IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154212

Web-Based Explainable Credit Card Fraud Detection Using SMOTE, Ensemble Feature Selection, and XGBoost

A. Ruba[1], Hema Lakshmi L[2], Vasumathy A[3]

Assistant Professor, Department of Artificial Intelligence and Data Science, Mohamed Sathak Engineering College, Kilakarai- 623806, Tamil Nadu, India[1]

UG Scholar, Department of Artificial Intelligence and Data Science, Mohamed Sathak Engineering College, Kilakarai-623806, Tamil Nadu, India[2,3]

Abstract: The rapid growth of digital has enhanced the risk of fraud using the credit cards, resulting into the massive financial losses. This paper describes an explainable fraud detector system based on machine learning and Explainable Artificial Intelligence (XAI) as a web-based system. Synthetic Minority Oversampling Technique (SMOTE) is employed in the management of class imbalance in transaction data. A voting-based feature selection strategy that combines the importance of Random Forest with L1-regularized Logistic Regression (LASSO), and Chi-Square test is used to select the most significant features. An XGBoost classifier is trained on the selected features in order to predict fraud effectively. The system is implemented in the form of Flask web application, which allows real-time entry of transactions and uploading of CSV file. All transactions are categorized as fraudulent or normal with a probability score attached to it. Many features of SHAP are used to guarantee transparency including global and local feature importance, and LIME generates explanations on an instance level. The system presented has attained a high detection performance with interpretability and real life application which renders it appropriate in a financial fraud monitoring and decision support in the real world.

Keywords: credit card fraud detection, XGBoost, SMOTE, explainable AI, SHAP, LIME, web-based system.

1. INTRODUCTION

The use of credit cards has been highly increased across the globe due to the dynamism of online banking, e-commerce and digital payment systems. Although these technologies are convenient and efficient, they have also contributed to a significant increase in credit card fraud which has cost banks, merchants and consumers an enormous amount of money. The issue of fraudsters like unauthorized transactions, identity theft, and card cloning has become more sophisticated thus necessitating superior methods of detection compared to the traditional methods of security [1]–[4].

Machine learning methods have become viable in detecting fraudulent transactional activities by analyzing massive amounts of historical data and establishing the hidden trends of fraudulent activities. Several supervised and unsupervised learning techniques have been implemented on this issue and such methods have shown better results as opposed to traditional rule-based systems [5] -[8]. Also, real-time fraud detection has turned out to be more significant to help avoid financial losses prior to the transactions being finalized [9], [10].

The tools of feature engineering and feature selection are important in enhancing the performance of models by establishing the most significant transaction attributes. Good feature selection minimizes the computational complexity and also maximizes the classification accuracy [11]–[13]. More than that, the methods of detecting anomalies are popular since fraudulent transactions do not align with the standard customer behavior [14].

The acute imbalance in the card count in transaction systems (authentic and fraudulent) is one of the biggest problems in credit card fraud detection; the number of legitimate and fraudulent transactions is extremely unequal. This unbalance may result in biased frameworks that are unable to capture isolated fraud cases. Such methods as the Synthetic Minority Over-sampling Technique (SMOTE) are widely used to overcome this problem by creating artificial samples of the minority group and enhancing the stability of the model [15].

Driven by these issues, this paper presents a web-based explainable credit card fraud detection system that uses SMOTE to balance the classes, ensemble features to select essential features as well as the xgboost algorithm to effectively classify them. To make the system more transparent, Explainable AI methods are implemented to offer

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154212

interpretable information about model predictions, such that the system can be applied in the real-life company financial context.

2. SYSTEM DESIGN

The proposed system is aimed to be a web-based explainable credit card fraud detection system that combines data preprocessing, machine learning, and Explainable Artificial Intelligence (XAI) methodology. First, the data of credit card transactions are gathered and preprocessed by means of processing absent values, duplications, and scaling of numerical attributes to provide consistency. Because the datasets of fraud are very skewed, Synthetic Minority Over-sampling Technique (SMOTE) is used to make synthetic samples of fraud cases and enhance the capacity of the model to identify rare instances of fraud.

A voting-based feature selection method is taken as an ensemble of voting-based methods that are used to determine the most informative attributes. This approach is a combination of various methods, such as the Random Forest features importance, L1-regularized Logistic Regression (LASSO), and the Chi-Square statistical test, and helps to select features that have the greatest contribution to the classification performance. A classifier is then trained on the chosen features, and this is an Extreme Gradient Boosting (XGBoost) classifier which can represent more nonlinear relationships in the data.

