

UPI Fraud Intelligence & Analytics Dashboard

A Unified Framework for Fraud Pattern Analysis and Transaction Investigation

Sayyed Alaa Mariya Irfan*, Dr. Manoj Singh**

*(MSc Computer Science Part II, SIES College of Arts, Science and Commerce, Sion, Mumbai, India.)
(Email: sayyedmariya39@gmail.com)

**(Computer Science, SIES College of Arts, Science and Commerce, Sion, Mumbai, India.)
(Email: manojks@sies.edu.in)

Abstract — The widespread use of the Unified Payments Interface (UPI) has made digital payments faster and more accessible, while also increasing the need to examine reported fraud in a structured way. Much of the existing UPI fraud literature studies machine-learning or deep-learning techniques that classify or predict fraudulent transactions. This paper describes the UPI Fraud Intelligence & Analytics Dashboard, a dataset-driven platform for analysing records that have already been labelled as fraudulent. The dashboard analyses records by state, bank, fraud type, transaction amount, and time. It also supports individual transaction checks, automatic statistical findings, and analysis of compatible uploaded files. The prototype uses Flask and Pandas on the backend and HTML, JavaScript, Bootstrap, and Chart.js on the frontend. Its findings are calculated from the loaded records; it does not generate a fraud probability or claim to identify fraud independently. The paper outlines the platform design, processing workflow, analytical features, and a functional evaluation using the supplied dataset.

Keywords — UPI fraud, fraud analytics, visual analytics, transaction investigation, financial fraud, dashboard, data visualization, digital payments

I. INTRODUCTION

UPI has become a widely used way to make account-to-account payments in India. As transaction volumes grow, the information available after a suspected or confirmed fraud event can also become harder to review manually. Recent UPI studies have examined machine-learning, ensemble, anomaly-detection, and explainable-AI methods for classifying or predicting fraudulent transactions [1]–[4].

Detection is only one part of responding to fraud. After records have been labelled, analysts may still need to compare locations and banks, identify common fraud categories, examine changes over time, and inspect individual transactions in context. Financial visual-analytics research has shown how linked views, interactive filtering, and record-level exploration can help people examine complex transaction data [5]–[8]. Building on this complementary line of work, the proposed dashboard focuses on analysis after labelling rather than on a new prediction model. It turns compatible transaction files into linked summaries and investigation views, allowing users to move from an overall picture to a specific record. Research on financial visual analytics has examined ways to explore transactions and identify suspicious activity [5]–[8]. The dashboard brings these functions together in one simple workflow. Users can review aggregate patterns, examine automatically calculated findings, investigate a selected record, and load another compatible dataset without relying on a trained fraud-prediction model.

II. PROBLEM STATEMENT AND OBJECTIVES

A. Problem Statement

Much of the UPI fraud literature centres on detection models and their classification or prediction performance. These

methods address whether a transaction is likely to be fraudulent, but an analyst also needs practical ways to explore records after a fraud label is available. Reviewing raw CSV or spreadsheet files often means repeatedly filtering, grouping, comparing, and interpreting data by hand. This can slow down investigation across several dimensions.

This work asks the following question: how can labelled UPI transaction records be presented in a transparent, interactive workspace that supports analysis by multiple dimensions, record-level investigation, automatically calculated statistical summaries, and examination of newly uploaded compatible files—without presenting the system as a machine-learning predictor?

B. Objectives

- To develop a unified dashboard for UPI fraud data analysis.
- To compare transaction patterns across states, banks, fraud types, transaction amounts, and time periods using interactive visualizations.
- To help users investigate individual fraud-labelled transactions through search, filters, transaction details, and related dataset statistics.
- To show key findings from the uploaded data, such as the state, bank, and fraud type with the highest number of records.
- To enable users to upload compatible CSV and Excel files and analyse their contents without rebuilding the dashboard.
- To check that the dashboard's displayed counts, transaction amounts, and summaries match the values calculated from the loaded dataset.
- To test data processing, analytical features, and transaction investigation workflows

