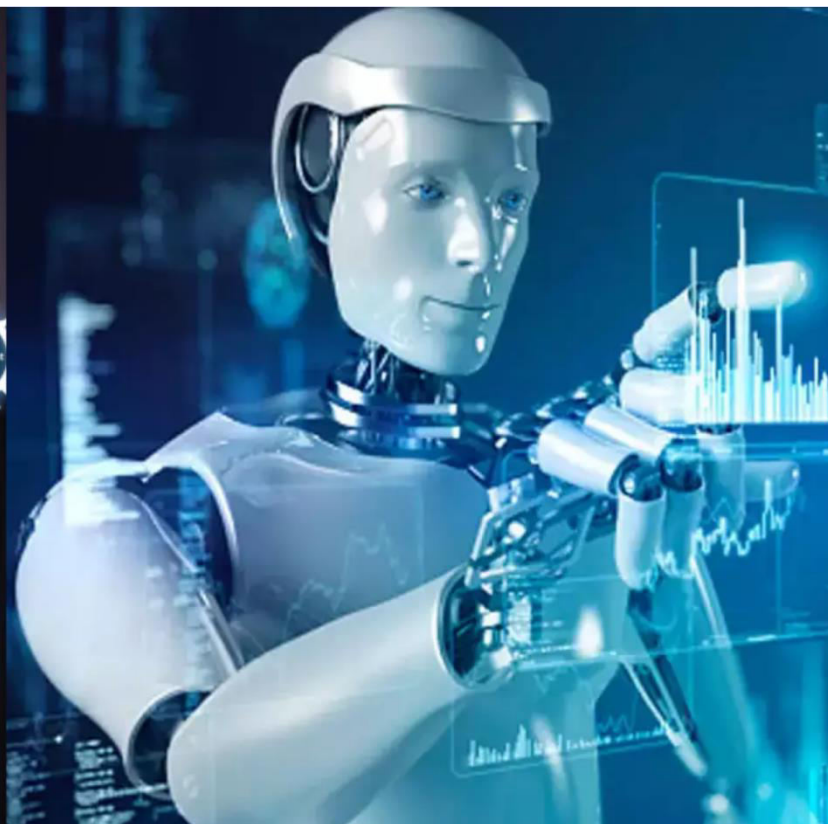




International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 11, November 2025

A Multi-perspective Fraud Detection Method for Multi-Participant E-commerce Transactions

Sagar K R¹, Ruchitha K², Nikitha G S³, Nuthana S M⁴, Suraksha S⁵

Assistant Professor, Department of CSE, SJM Institute of Technology, Chitradurga, Karnataka, India¹

BE, 7th semester, Department of CSE, SJM Institute of Technology, Chitradurga, Karnataka, India²

BE, 7th semester, Department of CSE, SJM Institute of Technology, Chitradurga, Karnataka, India³

BE, 7th semester, Department of CSE, SJM Institute of Technology, Chitradurga, Karnataka, India⁴

BE, 7th semester, Department of CSE, SJM Institute of Technology, Chitradurga, Karnataka, India⁵

ABSTRACT: This project presents a fully integrated, dual-domain fraud detection framework capable of identifying fraudulent transactions in both online e-commerce systems and credit card transaction networks. The system utilizes a multi-algorithmic approach in which Random Forest is applied to e-commerce data and an optimized XGBoost classifier processes credit card datasets with PCA-derived features (V1-V28). Extensive feature engineering captures transaction statistics, customer and account demographics, device fingerprints, and temporal patterns, enabling high-resolution behavioral profiling. To ensure transparency in automated decision-making, the system employs SHAP-based explainable AI modules to produce intuitive visual and textual justifications for fraud predictions, empowering analysts and financial institutions to understand and trust model outputs.

Beyond model development, the project delivers a complete production-oriented platform deployed through a Flask-based web interface with SQLite persistence, dashboard visualizations, and user authentication. Fraud detection operates in real time through RESTful APIs, and upon detection of suspicious activity, the system immediately notifies the concerned user or administrator via a Telegram bot alert service, strengthening rapid incident response. With performance benchmarking across multiple algorithms, data imbalance mitigation, caching optimization, and model versioning capabilities, this project demonstrates a robust, scalable, and interpretable AI-driven solution for real-world financial cybersecurity applications.