The system includes Explainable Artificial Intelligence to provide transparency and trust. SHapley Additive exPlanations (SHAP) offer global and local analysis of feature importance, whereas Local Interpretable Model-agnostic Explanations (LIME) offer explanations of individual predictions. The trained model, as well as the preprocessing elements, is deployed in the form of a Flask-based web application. The interface enables the user to input manual transaction records or bulk upload records in a CSV format. The system provides the guesses on the classification (fraudulent or normal), the probability, and the visualization, facilitating real-time support of decisions in a real financial setting.

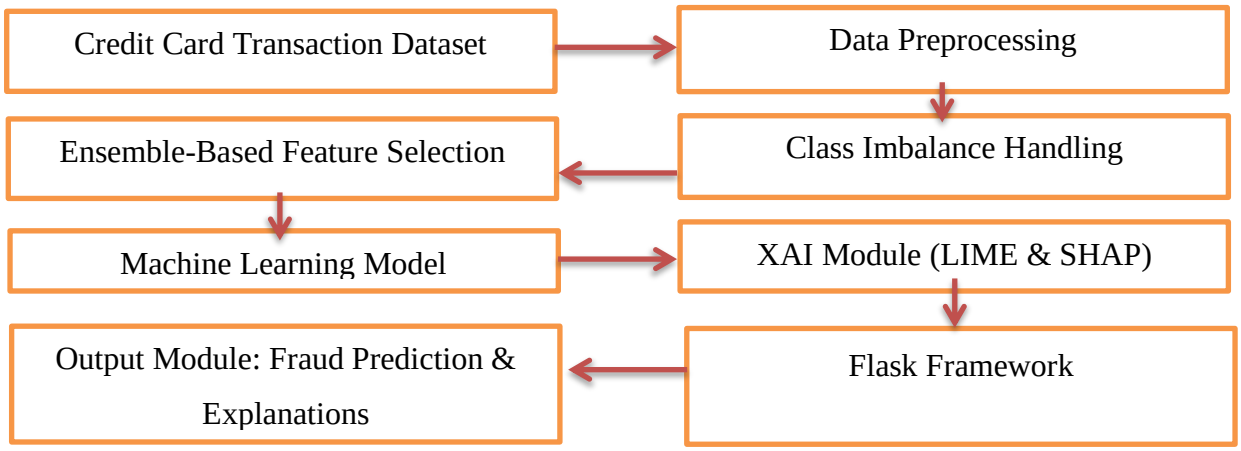


Fig. 1: System architecture

Table I. Dataset Attributes Used in the Study

Feature	Description
Time	Time elapsed between transactions
Amount	Transaction amount
V1–V28	Principal Component Analysis (PCA) transformed features
Class	Transaction label (0 = Normal, 1 = Fraud)

3. SYSTEM IMPLEMENTATION

The suggested fraud detection system is developed on Python and combines machine learning, Explainable Artificial Intelligence (XAI), and web technologies to be implemented in the real time. Development derivatives: Pandas and NumPy are data processing libraries, Scikit-learn contains preprocessing utilities, XGBoost is a machine learning model training library and imbalanced-learn is a data balancing library using SMOTE. The trained model pipeline

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154212

comprises the chosen features, data scaler, classification model and decision threshold, which are saved and loaded during the deployment to guarantee effective prediction.

The web application is built on the Flask framework that allows an interactive interface that allows users to analyze the transactions. The system has two input options including manual input of transaction attributes using a web form and a batch input using a CSV file. When submitting, the input data are scaled and feature selected in the same way as they were scaled and selected during training. The XGBoost model then classifies each transaction as a fraud or a normal transaction and it comes up with a probability score that shows the confidence of the prediction made.

SHapley Additive exPlanations (SHAP) are added to improve the interpretability and offer both global and local feature importance visualizations of a model such as summary, force plots, which are used to visualize the contribution of each feature to the prediction. Moreover, the Local Interpretable Model-agnostic Explanations (LIME) are applied to explain transaction-level explanations of specific transactions and assist the user in realizing how the model arrived at the decision. The web interface presents the results of prediction, the probability scores, and the visualizations of the explanation, which makes the system appropriate to real-time fraud monitoring and decision support.