III. RELATED WORK AND RESEARCH GAP

Recent UPI fraud literature is strongly oriented toward machine-learning-based detection. A 2025 IEEE study evaluated Decision Tree, Support Vector Machine, Random Forest, Logistic Regression, and ensemble voting techniques for UPI fraud detection [1]. Other recent works similarly investigate supervised, hybrid, and explainable approaches, commonly reporting accuracy, precision, recall, F1-score, ROC-AUC, or related detection metrics [2]–[4]. More recent studies continue this direction using hybrid and sequence-aware machine-learning architectures [9], Visual analytics research offers another way to study financial fraud. WireVis [5] helped users explore financial transactions and spot suspicious patterns using interactive charts. EVA [6] used visual tools to examine fraudulent events, while NEVA [7] focused on studying fraudulent networks. Interactive visual methods also support fraud analysis and investigation [8].

The gap addressed here is narrower than a claim that fraud dashboards or visual analytics do not exist. The proposed contribution is a lightweight, non-ML workflow tailored to UPI-labelled data that combines post-labelling analysis, automatic statistical summaries, transaction-level inspection, and re-analysis of uploaded datasets in one interface.

Research direction	Primary focus	Relation to proposed work
UPI ML studies [1]–[4]	Detection prediction	Provides the complementary analytical layer
WireVis [5]	Interactive financial visualization	Supports coordinated analytical views
EVA [6]	Visual fraud investigation	Motivates investigation oriented interaction
NEVA [7]	Fraudulent network exploration	Supports multi-view investigation concepts
Visualization research [8]	Fraud analysis through visualization	Supports human-centered analytical workflows

IV. DATASET AND DATA PREPARATION

The platform accepts structured UPI transaction files in CSV or Excel format. The evaluation file contains records labelled as fraudulent and includes fields used for analysis, such as fraud status, transaction amount, state, bank, fraud type, and transaction date. The dates in this file range from 01-Apr-2023 through 31-Mar-2025. Because every record in this evaluation file carries a fraud label, its class composition describes the supplied sample only; it must not be interpreted as the prevalence of fraud across real-world UPI transactions.

During upload, the system checks the file structure, maps supported field-name variations, converts numeric values, parses dates, and prepares the records for aggregation. Fraud-labelled records can then be examined in the fraud-specific views, while the uploaded dataset remains the source for the dashboard's overall analysis.

A. Data Integrity Requirements

- The displayed record count should match the uploaded data.
- Calculate the total fraud amount using the transaction values in the dataset.

- Fraud rates must be calculated from actual transaction and fraud counts.
- Date-based findings must use parsed transaction dates rather than simulated periods.
- Any missing or incomplete data should be clearly identified instead of being filled with invented values.

V. METHODOLOGY

A. Data Processing

Pandas is used to load the uploaded file and carry out validation, cleaning, type conversion, and filtering. The resulting records are passed to shared aggregation routines so that the different dashboard modules calculate their outputs from the same dataset.

B. Multi-Dimensional Fraud Analytics

The analytics component groups fraud-labelled records by state, bank, fraud type, transaction amount, and time. These summaries appear as KPI cards, charts, tables, search results, and filterable views. The purpose is to help users examine existing labels and patterns, not to predict whether a new transaction is fraudulent.

C. Transaction Investigation

The Transaction Investigation section shows the details of a chosen transaction in one place. Users can search or filter the available transactions and review their attributes alongside summary statistics calculated from the current dataset. Where records share selected attributes, the interface may show them as related for further review; this association alone does not establish a causal link.

D. Automatic Key Findings

Automatic Key Findings applies reusable statistical calculations to the current data. Depending on the fields available, it can report the state with the highest record count, the most represented bank, the most common fraud category, high-value records, and periods with the largest observed activity. Any rate is meaningful only when the required transaction and fraud counts are present and suitable for that calculation. The module reports dataset-derived observations rather than hard-coded messages or model-generated predictions.

E. Upload & Analyze

The feature accepts new CSV or Excel files and displays their analysis in the existing dashboard. Results are recalculated for each uploaded dataset.

