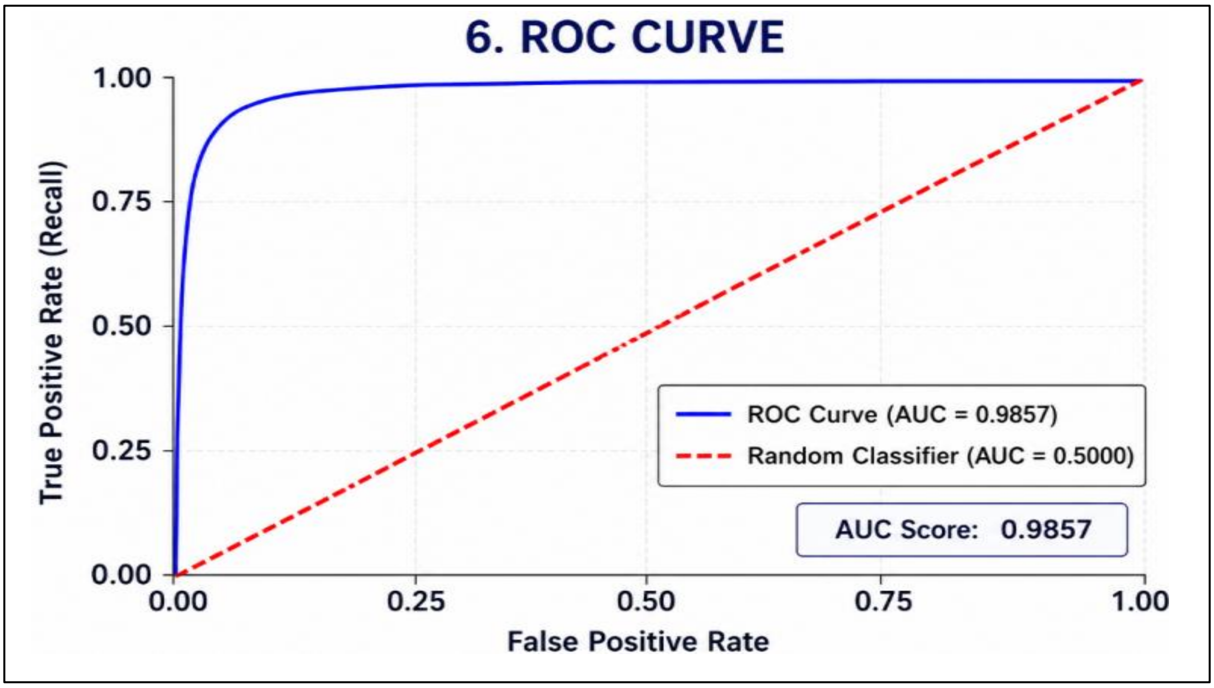

Fig 7 ROC Curve

The Figure 7 ROC (Receiver Operating Characteristic) Curve evaluates the classification performance of the XGBoost fraud detection model by comparing the True Positive Rate (Recall) against the False Positive Rate. The blue curve stays close to top-left corner and achieves an AUC score of 0.9857 (98.57%), indicating excellent fraud detection capability.