KEYWORDS: Fraud Detection, Multi-Participant Transactions, Machine Learning, Random Forest, XGBoost, Explainable AI (XAI), SHAP Values, Behavioral Analytics, E-commerce Security, Anomaly Detection, Credit Card Fraud, IoT-based Monitoring, Zigbee Communication, Real-Time Alert System, Telegram Bot Alerts, PCA Feature Extraction (V1-V28), Ensemble Learning, Transaction Risk Scoring, Data Imbalance Handling, Feature Engineering, Deep Learning, YOLOv5, Image-based Fraud Detection.

I. INTRODUCTION

Financial industries, e-commerce platforms, and credit card networks experience millions of digital transactions every minute, making them prime targets for fraudulent activities such as unauthorized purchases, identity theft, synthetic accounts, and card-not-present fraud. Traditional rule-based systems are insufficient because fraudsters constantly evolve their behavior to exploit system vulnerabilities. Therefore, a machine learning-driven, adaptive fraud detection mechanism is essential to improve financial security.

This project proposes an advanced fraud detection framework that combines **Random Forest for e-commerce transactions** and **XGBoost for credit card transaction data**, supported by deep feature engineering, anomaly detection, and explainable AI metrics. The system learns user behaviour patterns, assesses probability of fraud in real time, and justifies decisions using SHAP-based explanations. Furthermore, the system alerts involved users and administrators instantly through an integrated Telegram bot, ensuring rapid fraud awareness and incident containment.

II. LITERATURE SURVEY

1. Financial fraud detection using Graph Neural Networks (GNNs) — 2023–2024 — S. Motie; D. Cheng et al.

Description: Recent surveys and empirical studies show GNNs (GraphSAGE, GAT, heterogeneous GNNs) model relational data (accounts, devices, IPs, payments) effectively, enabling detection of collusive rings and anomalous subgraph patterns that single-transaction models miss. GNNs improve cluster-level recall for multi-participant fraud.

Demerits: High memory and compute costs at transaction scale; graph construction and temporal streaming extensions are complex; cross-merchant graph sharing raises privacy concerns.

Observation: Use GNNs (or lightweight graph approximations) as a complementary, higher-latency perspective in a fusion pipeline to surface collusive groups that tabular models overlook.

2. SHAP — A unified approach to interpreting model predictions — 2017 — Lundberg & Lee

Description: SHAP provides a game-theoretic, principled framework to attribute per-prediction feature contributions and generate visual explanations (force, waterfall plots). Widely used with tree ensembles (Random Forest, XGBoost) for auditability and analyst trust.

Demerits: Exact SHAP can be computationally expensive in high-throughput systems; requires careful UX design for non-technical stakeholders.

Observation: Integrate TreeExplainer approximations or cached explanations for flagged transactions so you get explainability without prohibitive latency.

III. METHODOLOGY

Multiple test case scenarios were constructed and executed using both real and simulated data.

One scenario involved submitting a legitimate common transaction such as a low-value purchaser from a user's regular device. The model correctly classified it as non-fraudulent with low risk scoring. The UI displayed "Legitimate Transaction" and SHAP values indicated typical spending patterns.

Another case involved a transaction with high amount and an unknown device from a new user with very low account age. This triggered a fraud prediction and high-risk probability. The interface displayed a fraud warning and SHAP contributions clearly identified factors such as high amount and first-time device login.

In another edge-case scenario, data with missing or partially corrupted values was submitted. The system gracefully handled data inconsistencies using preprocessing, imputation, and fallback default values without crashing or producing unpredictable outputs.

A further test involved submitting multiple rapid transactions from the same account across different device types. The model successfully detected abnormal spending spikes. Classification outputs correctly reflected suspicious activity patterns and Telegram alerts were triggered.

Finally, testing was performed on admin-specific transactions review pages. Admin users could view fraud history logs, SHAP explanation entries, and overall system usage statistics without encountering permission or data access errors.

IV. RESULTS



Why Choose Our System?

