



International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

HYBRID MACHINE LEARNING MODEL FOR FRAUD DETECTION IN UPI PAYMENT SYSTEMS

G. Deshna¹, Dr. Nancy Jasmine Golden²

Department of Computer Applications, Sarah Tucker College, Tirunelveli-7.

ABSTRACT :

The growing use of Unified Payments Interface (UPI) has made digital payments easier and more convenient, but it has also increased the risk of fraudulent transactions. This paper studies the use of machine learning for detecting fraud in UPI transactions by comparing four supervised learning algorithms: Logistic Regression, Decision Tree, Random Forest, and XGBoost. Before training, the transaction data is cleaned and prepared using one-hot encoding, feature scaling, train-test splitting, and SMOTE for handling class imbalance. The four models are evaluated using Accuracy, Precision, Recall, F1-Score, and ROC-AUC to compare their fraud detection performance. The results show that XGBoost gives the best overall performance among the four models and is selected for the final prediction task. Additionally, an XGBoostRF hybrid model is included to extend the comparative analysis and investigate an alternative approach to UPI fraud detection. Its performance is compared with the original XGBoost model to understand the differences in their fraud detection capabilities. SHAP is then used with XGBoost to explain the features that influence individual transaction predictions. This study shows that combining machine learning with Explainable Artificial Intelligence can support fraud detection while also making the model's decisions easier to understand.

Keywords: UPI, Fraud Detection, Machine Learning, XGBoost, XGBoostRF, Random Forest, Decision Tree, Logistic Regression, Explainable AI, SHAP, Flask, Spring Boot.

1. INTRODUCTION

Unified Payments Interface (UPI) has become an important part of digital payments by allowing users to transfer money quickly and conveniently through mobile devices. Its simple payment process and wide availability have encouraged the use of UPI for everyday transactions. As the volume of digital transactions continues to increase, the possibility of fraudulent activities also becomes a significant concern. Fraudulent transactions can result in financial loss and reduce users' trust in digital payment systems. Therefore, effective methods are required to identify fraudulent transactions accurately and at an early stage.

Traditional fraud detection methods generally depend on predefined rules and fixed patterns to identify suspicious transactions. Although these methods can detect known types of fraud, they may have difficulty identifying new or complex fraudulent patterns. Fraudulent activities can vary based on transaction amount, transaction type, user characteristics, device information, time, and other transaction-related factors. This makes it important to use methods that can learn patterns from transaction data and identify relationships that may not be easily detected using fixed rules.

Machine learning provides an effective approach for analysing transaction data and identifying patterns associated with fraudulent behaviour. Different machine learning algorithms have different learning mechanisms and may perform differently depending on the characteristics of the data. Logistic Regression provides a simple and interpretable baseline for classification, while Decision Tree can identify patterns through rule-based decisions. Random Forest combines multiple decision trees to improve prediction stability and handle complex relationships in the data. XGBoost uses a gradient boosting approach to build models sequentially and improve classification performance. Comparing these algorithms under the same dataset and evaluation conditions helps determine which approach is more suitable for UPI fraud detection.

Another important challenge in machine learning-based fraud detection is the interpretability of model decisions. Highly effective models may produce predictions without clearly showing why a transaction has been classified as fraudulent. In financial applications, understanding the factors behind a prediction is important for building confidence in the system and supporting further analysis. Explainable Artificial Intelligence (XAI) techniques can help address this issue by providing information about the contribution of individual features to a model's prediction. Therefore, incorporating explainability along with fraud detection can make machine learning-based decisions easier to understand.

In addition to the original four-model comparison, an XGBoostRF hybrid model is investigated as an experimental approach to explore the potential for improving fraud detection. Its performance is compared with the original XGBoost model to examine the differences in their predictive capabilities. This additional experiment extends the comparative study by considering an alternative model configuration without replacing the original model used in the web application.