F. Evaluation Method

Since this prototype does not classify transactions with an ML model, classifier measures such as accuracy, precision, recall, and F1-score are not appropriate as its primary evaluation criteria. Instead, the evaluation examines whether data is processed correctly, whether analytical functions operate as intended, whether displayed values agree with the loaded records, and whether upload and transaction-investigation workflows function as expected.

VI. SYSTEM ARCHITECTURE

Figure 1 shows how the system works. First, a file is uploaded and checked. The data is then prepared for analysis, and the analytics component calculates summaries. The dashboard presents state and bank data, fraud categories, transaction values, key findings, and details of specific transactions.

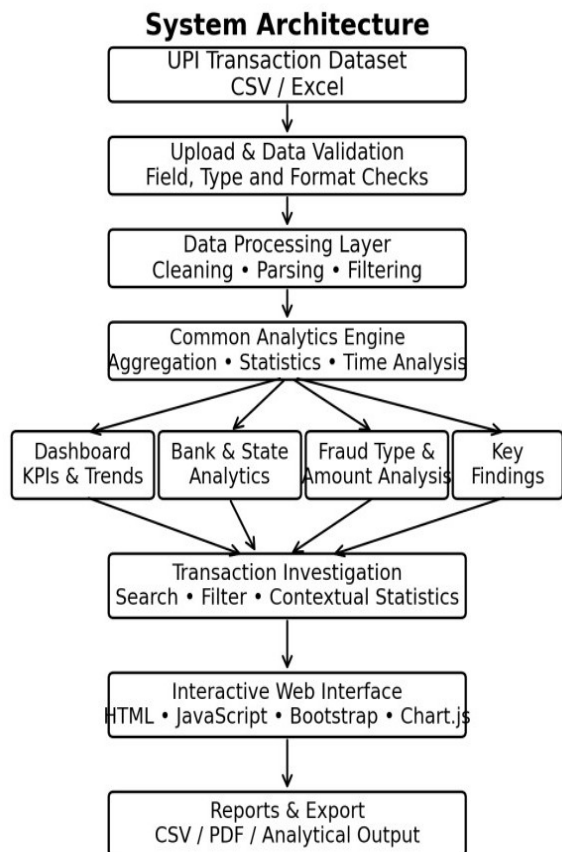


Fig. 1. System architecture of the UPI Fraud Intelligence & Analytics Dashboard.

VII. SYSTEM IMPLEMENTATION

The prototype uses Flask and Pandas for server-side processing. The interface is built with HTML and JavaScript and uses Bootstrap, Chart.js, PapaParse, SheetJS, Flatpickr, and Font Awesome. Its pages separate the main dashboard from functions such as fraud analysis, key findings, transaction investigation, bank analytics, state analysis, fraud awareness, report download, and settings. The core analysis operates on uploaded transaction files and does not depend on a conventional SQL database. The interface keeps the current dataset and the state needed by its analytical modules, while the backend processes the supplied records.

VIII. DASHBOARD AND ANALYTICAL INTERFACE

The dashboard is the starting point for the analysis workflow. It gives users an overview before they move to a particular dimension or open an individual record for closer inspection. Figure 2 shows the main dashboard interface used in the prototype.

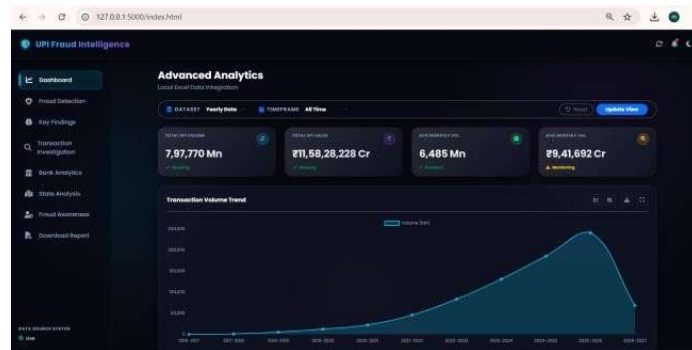


Fig. 2. UPI Fraud Intelligence & Analytics Dashboard

IX. EXPERIMENTAL RESULTS

The functional evaluation examined whether the implemented dashboard could analyse the supplied fraud-labelled records and support the main workflows: multi-dimensional summaries, automatically generated findings, individual-record investigation, and file upload followed by re-analysis. Because the evaluation file contains only fraud-labelled records, its label distribution is not used as an estimate of real-world fraud prevalence.

