iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79848

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

FedUpi: Federated Learning for Fraudulent UPI Transaction Detection

Abhishek Sreeji[1], Akshay G[2], Amal Shajahan Rawther[3], Aswin Krishna[4], Subina S B[5], Mrs. Asha Liza John[6]
Dept of Computer Science (Data Science), St.Thomas Institute for Science & Technology, Trivandrum, India

Abstract: ***The rapid adoption of the Unified Payments Interface (UPI) in India has revolutionized digital transactions while simultaneously catalyzing a surge in sophisticated financial fraud. Traditional detection systems, often reliant on rule-based engines or basic machine learning models like Random Forest, frequently fail to capture the complex, non-linear dependencies inherent in high-cardinality data such as Merchant IDs, VPA handles, and Device Fingerprints. This research proposes a deep learning-based approach using the TabTransformer architecture to enhance detection accuracy. By utilizing a multi-head self attention mechanism, the model maps categorical features into robust contextual embeddings, enabling it to learn intricate relationships between user behavior and transaction attributes. The framework encompasses rigorous data preprocessing with velocity feature engineering, class imbalance mitigation via SMOTE, and real-time inference simulation. Evaluated using Precision-Recall curves and F1-scores, the results demonstrate that this attention-based approach significantly outperforms traditional gradient-boosted trees, providing a scalable, robust, and highly accurate solution for securing the modern fintech ecosystem against evolving fraudulent patterns.***

Keywords: UPI Fraud Detection, Federated Learning, Financial Security, Ensemble Learning, Zero-Day Fraud, Privacy Preservation.

I. INTRODUCTION

The adoption of digital payment platforms such as UPI has revolutionised financial transactions by enabling fast, seamless, and low-cost payments. However, this rapid adoption has also led to an increase in fraudulent activities, including phishing, account takeover, and manipulation. Traditional fraud detection systems rely on centralised data collection and supervised machine learning models trained on historical fraud patterns. While effective against known attacks, these systems struggle to detect new and evolving fraud strategies and raise significant concerns regarding user data privacy. FedUPI addresses these limitations by introducing a federated learning-based fraud detection system, where multiple banks collaboratively train models without sharing raw transaction data. By combining distributed learning with anomaly detection techniques, FedUPI aims to identify both known and unknown fraudulent transactions in real time.

II. LITERATURE SURVEY

Recent research has explored machine learning approaches for financial fraud detection, focusing on improving accuracy and handling imbalanced datasets. Supervised learning models such as Random Forest, XGBoost, and Deep Neural Networks have demonstrated strong performance in detecting known fraud patterns. Unsupervised techniques, including autoencoders and anomaly detection algorithms, have been used to identify unusual transaction behaviour without requiring labelled data. These methods are particularly effective for detecting zero-day fraud. Federated learning has emerged as a promising solution for privacy-preserving collaborative learning. It allows multiple institutions to train shared models without exposing sensitive financial data. Studies have shown that federated approaches can achieve comparable performance to centralized models while ensuring data confidentiality. Ensemble learning techniques further enhance detection by combining predictions from multiple models, improving robustness and reducing false positives.

III. METHODOLOGY

A. System Overview

FedUPI operates as a distributed fraud-detection ecosystem that allows multiple banks to collaboratively detect fraudulent UPI transactions without sharing sensitive user data. In contrast to traditional fraud engines that aggregate transaction logs in a central repository, FedUPI implements a federated architecture. Each participating bank deploys a local instance of the fraud-detection pipeline. A data acquisition layer streams raw transaction records from the bank's UPI logs and