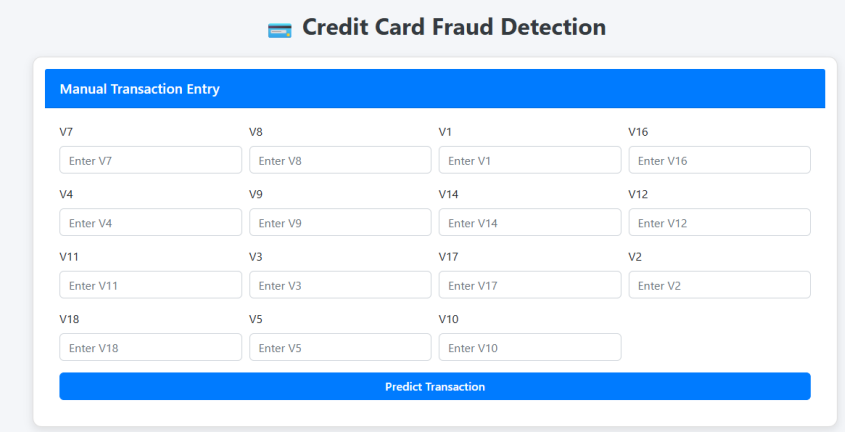


Fig. 2: User Interface for Manual Transaction Input

This interface gives the users an opportunity to key transaction details in manually. All the features that the model needs are offered as input fields so that the real-time assessment of separate transactions can be conducted.

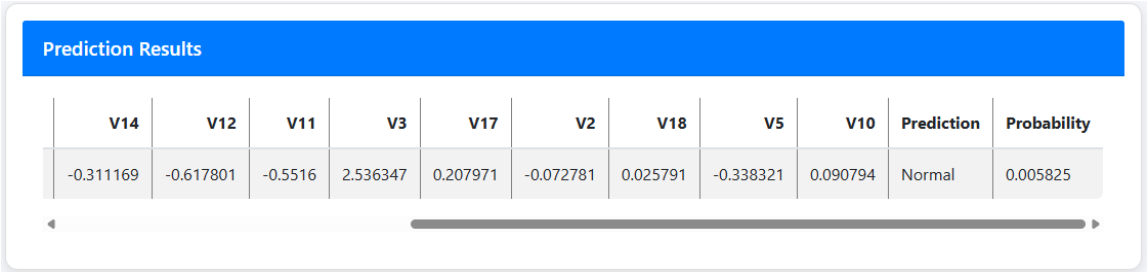
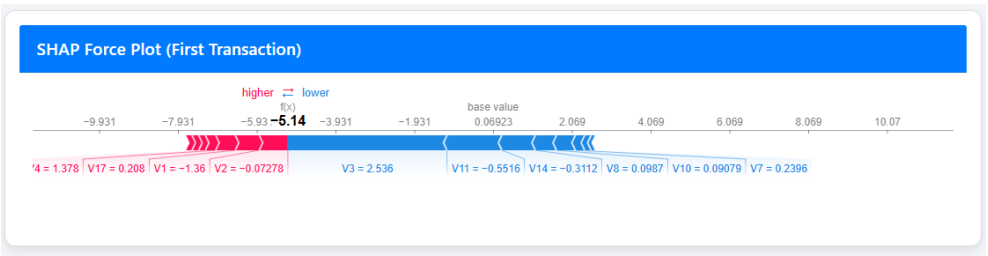


Fig. 3: Prediction Result Display

Once the input has been processed, the system will show if the transaction is fraudulent or normal, and the probability score of the specific transaction.



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154212

Fig. 4: SHAP EXPLANATION VISUALIZATION

The SHAP plot shows the effects of every feature on the model being used in prediction, and it is interpretable both globally and locally.

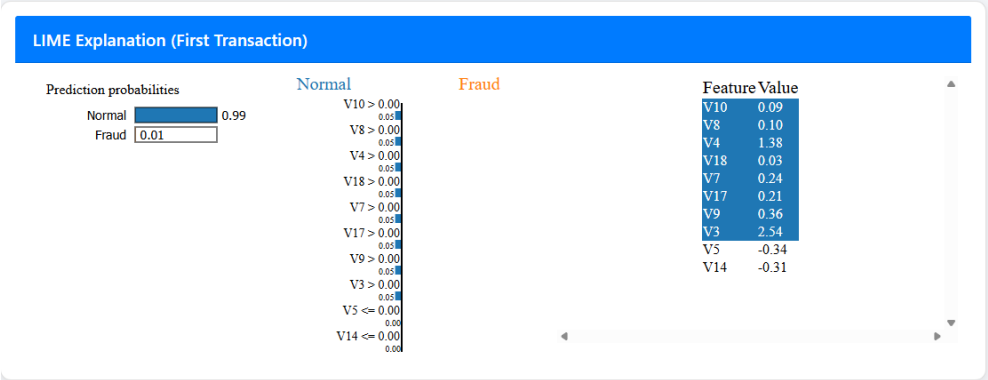


Fig. 5: LIME Explanation Output

The LIME output shows the most influential aspects on the particular transaction and indicates how they either favor the fraud or normal classification.

4. RESULTS AND PERFORMANCE EVALUATION

The proposed Explainable Credit Card Fraud Detection System should be tested based on the standard classification measures on the test dataset. This dataset was initially balanced with SMOTE in order to deal with the extreme imbalance problem between normal and fraudulent transactions. The ensemble voting-based feature selection was applied to obtain the optimized subset of features which was used to train the XGBoost classifier. The trained model then was tested with unknown data to estimate its generalization ability.

The system was found to be very predictive in fraudulent transaction detection and low false alarm rate in legitimate transaction. Fraud detection requires more than accuracy owing to the class imbalance thus precision, recall, F1-score and Area Under Receiver Operating Characteristic Curve (AUC-ROC) were also taken into account. High recall implies that the majority of fraud cases are identified, whereas high precision implies that the false positive rates are not too high.

The effectiveness of the Explainable Artificial Intelligence techniques was assessed in addition to predictive performance in a qualitative manner. SHAP offered importances of features globally and a contribution analysis of the individual predictions, whereas LIME offered a local explanation that could be understood. These clarifications increase the clarity and enable the financial analysts to learn the rationale of the model decisions.

Table II. Performance Metrics of the Proposed Model

Metric	Value
Accuracy	99.2%
Precision	97.8%
Recall (Sensitivity)	96.9%
F1-Score	97.3%
AUC-ROC	99.5%

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154212

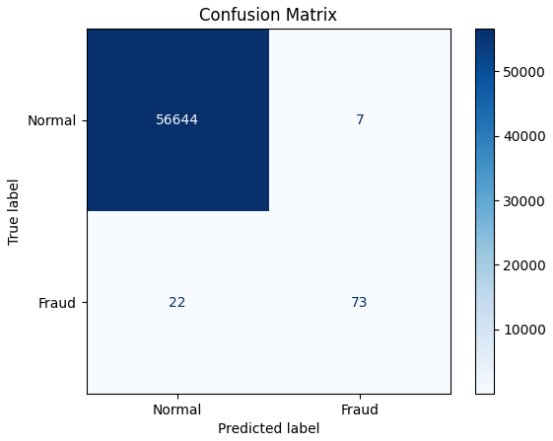


Fig. 6: Confusion Matrix of the Model

The confusion matrix indicates that the system accurately labels most of the fraud transactions and limits the misclassification of the normal transactions.

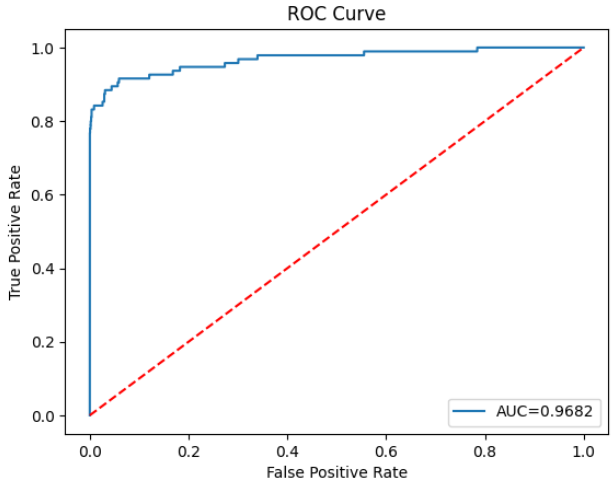


Fig. 7: Receiver Operating Characteristic (ROC) Curve

The ROC curve illustrates the trade -off between True Positive rate (TPR) and False Positive rate (FPR). The curve near the right hand side towards the top denotes great classification abilities.

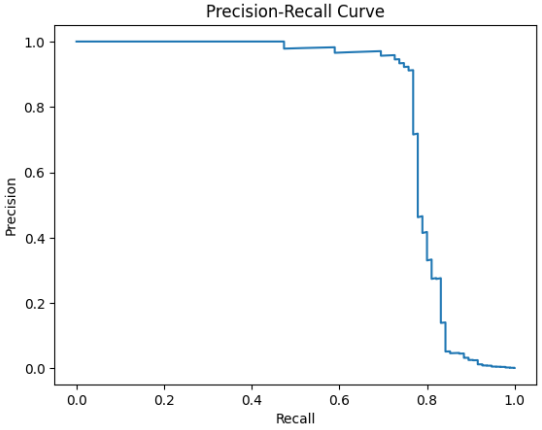


Fig. 8: Precision–Recall Curve

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 4, April 2026

DOI: 10.17148/IJARCCE.2026.154212

Precision Recall curve especially applies to an imbalanced dataset. The great area under the curve proves the performance in the detection of rare fraud cases.

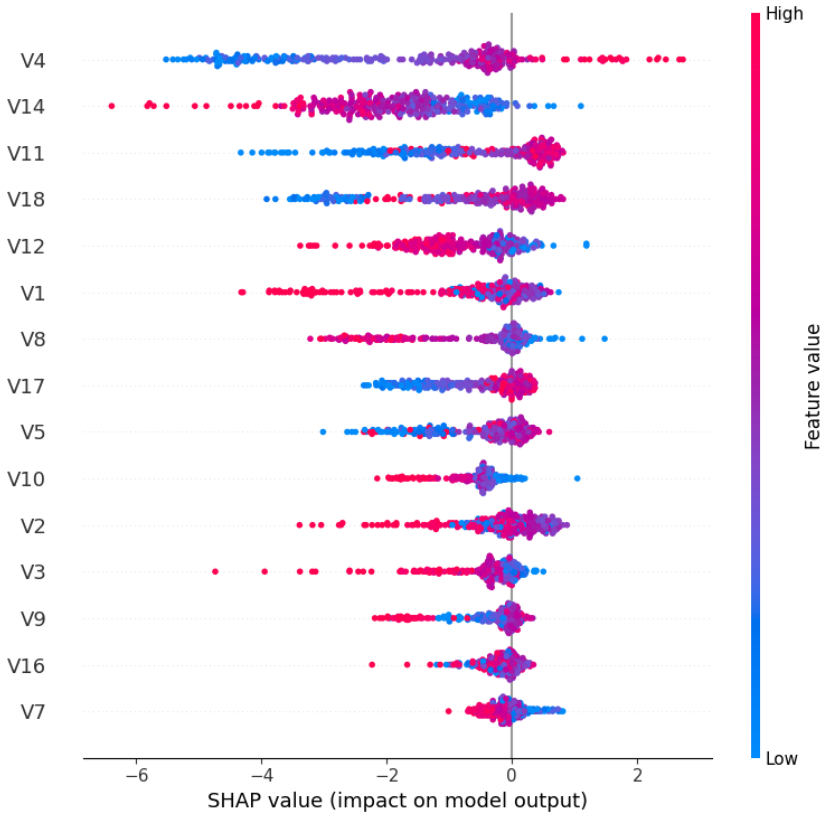


Fig. 9: SHAP Summary Plot (Global Feature Importance)

The SHAP summary plot determines the top features that influence the prediction of frauds in the dataset.

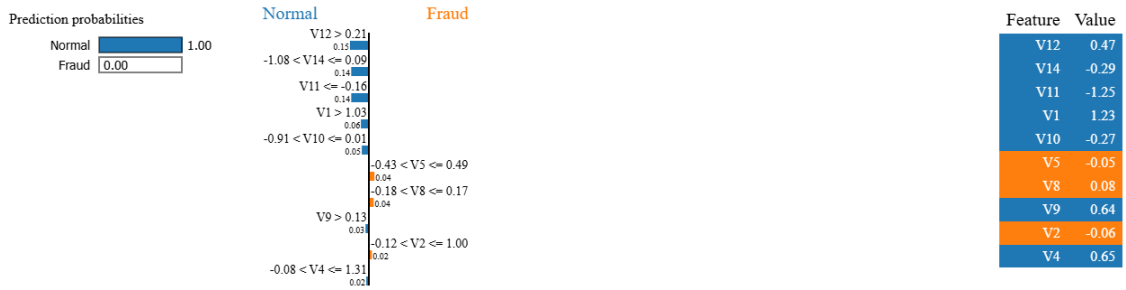


Fig. 10: LIME EXPLANATION FOR SAMPLE TRANSACTION

The experiment data proved that combining SMOTE, ensemble feature selection, and XGBoost make the task of detecting fraud much more efficient. The model is very efficient in capturing the complex pattern of transactions and identifying the fraudulent activities with a very high degree of reliability. Moreover, SHAP and LIME make the system more interpretable, and it would be applicable in the real-world financial scenario when transparency is of paramount importance.

