Federated Transformer Distillation for Scalable Financial Fraud Detection

M. Sabari Ramachandran, P. Kishore Kumar
Associate Professor/MCA, Mohamed Sathak Engineering College, Kilakarai
Final MCA, Mohamed Sathak Engineering College, Kilakarai.

Abstract - **The proposed UPI Fraud Detection system is designed to strengthen the safety and trustworthiness of digital financial transactions by utilizing advanced technologies such as machine learning (ML), artificial intelligence (AI), and data analytics. By examining transaction behaviours and spotting irregularities, the system can identify and prevent a variety of fraudulent activities, including phishing attacks, identity impersonation, and unauthorized access. It features a real-time surveillance mechanism to swiftly detect suspicious transactions and generate alerts for immediate intervention. As UPI-based payments continue to grow rapidly, there is a pressing demand for effective fraud prevention strategies. This research introduces a scalable solution capable of analysing large datasets, detecting fraudulent patterns, and learning from new data to enhance its predictive accuracy. Techniques such as Random Forest, Support Vector Machine (SVM), and Neural Networks will be used to distinguish between legitimate and fraudulent transactions. Real-time detection not only reduces monetary losses but also boosts user confidence in digital transactions, thereby contributing to a more secure UPI framework.**

I. INTRODUCTION

Digital payment systems, particularly the Unified Payments Interface (UPI), have transformed the way financial transactions are carried out, offering users unprecedented speed, convenience, and accessibility. However, this growth has also brought an increase in cyber threats like phishing, identity misuse, and unauthorized fund transfers. As these payments become a regular part of daily life, safeguarding them has become a top priority.

This paper proposes the development of a reliable and intelligent UPI fraud detection mechanism powered by modern technologies such as ML, AI, and data analytics. Its core objective is to detect suspicious behaviours by analysing transaction data and recognizing anomalies in real-time. The system includes a live monitoring component to instantly flag and respond to potential fraud.

To achieve this, we utilize algorithms such as Random Forest, SVM, and Neural Networks, trained on historical transaction records to classify each transaction accurately. These models are designed to continuously evolve by learning from newly detected fraudulent behaviours, thereby improving their detection performance over time.

Through this initiative, we aim to tackle the emerging challenges in digital security by building a scalable and intelligent fraud detection solution that not only minimizes financial damage but also reinforces user confidence in digital payment ecosystems.

II. LITERATURE SURVEY

The work by Yash Patil et al. (IRJMETS, Sept 2024) introduced a machine learning-based framework tailored to UPI fraud detection. It emphasizes behavioural analysis and transaction monitoring to identify anomalies, significantly improving UPI transaction security.

A study by S. Jagadeesan and colleagues (ResearchGate, Dec 2024) highlighted the application of the Random Forest algorithm in identifying UPI-related fraud. This ensemble method, combining multiple decision trees, was shown to effectively classify fraudulent behaviour through behavioural and transaction pattern analysis.

Miss Sayalee S. Bodde's review (IJRASET) presents a holistic perspective on fraud detection by integrating user behaviour, device data, and transactional trends. It emphasizes the importance of real-time detection and adaptive learning systems that keep pace with evolving fraud strategies.

Another approach by Shabreshwari R M et al. (IJAEM, June 2024) describes a machine learning-driven model that can handle vast transaction datasets for instant fraud detection. The model uses feature

engineering to isolate key indicators of fraud and enhances system security through continual learning.

Nagaraju Melam and team (ResearchGate, March 2024) explored the use of Convolutional Neural Networks (CNNs) for fraud detection in UPI systems. Their research tackles challenges like imbalanced datasets and complex feature transformations, showing how CNNs can uncover intricate fraud patterns with high accuracy.

2.1 EXISTING SYSTEM

Present-day UPI fraud detection mechanisms primarily rely on traditional rule-based systems that depend on static parameters, predefined thresholds, and heuristic logic to detect anomalies. Although these systems offer basic protection, they lack the flexibility needed to counter the fast-changing tactics of cybercriminals.

These outdated systems often generate numerous false positives, flagging legitimate transactions as fraudulent, which causes user dissatisfaction and operational inefficiencies. Furthermore, they are incapable of efficiently handling the vast and growing volume of real-time UPI transactions, leading to delayed responses and increased financial risks. Their inability to identify subtle irregularities or complex fraud patterns leaves them vulnerable to exploitation.

Given these limitations, it is crucial to adopt more advanced, intelligent, and scalable fraud detection technologies capable of securing digital transactions in an ever-evolving threat landscape. The rapid expansion of digital payments has created an urgent need for more sophisticated, adaptive, and scalable fraud detection systems. These systems must effectively safeguard digital transactions while adapting to the constantly evolving nature of security threats.