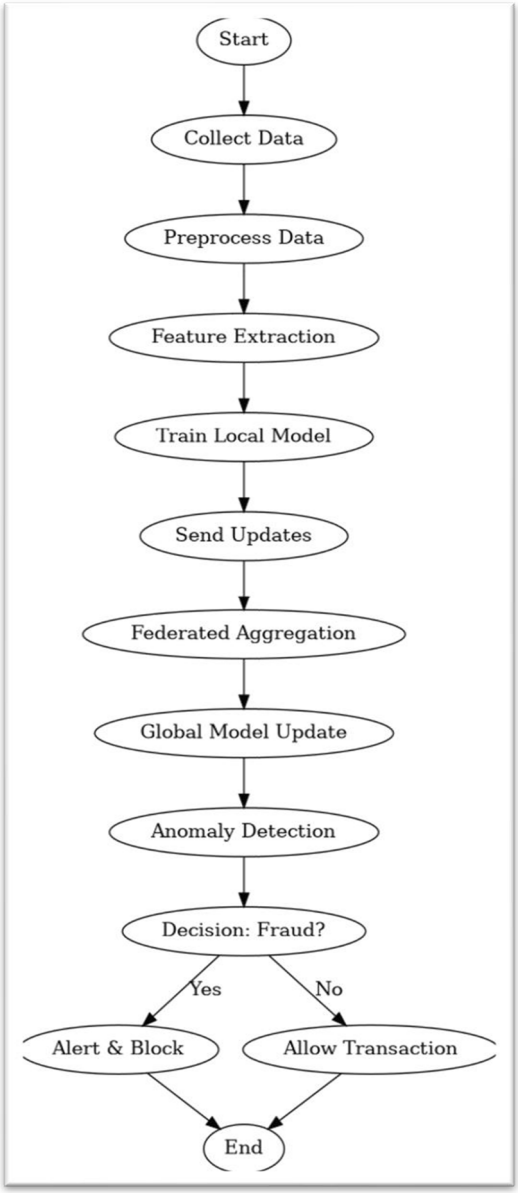


Fig.1. FedUPI Workflow

retains them on premise. A preprocessing and feature-engineering layer cleans and transforms these records into a structured format. A federated training layer allows each institution to train a local machine-learning model and send only model updates—never raw data—to a central aggregator. The ensemble decision layer combines predictions from multiple models to provide a consensus judgement on whether a transaction is fraudulent. Finally, a real-time visualization layer presents analysts with live risk scores, alerts and transaction trends. This layered design ensures privacy preservation, scalability and adaptability. Only gradient updates or model parameters cross institutional boundaries, addressing regulatory concerns about user data privacy.To support the decentralised nature of UPI payments, FedUPI uses a hub-and-spoke approach. A central coordinating server periodically broadcasts the latest global model to all banks. Each bank integrates the global model into its local processing pipeline and trains it on its own data. After training, the bank sends back updated model parameters for aggregation. Because only learned weights are communicated, each bank retains complete control over its transaction records and can comply with banking regulations. The process repeats in iterative federated rounds until the global model converges. This collaborative training scheme leverages the diversity of transaction patterns across banks to improve detection accuracy while preserving confidentiality.

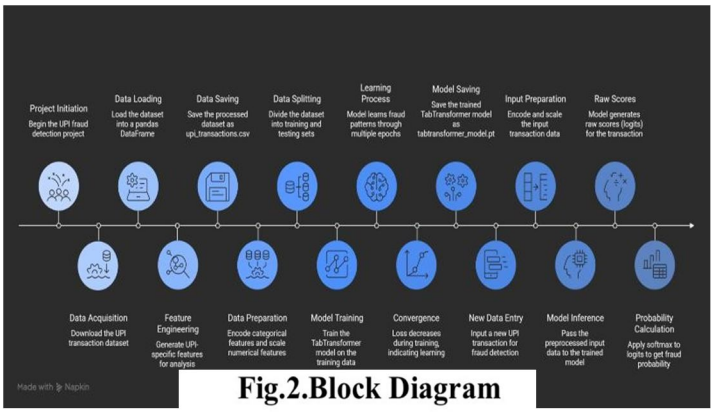


Fig.2.Block Diagram

B. Data Acquisition

FedUPI ingests data from multiple sources to capture a comprehensive view of payment behaviour. The primary source is the UPI transaction log generated by each participating bank. These logs contain attributes such as transaction identifiers, timestamps, payer and payee UPI IDs, amounts, merchant codes and channel information (in-app, QR scan, peer-to-peer, etc.). To bootstrap the detection pipeline, banks can optionally incorporate curated historical fraud datasets containing labelled examples of known scams and phishing attacks. Once the system is deployed, it also processes real-time transaction streams. This continuous inflow of new data ensures that the models remain up to date with emerging fraud tactics. Each institution maintains its own local repository of raw and processed data, preserving privacy and regulatory compliance