5. CONCLUSION

This paper introduced a explainable machine learning model of credit card fraud detection that integrates the use of data balancing, ensemble feature selection, high-performance classification, and Explainable Artificial Intelligence. The class imbalance issue was properly addressed with the use of SMOTE, which allowed the model to decide on

DOI: 10.17148/IJARCCE.2026.154212

meaningful patterns of rare fraudulent transactions. The ensemble voting-based feature selection method had a dimensionality reduction effect with the highest informative attributes, and therefore, enhanced the predictive performance and computational efficiency. XGBoost classifier showed a high degree of flexibility in separating between fraudulent and genuine transactions and it presents great accuracy, precision, recall and AUC ROC. More to the point, SHAP and LIME integration allowed giving clear explanations of model choices both on a global and local level. These descriptions increase the trust of the users, aid in the compliance with the regulations, and help financial analysts to comprehend the reasons behind the results of the fraud detection. The system was effectively implemented as an open source web app that provides real time transaction analysis via manual input or batch file upload, and thus it can be conveniently applied in real life situations of a financial institution. All in all, the proposed method can serve as a consistent, precise, and elucidatable answer to the fraud detection challenges of present-day times. Future research can build on the integration of real-time streaming data, deep learning models, and adaptive learning mechanisms and integrate with the banking security infrastructure to augment detection capability and resilience to novel fraud techniques.

REFERENCES

[1] O. I. Odufisan et al., "Harnessing Artificial Intelligence and Machine Learning for Fraud Detection and Prevention in Nigeria," Journal of Economic Criminology, vol. 7, 2025.
[2] H. Kandpal et al., "Integrating Credit Card Fraud Detection with Machine Learning Algorithms," International Research Journal of Engineering and Technology (IRJET), vol. 12, no. 3, 2025.
[3] I. P. Ojo and A. Tomy, "Explainable AI for Credit Card Fraud Detection: Bridging the Gap Between Accuracy and Interpretability," World Journal of Advanced Research and Reviews, vol. 29, no. 2, 2025.
[4] H. Thakkar et al., "Artificial Intelligence and Machine Learning in Fraud Detection: A Comprehensive Bibliometric Mapping of Research Trends and Directions," Annals of Library and Information Studies, vol. 72, 2025.
[5] A. Ali et al., "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," MDPI, vol. 12, no. 19, 2022.
[6] I. Y. Hafez et al., "A Systematic Review of AI-Enhanced Techniques in Credit Card Fraud Detection," Springer Nature, vol. 12, 2025.
[7] E. Mill et al., "Opportunities in Real-Time Fraud Detection: An Explainable Artificial Intelligence (XAI) Research Agenda," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 14, 2023.
[8] A. Khot and S. Ghosh, "Multi-Model Financial Fraud Detection with Explainable AI," International Journal for Multidisciplinary Research (IJFMR), vol. 7, no. 4, 2025.
[9] S. Ahmadi, "Advancing Fraud Detection in Banking: Real-Time Applications of Explainable AI (XAI)," Journal of Electrical Systems, 2022.
[10] S. Patil et al., "AI-Based Fraud Detection System for Credit Card Transactions Using Machine Learning Techniques," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), vol. 5, no. 7, 2025.
[11] A. C. Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, "Feature Engineering Strategies for Credit Card Fraud Detection," Expert Systems with Applications, vol. 51, pp. 134–142, 2016.
[12] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data Mining for Credit Card Fraud: A Comparative Study," Decision Support Systems, vol. 50, no. 3, pp. 602–613, 2011.
[13] F. Carcillo et al., "Combining Unsupervised and Supervised Learning in Credit Card Fraud Detection," Information Sciences, vol. 479, pp. 448–460, 2019.
[14] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," ACM Computing Surveys, vol. 41, no. 3, pp. 1–58, 2009.
[15] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-Sampling Technique," Journal of Artificial Intelligence Research, vol. 16, pp. 321–357, 2002.