In the supplied evaluation file, the platform processed 1,000 records, and all 1,000 were labelled as fraud. The dataset includes records from 16 states, 11 bank categories, and 10 types of fraud. Their combined transaction amount is ₹15,911,454, and the largest single observed transaction is ₹495,050. Karnataka has the highest state count, at 132 records; SBI is the most represented linked bank, with 232 records; and Phishing is the most frequent fraud type, with 218 records. These are descriptive results for this particular labelled dataset, not estimates of the real-world UPI fraud prevalence

A. Functional Evaluation

TABLE II. FUNCTIONAL EVALUATION OF THE PROPOSED PLATFORM

Analytical function	Implemented capability	Evaluation evidence
Multi-dimensional analysis	State, bank, fraud type, amount, and time analysis	Dataset-derived charts, KPIs, tables, and filters
Automatic Key Findings	Automatic statistical observations from current data	Ranked findings generated from dataset aggregations
Transaction Investigation	Search, filtering, detailed transaction view, contextual statistics	Transaction-level inspection and related-record view
Upload & Analyze	CSV/Excel dataset loading and re-analysis	Analytical modules recalculate from uploaded data
Reporting and export	Download/export of analytical results	Report/export workflow available from the interface

B. Analytical Dimensions

TABLE III. ANALYTICAL DIMENSIONS AND SUPPORTED OUTPUTS

Analytical dimension	Primary measure	Supported output
State	Fraud-labelled transaction count and amount	State-wise comparison and visualization
Bank	Fraud-labelled transaction count and amount	Bank ranking and distribution
Fraud type	Frequency and amount	Fraud-type distribution
Time	Transaction count and amount over date/time	Trend analysis
Transaction	Transaction ID, date, state, bank, amount, type, and status	Investigation details and contextual statistics

The dashboard uses the uploaded dataset to generate results for all the categories listed in Table III. This allows users to analyse different datasets using the same process without adding a separate fraud prediction model.

X. CASE STUDY: TRANSACTION-LEVEL INVESTIGATION

This case study examines transaction TXN532718178385, dated 16-May-2023 at 11:32:34. The record is linked to Karnataka and the bank category "Other." It uses Google Pay, is a P2M transaction worth ₹70,400, and is labelled as Phishing fraud. The investigation view shows these details along with statistics from the supplied dataset: Karnataka has 132 fraud-labelled records, while Phishing is the most frequent category, with 218 records. This example shows how users can move from an individual transaction to the wider dataset context without assigning an unsupported probability or risk score.

XI. DISCUSSION

The platform focuses on a different part of fraud management than UPI studies that mainly use machine learning to detect fraud. It helps users study fraud-labelled records using charts, filters, transaction details, and other analysis features. It is intended to help users examine records once labels are available, bringing aggregate charts, filters, transaction-level details, statistical findings, and file upload into a shared interface.

Transparency is a central design choice: findings are calculated from the loaded records, and users can return to the underlying data to check the reported values. This is useful when the task is to understand and investigate an existing dataset rather than to produce an automated prediction.

The dashboard should be used alongside, not as a substitute for, an upstream detection process. When a file includes an 'is_fraud' field, the system analyses the label supplied in that file; it does not independently verify the transaction or use a trained model to predict fraud.

XII. LIMITATIONS

- The system depends on the quality, completeness, and consistency of the uploaded dataset.

- The current analytical workflow is dataset-driven rather than connected directly to live UPI or bank transaction APIs.
- The system does not independently establish whether a transaction is fraudulent; it analyzes fraud labels supplied in the dataset.
- Statistical findings may be limited when required fields are missing or when the dataset is too small for meaningful comparisons.
- Real-world deployment would require security, privacy, access-control, audit, and regulatory considerations beyond the current academic prototype.

