International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

UPI Fraud Detection System using Ensemble Models

Ms Sanjana R
Assistant professor
Department of Cyber Security ACS College of Engineering (VTU affiliated)
College Address: 207, Kambipura, Mysore Road, Kengeri Hobli, Bengaluru-560074
ORCHID: 0009-0003-3988-8326
sanjanachavan98@gmail.com

Ms. Amrutha A
Bachelor of Engineering Student
Department of Cyber Security
ACS College of Engineering
(VTU affiliated)
College Address: 207, Kambipura, Mysore Road, Kengeri Hobli, Bengaluru-560074
amrutha.a0305@gmail.com

Ms. Hithashree K
Bachelor of Engineering Student
Department of Cyber Security
ACS College of Engineering
(VTU affiliated)
College Address: 207, Kambipura, Mysore Road, Kengeri Hobli, Bengaluru-560074
hithashree.govi@gmail.com

Ms. Karishma I
Bachelor of Engineering Student
Department of Cyber Security ACS College of Engineering
(VTU affiliated)
College Address: 207, Kambipura, Mysore Road, Kengeri Hobli, Bengaluru-560074
karishmai2404@gmail.com

***Abstract*— The Unified Payments Interface (UPI) and other digital payment systems have grown quickly, which has led to more fraudulent transactions that put people's money and trust at risk. This study examines detection techniques leveraging Machine Learning and Natural Language Processing to identify and prevent UPI fraud. It explores advanced models such as deep neural networks and graph-based methods for looking at patterns in transactions, how users act, and the situation data. The research also addresses key challenges, including real-time detection, data imbalance, privacy preservation, and model adaptability, aiming to enhance the reliability and security of digital payment ecosystems (*Abstract*)**

Keywords*— *UPI fraud, Machine Learning, Deep Learning, Transaction Analysis, Fraud Detection.

I. INTRODUCTION

The quick rise of digital payments in India has transformed the nation's financial ecosystem, with the UPI (Unified Payments Interface) emerging as one of the most widely used platforms for instant and seamless transactions. However, alongside its popularity, there has been a sharp rise in scams like phishing, fake payment requests, and identity theft. Systems for finding fraud that have been around for a long time, based on static rules, are often ineffective against evolving threats. To address this challenge, machine learning (ML) and artificial intelligence (AI) offer intelligent, data-driven solutions capable of identifying suspicious transaction patterns and enhancing the overall security of digital payment systems. The exponential growth of UPI transactions has undeniably brought convenience and financial inclusivity to millions of users. Yet, this digital revolution also presents new vulnerabilities that fraudsters continue to exploit through advanced social engineering, identity theft, and unauthorised access techniques. With the volume and velocity of digital transactions increasing daily, banks and payment service providers now have a big problem with finding fraudulent behavior in real time. Traditional rule-based systems, though once effective, now struggle to adjust to the ever-changing patterns of fraud that are emerging. This has led to a pressing need for intelligent solutions capable of learning and evolving with changing data trends

A. Problem Statement

Digital payment systems have changed the way people do business in India, especially the Unified Payments Interface (UPI), standing out as a convenient, fast, and user-friendly platform. However, this convenience has also made UPI a prime target for cybercriminals. Fraudulent actions like fake payment requests, identity theft, and social engineering scams have increased significantly. Traditional rule-based detection systems, which rely on predefined thresholds and static rules, often fail to recognise new or evolving fraud patterns. These systems produce numerous false positives or overlook sophisticated attacks, thereby reducing user trust and threatening financial security.

B. Objective

The primary aim of this review is to investigate the increasing demand for artificial intelligence (AI) and machine learning (ML)–based systems in the detection of UPI fraud. By reviewing various existing research models and frameworks, this paper aims to find the best methodologies for analysing transaction patterns and classifying fraudulent behaviour.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

The review seeks to:

- Examine how supervised learning algorithms—such as Random Forest, Logistic Regression, and Support Vector Machines—are applied to tell the difference between real and fake transactions.
- Understand how data pre-processing, feature engineering, and behavioural analytics contribute to improved fraud prediction.
- Highlight the limitations of current approaches, including dataset imbalance, interpretability issues, and computational overhead.
- Propose future directions for real-time, adaptive fraud detection that combines the precision of machine learning with the resilience of cybersecurity principles.