2.2 PURPOSE OF THE WORK

This project aims to develop a robust UPI fraud detection system that harnesses advanced machine learning techniques to enhance the security and reliability of digital transactions. As UPI-based payment systems continue to grow, traditional rule-based fraud detection methods fall short due to their limited adaptability. To address this, the project will implement a data-driven approach, designed to improve the accuracy of fraud detection, reduce false positives, and enable real-time analysis of vast transactional data. The system will continuously learn from emerging fraud patterns, ensuring resilience against new types of fraudulent activities. Additionally, it will be scalable and efficient, capable of processing large datasets swiftly while delivering accurate results. The ultimate goal is to build user trust, mitigate financial losses due to fraud, and provide a secure digital payment environment.

III. PROPOSED SYSTEM

The proposed UPI fraud detection system is designed as an intelligent, machine learning-powered solution to tackle the complex challenges associated with safeguarding digital transactions. Unlike conventional rule-based systems that depend on fixed thresholds and heuristic methods, this approach is more adaptive, capable of processing extensive transactional data in real-time. The system excels in identifying subtle anomalies and suspicious behaviours with high precision, effectively distinguishing between legitimate and fraudulent transactions. This significantly lowers the occurrence of false positives while minimizing disruptions for genuine users.

Furthermore, the system's capability to detect fraud instantly and issue real-time alerts allows for swift intervention, minimizing financial damage and reducing the risk of widespread fraud. Its adaptive nature, characterized by continuous learning from emerging fraud patterns, makes it more resilient to new threats compared to traditional systems. By integrating advanced anomaly detection and behavioural analysis, the system not only achieves high detection accuracy but also predicts and prevents increasingly sophisticated fraud schemes. This results in a smarter, more effective, and scalable solution that ensures the security of UPI transactions. Consequently, the system bolsters user confidence, promotes the adoption of digital payments, and fosters a secure, transparent, and reliable digital payment environment.

IV. MODULES

PREPROCESSING MODULE

The preprocessing module is responsible for preparing the input data for analysis. It involves several crucial tasks, such as extracting frames, resizing them to a consistent resolution, and

normalizing pixel values to standardize inputs for the detection model. Additionally, this module may include techniques like background subtraction or object segmentation to differentiate dynamic objects from static backgrounds, thus enhancing anomaly detection efficiency. The preprocessing stage also handles noise reduction and frame rate adjustments, ensuring uniform data quality for subsequent processing phases.

FEATURE EXTRACTION MODULE

The feature extraction module leverages Convolutional Neural Networks (CNNs) to identify spatial characteristics within individual video frames. It detects key features such as objects, edges, and textures, enabling the model to analyse the structural components of each frame. The output from this module consists of feature maps that effectively capture the visual content of the frames. These maps play a crucial role in detecting deviations or irregularities during the later stages of the process.

TEMPORAL PATTERN LEARNING

This module employs long short-term memory (last) networks or similar recurrent models to analyse the temporal relationships between consecutive frames. Since anomalies often develop over a period of time, it is essential to track the progression of video content. The temporal pattern learning module captures the dynamic changes in objects and scenes, offering a comprehensive understanding of normal and unusual behaviours. It processes the sequences of features generated by the previous module, helping the system distinguish between typical and atypical events over time.

ANOMALY DETECTION

The anomaly detection module serves as the system's core, where it identifies irregular patterns and events. It compares spatial and temporal patterns learned by the CNN and LSTM models with the system's established normal behaviour. Any deviations from expected patterns are flagged as potential anomalies. This module may also use unsupervised learning techniques, allowing the system to detect new or previously unknown abnormal events without requiring labelled training data.

ATTENTION MECHANISM

This module enhances the system's focus by directing attention to specific regions or objects within the video that are more likely to exhibit abnormal behaviour. Instead of analysing the entire frame uniformly, it prioritizes areas of interest, improving both detection efficiency and accuracy. By concentrating computational resources on significant regions, the module can detect subtle or localized anomalies more effectively, even when processing large-scale video data.

POST-PROCESSING AND DECISION MODULE

Once the anomaly detection module flags irregularities, the post-processing and decision module performs additional analysis to validate the findings. This step includes filtering out false positives and applying context-based reasoning to determine whether the detected anomaly matches expected behaviours or predefined rules. The module may also aggregate multiple anomaly occurrences over time to assess the significance of an event. Depending on the results, it can trigger alerts, log incidents, or initiate corrective measures

VISUALIZATION AND USER INTERFACE (UI)

The visualization and UI module provides an interactive platform for users to monitor video feeds, highlight detected anomalies, and assess system outputs. It offers visual representation of video activities, marks anomalous events on a timeline, and provides playback options to review specific moments where irregularities occurred. Additionally, the UI allows users to customize detection thresholds, anomaly types, and alert preferences for tailored monitoring. The module is optimized to handle video data in real-time, balancing computational load and reducing latency while maintaining high detection accuracy.