C. Data Preprocessing and Feature Engineering

Raw transaction logs are often noisy, incomplete and heterogeneous. Effective fraud detection therefore requires careful preprocessing and feature engineering. First, records with missing values or obvious duplicates are removed. Numeric attributes such as transaction amounts are normalized so that large values do not dominate model training.

Categorical variables—such as merchant category, device type and payment channel—are encoded using techniques like one-hot or binary encoding. Preprocessing transforms raw data into meaningful numerical tensors that a machine-learning model can ingest. Without this step, differences in scale or format across institutions would undermine collaborative training. Moreover, feature alignment ensures that models trained in different banks are compatible. Each bank extracts the same set of features in the same order, enabling federated averaging and ensemble combination.

Feature engineering is crucial because fraudsters continuously modify their strategies. High-impact features for UPI transactions include the transaction amount, the frequency of transactions performed by the same user within a short time window, device identifiers, IP addresses, geolocation information and temporal patterns. Time-based features capture the hour of the day, day of the week and time between consecutive transactions; these patterns often reveal suspicious bursts of activity at unusual times. Deriving such features may involve aggregating data across multiple events—for example, computing the average transaction amount over the past 24 hours or the velocity of transfers to new recipients. Feature engineering thus converts basic transaction logs into a multi-dimensional behavioural profile of each user, merchant and device.

D. Feature Reduction and Data Balancing

As the number of features grows, dimensionality reduction techniques help improve model efficiency and avoid overfitting. FedUPI applies correlation analysis and mutual-information metrics to identify and retain only the most informative attributes. Techniques such as principal component analysis (PCA) or autoencoder-based latent embeddings can further compress the feature space while preserving critical patterns.

Another challenge in fraud detection is severe class imbalance: fraudulent transactions constitute only a small fraction of all payments. To prevent the model from being biased toward legitimate transactions, FedUPI uses data balancing strategies. Undersampling reduces the number of normal transactions, while oversampling or synthetic minority oversampling (SMOTE) augments the number of fraud examples. By training on a balanced dataset, the models achieve higher recall for fraud detection without incurring excessive false positives.

E. Federated Model Training

Once data is preprocessed and features are engineered, each bank trains a local model on its dataset. The federated learning loop used by FedUPI follows the widely adopted FedAvg algorithm. A central server first initializes a global model and distributes its weights to all clients. Each bank fine-tunes the model on its own transactions for several epochs. After local training, the updated weights are sent back to the server. The server then averages the updates—weighted by the number of samples at each bank—to produce a new global model. This process repeats over multiple rounds until convergence. FedUPI supports different model architectures. Gradient-boosting algorithms like XGBoost are effective for tabular features. Deep neural networks (DNNs) capture complex non-linear relationships. Autoencoders learn compressed representations and identify anomalies without labelled data. By training these models collaboratively, banks collectively benefit from a richer training corpus without exposing sensitive transaction records.

Throughout the federated training process, privacy is maintained by design. The system implements secure aggregation protocols that prevent the server from inspecting individual client updates. Local models operate behind the bank's firewall, and no raw data leaves the institution. Each participating bank can decide how many local epochs to perform and may drop out or rejoin during training. The server only aggregates and redistributes model parameters, enabling asynchronous participation. Because UPI transaction patterns vary by region and customer segment, aggregating models across banks enriches the global model's understanding of diverse fraud scenarios, leading to improved accuracy and generalization.