Based on these considerations, there is a need to comparatively study different machine learning algorithms for UPI fraud detection and identify an effective model while also considering the interpretability of its predictions. This paper focuses on comparing Logistic Regression, Decision Tree, Random Forest, and XGBoost for fraudulent transaction detection, investigating the XGBoostRF hybrid experiment, and using SHAP to provide

explanations for the original XGBoost model's predictions. The study aims to contribute to a more reliable and understandable approach to detecting fraudulent UPI transactions.

2. RELATED WORK

Machine learning is widely used for financial fraud detection. West and Bhattacharya [3] reviewed intelligent fraud detection methods, while Buczak and Guven [4] discussed machine learning and data mining techniques. Dash et al. [6] explored AI-based fraud detection in banking. These studies lay a foundation but mainly focus on general financial transactions. Chen and Guestrin [1] introduced XGBoost, a gradient boosting algorithm for classifying structured data. Nijwala et al. [2] applied gradient boosting to credit card fraud, and Misra et al. [5] used an autoencoder for the same task. These studies show the effectiveness of different algorithms but focus on credit card or general fraud. More recent work targets UPI fraud. Sethi et al. [7] used Random Forest for UPI fraud detection. Sree et al. [8] proposed a Transformer and federated learning approach. Siva et al. [9] developed a machine learning framework for fraudulent UPI transactions. Ramya et al. [10] combined XGBoost and SHAP for explainable UPI fraud detection.

These studies demonstrate that several machine learning algorithms are capable of effectively identifying fraudulent transactions; however, the effectiveness of these algorithms varies according to the dataset, characteristics, and detection strategy employed. Direct comparison under the same experimental settings is challenging because the majority of current systems concentrate on a single algorithm or a specialized method. Furthermore, many studies concentrate on prediction without integrating explainability and model comparison into a single practical system.

Thus, comparing Logistic Regression, Decision Tree, Random Forest, and XGBoost using the same UPI transaction dataset and evaluation metrics presents a research gap. By analysing the four algorithms, selecting XGBoost based on its performance, and incorporating SHAP to explain individual fraud predictions, this work addresses the identified gap. Additionally, an XGBoostRF hybrid model is investigated as an experimental extension to the original comparison to explore an alternative approach to fraud detection and evaluate its performance against the original XGBoost model. This further extends the study by examining the potential benefits and limitations of combining machine learning algorithms for UPI fraud detection.

3. RESEARCH METHODOLOGY

This system uses supervised machine learning methods to detect fraudulent UPI transactions. The overall process consists of several stages, including dataset collection, data preprocessing, model training, performance evaluation, model selection, and the integration of Explainable Artificial Intelligence using SHAP. The approach follows a sequence of tasks that includes collecting the dataset, preparing the data, handling class imbalance, training the models, evaluating their performance, comparing different models, and analysing model explainability. Four supervised machine learning algorithms are trained using the preprocessed UPI transaction data. Their performance is compared using standard classification metrics, and the best-performing model is selected for the final fraud detection system. In addition, an XGBoostRF hybrid model is investigated as a separate experiment and compared with the original XGBoost model to explore an alternative approach to fraud detection. Finally, Explainable Artificial Intelligence (XAI) using SHAP is applied to interpret the predictions generated by the original XGBoost model used in the application.

3.1 Dataset Description

This study uses a dataset consisting of UPI transaction records. It contains different attributes related to transaction characteristics and user behaviour. The dataset includes both numerical and categorical features that can help identify patterns associated with fraudulent transactions. The features include transaction type, merchant category, transaction amount, sender age group, sender state, sender bank, receiver bank, device type, network type, and time-related information. Each feature provides different information about a transaction that can be used by machine learning models for classification.

The target variable is `fraud_flag`, where a value of 0 represents a genuine transaction and a value of 1 represents a fraudulent transaction. For training and testing purposes, the dataset is divided into separate training and testing sets. This allows the performance of the trained models to be evaluated on previously unseen transaction records.