XIII. FUTURE WORK

- Integration with secure real-time transaction streams or authorized institutional data sources.
- Role-based access control and audit logging for investigation workflows.
- Cross-dataset comparison and longitudinal fraud trend analysis.
- Advanced visual exploration of relationships between entities when suitable identifiers are available.
- User studies with analysts to evaluate investigation efficiency and usability.
- Optional integration of ML-based detection as a separate upstream component while preserving the dashboard's transparent analytical layer.

XIV. CONCLUSION

This paper describes a non-ML dashboard for exploring and investigating UPI transaction records that have already been labelled as fraudulent. It combines analysis by state, bank, fraud type, amount, and time with transaction-level inspection, automatically calculated findings, and re-analysis of uploaded datasets. The platform is intended to complement detection systems by helping users interpret labelled records in a single workflow.

The evaluation reports functional behaviour and dataset-derived summaries rather than classification performance. Runtime measurements and structured user studies remain useful next steps, once the deployment environment and evaluation protocol have been defined.

REFERENCES

- [1] V. Kamra, "A Novice Approach for UPI Fraud Detection by Using Machine Learning Techniques," Proc. 2025 IEEE 7th International Conference on Computing, Communication and Automation, 2025, doi: 10.1109/ICCCA66364.2025.11325722.
- [2] A. S. Gayakwad and P. B. T. Kunta, "UPI Fraud Detection Using Machine Learning," International Journal of Creative Research Thoughts, vol. 13, no. 4, pp. k570–k574, 2025.
- [6] R. A. Leite, T. Gschwandtner, S. Miksch, S. Kriglstein, M. Pohl, E. Gstrein, and J. Kuntner, "EVA: Visual Analytics to Identify Fraudulent Events," IEEE Transactions on Visualization and Computer Graphics, vol. 24, no. 1, pp. 330–339, 2018, doi: 10.1109/TVCG.2017.2744758.
- [3] T. Sekhar and G. Vijaya Kumar, "UPI Fraud Detection Using Hybrid Machine Learning Models with Explainable Risk Scoring and Real-Time Monitoring," International Journal of Advanced Research in Computer and Communication Engineering, vol. 15, no. 4, 2026, doi: 10.17148/IJARCCE.2026.15419.

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

[5] R. Chang, A. Lee, M. Ghoniem, R. Kosara, W. Ribarsky, J. Yang, E. Suma, C. Ziemkiewicz, D. Kern, and A. Sudjianto, "Scalable and Interactive Visual Analysis of Financial Wire Transactions for Fraud Detection," *Information Visualization*, vol. 7, no. 1, pp. 63–76, 2008, doi: 10.1057/palgrave.ivs.9500172.

[6] R. A. Leite, T. Gschwandtner, S. Miksch, S. Kriglstein, M. Pohl, E. Gstrein, and J. Kuntner, "EVA: Visual Analytics to Identify Fraudulent Events," *IEEE Transactions on Visualization and Computer Graphics*, vol. 24, no. 1, pp. 330–339, 2018, doi: 10.1109/TVCG.2017.2744758.

[7] R. A. Leite, T. Gschwandtner, S. Miksch, E. Gstrein, and J. Kuntner, "NEVA: Visual Analytics to Identify Fraudulent Networks," *Computer Graphics Forum*, vol. 39, pp. 344–359, 2020, doi: 10.1111/cgf.14042.

[8] W. N. Dilla and R. L. Raschke, "Data visualization for fraud detection: Practice implications and a call for future research," *International Journal of Accounting Information Systems*, vol. 16, pp. 1–22, 2015, doi: 10.1016/j.accinf.2015.01.001.

[9] "UPI Sentinel: Anomaly-Aware Fraud Detection Using Hybrid ML Models," *Proc. 2026 International Conference on Visual Analytics and Data Visualization*, 2026, doi: 10.1109/ICVADV67766.2026.11470456.