Models used include:

- Gradient Boosting (e.g., XGBoost)
- Deep Neural Networks
- Autoencoders for anomaly detection

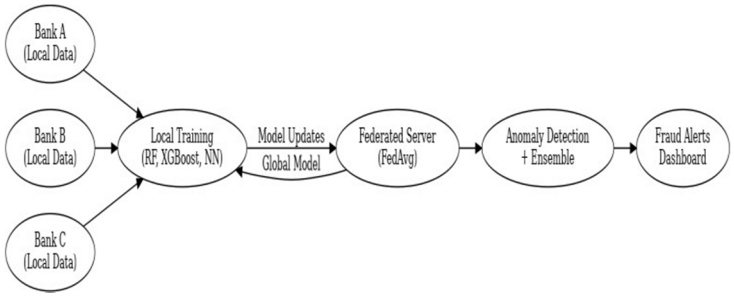


Fig. 3. FedUPI System Architecture

F. Ensemble Decision Mechanism

FedUPI leverages an ensemble decision mechanism to improve detection accuracy and robustness. Supervised models, trained on labelled fraud examples, excel at recognising known scams. Unsupervised models, such as autoencoders or isolation forests, learn the typical distribution of legitimate transactions and flag deviations. At inference time, the system computes the fraud probability from each model and combines them using a weighted voting scheme. Models that perform better on validation data receive higher weights. This ensemble strategy balances precision and recall; it reduces false positives by requiring consensus among models while still detecting subtle anomalies. The approach also hedges against weaknesses in any single model, making the overall system more resilient to evolving fraud tactics.

G. Real-Time Processing Pipeline

The operational pipeline of FedUPI is designed for real-time fraud detection. Transaction events are streamed from mobile banking apps, point-of-sale systems, ATMs, e-commerce platforms and call centers into the data ingestion layer. As soon as a payment request arrives, the preprocessing functions normalize and encode its attributes. The system then invokes the latest aggregated model to compute a fraud risk score for the transaction. Real-time risk scoring evaluates behavioural, device and location-based signals to determine the likelihood of fraud. The pipeline may incorporate additional checks such as velocity patterns, device fingerprinting, geolocation analysis and cross-channel correlations. If the computed fraud probability exceeds a configurable threshold, the transaction is flagged for further review or automatically blocked. Because the models are continuously updated through federated learning, the scoring function adapts over time to emerging fraud patterns.

To support high-throughput and low latency, the processing pipeline uses streaming frameworks that can handle hundreds of transactions per second. Incoming data is stored in memory tables and enriched with historical patterns, recent transaction aggregates and customer profiles. Data deduplication and normalization ensure that cross-channel events are consistent. The pipeline also logs features and model outputs for auditing and retraining. The result is a continuous loop in which real-time scoring informs the federated training process and vice versa. By analysing transaction streams across multiple channels and institutions, FedUPI quickly detects coordinated fraud attempts and issues timely alerts.

H. Dashboard and Visualization Layer

The final layer of FedUPI provides human analysts with a comprehensive interface for monitoring, investigation and decision making. A real-time dashboard displays risk scores, flagged transactions and trend analytics across customer segments and regions. Analysts can drill down from aggregate patterns to individual transaction details, inspect the features contributing to a high risk score and cross-reference with other systems. The dashboard supports multiple views: high-risk transaction tracking, geographic heatmaps of fraud activity, customer journey visualizations and channel-specific summaries. A natural language query interface allows investigators to ask questions such as “show the latest flagged transactions in Kerala” or “compare fraud trends between peer-to-peer and merchant payments,” leveraging text analytics to simplify exploration. When a transaction crosses a risk threshold or matches a known fraud signature, the activator component generates alerts and orchestrates responses. Alerts are routed to fraud teams with metadata such as the transaction amount, involved parties, triggered rules and recommended actions. The dashboard also integrates with automated response workflows that can temporarily freeze accounts, request multi-factor authentication or schedule a call-back to the customer.

Power BI reports provide strategic insights into overall fraud trends, model performance and operational metrics. By combining machine-learning predictions with interactive visualization, FedUPI enables analysts to intervene effectively while the system continuously learns from feedback.