3.2 Data Preprocessing

The UPI transaction dataset is preprocessed before training the machine learning models. Unnecessary columns that do not contribute to fraud prediction are removed from the dataset. Categorical features are converted into numerical form using One-Hot Encoding. Numerical features are scaled to maintain a consistent range across the dataset. The preprocessed data is then divided into training and testing sets. SMOTE is applied to the training data to handle class imbalance between genuine and fraudulent transactions. The resulting data is used for training and evaluating the four machine learning models. The stacking ensemble is also trained and evaluated using the prepared transaction data, with the preprocessing procedure verified to ensure consistency between training and testing.

3.3 Machine Learning Models

For comparison and analysis, four supervised machine learning models are employed. These models illustrate various classification techniques, including gradient boosting, ensemble learning, tree-based learning, and linear classification. To determine which model is best for detecting UPI fraud, their performances are compared.

3.3.1 Logistic Regression

The probability that a transaction falls into a specific class is predicted using logistic regression. Because of its straightforward structure and probability-based output, it functions as a baseline model. The sigmoid function is used by the model to determine the likelihood of the positive class:

$$P(y = 1 | X) = 1 / (1 + e^{-z})$$

where,

$$z = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \dots + \beta_n X_n$$

where $z = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \dots + \beta_n X_n$, where X_1 to X_n are the input characteristics, β_0 is the intercept, and β_1 to β_n are the model coefficients. A probability threshold is used to determine the final class.

3.3.2 Decision Tree

A Decision Tree is a learning technique that categorizes transactions using a set of rules. Based on feature values, it splits the dataset into smaller groups and keeps doing so until a final classification is achieved.

Usually, Gini Impurity is used to decide how to divide the data:

$$Gini = 1 - \sum_{i=1}^c p_i^2$$

where the percentage of samples in class I is represented by p_i . A purer group is indicated by a lower Gini rating. Until a final classification is determined, the fraud detection tree continues to divide the data into smaller groups according to transaction characteristics. As a result, nonlinear relationships in the transaction data can be captured by the model.

3.3.3 Random Forest

An ensemble method called Random Forest combines several Decision Trees to increase prediction stability and accuracy. Every tree gains knowledge from various training data samples and characteristics.

Majority voting is used to determine the final classification:

$$\hat{y} = \text{mode}\{T_1(X), T_2(X), \dots, T^B(X)\}$$

where B is the total number of trees and $T_1, T_2, \dots, T^B$ stand for the individual decision trees.

Random Forest offers more accurate forecasts and lessens the drawbacks of a single Decision Tree by merging multiple trees. It is helpful for spotting various trends in UPI transaction data.

3.3.4 XGBoost

XGBoost is a gradient boosting-based ensemble learning method. It constructs decision trees one after the other, attempting to fix the mistakes of the earlier trees.

The overall goal function is:

$$Obj = \sum_{i=1}^n L(y_i, \hat{y}_i) + \sum_{k=1}^K \Omega(f_k)$$

where $\Omega(f_k)$ is the regularization term for each tree, L is the loss function, y_i is the actual value.

Boosting and regularization are combined in XGBoost to enhance prediction performance and manage model complexity. It is appropriate for fraud detection because of its capacity to learn intricate correlations. XGBoost is chosen as the final model for the suggested system based on the comparison analysis.

3.3.5 XGBoostRF

XGBoostRF is an experimental hybrid model that combines XGBoost and Random Forest using a stacking approach. In this method, XGBoost and Random Forest act as base models, and their predictions are combined to produce the final output.

The final prediction is represented as:

$$y_{pred} = g(P_X(X), P_R(X))$$

where $(P_X(X))$ represents the prediction from XGBoost, $(P_R(X))$ represents the prediction from Random Forest, and (g) represents the Logistic Regression meta-model. The meta-model learns to combine the predictions of both base models to classify a transaction as genuine or fraudulent.