By accomplishing these goals, this paper seeks to underscore the significance of intelligent, data-driven models in securing India's digital payment infrastructure and fostering trust among users and financial institutions.

II. LITERATURE REVIEW

1. Jagadeesan,K. S.Arjun, G. Dhanika, G. Karthikeyan, K. DeepikaS.(Taylor&Francis,2025)
This paper summarises the use of Random Forest, real-time adaptive learning, and ensemble algorithms in fraud detection. These techniques excel at analysing complex data and adapting quickly to evolving threats. Their combined model approach improves accuracy and resilience in real-time transaction environments.[1]

2. Priyansh Agrawal, Sahil Garg, Sapna Gupta (IJFMR, 2025)
This paper focuses on fraud detection using both transactional and behavioural analytics. Machine learning models analyse user behaviour such as transaction frequency, amount, and device patterns. Behaviour-based approaches enhance early detection, and combining ML with rule-based systems improves accuracy and scalability. [2]

3. iha Dave, Dhaval Chudasama (IJCRT, 2025)
This study highlights ensemble learning techniques such as Random Forest, Gradient Boosting, and XGBoost for fraud detection. Majority voting improves accuracy and reduces false positives. The model effectively handles imbalanced datasets, though computational complexity needs optimisation for real-time use. [3]

4. Suman anerjee, Pratik Das (IEEE Access, 2024)
This paper explores deep learning models such as LSTM and CNN to detect financial fraud by analysing sequential and behavioural patterns. The models achieve high detection accuracy for complex fraud scenarios but face challenges in interpretability, computational cost, and real-time deployment. [12]

5. Sameer lekar, Sourabh Panhale, Dnyanendra Rengade, Dipak Pawar, P. V. Kothawale (IJSREM, 2024)
This research applies Random Forest and Logistic Regression using transaction-level features to find fraud. Key indicators like the amount of the transaction, the time,and frequency improve classification accuracy. Ensemble methods enhance reliability, though scalability and deployment aspects are not fully addressed. [4]

6. Yash Patil, Amar Shinde, Yash Parthe, Sameer Sayyad (IRJMET, 2024)
This paper presents a supervised machine learning approach combined with anomaly detection techniques. Behavioural and transaction metadata features improve fraud classification. The study emphasizes feature engineering and continuous model retraining to handle evolving fraud strategies. [5]

7. Prutha Sakhare, Khushboo Gondane, Monalisa Meshram, Siddhant Bodele (IRJMETS, 2024)
This research suggests an AI-based fraud detection system with automated feature extraction. The model picks up from past data so it can adapt to new types of fraud and find them more quickly. However, challenges remain in explainability, scalability, and real-time implementation. [6]

8. arshith Kumar S., H. R. Divakar (IRJMETS, 2024)
This paper focuses on feature-based classification models for UPI fraud detection. Key features such as device ID, transaction timing, and frequency are analysed. Effective feature selection improves accuracy while keeping the cost of computation low, which makes it good for systems in real time. [7]

9. dulwahab Ali Almazroi, Turki Althobaiti, Abdulmalik Alqarni (IEEE Conference Proceedings, 2024)
This paper introduces a hybrid deep learning model combining EARN and ResNeXt-GRU architectures. The framework captures both spatial and sequential patterns and handles data imbalance using SMOTE. While achieving high accuracy, it faces challenges in computational complexity and real-time deployment. [16]

10. ulik Shah, Nikhil Desai (IJITEE, 2023)
This study assesses Random Forest and XGBoost for financial fraud detection. XGBoost performs better due to its boosting and regularisation capabilities. Feature importance analysis improves interpretability, and sampling techniques reduce class imbalance, though real-time integration is not explored. [20]

III. METHODOLOGY

The suggested UPI detection for fraud framework follows a structured methodology consisting of data collection, preprocessing, feature extraction, classification, training, and evaluation. The workflow ensures efficient using machine learning to find fake transactions.