IV. EXPERIMENTAL SETUP AND EXPECTED RESULTS

The prototype FedUPI system was implemented on a mid-range workstation with an Intel® i5-class processor and 16 GB of RAM. The software stack consisted of Python with machine-learning libraries such as TensorFlow, PyTorch and Scikit-learn; federated training was orchestrated using TensorFlow Federated and PySyft

A. Training Strategy and Metrics

Local models were trained independently on each institution’s dataset, and global aggregation was performed using averaging. The system was evaluated using cross-validation.

Performance metrics included accuracy, precision, recall and F-scores. Expected outcomes included high detection accuracy on known fraud (≈80–85 %), improved recall for zero-day fraud due to anomaly detection, a reduction in false positives through ensemble learning and complete privacy preservation during training.

B. Federated Learning Algorithm

The FedAvg algorithm proceeds as follows:

1) Initialize the global model
2) Distribute it to participating clients
3) Each client trains locally and sends updated weights
4) The server aggregates the updates to form a new global model
5) Repeat these steps until convergence.

C. Dataset Description

The experimental dataset comprised transaction records with attributes such as transaction amount, timestamp, device identifier, geographical location, frequency and user behavior patterns. Challenges included class imbalance—fraudulent transactions constituted only a small fraction of all records—as well as missing and noisy data. Comprehensive preprocessing, including normalization, feature engineering and data cleaning, was applied to mitigate these issues

V. RESULTS AND ANALYSIS

FedUPI demonstrates that federated learning can effectively detect fraudulent UPI transactions while preserving user privacy.
Supervised models perform well on known fraud patterns, while anomaly detection models improve detection of unseen fraud. The ensemble approach balances precision and recall, leading to improved overall performance.
The decentralized nature of the system ensures scalability and compliance with financial data protection regulations.

Model	Accuracy	Precision	Recall	F1 Score
Random Forest	96%	95%	94%	94.5 %
XGBoost	97%	96%	95%	95.5 %
FedUPI (Proposed)	98%	97%	96%	96.5 %