Table 1. Performance comparison of machine learning models

Model	Accuracy	Precision	Recall	F1-Score	ROC-AUC
Logistic Regression	89.77%	49.33%	84.15%	62.20%	94.39%
Decision Tree	95.33%	73.83%	82.50%	77.92%	89.63%
Random Forest	97.10%	87.14%	83.35%	85.20%	98.05%

XGBoost	97.52%	91.55%	82.85%	86.98%	98.35%
XGBoostRF	97.04%	83.24%	88.15%	85.62%	98.29%

3.4 Handling Class Imbalance Using SMOTE

Because there are typically more legitimate transactions than fraudulent ones, fraud detection datasets are frequently unbalanced. A machine learning algorithm may favor the majority class as a result of this imbalance and mistakenly identify fraudulent transactions as legitimate.

The training data is subjected to the Synthetic Minority Over-sampling Technique (SMOTE) in order to solve this issue. Using current minority-class samples and their closest neighbors, SMOTE creates new synthetic samples for the minority fraud class. As a result, during model training, fraudulent transactions are more frequently represented.

Instead of relying mostly on the majority class, SMOTE enables the models to learn a greater variety of fraud behaviors. In order to maintain the independence of the testing data for objective model evaluation, it is only applied to the training data.

A synthetic sample can be shown as:

$$X_{new} = X_i + \lambda(X_{nn} - X_i)$$

3.5 Model Evaluation Metrics

Accuracy, Precision, Recall, F1-Score, and ROC-AUC are used to evaluate the four machine learning models. These criteria are used to assess several facets of the model's ability to distinguish between legitimate and fraudulent UPI transactions. Relying solely on accuracy might not yield a comprehensive assessment because fraud detection requires an imbalanced classification problem. For a more trustworthy comparison of the models, certain evaluation indicators are taken into account.

3.5.1 Accuracy

The percentage of transactions that the model properly classifies out of all transactions is known as accuracy. It takes into account both accurately detected legitimate transactions and accurately detected fraudulent transactions.

The accuracy is computed as follows:

$$Accuracy = (TP + TN) / (TP + TN + FP + FN)$$

where TP stands for correctly identified fraudulent transactions, TN for correctly identified genuine transactions, FP for genuine transactions that were mistakenly classified as fraud, and FN for fraudulent transactions that were mistakenly classified as genuine. A higher accuracy means that a greater percentage of the transactions are accurately classified by the model. However, when the courses are unbalanced, precision might not be enough to detect fraud.

3.5.2 Precision

The percentage of transactions that are accurately classified as fraudulent out of all transactions that are anticipated to be fraudulent is known as precision. It shows the accuracy of the model's fraud forecasts.

$$Precision = TP / (TP + FP)$$

The model generates fewer false fraud alarms when the precision value is high. This is crucial because misclassifying legitimate transactions as fraudulent might result in needless notifications and user inconvenience.

3.5.3 Recall

Recall quantifies the model's accuracy in identifying real fraudulent transactions. It is especially crucial for fraud detection since missing a fraudulent transaction could cost you money..

$$Recall = TP / (TP + FN)$$

A higher recall means that a greater percentage of real fraudulent transactions may be identified by the model. As a result, recall is a crucial statistic for assessing the fraud detection system's efficacy.

3.5.4 F1-Score

Precision and recall are balanced by the F1-Score. It is particularly helpful when there is an imbalance between legitimate and fraudulent transactions in the dataset.

$$F1 = 2 \times (Precision \times Recall) / (Precision + Recall)$$

A higher F1-Score shows that the model strikes a better balance between avoiding incorrect fraud predictions and accurately recognizing fraudulent transactions. As a result, F1-Score offers a more impartial assessment than accuracy alone.

3.5.5 ROC-AUC

ROC-AUC evaluates a model's ability to discriminate between legitimate and fraudulent transactions. It shows the Area Under the Receiver Operating Characteristic Curve, which assesses how well the model can classify data across various decision criteria.

The True Positive Rate (TPR) and False Positive Rate (FPR) are used to plot the ROC curve.

$$UC = \int_0^1 TPR(FPR) d(FPR)$$

where:

$$TPR = TP / (TP + FN)$$

and

$$FPR = FP / (FP + TN)$$

The range of the ROC-AUC value is 0 to 1. Better discrimination between the two classes is indicated by a value closer to 1, whereas performance comparable to random categorization is indicated by a value closer to 0.5. In order to provide a thorough assessment of the four machine learning models, ROC-AUC is utilized in conjunction with the other measures.

3.6 Explainable AI using SHAP

Even if machine learning models are capable of making precise forecasts, it is crucial to comprehend the rationale behind a prediction in order to detect financial fraud. Thus, the suggested system uses SHAP to integrate Explainable Artificial Intelligence (XAI). The basic formula for SHAP is:

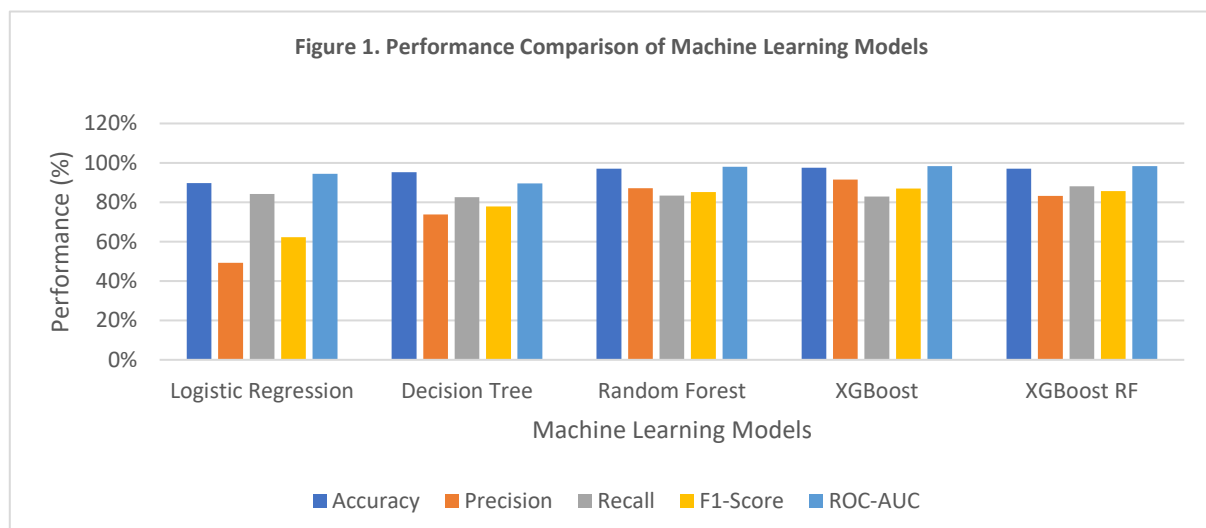
$$f(x) = \varphi_0 + \sum_{i=1}^M \varphi_i$$

By giving each input feature a contribution value, SHAP explains specific XGBoost predictions. Depending on the class being described, a positive contribution shows that the feature supports the predicted class, whilst a negative contribution shows that the feature contributes in the other direction. For instance, a prediction may be influenced differently by the transaction amount, transaction type, device type, network type, or other transaction variables. SHAP facilitates the identification of these contributions and offers a more transparent justification for the classification of a transaction as genuine or fraudulent.

The incorporation of SHAP enhances the suggested fraud detection system's transparency and facilitates comprehension of the machine learning predictions. In financial applications, where customers would need to comprehend the elements impacting an automated choice, this is very helpful.