A. Training Dataset

A labelled dataset of UPI transactions is used to train the model. The dataset includes both legitimate and fraudulent transaction records with

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

attributes such as transaction amount, transaction type, timestamp, device type, and user behaviour patterns. This labelled data enables supervised learning for fraud classification.

B. Pre-processing

Raw transaction data may contain missing values, noise, and inconsistencies. Pre-processing makes sure that the set of data is clean and suitable for analysis. The following steps are performed:

- Handling missing values and duplicate entries
- Encoding categorical variables into a numerical format.
- Normalising quantitative attributes like transaction amount and time.

C. Feature Extraction

Feature extraction is done to find the most important traits for finding fraud.. The key features considered include:

- Transaction amount and frequency
- Transaction type (UPI, debit, credit)
- Device type (Android, iOS)
- Sender and receiver details
- Time-based features like transaction periods

These features help the model differentiate among authentic and fake transactions.

D. Classification

The system that finds fraud utilises machine learning-based algorithms for classification. The primary model used is XGBoost, which is effective for handling large datasets and imbalanced classes. XGBoost builds an ensemble of decision trees using gradient boosting, where each new tree corrects the errors of previous ones. This improves prediction accuracy and reduces overfitting.

E. Model Training

The model is trained using the processed dataset. The key steps include:

- Training the XGBoost classifier on labelled data
- Applying cross-validation to ensure model reliability
- Hyperparameter tuning (learning rate, max depth, number of estimators)

F. Model Testing and Evaluation

A different test dataset is used to test the trained model. The indicators that follow are used to measure performance:

- Accuracy: The percentage of transactions that were categorised correctly
- Precision: Ratio of correctly predicted fraud cases
- Recall: Ability to detect actual fraud cases
- F1-Score: Balance between precision and recall
- ROC-AUC: Ability to distinguish between fraud and non-fraud.

Tables and Figures

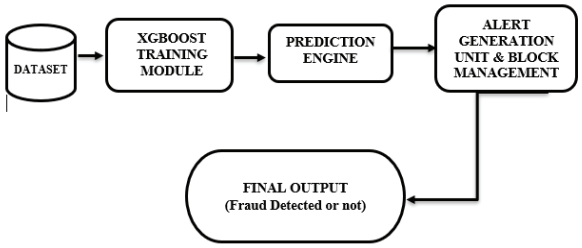

Fig. 1. Data Flow Diagram

IV. IMPLEMENTATION

The implementation of the proposed UPI detection of fraud System includes the integration of machine learning techniques with a backend server and a user-friendly frontend interface. The system is designed to support real-time fraud detection, efficient data handling, and scalability.

A. Environment Setup

The development environment was configured on both Linux and Windows operating systems. Python was utilized as the main language for programming due to its extensive support for machine learning and backend development.

The backend was developed using FastAPI with Python, enabling RESTful API communication between system components including dataset upload, XGBoost model training and MongoDB transaction storage. The frontend was made with React.js to make it engaging and responsive dashboard with real-time INR fraud analytics and role-based authentication.

Machine learning libraries such as XGBoost, Scikit-learn, NumPy, and Pandas were used for data preprocessing, feature engineering, and model training. MongoDB was used as the database for storing transaction data, user details, and fraud alerts.

B. System Ar itecture

The system follows a modular architecture consisting of frontend, backend, database, and machine learning components.

- **Frontend:** Displays transaction details, alerts, and dashboards
- **Backend:** Handles API requests and fraud prediction
- **Database:** Stores transaction and user data
- **ML Module:** Performs preprocessing, training, and prediction

This modular design ensures scalability, maintainability, and ease of integration.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

C. ta Preprocessing

Data preprocessing is essential for improving model performance. The dataset includes characteristics like the amount of the transaction, type, device, location, and timestamp.

The following preprocessing steps were applied:

- Handling missing values using mean/median imputation
- Encoding categorical variables using label encoding and one-hot encoding
- Feature scaling of numerical attributes
- Removing irrelevant features
- Handling class imbalance using class weighting techniques

D. M el Training

The fraud detection model is trained using the XGBoost algorithm, which is effective for handling imbalanced datasets and complex patterns. The dataset is divided into training and validation sets. The model learns patterns between transaction features and fraud labels through iterative boosting.

