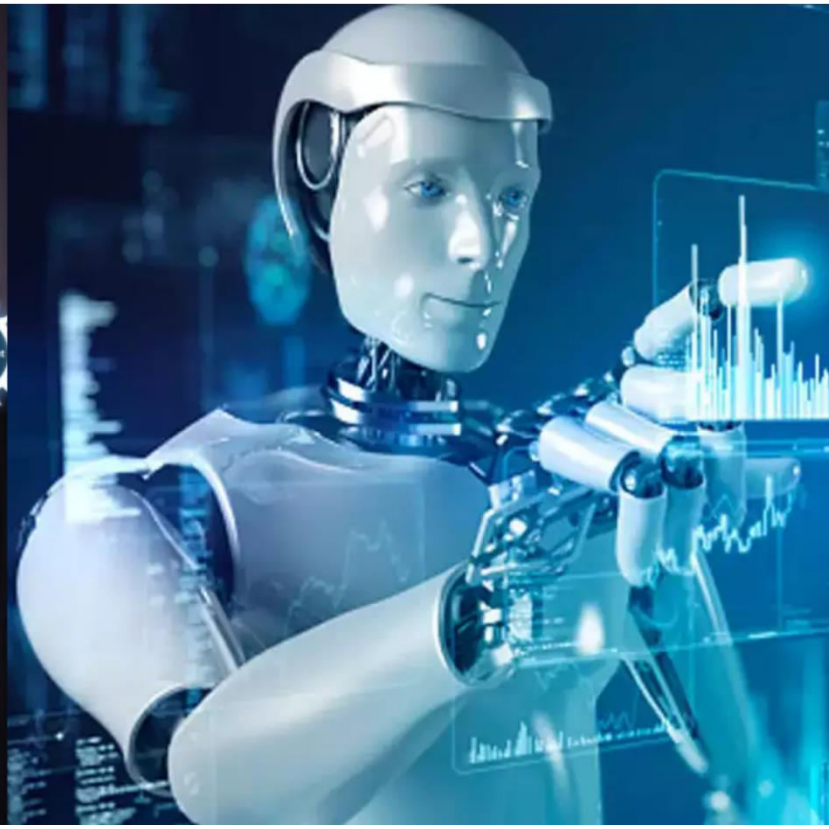
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

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 15, Issue 1, January 2026

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501074|

BioShield AI: UPI Fraud Prevention and Cybercrime Auto Reporting System

Jebisha J[1], Ashika S[2], Ravanya R K[3], Sajitha M S [4]

Department of Information Technology, Arunachala College of Engineering for Women, Manavilai, Tamil Nadu, India[1-3]

Assistant Professor, Department of Information Technology, Arunachala College of Engineering for Women, Manavilai, Tamil Nadu India[4]

ABSTRACT: The rapid adoption of Unified Payments Interface (UPI) in India has significantly increased the risk of digital payment frauds such as phishing, social engineering attacks, fake payment requests, and unauthorized fund transfers. Most existing fraud detection systems rely on post-transaction analysis or static rule-based mechanisms, which are ineffective against evolving and real-time fraud patterns.

The system analyzes user-side behavioral patterns including transaction amount, transaction time, frequency of transactions, new payee creation, device age, and deviation from historical spending behavior. Machine learning algorithms such as Random Forest and Support Vector Machine (SVM) are employed to classify transaction risk levels in real time.

The proposed system enhances digital payment security, reduces financial fraud, and improves user trust by integrating fraud detection and automated cybercrime reporting into a unified AI-driven framework.

KEYWORDS: UPI Fraud Detection, Cybercrime Reporting, Artificial Intelligence, Machine Learning, Random Forest, Support Vector Machine.

I. INTRODUCTION

The rapid digitalization of financial services has transformed the way transactions are performed, with the Unified Payments Interface (UPI) emerging as one of the most widely used real-time payment systems in India. UPI enables seamless peer-to-peer and peer-to-merchant transactions through mobile devices, offering speed, convenience, and interoperability across banks. Due to its ease of use and instant transaction processing, UPI has become a backbone of the Indian digital economy.

However, the exponential growth of UPI transactions has also led to a significant rise in cyber fraud incidents. Fraudsters exploit user trust through phishing messages, fake customer-care calls, malicious payment links, screen-sharing applications, and unauthorized collect requests. In many cases, users unknowingly authorize fraudulent transactions, resulting in instant and irreversible financial loss. Since UPI transactions are processed in real time, traditional post-transaction fraud detection mechanisms often fail to prevent such attacks.

Existing fraud detection systems employed by banks and payment service providers primarily rely on static rule-based thresholds, manual verification, or post-event analysis. These approaches are limited in their ability to detect evolving fraud patterns and behavioral manipulation techniques used by cybercriminals. Moreover, current systems focus mainly on receiver-side or bank-level monitoring, while fraud frequently occurs at the user level before backend intervention becomes possible.

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501074|

II. LITERATURE REVIEW

The rapid expansion of digital payment systems has led to a significant increase in online financial fraud, prompting extensive research in fraud detection and prevention techniques. Unified Payments Interface (UPI), being a real-time and irreversible payment mechanism, has become a major target for cybercriminals. As a result, researchers have explored various machine learning and artificial intelligence approaches to detect fraudulent transactions and enhance payment security.