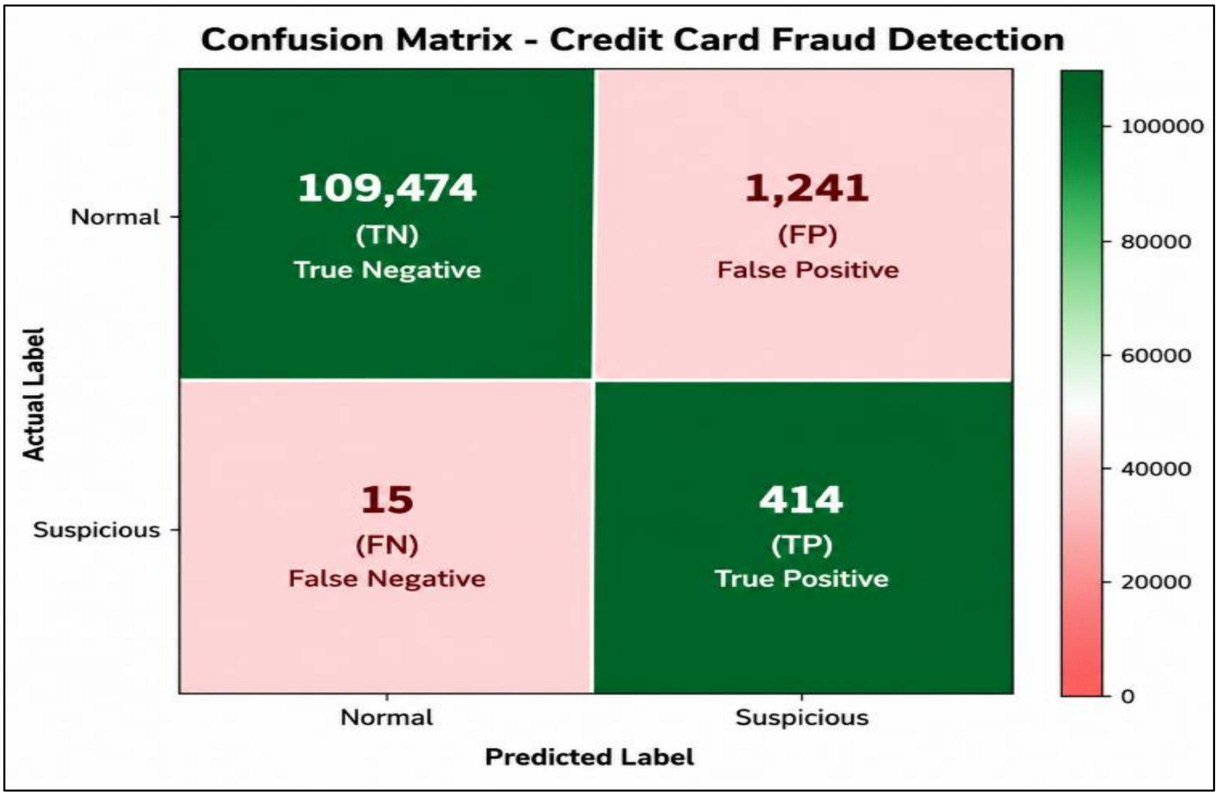

Fig 8 Confusion Matrix

The figure 8 shows the confusion matrix. The performance of the Credit Card Fraud Detecting model by comparing actual transaction labels with predicted labels. The model correctly classified 109,474 normal transactions and 414 suspicious (fraud) transactions, while only 1,241 normal transactions were wrongly flagged as fraud and 15 fraud transactions were missed.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1943

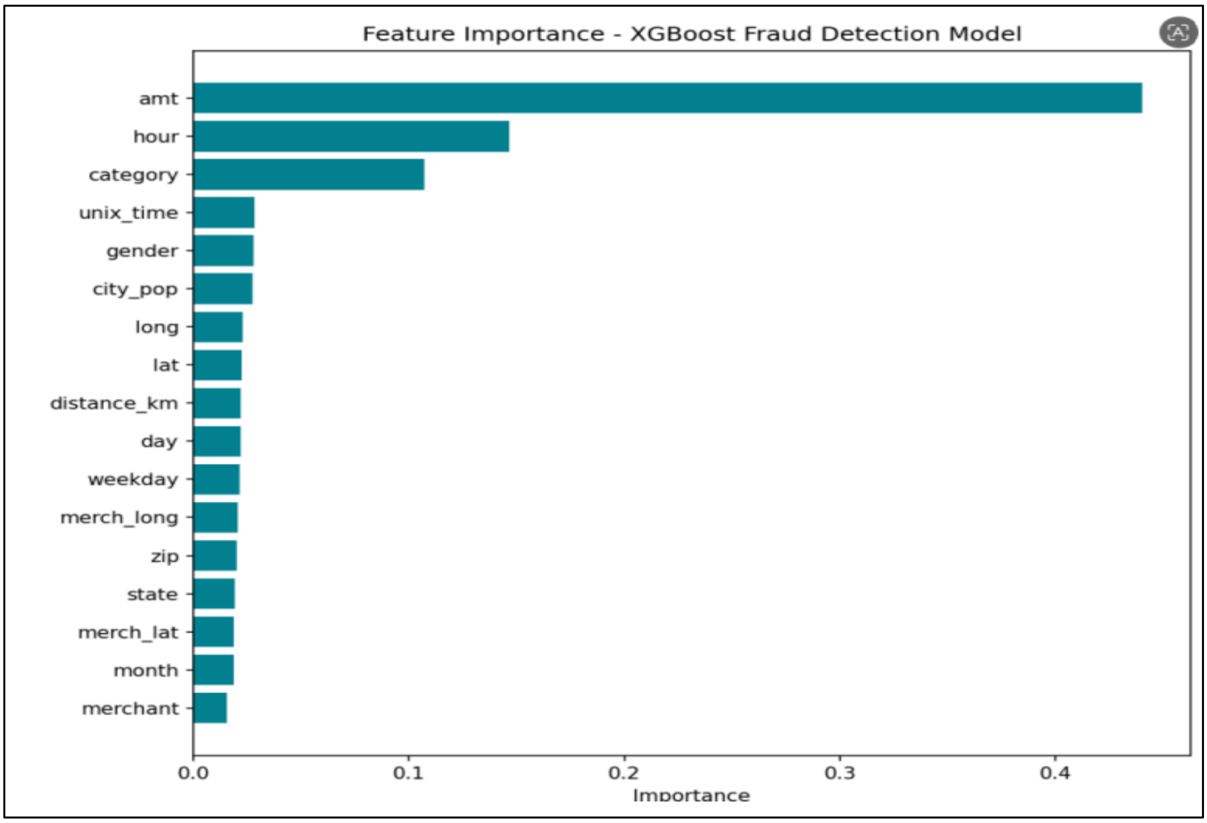

Fig 9 The Feature Importance Graph

The figure 9 shows the input features contributed to the XGBoost Credit Card Fraud Detecting model's predictions. The feature amount (transaction amount) has the highest importance, followed by hour and category, indicating that transaction value, transaction time, and merchant category strongly influence fraud detection.

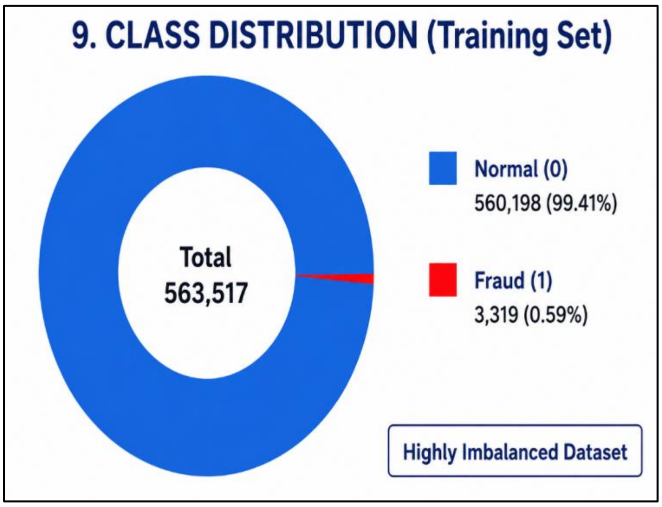

Fig 10 Class Distribution

The figure 10 Class Distribution (Training Set) chart shows the proportion of normal and fraud transactions are used in the training dataset. Out of 563,517 total transactions, 560,198 (99.41%) are normal while only 3,319 (0.59%) are fraud cases, showing that fraud samples are very limited.