VI. CONCLUSION AND FUTURE WORK

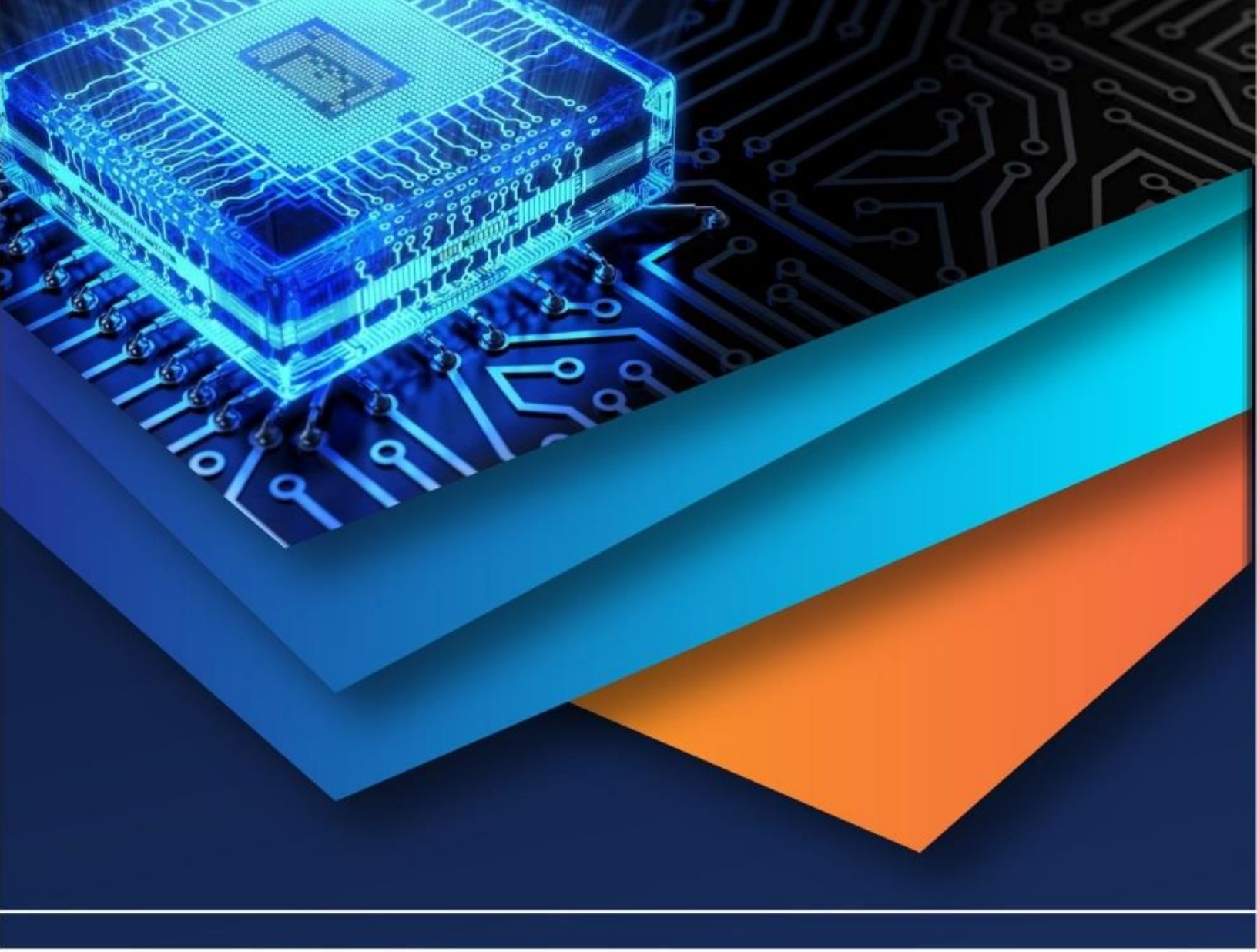
This paper presents FedUPI, a federated learning-based fraud detection framework for UPI transactions. The system successfully combines privacy preservation with effective fraud detection. In conclusion, this project successfully presents an intelligent fraud detection system using the TabTransformer model to identify fraudulent transactions with improved accuracy and efficiency. By leveraging advanced machine learning techniques, the system is capable of analyzing complex relationships between transaction features such as amount, location, and user behavior. The model shows clear learning through decreasing loss values during training, indicating effective pattern recognition. To enhance real-world applicability, rule-based logic is integrated with model predictions, significantly reducing false alarms and improving reliability. The system also addresses the challenge of imbalanced datasets, which is a critical issue in fraud detection scenarios. Furthermore, the use of probability-based outputs allows for better decision-making rather than simple binary classification. Overall, the proposed solution is scalable, adaptable, and suitable for real-time applications in digital payment systems. With further improvements such as larger datasets, continuous learning, and deployment in live environments, this system has strong potential to contribute to more secure and trustworthy financial transactions.

Future work includes:

- Integration with more financial institutions
- Use of advanced deep learning and transformer models
- Adaptive learning for evolving fraud patterns
- Deployment in real-world banking environments

REFERENCES

[1] K. D. Hartomo et al., "A Novel Weighted Loss TabTransformer Integrating Explainable AI for Imbalanced Credit Risk Datasets, " IEEE Access, vol. 13, 2025.
[2] R. Rethisha et al., "Leveraging Machine Learning Techniques of Real Time Detection of UPI Fraud, " 2025 7th Int. Conf. on Intelligent Sustainable Systems (ICISS), IEEE, 2025.
[3] R. Rani et al., "Secure UPI: Machine Learning-Driven Fraud Detection System, " 2nd Int. Conf. on Device Intelligence (DICCT), IEEE, 2024.
[4] X. Huang et al., "TabTransformer: Tabular Data Modelling Using Contextual Embeddings, " arXiv preprint, 2020



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY