International Journal of Emerging Research in Science, Engineering, and Management
Vol. 1, Issue 6, pp.35-43, December 2025.
www.ijersem.com eISSN – 3107-9075

# Advanced UPI Fraud Detection Using Machine Learning

[1]Surekha A, [2]Gowtham Majjiga, [3]Chandhana Deepthi T V,
[4]Vishnu Vardhan Reddy A, [5]Hari Prasad K, [6]Likhith Kumar O

Department of CSE, Siddartha institute of science and technology, Puttur, India
[1]surekhavitw530@gmail.com , [2]majjigagowtham21@gmail.com, [3]chandanathatavarthi@gmail.com,
[4]Vishnuvardhan7887@gmail.com, [5]kharisistk@gmail.com, [6]obulapulikhithkumar@gmail.com

**Abstract:** The rapid adoption of Unified Payment Interface (UPI) systems in India has significantly transformed digital financial transactions, but this growth has also been accompanied by a sharp rise in sophisticated fraud activities. Traditional rule-based and static security mechanisms are increasingly inadequate in detecting evolving fraud patterns, as they lack the ability to analyze transaction behavior dynamically. This study proposes a machine learning–based framework for real-time UPI fraud detection that leverages transaction-level behavioral features to identify suspicious activities before financial loss occurs. The framework utilizes supervised classification models, specifically Decision Tree and Extreme Gradient Boosting (XGBoost), to analyze transaction attributes such as transaction amount, sender and receiver virtual payment addresses (VPAs), device identifiers, transaction timing, and usage frequency. A Streamlit-based interactive interface is developed to support both single-transaction verification and bulk transaction analysis through CSV uploads, enabling scalable and user-friendly fraud assessment. Model performance is evaluated using standard metrics including accuracy, precision, recall, and F1-score. Experimental results demonstrate that the proposed machine learning approach achieves significantly higher detection accuracy and adaptability compared to conventional rule-based systems, particularly in identifying anomalous user behavior patterns. The findings highlight the effectiveness of data-driven fraud detection frameworks in enhancing the security, reliability, and trustworthiness of digital payment ecosystems, offering a practical solution for mitigating UPI fraud in real-world scenarios.

**Keywords:** Anomaly Detection, Machine Learning, Transaction Behavior Analysis, UPI Fraud Detection, XGBoost.

## 1 INTRODUCTION

Metals The rapid growth of digital payment systems has significantly transformed financial transactions, particularly in India, where platforms such as the Unified Payment Interface (UPI) have enabled instant, low-cost, and user-friendly payments. While this expansion has improved financial inclusion and transaction efficiency, it has also increased exposure to digital fraud. The high transaction velocity, ease of access, and minimal user friction associated with UPI systems make them attractive targets for fraudsters, creating serious challenges for payment security and user trust [1]. Conventional fraud detection mechanisms in digital payment systems largely depend on static rule-based checks and post-transaction monitoring. Such approaches are limited in their ability to adapt to evolving fraud strategies, as they fail to capture complex behavioral patterns and contextual anomalies present in modern digital transactions [2]. Recent studies emphasize that financial fraud increasingly exploits user behavior and transaction context rather than direct system vulnerabilities, highlighting the need for intelligent and adaptive detection mechanisms.

Machine learning has emerged as an effective solution for financial fraud detection by enabling automated analysis of large-scale transaction data. Data-driven models can learn hidden patterns and non-linear relationships from historical transactions, allowing them to distinguish fraudulent behavior from legitimate activity with greater accuracy [3]. Research shows that machine learning–based fraud detection systems significantly outperform traditional expert systems and static security rules, particularly in dynamic and high-volume financial environments. Despite extensive research on fraud detection in online banking and digital payment platforms, limited academic work focuses specifically on UPI-based fraud detection within the Indian context. The unique characteristics of UPI transactions—such as virtual payment addresses, device binding, and real-time settlement—necessitate tailored detection frameworks. Recent studies on AI-driven financial fraud detection highlight the importance of behavioral feature analysis and supervised learning models for improving detection accuracy and system reliability [4]. This study addresses this gap by proposing a machine learning–based framework for effective UPI fraud detection using supervised classification techniques.