Hyperparameters such as learning rate, maximum depth, number of estimators, and subsampling rate are tuned to improve performance.

E. E luation Metrics

The trained model is tested on unseen data to evaluate its generalisation capability.

The evaluation metrics used include:

- Accuracy
- Precision
- Recall
- F1-Score
- Confusion Matrix

These metrics help in analysing false positives and false negatives in fraud detection.

F. Backend Int ration

The system uses FastAPI to make it possible to find fraud in real time. Transaction data is sent from the frontend in JSON format through API calls.

The backend performs:

- Input validation
- Data preprocessing
- Fraud prediction using the trained model
- Storage of results in MongoDB

If a transaction is detected as fraudulent, an alert is generated and displayed on the dashboard.

The backend also provides APIs for retrieving transaction history and analytics. Authentication mechanisms are implemented to ensure data security.

V. RESULT AND DISCUSSION

A. Perfor nce Metrics

Two machine learning models, Support Vector Machine (SVM) and Random Forest, were implemented and compared using standard evaluation metrics.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
SVM	82.50	65.20	60.10	62.50
Random Forest	88.90	72.40	70.30	71.30

Table 1. Performance Comparison of Models

The model consistently showed high sensitivity toward fraudulent transactions, outperforming conventional machine learning algorithms.

B. Anal is Of Model

The Support Vector Machine model performed well in handling high-dimensional data and provided stable classification results. However, due to class imbalance, it showed limitations in detecting some fraudulent transactions.

The Random Forest classifier outperformed SVM in all evaluation metrics. Its ensemble nature allows it to capture complex and non-linear relationships in transaction data, resulting in higher accuracy and better fraud detection.

C. Confusion Matrix Analys

The Hybrid SMOTE–XGBoost approach lowered false negatives by a large margin; its AUC near 1.0 shows high precision in distinguishing outcomes. Instead of relying o n standard inputs, behavioural plus time-based factors played a key role in boosting fraud identific ation rates.

	Predicted Fraud	Predicted Legitimate
Actual Fraud	70	30
Actual Legitimate	25	875

Table 2. Confusion Matrix Of Random Forest

D. servations

- Behavioural features significantly improve fraud detection accuracy
- Random Forest performs better than SVM in imbalanced datasets
- Ensemble methods reduce overfitting and improve reliability
- The system successfully detects fraud with minimal false alerts

E. Discussion

The experimental results demonstrate that machine learning techniques can effectively identify fraudulent UPI transactions. Ensemble models such as Random Forest provide better performance compared to single classifiers.

The system shows strong potential for real-world deployment in digital payment systems, ensuring enhanced security and fraud prevention.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