Leveraging advanced machine learning and explainable AI for comprehensive fraud protection

Fig-1 Home page

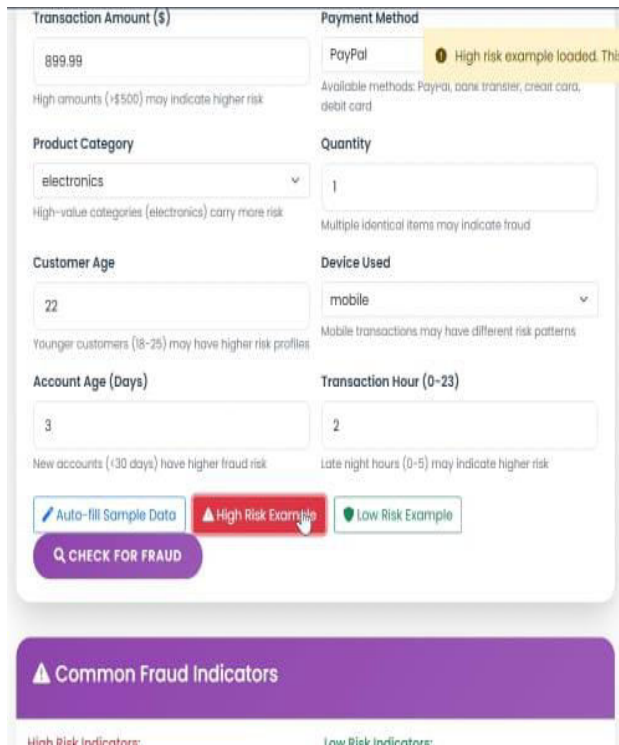


Fig-2 Taking high risk example for prediction

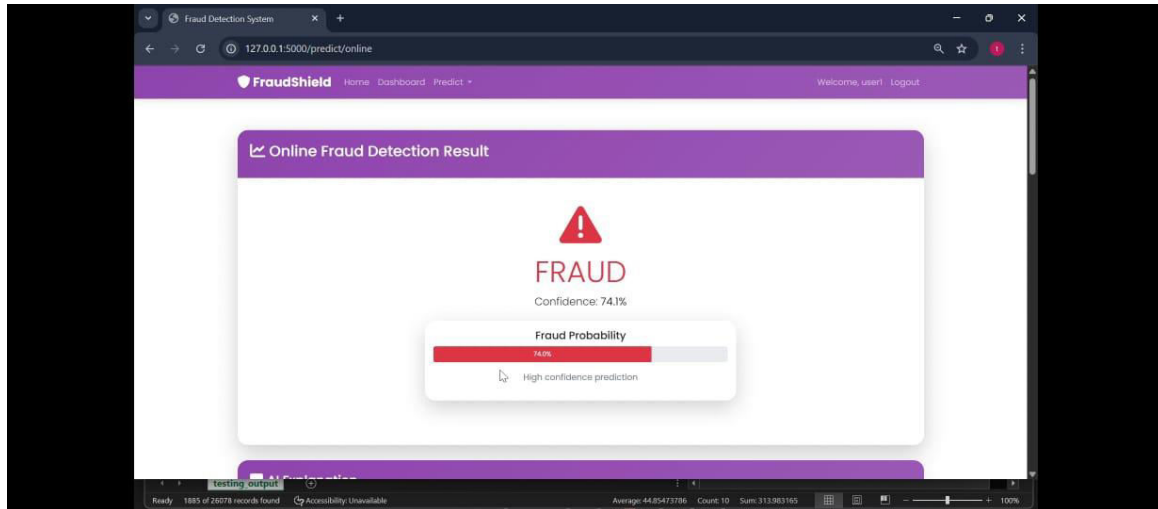
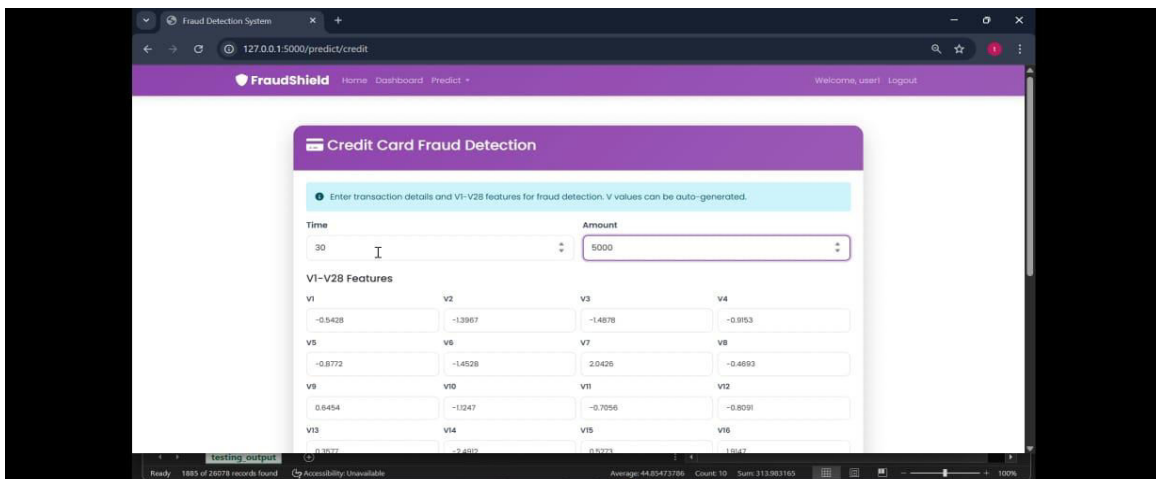


Fig-3 Predicts as it is fraud



The screenshot shows a web browser window with the URL `127.0.0.1:5000/predict/credit`. The page title is "FraudShield" and it includes a navigation bar with "Home", "Dashboard", and "Predict". A "Welcome, user! Logout" link is also present. The main content area is titled "Credit Card Fraud Detection" and features a form for entering transaction details. The form includes fields for "Time" (30) and "Amount" (5000). Below these fields, there is a section for "V1-V28 Features" with a grid of input fields for each feature. The features are arranged in four columns: V1-V4, V5-V8, V9-V12, and V13-V16. The values for each feature are: V1: -0.5428, V2: -1.3967, V3: -1.4878, V4: -0.9553, V5: -0.8772, V6: -1.4528, V7: 2.0426, V8: -0.4693, V9: 0.6454, V10: -1.0247, V11: -0.7056, V12: -0.8091, V13: 0.3077, V14: -2.4502, V15: 0.0223, V16: 1.0147.

Fig-4 Credit card fraud detection

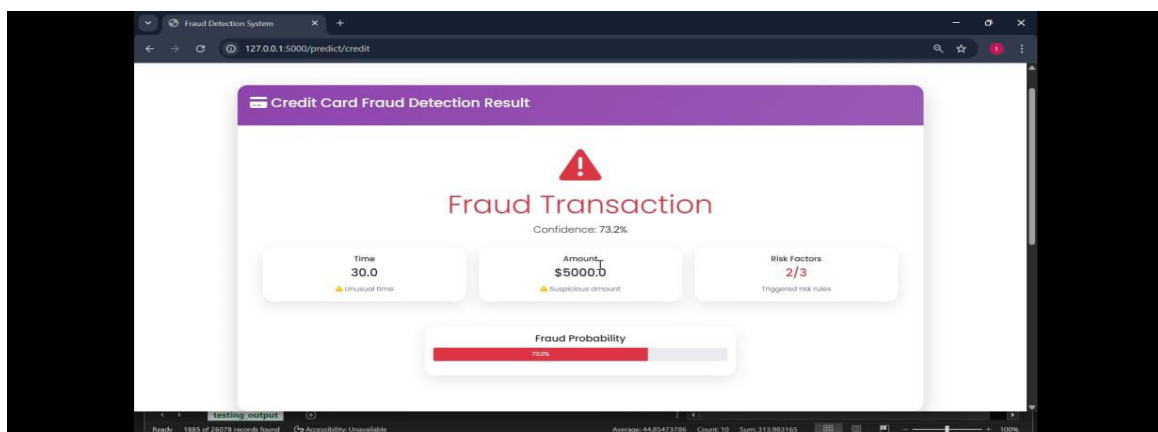


Fig-5 Predict as it is fraud

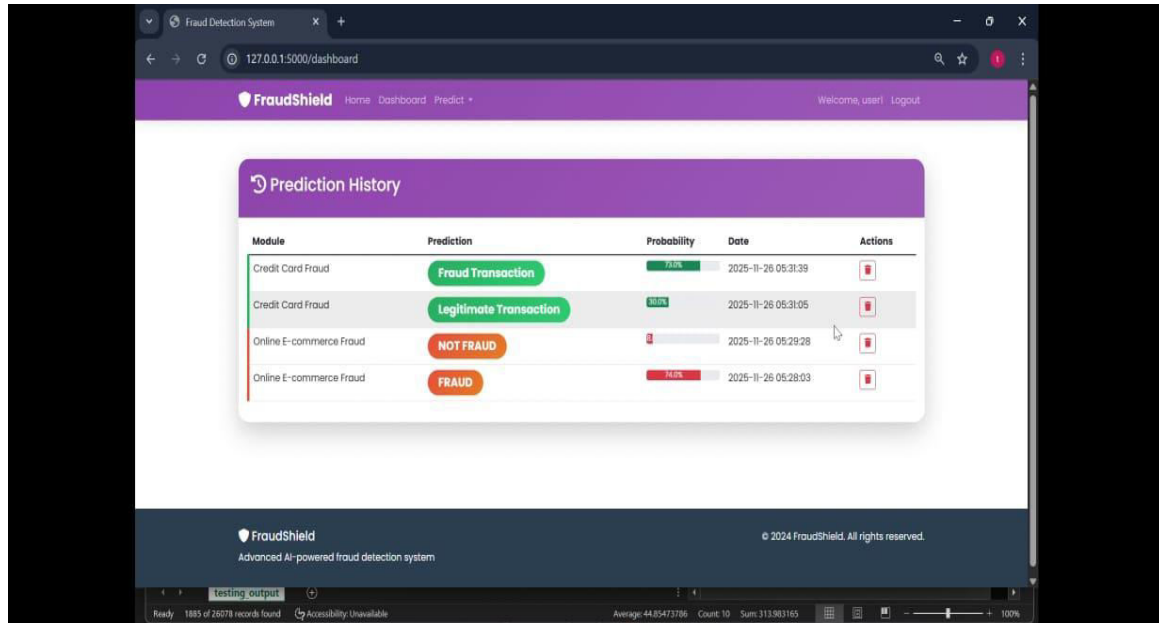


Fig-6 Prediction history

V. CONCLUSION

The completed fraud detection system fulfills its intended purpose by successfully detecting fraudulent transactions across e-commerce and credit card domains using modern machine learning techniques combined with explainable AI. The study demonstrates that hybrid model usage — Random Forest for heterogenous business-commerce transactions and XGBoost for dense credit card vectors — can provide robust detection performance while respecting execution time constraints suitable for real-time operations. The inclusion of SHAP-based explanations adds a vital layer of transparency, translating abstract model decisions into human-cultural reasoning. This innovative feature bridges the gap between automated systems and human fraud analysts, enabling accountable decision-making.

The system contributes meaningful advancements over existing solutions by addressing the critical shortcomings of traditional fraud detection methods that lack interpretability and adaptability. The model adapts to evolving fraud patterns by learning from historical anomalies rather than relying purely on fixed rule-sets. This flexibility enables improved coverage against emerging cybercrime techniques. Most importantly, the system avoids the common pitfall of operating as an opaque black-box, providing full interpretative context so that banking institutions, auditors, and users can justify the legitimacy of fraud detection decisions.

The successful implementation and validation of this system establish a solid foundation for further expansion and deployment. With additional refinement, the system could be integrated into enterprise-level e-commerce platforms or digital payment ecosystems as a defensive layer of fraud mitigation. Additionally, by employing incremental model retraining or continuous learning architecture, the system could become even more adaptive over time. Integrating this model with live streaming transaction networks — such as direct banking APIs — can provide instant risk scoring for every financial transaction flowing through the digital infrastructure.

REFERENCES

- [1] D. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Calibrating Probability with Undersampling for Unbalanced Classification," *2015 IEEE Symposium on Computational Intelligence and Data Mining*, pp. 159–166, 2015.
- [2] S. Jurgovsky, M. Granitzer, and E. Zangerle, "Sequence Classification for Credit-Card Fraud Detection," *Expert Systems with Applications*, vol. 100, pp. 234–245, 2018.

- [3] S. Behera and D. Nayak, "A Study of Imbalanced Data Sampling for Fraud Detection," *International Journal of Computer Applications*, vol. 975, pp. 8887, 2018.
- [4] S. Lundberg and S.-I. Lee, "A Unified Approach to Interpreting Model Predictions," *Advances in Neural Information Processing Systems*, pp. 4765–4774, 2017.
- [5] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 785–794, 2016.
- [6] J. Brownlee, "Implementing Ensemble Learning for Anomaly Detection," *Machine Learning Mastery*, 2016.
- [7] A. Nakamoto and J. Chang, "Real-Time Messaging Alerts for Payment Fraud Detection," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 4, pp. 671–683, 2020.
- [8] European Data Security Commission, "Guidelines on Automated Decision Systems and Model Interpretability," *EDSC Whitepaper*, 2018.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details