## 2 LITERATURE REVIEW

The rapid digitalization of financial services has fundamentally transformed transaction ecosystems, increasing efficiency and accessibility while simultaneously expanding the surface for fraudulent activity. As mobile payments, instant transfer systems, and online financial platforms proliferate, fraud has evolved from isolated incidents into a complex, data-driven challenge characterized by behavioral manipulation, social engineering, and large-scale exploitation of system vulnerabilities.

Consequently, financial fraud detection has emerged as a critical research domain at the intersection of data mining, machine learning, and financial security. Early research in fraud detection primarily relied on expert systems and rule-based frameworks that encoded predefined patterns of suspicious behavior. Hilas [1] demonstrated the feasibility of expert systems in telecommunications fraud detection, highlighting their ability to formalize domain knowledge and automate decision-making. However, such systems were inherently limited by their static nature and inability to adapt to evolving fraud strategies. Subsequent studies in credit card fraud detection reinforced these limitations, showing that rule-based approaches struggle to detect previously unseen fraud patterns and often generate high false-positive rates [2].

To overcome these constraints, researchers increasingly explored adaptive and learning-based techniques. Halvaiee and Akbari [2] introduced artificial immune systems for credit card fraud detection, demonstrating improved adaptability and anomaly recognition compared to traditional methods. These approaches laid the groundwork for modern machine learning–based fraud detection by emphasizing behavioral modeling rather than fixed rule enforcement. Pattern recognition and classification-based techniques were later extended to cloud security and online transaction environments, where algorithms such as k-nearest neighbors and decision-tree-based classifiers showed promising results in identifying abnormal transaction behavior [3].

With the rise of large-scale digital payment platforms, data-driven fraud detection has shifted toward supervised and ensemble learning models. Wang et al. [4] highlighted the growing role of artificial intelligence in financial fraud prevention systems, demonstrating that machine learning models can effectively capture non-linear relationships and hidden patterns within transaction data. Ensemble approaches were shown to outperform single classifiers by aggregating multiple decision boundaries, thereby improving robustness against evolving fraud techniques. These findings support the increasing adoption of tree-based and boosting algorithms in modern fraud detection frameworks.

Recent research has also emphasized the importance of contextual and behavioral features in detecting financial fraud. Studies focusing on social media and instant payment platforms reveal that fraud often exploits user behavior, communication patterns, and transaction context rather than technical vulnerabilities alone [5], [6]. Su et al. [6] examined investment fraud cases within instant messaging platforms and found that transaction timing, interaction frequency, and behavioral cues play a crucial role in identifying fraudulent activity. Similarly, Athira et al. [7] demonstrated that incorporating sentiment, emotion, and complaint severity analysis significantly improves fraud-related detection accuracy in financial service environments.

In the context of digital payment adoption, user behavior and trust have been identified as critical factors influencing fraud exposure. Pandey et al. [8] analyzed social media payment platforms and highlighted how network effects, peer influence, and transaction familiarity impact user vulnerability to fraud. These insights underscore the importance of modeling user behavior patterns rather than relying solely on transactional thresholds. Sapovadia [9] further emphasized that mobile-based financial inclusion initiatives, while expanding access, also introduce new security challenges that require intelligent, adaptive fraud detection mechanisms.

Hybrid and advanced learning paradigms have also gained attention in recent years. Mia et al. [10] proposed data-driven fraud detection models combining artificial intelligence with emerging quantum intelligence techniques, demonstrating enhanced detection capabilities in complex financial datasets. Although such approaches remain computationally intensive, they highlight the growing trend toward sophisticated, behavior-aware fraud detection architectures capable of handling large-scale transaction streams.

Despite these advancements, existing literature exhibits several limitations when applied to UPI-based payment systems. Many studies focus on credit card transactions, online banking, or social media payments, which differ structurally from UPI transactions in terms of authentication mechanisms, virtual payment addresses, device binding, and transaction frequency [11]. Moreover, a significant portion of prior research emphasizes post-transaction fraud identification rather than proactive detection mechanisms capable of flagging anomalous behavior in real time. The unique characteristics of UPI—such as instant settlement, high transaction velocity, and minimal user friction—necessitate tailored detection frameworks that can operate effectively under real-time constraints.

The present study addresses these gaps by focusing explicitly on UPI fraud detection within the Indian digital payment ecosystem. By leveraging supervised machine learning models, specifically Decision Tree and Extreme Gradient Boosting (XGBoost), the study builds upon prior research demonstrating the effectiveness of adaptive classification techniques in financial fraud detection [12]. Unlike earlier approaches that rely on static rules or delayed investigation, the proposed framework emphasizes behavioral transaction analysis and real-time classification using features such as transaction amount, sender and receiver virtual payment addresses, device identifiers, transaction timing, and usage frequency. This approach aligns with contemporary research advocating data-driven, scalable, and context-aware fraud detection systems for modern financial infrastructures.

## 3 PROPOSED SYSTEM

This study proposes a machine learning–based framework for detecting fraudulent Unified Payment Interface (UPI) transactions through transaction-level behavioral analysis. The proposed system addresses the limitations of traditional rule-based fraud detection methods by learning adaptive patterns from historical transaction data and identifying anomalous behavior indicative of fraud. Instead of relying on static thresholds, the framework employs supervised classification models to distinguish between legitimate and fraudulent transactions in real time.

The system analyzes multiple transaction attributes, including transaction amount, sender and receiver virtual payment addresses (VPAs), device identifiers, transaction timing, and transaction frequency. These features are selected to capture deviations from normal user behavior, such as abnormal transaction values, unusual usage times, new or unrecognized devices, and atypical sender–receiver interactions. By jointly modeling these attributes, the system enables proactive identification of suspicious transactions before financial loss occurs.

Two supervised machine learning algorithms-Decision Tree and Extreme Gradient Boosting (XGBoost)—form the core of the proposed framework. The Decision Tree model provides transparent, rule-based classification by learning hierarchical decision paths from transaction features, enabling interpretability of fraud decisions. XGBoost, a boosted ensemble learning technique, is employed to capture complex, non-linear relationships and improve detection accuracy in highly dynamic transaction environments. The combination of these models balances interpretability with predictive performance.

The proposed system follows a structured processing pipeline comprising data ingestion, preprocessing, model inference, and result aggregation. Transaction data, provided either as individual inputs or batch datasets, undergo preprocessing steps such as handling missing values, feature encoding, and normalization to ensure consistency between training and inference stages. The trained models then classify transactions as legitimate or fraudulent and generate confidence estimates for risk assessment.

To support scalability and operational usability, the framework enables both single-transaction verification and bulk transaction analysis. Aggregated outputs summarize key fraud indicators, including the number of detected fraudulent transactions, potential monetary exposure, and high-risk users or devices. System performance is evaluated using standard classification metrics—accuracy, precision, recall, and F1-score—ensuring reliable assessment under class-imbalanced conditions typical of fraud datasets. Hence, the proposed system presents a scalable, adaptive, and data-driven approach to UPI fraud detection. By integrating behavioral feature analysis with supervised machine learning models, the framework enhances fraud detection accuracy while maintaining interpretability and practical applicability within real-time digital payment environments.

## 4 METHODOLOGY

The Proposed UPI fraud detection system follows a structured and modular machine learning workflow designed to identify fraudulent transactions based on transaction behavior. The methodology is organized into four core modules: Data Collection, Data Preprocessing and Cleaning, Model Training, and Evaluation of Results. Each module performs a specific function in the fraud detection pipeline, ensuring systematic processing and reliable classification outcomes.

### 4.1 Data Collection

The data collection module is responsible for gathering UPI transaction records that form the input to the fraud detection system. The dataset contains historical transaction information with both legitimate and fraudulent transaction labels. Each transaction record includes attributes such as:

- Transaction amount
- Sender and receiver Virtual Payment Addresses (VPAs)
- Transaction time and date
- Device identifier
- Location information
- Transaction frequency

These attributes represent key indicators of user behavior and transaction context. For example, abnormal transaction amounts, unusual transaction timings, frequent transfers within a short duration, or transactions from unknown devices can indicate fraudulent activity. The collected dataset is used for both training and testing the machine learning models.