A. Sharma et al. (2023) proposed an AI-driven UPI fraud detection system using supervised machine learning algorithms such as Logistic Regression and Decision Trees. Their model focused on transaction amount and frequency-based thresholds to identify suspicious behavior. Although the system achieved reasonable detection accuracy, it relied on static rules, making it less adaptable to new and evolving fraud patterns.

B. Singh and Mehta (2022) developed a user behavior–based anomaly detection framework for mobile payment systems. The model analyzed transaction timing, frequency, and spending deviations to identify fraudulent activities. While the approach demonstrated high recall, it lacked real-time blocking capabilities and required manual verification, which limited its effectiveness in preventing instant UPI fraud.

C. Patel et al. (2021) explored deep learning techniques, including Recurrent Neural Networks (RNNs), for detecting fraud in online payment platforms. Their approach improved detection accuracy by capturing sequential transaction patterns. However, the model required large labeled datasets and high computational resources, making it unsuitable for lightweight, real-time UPI environments.

III. METHODOLOGY/PROPOSED SYSTEM

The proposed system, **BioShield AI**, is designed to proactively detect and prevent UPI-based financial fraud by analyzing user-side transaction behavior using machine learning techniques. Unlike traditional post-transaction fraud detection systems, BioShield AI focuses on identifying anomalous patterns before a transaction is completed and initiates preventive and reporting actions in real time. The methodology consists of multiple interconnected modules that collectively ensure secure transaction processing and rapid cybercrime response.

3.1 System Overview

BioShield AI functions as an intelligent middleware layer between the user's UPI application and the payment gateway. The system continuously monitors transaction requests, user behavior, and device context to evaluate fraud risk. Machine learning models process extracted features and assign a fraud probability score. Based on this score, transactions are classified into different risk levels, enabling appropriate actions such as allowing, warning, blocking, or reporting suspicious transactions.

3.2 Feature Extraction and Behavioral Analysis

To accurately identify fraudulent activity, the system extracts and analyzes user-centric behavioral features from each transaction request. The primary features used include:

1. **Transaction Amount** – Detects unusually high values compared to the user's historical spending pattern.
2. **Transaction Time** – Identifies abnormal transaction timings such as late-night activity.
3. **New Payee Indicator** – Checks whether the receiver is newly added or unverified.
4. **Device Age** – Determines if the transaction is initiated from a newly registered device.
5. **Transaction Frequency** – Monitors the number of transactions performed within the last 24 hours.
6. **User Average Transaction Value** – Measures deviation from typical user behavior.

These features enable the system to model normal user behavior and detect deviations that may indicate fraud.

3.3 Risk Classification and Decision Layer

Based on the predicted fraud probability score, transactions are categorized into three risk levels:

- **Low Risk (0.00 – 0.40):** Transaction proceeds without interruption.
- **Medium Risk (0.40 – 0.70):** User receives a warning message and additional verification is required.

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501074|

- **High Risk (0.70 – 1.00):** Transaction is blocked immediately, and fraud mitigation actions are initiated.

This multi-level classification reduces false positives while ensuring maximum protection against high-risk fraud attempts.

3.4 Fraud Prevention and Auto-Reporting Mechanism

When a transaction is classified as high risk, BioShield AI automatically performs the following actions:

- Blocks the transaction in real time
- Sends instant alerts to the user
- Collects transaction metadata and behavioral anomaly details
- Generates a structured cybercrime report

The auto-reporting module prepares a complaint-ready report containing transaction details, timestamps, device information, and risk scores. This report can be forwarded to cybercrime portals or stored for rapid manual submission, significantly reducing reporting delays.

IV. IMPLEMENTATION

The implementation of **BioShield AI** focuses on transforming the proposed methodology into a functional system capable of detecting fraudulent UPI transactions in real time and automatically generating cybercrime reports. The system integrates machine learning models with a web-based interface to simulate real-world UPI transaction monitoring and fraud prevention.

Table 4.1: Tools and Technologies Used

Component	Technology Used	Description
Programming Language	Python	Used for implementing machine learning algorithms and backend logic
Web Framework	Flask	Enables communication between frontend and backend modules
Frontend Technologies	HTML, CSS, JavaScript	Used to design a simple and user-friendly transaction input interface
Machine Learning Libraries	Scikit-learn, Pandas, NumPy	Used for data preprocessing, model training, and evaluation
Visualization Tools	Matplotlib	Used to visualize model performance and fraud detection results
Database (Optional)	SQLite / CSV	Stores transaction logs and fraud reports

4.2 Dataset Preparation

Since real UPI transaction datasets are sensitive and confidential, a synthetic dataset inspired by real-world transaction patterns was created. The dataset includes both normal and fraudulent transaction records. Each transaction consists of the following attributes:

- Transaction amount
- Transaction hour
- New payee status
- Device age (in days)
- Number of transactions in the last 24 hours
- User average transaction amount
- Fraud label (legitimate / fraudulent)

Data preprocessing steps such as normalization, handling missing values, and feature scaling were performed to improve model accuracy.