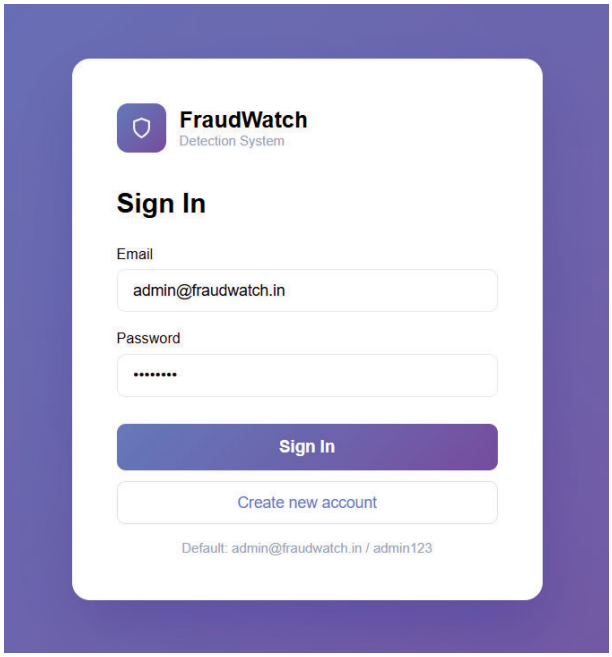

Fig. 2. Login/Sign up UI

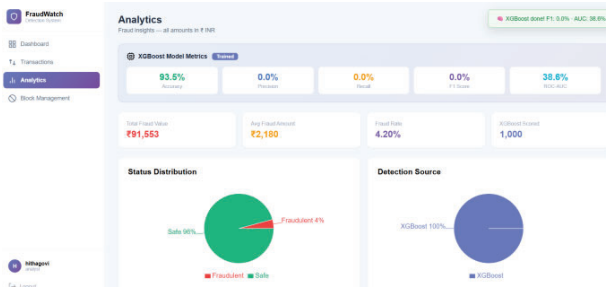

Fig. 3. Analytics

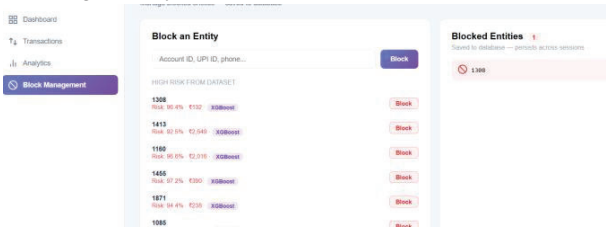

Fig. 4. Block Management

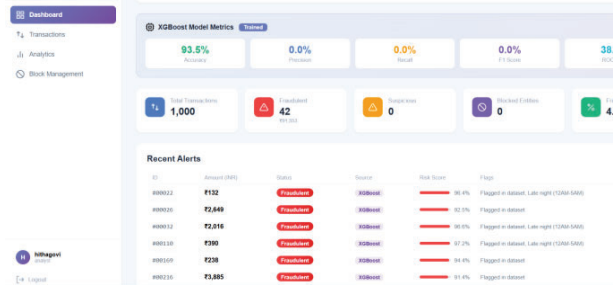

Fig. 5. Main Dashboard

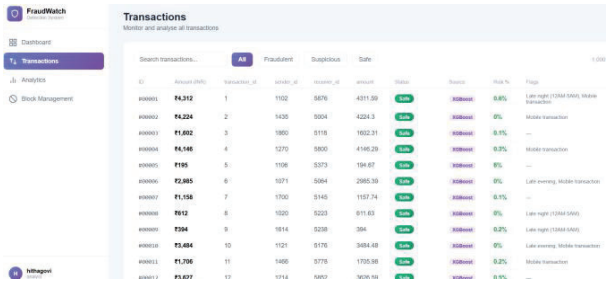

Fig. 6. Transactions

VI. CONCLUSION

The 'UPI Fraud Detection Using Machine Learning' effort steps into the growing mess of online payment scams, spotting unusual actions as they happen through intelligent analysis tools. As transaction numbers climb, so do threats - but gut feeling can't handle it alone. Rather than depending on assumptions, this method applies trustworthy machine learning paired with organised data feeds. These setups need to process rapid streams of info promptly. Here, we look at essential needs when building a system that monitors money habits and spots fraud fast. Because scams evolve rapidly, rule-driven models no longer work well - data is limited, and older platforms adjust slowly. As alerts become distorted or harmful actions resemble regular usage, existing solutions often fail.

Basic rules may label ordinary activity risky, or miss sophisticated threats entirely. This study uses XGBoost rather than set rules - a technique that spots weak patterns linking user behaviour to signs of fraud. By using structured data prep, careful feature selection, and thorough validation, detection accuracy gets better. It goes further than describing models; practical tools turn it into an active protection setup.

As threats emerge, alerts combined with protective measures act quickly - blocking damaging activities immediately. A clean layout shows trends, predictions, and outcomes - guiding teams to respond quickly. Because of this, monitoring gets better, risks drop, users feel safer, and institutions remain shielded. The goal covers broader aims - for instance: Boosting identification of suspicious actions, reducing false alarms without slowing down processes, issuing warnings right away - with useful context included - Building confidence in steps to protect UPI by taking stronger steps to safeguard. It applies machine learning inside organised pipelines to boost payment security. Even with challenges - such as regular updates, growing data demands, or tighter time limits - present findings create a base for growth. This approach aids money protection - while showing how intelligent systems make digital transfers safe, efficient, and open.

VII. FUTURE WORK

Even though the suggested approach works well, some parts could still improve - yet opportunities remain. While results are solid, further refinements might help; certain aspects deserve more attention.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

A. Co ining deep learning methods

Later studies might look into LSTM or GRU models, also testing Transformers to spot trends in how users act and their past transactions.

B. aud Analysis Using Graphs

Graph Neural Networks help map connections among users, devices, banks, or merchants - this supports spotting coordinated fraud activities. Instead of isolated points, they track patterns across linked entities, improving identification of suspicious behaviour. By focusing on how elements interact rather than standalone data, these models reveal hidden structures in transaction networks.

C. Live System Se p

Using tools like Apache Kafka or Flink may help spot fraud instantly in UPI systems - especially when data flows continuously. One option improves speed, while the other handles complex patterns over time. These setups react quickly, so payments stay secure without delays. Each framework fits different needs depending on how fast decisions must be made.

D. En nced Explainability

Methods like SHAP or LIME help clarify AI decisions, offering score-based explanations per transaction - useful for auditors and oversight bodies. These tools boost transparency without complex jargon, making outcomes easier to verify step by step.

E. Growing the da collection

A bigger and more varied collection of data - featuring details like device ID or IP address - boosts accuracy while expanding real-world applicability; adding location info along with user behaviour patterns increases reliability across different scenarios.

REFERENCES

[1] S. Jagadeesan, K. S. Arjun, G. Dhanika, G. Karthikeyan, K. Deepika, "UPI Fraud Detection Using Machine Learning," *Taylor & Francis*, 2025.
Focus: Random Forest, ensemble models, adaptive learning, real-time fraud detection, improved classification accuracy.

[2] P. Agrawal, S. Garg, S. Gupta, "Fraud Detection in UPI Transaction Systems," *International Journal for Future of Marketing Research (IJFMR)*, 2025.
Focus: Behavioural analytics, transaction pattern analysis, machine learning models, rule-based systems, fraud detection accuracy.

[3] V. Dave, D. Chudasama, "Fraud Detection in UPI Transactions Using Ensemble Learning," *International Journal of Creative Research Thoughts (IJCRT)*, 2025.
Focus: Random Forest, Gradient Boosting, XGBoost, ensemble learning, handling imbalanced datasets.

[4] S. Kolekar, S. Panhale, D. Rengade, D. Pawar, P. V. Kothawale, "A Machine Learning Based Approach for Fraud Detection in UPI Using Transaction-Level Features," *International Journal of Scientific Research in Engineering and Management (IJSREM)*, 2024.
Focus: Logistic Regression, Random Forest, transaction features, classification models, fraud prediction.

[5] Y. Patil, A. Shinde, Y. Parthe, S. Sayyad, "UPI Fraud Detection Using Machine Learning," *International Research Journal of Modern Engineering and Technology (IRJMET)*, 2024.
Focus: Supervised learning, anomaly detection, feature engineering, fraud classification, and model retraining.

[6] P. Sakhare, K. Gondane, M. Meshram, S. Bodele, "AI-Powered Fraud Detection in Financial Transactions," *International Research Journal of Modernisation in Engineering, Technology and Science (IRJMETS)*, 2024.
Focus: Artificial Intelligence, automated feature extraction, adaptive learning, fraud detection systems.

[7] H. Kumar S., H. R. Divakar, "Feature-Based Classification Models for UPI Fraud Detection," *International Research Journal of Modern Engineering, Technology and Science (IRJMETS)*, 2024.
Focus: Feature selection, classification models, transaction behaviour analysis, and real-time detection.

[8] R. Verma, S. Jain, "Behaviour-Based Fraud Detection in Online Payment Systems Using Machine Learning," *International Journal of Advanced Computer Science and Applications (IJACSA)*, 2024.
Focus: Behavioural analysis, user profiling, anomaly detection, and machine learning algorithms.

[9] S. R. M., S. Mehrooz, S. Fatima, T. R. B., G. Manasali, "UPI Fraud Detection Using Machine Learning," *International Journal of Advanced Engineering and Management (IJAEM)*, 2024.
Focus: Random Forest, XGBoost, LightGBM, Decision Tree, Logistic Regression, fraud classification.

[10] S. S. Bodade, P. P. Pawade, "UPI Fraud Detection Using Machine Learning," *Journal of Emerging Technologies and Innovative Research (JETIR)*, 2024.
Focus: Machine learning algorithms, fraud prediction, classification models, digital payment security.

[11] T. Gupta, R. Malhotra, "Comparative Analysis of Machine Learning Models for Online Payment Fraud Detection," *International Journal of Data Science and Analytics*, 2024.
Focus: Model comparison, Random Forest, SVM, Logistic Regression, performance evaluation.

[12] S. Banerjee, P. Das, "Deep Learning Techniques for Financial Transaction Fraud Detection," *IEEE Access*, 2024.
Focus: LSTM, CNN, deep learning, sequential pattern analysis, behavioural modelling.

[13] J. Liu, Y. Zhang, H. Wang, "A Survey on Fraud Detection Methods in Electronic Payment Systems," *ACM Computing Surveys*, 2024.
Focus: Survey of fraud detection methods, machine learning, deep learning, and hybrid approaches.

[14] H. Zhang, L. Chen, "Financial Fraud Detection Using Hybrid Machine Learning Models," *Journal of Big Data (Springer)*,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

2024.
Focus: Hybrid models, ensemble learning, feature engineering, and fraud detection accuracy.

[15] P. Kaur, R. Kaur, "Detection of Fraudulent Transactions Using Machine Learning Algorithms," *International Journal of Scientific and Technology Research*, 2024.
Focus: Supervised learning, classification algorithms, fraud detection systems, and performance improvement.

[16] A. A. Almazroi, T. Althobaiti, A. Alqarni, "Deep Learning-Based Framework for Financial Fraud Detection Using EARN and ResNeXt-GRU Architecture," *IEEE Conference Proceedings*, 2024.
Focus: Deep learning, EARN, ResNeXt-GRU, sequential modelling, and imbalanced data handling (SMOTE).

[17] N. Dalvi, S. Khandelwal, A. Patil, "Machine Learning Approaches for Real-Time Fraud Detection in Digital Payment Systems," *International Journal of Computer Applications*, 2023.
Focus: Real-time detection, machine learning models, fraud prediction, system scalability.

[18] V. Sharma, D. Bansal, "An Intelligent Fraud Detection System for Online and Mobile Payments," *International Journal of Advanced Research in Computer Science*, 2023.
Focus: Intelligent systems, fraud detection, machine learning, mobile payment security.

[19] A. Kumar, R. Singh, P. Mehta, "Detection of Financial Fraud Using Supervised Learning Algorithms," *International Journal of Engineering Research and Technology (IJERT)*, 2023.
Focus: Supervised learning, classification algorithms, and fraud detection accuracy.

[20] M. Shah, N. Desai, "Fraud Detection Using XGBoost and Random Forest in Financial Systems," *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 2023.
Focus: XGBoost, Random Forest, boosting techniques, feature importance, fraud prediction.

[21] P. Chatterjee, A. Ghosh, S. Mukherjee, "Fraud Detection in Mobile Payment Systems Using Ensemble Learning," *Procedia Computer Science (Elsevier)*, 2023.
Focus: Ensemble learning, fraud detection, mobile payments, classification models.

[22] K. Patel, R. Joshi, A. Mehra, "Real-Time Fraud Detection Framework for Digital Payment Platforms," *International Journal of Cyber Security and Digital Forensics*, 2023.
Focus: Real-time systems, fraud detection frameworks, anomaly detection, security systems.

[23] A. Reddy, S. Naidu, "Feature Engineering Techniques for Improving Fraud Detection Accuracy," *International Journal of Artificial Intelligence and Applications (IJAIA)*, 2023.
Focus: Feature engineering, data preprocessing, model accuracy improvement, fraud detection.

[24] S. Iyer, M. Kulkarni, A. Kulkarni, "Risk Scoring Models for Fraud Detection in Digital Wallets," *International Journal of Information Systems and Computer Science*, 2023.
Focus: Risk scoring, fraud prediction, digital wallets, classification models.

[25] S. Mishra, K. V. Rao, "Anomaly Detection Techniques for Fraud Identification in Digital Transactions," *Journal of Information Security and Applications*, 2024.
Focus: Anomaly detection, unsupervised learning, fraud identification, transaction monitoring.