V. CONCLUSION

The proposed AI-Based Credit Card Fraud Detecting System using XGBoost demonstrates an effective and intelligent approaching to identify the fraud credit card transactions from large-scale financial datasets. By applying preprocessing techniques, feature engineering, data normalization, and the machine learning classification, the system successfully identify the difference between normal and suspicious transactions. Experimental results showed strong performance across the evaluation metrics like Accuracy, Precision, Recall, F1-Score, ROC-AUC, Confusion Matrix, and Log Loss, indicating stable and reliable prediction capability.

The feature importance analysis is revealed to the transaction-related attributes like amount, transaction time, and category significantly influenced fraud prediction. The ROC curve and confusion matrix confirmed that the model achieved excellent classification ability with minimal false predictions and improved fraud detection efficiency. Additionally, training analytics demonstrated continuous improvement across boosting rounds, resulting in better convergence and lower prediction error.

Although the dataset exhibited a high class imbalance, the proposed model maintained good generalization and effectively detected minority fraud cases without sacrificing overall accuracy. This highlights the robustness of the XGBoost algorithm in handling real-world financial transaction data.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26jun1943

Overall, the developed system can serve as a practical solution for real-time fraud monitoring, financial risk reduction, and automated decision support in banking and the digital payments systems. In future work, advanced techniques like ensemble learning, the deep learning model, hybrid feature selection, and real-time streaming analysis can be incorporated to the further improvement of fraud detection performance and the scalability in the financial environments.

REFERENCES

[1]. Y. Lucas and J. Jurgovsky, "Credit card fraud detecting using machine learning: A survey," arXiv preprint arXiv: 2010.06479, 2020.

[2]. A. S. Gorte, S. W. Mohod, and R. R. Keole, "A survey is on the credit card fraud detecting using different machine learning and the deep learning techniques," AIP Conference Proceedings, vol. 2800, no. 1, 2023.

[3]. K. Ghosh Dastidar, O. Caelen, and M. Granitzer, "Machine learning methods to the credit card fraud detection: A survey," IEEE Access, 2024.

[4]. S. Naik and A. Dahale, "Credit card fraud detecting system using machine learning," Journal of IoT and Machine Learning, 2024.

[5]. S. Verma and J. Dhar, "Credit card fraud detecting: A deep learning approach," arXiv preprint arXiv: 2409.13406, 2024.

[6]. S. Kokate and M. S. R. Chettyi, "Fraudulent event detection in the credit card data using SVM-RBF," Journal of Applied Artificial Intelligence, 2025.

[7]. F. Carcillo et al., "SCARFF: A scalable framework used for streaming the credit card fraud detection with Spark," arXiv preprint arXiv: 1709.08920, 2017.

[8]. P. Tiwari et al., "Credit card fraud detecting using machine learning: A study," arXiv preprint arXiv: 2108.10005, 2021.

[9]. R. J. Bolton and D. J. Hand, "Statistical fraud detecting: A reviews," Statistical Science, vol. 17, no. 3, pp. 235–255, 2002.

[10]. [10] S. Bhattacharyya et al., "The Data mining to credit card fraud: A comparative study," The Decision Supporting Systems, vol. 50, no. 3, pp. 602–613, 2011.

[11]. A. Dal Pozzolo et al., "Calibrating probability to the under sampling for the unbalanced classification," IEEE Symposium on the Computational Intelligence and Data Mining, pp. 159–166, 2015.

[12]. A. Dal Pozzolo, O. Caelen, Y. Le Borgne, S. Waterschoot, and G. Bontempi, "Learns the lessons on the credit card fraud detecting from the practitioner perspective," Expert Systems with Applications, vol. 41, no. 10, pp. 4915–4928, 2014.

[13]. O. Randhawa et al., "Credit card fraud detecting using the AdaBoost and majority voting," International Journal of the Computer Applications, vol. 124, no. 17, 2015.