4. RESULTS AND DISCUSSION

The four machine learning models were evaluated using Accuracy, Precision, Recall, F1-Score, and ROC-AUC. The numerical results are presented in Table 1, while Figure 1 provides a graphical comparison of the model performances. The results show clear differences among the four algorithms. Logistic Regression records the lowest overall performance, particularly in Precision and F1-Score, although it provides a reasonable Recall. Decision Tree performs better than Logistic Regression by capturing nonlinear relationships in the transaction data. Random Forest provides further improvement by combining multiple decision trees, resulting in more stable and accurate predictions.



Among the evaluated models, XGBoost provides the best overall performance. It achieves an Accuracy of 97.52%, Precision of 91.55%, F1-Score of 86.98%, and ROC-AUC of 98.35%. Random Forest records a slightly higher Recall of 83.35%, compared with 82.85% for XGBoost. However, XGBoost performs better in the other major evaluation metrics. Its gradient boosting approach builds decision trees sequentially, allowing the model to improve previous prediction errors, while regularization helps control model complexity. Based on the overall performance, XGBoost is selected as the final model for the proposed UPI fraud detection system.

Additionally, an experimental XGBoostRF model is evaluated to investigate an alternative approach to UPI fraud detection. The model combines

XGBoost and Random Forest as base estimators, with Logistic Regression acting as the final estimator in the stacking process. The experimental model achieves an Accuracy of 97.04%, Precision of 83.24%, Recall of 88.15%, F1-Score of 85.62%, and ROC-AUC of 98.29% in the reported experiment. Compared with the original XGBoost model, XGBoostRF provides higher Recall but slightly lower Accuracy, Precision, F1-Score, and ROC-AUC. These results indicate a difference in the models' fraud detection performance. However, further validation under consistent preprocessing and experimental conditions is required before making a direct performance comparison. Therefore, the original XGBoost model remains the final model integrated into the existing web application, while XGBoostRF is considered an experimental extension of the study.

The selected XGBoost model is used to classify individual transactions as Genuine or Fraud. To make these predictions easier to understand, SHAP is integrated with the model to identify the contribution of individual transaction features to each prediction. Instead of providing only the final classification, the system provides information about the features that influence the prediction towards the Fraud or Genuine class. This improves the transparency of the model and helps users understand the factors behind individual transaction decisions.

The selected model is integrated with the Flask ML API and Spring Boot backend to provide transaction-level prediction through the developed web application. When transaction details are submitted through the interface, the system processes the input and returns the prediction along with its SHAP-based explanation. Transaction and prediction information can also be maintained for further analysis. Overall, the results demonstrate that XGBoost provides the strongest overall performance among the evaluated models, while SHAP improves the interpretability of its predictions. The combination of machine learning and Explainable Artificial Intelligence therefore provides a practical approach for detecting fraudulent UPI transactions while providing meaningful information about the reasons behind the model's decisions.

5. CONCLUSION

In this work, four machine learning algorithms, Logistic Regression, Decision Tree, Random Forest, and XGBoost, were studied for detecting fraudulent UPI transactions. The models were trained using the prepared transaction data, and their performance was evaluated using Accuracy, Precision, Recall, F1-Score, and ROC-AUC. The comparison showed that each model behaved differently when used for fraud detection.

Among the four models, XGBoost gave the best overall results. Random Forest also performed well, while Decision Tree and Logistic Regression showed lower performance in comparison. Based on the overall results, XGBoost was selected as the final model for detecting fraudulent transactions in the developed system.

In addition, an experimental XGBoostRF model was evaluated to explore an alternative approach to fraud detection. The experimental model achieved a Recall of 88.15%, compared with 82.85% for the original XGBoost model. Recall measures the proportion of actual fraudulent transactions correctly identified by the model. Therefore, the higher Recall of XGBoostRF indicates that it identified a larger proportion of fraudulent transactions in the reported experiment. This can be particularly useful in fraud detection, where missing suspicious transactions is an important concern. However, the experiment requires further validation under consistent preprocessing conditions before confirming its comparative advantage. XGBoostRF is therefore considered an experimental extension, while the original XGBoost model remains integrated into the existing application.

Along with prediction, this work also focused on making the model's decisions easier to understand. SHAP was used with the original XGBoost model to show which transaction features influenced each prediction. The system does not simply display whether a transaction is Fraud or Genuine; it also provides information about the factors that affected the result. This improves the interpretability of the fraud detection process.

The selected XGBoost model was integrated into the developed application to analyse individual transactions. The application displays the prediction and its SHAP-based explanation and provides features such as model comparison and transaction history. This makes it easier for users to view the results and understand the behaviour of the fraud detection model.

The system can be improved further in several ways. Real-time transaction monitoring can be added so that suspicious transactions can be identified as soon as they occur. The model can also be updated regularly with newer transaction data because fraud patterns may change over time. Additional transaction-related features can be considered to improve the detection of different types of fraud. Future work can also explore deep learning models, other machine learning algorithms, and additional Explainable AI techniques. Furthermore, the system could be deployed on cloud infrastructure to handle a larger number of transactions in real-world applications.

REFERENCE

- [1] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," in *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 785–794, 2016.
- [2] D. S. Nijwala, S. Maurya, M. P. Thapliyal, and R. Verma, "Extreme Gradient Boost Classifier Based Credit Card Fraud Detection Model," in *Proceedings of the IEEE International Conference on Device Intelligence, Computing and Communication Technologies (DICCT)*, pp. 500–504, 2023.
- [3] J. West and M. Bhattacharya, "Intelligent Financial Fraud Detection: A Comprehensive Review," *Computers & Security*, vol. 57, pp. 47–66, 2016.
- [4] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.
- [5] S. Misra, S. Thakur, M. Ghosh, and S. K. Saha, "An Autoencoder Based Model for Detecting Fraudulent Credit Card Transaction," *Procedia Computer Science*, vol. 167, pp. 254–262, 2020.
- [6] S. Dash, S. Das, S. Sivasubramanian, N. Kalyana Sundaram, G. K. Harsha, and T. Sathish, "Developing AI-based Fraud Detection Systems for Banking and Finance," in *Proceedings of the 5th International Conference on Inventive Research in Computing Applications (ICIRCA)*, pp. 891–897, 2023.
- [7] B. Sethi, S. Mhatre, S. Yadav, S. Das, and V. Jadhav, "Machine Learning-Based UPI Fraud Detection: A Comprehensive Approach Using Random Forest," in *Proceedings of the MULTINOVA: First International Conference on Artificial Intelligence in Engineering, Healthcare and Sciences (ICAIEHS)*, pp. 462–470, 2025. DOI: 10.2991/978-94-6463-852-3_29.
- [8] M. V. Sree, P. Bhuvaneshwari, K. Nandini, K. R. P. Amulya, P. Swetha, and B. Chandrakala, "Enhanced Detection of UPI Frauds Using Advanced Machine Learning Techniques for Secure Digital Transactions," in *Proceedings of the 4th International Conference on Information Technology, Civil*

Innovation, Science, and Management (ICITSM), 2025. DOI: 10.4108/eai.28-4-2025.2357830.

[9] N. Siva, K. Durgadevi, J. Naga Jyothi, D. Dadakhalandhar, K. Guruteja, and M. Keerthan Reddy, "A Machine Learning Framework for Detecting Fraudulent Transactions in UPI Systems," in *Proceedings of the 2025 conference*, 2025.

[10] G. Ramya, A. Naga Venkata Gayathri, H. Althaf, and M. I. K. Shariff, "Explainable UPI Fraud Detection Using XGBoost and SHAP-Based Interpretable AI," *International Journal of Engineering Research and Science & Technology*, vol. 22, no. 1, pp. 289–295, 2026. DOI: 10.62643/ijerst.2026.v22.n1(2).pp289-295.