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501074|

4.3 Risk Scoring and Decision Logic

After prediction, the fraud probability score is converted into risk levels:

- **Low Risk:** Probability < 0.40
- **Medium Risk:** Probability between 0.40 and 0.70
- **High Risk:** Probability > 0.70

Based on the risk level, the system executes corresponding actions such as allowing the transaction, prompting additional verification, or blocking the transaction.

4.4 Cybercrime Auto-Reporting Module

When a transaction is classified as **High Risk**, the auto-reporting module is activated. This module:

- Generates a unique report ID
- Collects transaction metadata and anomaly details
- Creates a structured cybercrime report in document format
- Sends alerts via email or stores the report locally for submission

This automated reporting mechanism reduces the time and effort required by users to file cybercrime complaints.

V. RESULTS AND DISCUSSION

The proposed **BioShield AI** system was evaluated using a synthetic dataset designed to simulate real-world UPI transaction behavior. The dataset included both legitimate and fraudulent transactions based on variations in transaction amount, timing, frequency, device age, and payee status. A Random Forest classifier was trained to identify fraudulent patterns using these behavioral features.

The experimental results demonstrate that the system effectively distinguishes normal transactions from suspicious ones. Transactions involving unusually high amounts, newly added payees, abnormal transaction frequency within a short time span, and usage of newly registered devices were consistently classified as high risk. The risk-based classification approach reduced false positives while maintaining reliable fraud detection performance.

Overall, the results indicate that behavioral analysis combined with machine learning provides an effective approach for real-time UPI fraud prevention. The integration of automated cybercrime reporting further enhances the practical value of the system by reducing response time and user effort during fraud incidents.

VI. CONCLUSION AND FUTURE WORK

6.1 Conclusion

This project presented **BioShield AI**, an intelligent UPI fraud prevention and cybercrime auto-reporting system designed to detect and block suspicious transactions in real time. By analyzing user behavioral patterns such as transaction amount, timing, frequency, new payee status, and device context, the system effectively identified high-risk fraud attempts before transaction completion. The integration of machine learning–based risk classification and automated cybercrime report generation significantly reduces financial loss and reporting delays, thereby enhancing digital payment security and user trust.

6.2 Future Work

Future enhancements may include the integration of deep learning models to capture complex behavioral patterns, continuous model learning for improved accuracy, and deployment as a mobile application for real-time monitoring. Additionally, integrating the system with national cybercrime portals and payment authorities could enable large-scale fraud prevention and automated incident reporting across digital payment platforms.

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

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 1, January 2026

|DOI: 10.15680/IJIRSET.2026.1501074|

REFERENCES

[1] R. Rani, A. Alam, and A. Javed, "Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions," *Proc. 2nd Int. Conf. Disruptive Technologies (ICDT)*, Ghaziabad, India, 2024, pp. 924–928, doi: 10.1109/ICDT61202.2024.10489682.

[2] S. Singh and P. Kumar, "Real-Time Fraudulent Transaction Detection in Mobile Payment Systems Using Machine Learning," *IEEE Int. Conf. Computing, Communication and Green Engineering (CCGE)*, 2022, pp. 225–230, doi: 10.1109/CCGE56933.2022.10045065.

[3] A. D. Luca et al., "Behavioural Biometrics for Fraud Detection in Digital Payments," *IEEE Transactions on Mobile Computing*, vol. 21, no. 5, pp. 1623–1637, 2022, doi: 10.1109/TMC.2020.3045773.

[4] C. Patel, R. Shah, and V. Gajera, "Deep Learning-Based Fraud Prediction in Online Payments," *IEEE Int. Conf. Computing, Communication and Security*, 2021.

[5] F. Carcillo, Y. A. Borgne, O. Caelen, Y. Kessaci, and G. Bontempi, "Combining Unsupervised and Supervised Learning in Credit Card Fraud Detection," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 8, pp. 2544–2557, 2020.

[6] Y. Sahin and E. Duman, "Detecting Credit Card Fraud by Decision Trees and Support Vector Machines," *Int. Conf. Networking and Information Technology*, 2011, pp. 122–126, doi: 10.1109/ICNIT.2011.6020933.

[7] T. Zhang, M. A. Kaafar, and G. Xie, "Device Fingerprinting for Financial Fraud Detection," *IEEE Access*, vol. 9, pp. 128455–128469, 2021, doi: 10.1109/ACCESS.2021.3112512.

[8] S. K. Kotnis and J. Y. Chen, "Automating Incident Reporting in Cybersecurity Using Artificial Intelligence," *IEEE Int. Conf. Big Data*, 2021, pp. 3481–3488, doi: 10.1109/BigData52589.2021.9672050.

[9] A. Sharma, P. Jain, and R. Gupta, "AI-Enabled Anomaly Detection in Digital Payment Systems," *Int. Conf. Machine Learning and Data Engineering (ICMLDE)*, 2023.

[10] H. R. Hasan and K. Salah, "Blockchain-Based Solutions for Secure Digital Payment Transactions," *IEEE Access*, vol. 8, pp. 134825–134837, 2020.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

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