V. ALGORITHMS

The UPI fraud detection system leverages a combination of machine learning algorithms, including Random Forest, Support Vector Machines (SVM), and Neural Networks, to analyse transactional data and classify transactions as either genuine or fraudulent. These algorithms work together to identify suspicious activities promptly, allowing for real-time monitoring and rapid alert generation. By examining patterns in transactions, user behaviours, and anomalies, the system effectively detects potential fraud.

To address evolving threats such as phishing, identity theft, and unauthorized transactions, the system is

designed to be highly adaptive. It continuously learns from new fraud patterns, thereby enhancing detection accuracy over time. This adaptive capability ensures that the system remains robust against emerging risks, ultimately contributing to a safer digital payment environment.

VI. RESULT AND CONCLUSION

With the increasing use of UPI for smooth digital transactions, the risk of fraud has also escalated. This project addresses this challenge by developing a resilient and adaptive UPI fraud detection system that utilizes advanced machine learning techniques combined with behavioural analytics. The implemented model efficiently detects suspicious patterns and irregularities within real-time transaction data, providing a proactive defines mechanism that helps mitigate financial fraud before it leads to significant loss.

The model analyses various features, including transaction frequency, discrepancies in amounts, mismatched device IDs, and irregular geolocation patterns. It demonstrates high accuracy in identifying fraudulent activities, even when the fraud patterns are complex or subtle.

The system's ability to continuously learn and adapt to new fraud patterns ensures that remains effective against evolving cyber threats. By training machine learning models on diverse datasets, the system can detect new and previously unknown types of fraud, thereby continuously improving the detection capabilities.

Future advancements may include integrating more sophisticated deep learning techniques, such as transformer-based architectures, to process complex data relationships more efficiently. This would enhance prediction accuracy and the system’s ability to handle diverse fraud scenarios. Ultimately, the developed system strengthens user trust in UPI transactions, fostering secure digital payments and encouraging the widespread adoption of digital payment platforms. By delivering real-time and accurate fraud detection, the system significantly contributes to a safer and more reliable digital payment landscape.

VII. FUTURE ENHANCEMENTS

Behavioural biometrics: Incorporating metrics like typing speed, swipe patterns, and pressure sensitivity on mobile devices. Analysing device motion data (gyroscope/accelerometer) during transactions to detect unauthorized users or bots

Temporal features: Examining the time of day to detect transactions made at unusual hours. Analysing trends in transaction frequency over time. Monitoring the time since the last successful transaction to identify sudden re-activation attempts.

Geo-location intelligence: Identifying location-based anomalies, such as sudden changes in city or country combining location data with ip address tracking to detect potential remote fraud. Measuring the distance between consecutive transaction locations to flag suspicious activity.

Device & network features: Monitoring changes in device id or sim card information. Detecting the use of unfamiliar devices, emulators, or networks. Differentiating transactions made over public versus private wi-fi networks.

Social graph & contact patterns: Analysing transaction history with both known and unknown contacts. Tracking the frequency of payments to new upi ids. Using graph-based anomaly detection to evaluate the transaction network.

Transaction context & metadata: Utilizing merchant category codes (mccs) and transaction purposes to assess risk. Detecting deviations from typical transaction amounts and user-specific historical patterns. Monitoring for rapid increases the transaction amounts or frequencies.

REFERENCES

[1] “Fraud Detection in UPI Transactions Using ML” EPRA International Journal
[2] “UPI Fraud Detection Using Machine Learning and Deep Learning” International Journal for Research in Applied Science and Engineering Technology (IJRASET)
[3] “UPI Fraud Detection Using Machine Learning Algorithms” International Journal of Emerging Research in Science and Technology (IJERST)
[4] “Detecting Fraud in UPI Transactions Using Random Forest and XG Boost” International Journal of Scientific Research in Engineering and Management (IJSREM)
[5] “UPI Fraud Detection Using CNN” ResearchGate (Preprint)

[6] "A Review on UPI Fraud Detection Using ML and DL" International Journal of Advanced Research in Computer Science (IJARCS)
[7] "UPI Fraud Detection Using Logistic Regression and Random Forest" Eudoxus Press Journal
[8] "Analysis of UPI Transaction Fraud Using AI Techniques" International Journal of Computer Applications (IJCA)
[9] GitHub Project: UPI Fraud Detection Using ML
[10] "Real-Time Fraud Detection in UPI Using AI/ML", IEEE Xplore