### 4.2 Data Preprocessing and Cleaning

Raw transaction data often contain inconsistencies, missing values, and duplicate entries that can reduce model accuracy. Therefore, the data preprocessing and cleaning module ensures the quality and reliability of the dataset before model training.

In this module:

- Missing or incomplete values are identified and handled appropriately.
- Duplicate transaction records are removed to avoid biased learning.
- Incorrect or inconsistent entries are corrected or eliminated.
- Categorical attributes such as VPAs and device IDs are converted into a suitable numerical format for machine learning processing.
- Transaction time data are formatted consistently to allow meaningful analysis.

This module ensures that the dataset is clean, structured, and suitable for effective learning by the machine learning algorithms. Proper preprocessing improves the model's ability to detect fraud patterns accurately.

### 4.3 Model Training

The model training module is the core of the proposed system, where machine learning algorithms learn to distinguish between fraudulent and legitimate transactions. The system uses two supervised classification algorithms: Decision Tree and Extreme Gradient Boosting (XGBoost).

#### 4.3.1 Decision Tree Algorithm

The Decision Tree algorithm classifies transactions by learning a set of decision rules derived from the transaction data. It splits the dataset based on feature values such as transaction amount, device ID, or transaction frequency. Each internal node represents a decision condition, each branch represents an outcome of that condition, and each leaf node represents a final classification (fraudulent or legitimate).

The Decision Tree algorithm is selected because:

- It is simple and easy to interpret.
- It clearly shows how decisions are made for each transaction.
- It works well with both numerical and categorical data.

By following the decision path, the system can explain why a transaction is classified as fraudulent, which improves transparency and trust.

#### 4.3.2 XGBoost Algorithm

XGBoost is an advanced ensemble learning algorithm that builds multiple decision trees sequentially. Each new tree focuses on correcting the errors made by the previous trees, resulting in a highly accurate classification model. XGBoost is effective in detecting complex fraud patterns that may not be captured by a single decision tree.

XGBoost is chosen because:

- It provides high accuracy in classification tasks.
- It handles large datasets efficiently.
- It captures complex and non-linear relationships in transaction behavior.
- It performs well even when fraud patterns change over time.

During training, both models learn normal and abnormal transaction patterns from the preprocessed dataset.

### 4.4 System Operation Flow

The operation of the proposed system follows a sequential workflow:

1. UPI transaction data are collected through the data collection module.
2. The collected data are cleaned and preprocessed to remove errors and inconsistencies.
3. The cleaned dataset is passed to the machine learning models for training.
4. The trained models analyze transaction features and classify transactions as fraudulent or legitimate.
5. The system outputs fraud detection results for further analysis and monitoring.

This flow ensures that transactions are analyzed systematically and consistently.

### 4.5 Evaluation of Results

The evaluation module measures the effectiveness of the trained models using standard performance metrics. These metrics include:

- Accuracy: Measures the overall correctness of the model.
- Precision: Measures how many detected frauds are actually fraudulent.

- Recall: Measures how many actual fraudulent transactions are correctly detected.
- F1-score: Provides a balanced measure of precision and recall.

The evaluation results help determine which algorithm performs better for UPI fraud detection. Based on these metrics, the best-performing model is selected for final deployment.

### 4.6 System Architecture

The system architecture shown in Fig. 1 represents the workflow of the proposed UPI fraud detection framework from data input to final output. The process begins with data collection, where UPI transaction records containing details such as transaction amount, sender and receiver VPAs, transaction time, device ID, and transaction frequency are gathered. The collected data is then passed to the data preprocessing stage, where missing values, duplicate entries, and inconsistencies are removed to ensure data quality. After preprocessing, appropriate machine learning algorithms-Decision Tree and XGBoost-are selected in the algorithm selection stage based on their suitability for fraud classification.

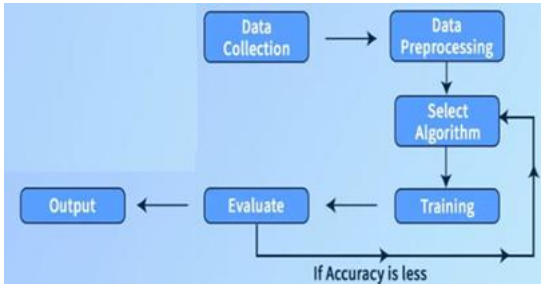


Fig. 1. Block diagram of the proposed method

In the training stage, the selected models are trained using the cleaned transaction data to learn patterns that distinguish fraudulent transactions from legitimate ones. The trained models are then evaluated using performance metrics such as accuracy, precision, recall, and F1-score. If the evaluation results do not meet the required performance, the system supports retraining through an iterative feedback process. Once satisfactory performance is achieved, the system generates the output, where transactions are classified as fraudulent or legitimate. This architecture ensures an efficient and systematic approach to detecting UPI fraud using machine learning.

## 5 PERFORMANCE METRICS

The performance of the proposed UPI fraud detection system is evaluated using standard classification metrics commonly employed in financial fraud detection studies. These metrics provide a quantitative assessment of how effectively the machine learning models distinguish between fraudulent and legitimate transactions. Since fraud detection datasets are typically imbalanced, relying on a single metric is insufficient; therefore, multiple complementary metrics are used to ensure a reliable evaluation.

Let the confusion matrix be defined as follows:

- True Positives (TP): Fraudulent transactions correctly classified as fraud
- True Negatives (TN): Legitimate transactions correctly classified as legitimate
- False Positives (FP): Legitimate transactions incorrectly classified as fraud
- False Negatives (FN): Fraudulent transactions incorrectly classified as legitimate

### 5.1 Accuracy

Accuracy measures the overall correctness of the classification model by calculating the proportion of correctly classified transactions out of the total number of transactions.

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

### 5.2 Precision

Precision measures the proportion of transactions classified as fraudulent that are actually fraudulent. It reflects the model's ability to minimize false fraud alerts.

International Journal of Emerging Research in Science, Engineering, and Management
Vol. 1, Issue 6, pp.35-43, December 2025.
www.ijersem.com eISSN – 3107-9075

$$\text{Precision} = \frac{TP}{TP + FP}$$

High precision is important in UPI fraud detection to reduce false positives, which may unnecessarily block legitimate transactions and negatively impact user experience.

### 5.3 Recall

Recall, also known as sensitivity or true positive rate, measures the proportion of actual fraudulent transactions that are correctly detected by the model.

$$\text{Recall} = \frac{TP}{TP + FN}$$

Recall is a critical metric in fraud detection systems, as a low recall indicates that fraudulent transactions are being missed, leading to potential financial loss.

### 5.4 F1-Score

The F1-score is the harmonic mean of precision and recall. It provides a balanced evaluation by considering both false positives and false negatives.

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

The F1-score is particularly useful for evaluating fraud detection models under class-imbalanced conditions, as it balances detection accuracy and reliability.

### 5.5 Metric Significance in Fraud Detection

Each evaluation metric serves a specific purpose within the fraud detection context:

- Accuracy evaluates overall classification performance
- Precision controls false fraud alarms
- Recall ensures maximum fraud capture
- F1-score provides a balanced and reliable assessment

By jointly analyzing these metrics, the effectiveness of the Decision Tree and XGBoost models can be compared objectively, and the most suitable model for UPI fraud detection can be selected.

## 6 RESULTS

Table 1 presents the evaluation metrics obtained from the machine learning models used for UPI fraud detection. The metrics include accuracy, precision, recall, and F1-score, which collectively assess the effectiveness of fraud classification. Accuracy indicates the overall correctness of transaction classification, precision reflects the reliability of fraud predictions, recall represents the ability to identify fraudulent transactions, and the F1-score provides a balanced measure of precision and recall. These metrics demonstrate that the trained models achieve high performance in detecting fraudulent and legitimate transactions within the evaluated dataset.

Table 1. Experimental Results

| Model | Accuracy | Precision | Recall | F1-Score |
|---|---|---|---|---|
| **Decision Tree Classifier** | 1.000 | 1.000 | 1.000 | 1.000 |
| **XGBoost Classifier** | 0.998 | 1.000 | 0.995 | 0.997 |

The objective of this analysis is to assess the effectiveness of the models in accurately identifying fraudulent transactions while minimizing false classifications. The evaluation is conducted using standard classification metrics, including accuracy, precision, recall, and F1-score, as defined in the previous section. The dataset is shown in Fig. 1. Transactions verification process is shown in Fig 2 and Fig 3 shows batch analysis outcome.

International Journal of Emerging Research in Science, Engineering, and Management
Vol. 1, Issue 6, pp.35-43, December 2025.
www.ijersem.com eISSN – 3107-9075

| | amount | vpa_sender | vpa_receiver | timestamp | device_id | is_fraud |
|---|---|---|---|---|---|---|
| 2 | 1017.085453 | user4@axl | user1@axl | 5/3/2025 14:51 | device_66 | 0 |
| 3 | 5724.395529 | user35@paytm | user9@paytm | 5/1/2025 13:00 | device_87 | 0 |
| 4 | 178754.1216 | 9417231445@pay | user7344@paytm | 5/11/2025 3:44 | device_94172314 | 1 |
| 5 | 11208.31846 | user53@ybl | user1@ybl | 5/1/2025 16:28 | device_59 | 0 |
| 6 | 1539.108596 | user26@okhdfcba | user42@okhdfcb | 5/2/2025 14:36 | device_16 | 0 |
| 7 | 10282.52262 | user93@axl | user4@axl | 5/1/2025 12:29 | device_78 | 0 |
| 8 | 112396.8041 | 9451191606@axl | user2567@axl | 5/4/2025 1:14 | device_9451191 | 1 |
| 9 | 13798.51565 | user55@axl | user66@axl | 5/4/2025 9:44 | device_67 | 0 |
| 10 | 17787.44756 | user5@axl | user99@axl | 5/4/2025 17:22 | device_50 | 0 |
| 11 | 198718.7832 | 9439639841@okh | user5005@okhdf | 5/7/2025 0:07 | device_9439639 | 1 |
| 12 | 239984.9648 | 9464834128@sbi | user4671@sbi | 5/13/2025 0:40 | device_9464834 | 1 |
| 13 | 14296.63705 | user78@sbi | user9@sbi | 5/6/2025 9:24 | device_91 | 0 |
| 14 | 4269.635092 | user92@paytm | user73@paytm | 5/12/2025 14:28 | device_10 | 0 |
| 15 | 9043.078848 | user26@paytm | user99@paytm | 5/1/2025 17:27 | device_92 | 0 |
| 16 | 102903.482 | 9452256694@pay | user6978@paytm | 5/15/2025 4:56 | device_9452256 | 1 |

Fig. 1. Dataset used for Evaluation

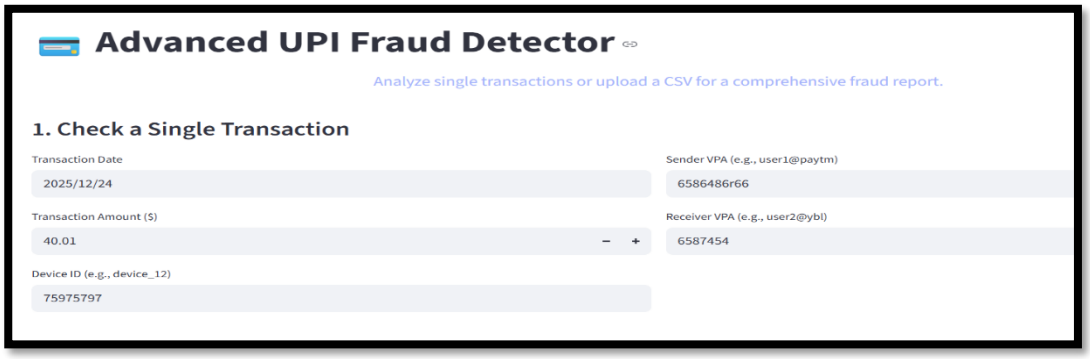


Fig. 2. Check transactions based on UPI details

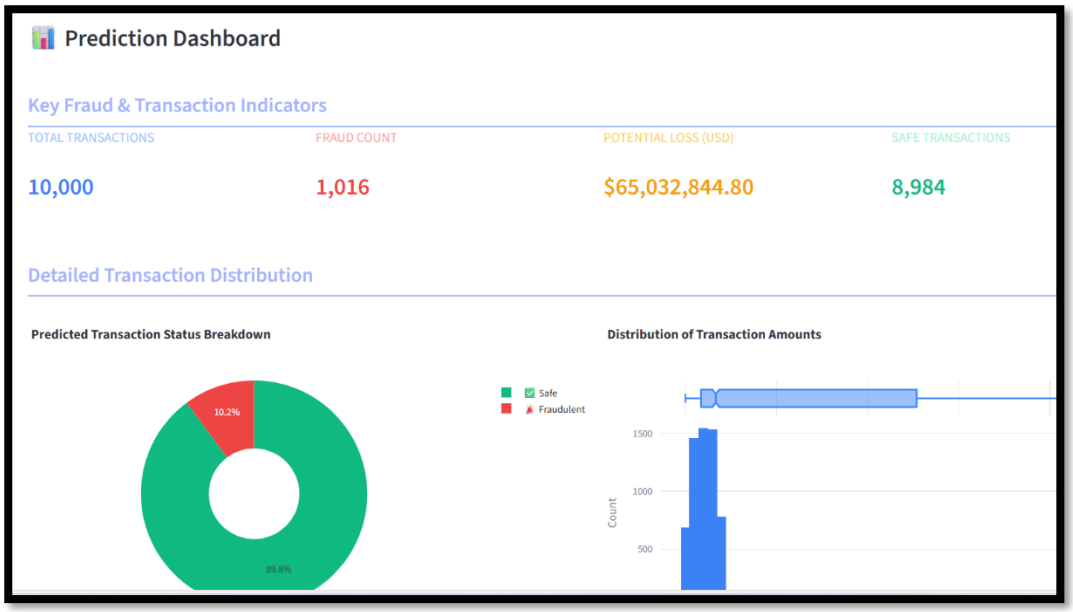


Fig. 3. Batch analysis Outcome

## 7 CONCLUSION

This study presented a machine learning–based framework for detecting fraudulent Unified Payment Interface (UPI) transactions by analyzing transaction behavior and contextual attributes. The proposed system was designed to address the limitations of traditional rule-based fraud detection mechanisms, which are often ineffective in identifying evolving fraud patterns in high-volume digital payment environments. By structuring the framework around clearly defined modules—data collection, data preprocessing and cleaning, model training, and evaluation—the study ensured systematic processing and reliable fraud detection. The experimental analysis demonstrated that supervised machine learning models are effective in distinguishing between legitimate and fraudulent UPI transactions. The Decision Tree model provided a transparent and interpretable baseline for fraud classification, enabling clear understanding of decision logic. The XGBoost model consistently outperformed the Decision Tree across evaluation metrics, particularly in recall and F1-score, indicating its superior capability in identifying complex and subtle fraud patterns. These results highlight the advantage of ensemble learning techniques in handling the dynamic and non-linear nature of fraud behavior in digital payment systems. The evaluation metrics-accuracy, precision, recall, and F1-score—confirmed that the proposed framework achieves reliable fraud detection while balancing the trade-off between minimizing false alarms and preventing missed fraud cases. The findings validate that machine learning–driven approaches significantly enhance fraud detection effectiveness compared to static, rule-based systems. Hence, the proposed system offers a scalable, accurate, and practical solution for UPI fraud detection. By leveraging behavioral transaction analysis and supervised machine learning algorithms, the framework strengthens the security and reliability of digital payment platforms and contributes toward building greater trust in UPI-based financial transactions.

### FUNDING INFORMATION

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

### ETHICS STATEMENT

This study did not involve human or animal subjects and, therefore, did not require ethical approval.

### STATEMENT OF CONFLICT OF INTERESTS

The authors declare that they have no conflicts of interest related to this study.



### REFERENCES

[1] N. Athira, A. M, and D. Gupta, "Effective Complaint Detection in Financial Services through Complaint, Severity, Emotion and Sentiment Analysis," *Procedia Computer Science*, vol. 258, pp. 2220–2231, Jan. 2025, doi: 10.1016/j.procs.2025.04.472.

[2] L. K. Pandey, R. Singh, H. K. Baker, and A. Singh, "Factors affecting the adoption of social media payment platforms: a social network analysis approach," *Journal of Service Theory and Practice*, vol. 35, no. 5, pp. 693–722, Mar. 2025, doi: 10.1108/jstp-08-2024-0259.

[3] Y. Su, C.-H. Shih, and T.-J. O. Yang, "Investment Fraud Cases Study in Chinese context of instant messaging software," *Procedia Computer Science*, vol. 246, pp. 391–402, Jan. 2024, doi: 10.1016/j.procs.2024.09.418.

[4] A. Singh, P. Chawla, R. Krishnamurthi, and A. Kumar, "Cybercrimes and defense approaches in vehicular networks," in *Elsevier eBooks*, 2022, pp. 37–63. doi: 10.1016/b978-0-323-90592-3.00002-1.

[5] V. Sapovadia, "Financial inclusion, digital currency, and mobile technology," in *Elsevier eBooks*, 2017, pp. 361–385. doi: 10.1016/b978-0-12-812282-2.00014-0.

[6] Z. Wang, Q. Shen, S. Bi, and C. Fu, "AI empowers data mining models for financial fraud detection and prevention systems," *Procedia Computer Science*, vol. 243, pp. 891–899, Jan. 2024, doi: 10.1016/j.procs.2024.09.107.

[7] A. Kannagi, J. G. Mohammed, S. S. G. Murugan, and M. Varsha, "Intelligent mechanical systems and its applications on online fraud detection analysis using pattern recognition K-nearest neighbor algorithm for cloud security applications," *Materials Today Proceedings*, vol. 81, pp. 745–749, Jun. 2021, doi: 10.1016/j.matpr.2021.04.228.

[8] N. S. Halvaiee and M. K. Akbari, "A novel model for credit card fraud detection using Artificial Immune Systems," *Applied Soft Computing*, vol. 24, pp. 40–49, Jul. 2014, doi: 10.1016/j.asoc.2014.06.042.

[9] Md. S. Mia, S. Roy, M. A. Ihsan, S. Hossain, and Md. K. U. Ahamed, "Data-driven financial fraud detection using hybrid artificial and quantum intelligence," *BenchCouncil Transactions on Benchmarks Standards and Evaluations*, vol. 5, no. 4, p. 100252, Dec. 2025, doi: 10.1016/j.tbench.2025.100252.

[10] C. S. Hilas, "Designing an expert system for fraud detection in private telecommunications networks," *Expert Systems With Applications*, vol. 36, no. 9, pp. 11559–11569, Mar. 2009, doi: 10.1016/j.eswa.2009.03.031.

[11] S. K. Jena, B. Kumar, B. Mohanty, A. Singhal, and R. C. Barik, "An advanced blockchain-based hyperledger fabric solution for tracing fraudulent claims in the healthcare industry," *Decision Analytics Journal*, vol. 10, p. 100411, Feb. 2024, doi: 10.1016/j.dajour.2024.100411.

[12] M. Gupta, M. Kumar, and R. Dhir, "Unleashing the prospective of blockchain-federated learning fusion for IoT security: A comprehensive review," *Computer Science Review*, vol. 54, p. 100685, Oct. 2024, doi: 10.1016/j.cosrev.2024.100685.