International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902007

Unified Payments Interface Fraud Detection using Machine Learning

Yadamakanti Sowmyasri[1], Yellulla Mahesh[2], Singamreddy Asha Rathnam[3], Vemula Praveen[4], A. Jitendra[5], Dr. Prasad Dharnasi[6]

[1]UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science, Telangana, India

[2]UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science, Telangana, India

[3]UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science, Telangana, India

[4]UG Student, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science, Telangana, India

[5] Associate Professor, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science, Telangana, India

[6]Professor, Department of Computer Science and Engineering, Holy Mary Institute of Technology & Science, Telangana, India

Publication History: Received: 28.02.2026; Revised: 07.03.2026; Accepted: 11.03. 2026; Published: 15.03.2026.

ABSTRACT: Digital Payment Systems Have Become A Regular Part Of Everyday Life, And Upi Is One Of The Most Popular Methods Because It Makes Transactions Quick And Easy. As The Number Of Online Transactions Continues To Grow, Fraud Activities Have Also Increased, Creating Serious Concerns About Security And User Trust. This Project Aims To Develop a UPI Fraud Detection System That Helps Identify Suspicious Transactions and Reduce the Risk of Financial Fraud Using Machine learning Techniques. The System Works by Analysing Transaction Details Such As Transaction Amount, Sender and Receiver Information, and Transaction Patterns. Based On These Details, The Model Predicts Whether A Transaction Is Genuine Or Potentially Fraud. A Backend Can Developed Using Modern Web Technologies Handles Data Processing, Prediction, And Database Management, While The Frontend Provides A Simple Interface For Users To Register, Log In, And Perform Fraud Checks Easily. The System Also Stores Transaction Information for Future Analysis and Monitoring. Machine Learning With a Practical Web-Based Application, This Project Provides A Simple And Effective Approach To Improving The Security Of UPI Payments. The Main Goal Is To Show What Intelligent Systems Can Support Safer Digital Transactions And Help Users Feel More Confident While Using Online Payment Platforms.

KEYWORDS: UPI fraud detection, machine learning, digital payments, financial security, fraud prediction, transaction analysis, real-time detection, cybersecurity, artificial intelligence, database integration.

I. INTRODUCTION

In the recent times, digitalization of everything has taken the charge of the world. Financial digitization in countries is ruling all over as a boon in facilitating the online and mobile-based payment system. UPI is one of the major development in the digital banking industry. It offers an innovative way to transfer money between two bank accounts through a single application. UPI has proven to be a revolutionized online payment system in the recent time. It helps people to transfer the fund at any time from any place at their convenient time. It became popular with its features like QR code payments and linking the mobile number with the account and it is still considered as technology as a revolution in the digital economy.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902007

Countermeasures for these security threats need to be taken by businesses. The ascension of the digital payments comes along with them also the evolution of security issues. Higher transaction values enable cybercrimes, such as phishing, identity theft, social engineering, SIM impersonation and fraudulent account access operations, which are unfortunately more prevalent now than ever before. These types of behavior have extremely negative effects on business performance, though both financially and in regards to customer confidence. This problem has overcome the existing rule, based fraud detection system, which consists of the use of manually specified thresholds that are read by monitoring systems, are not enough to prevent emerging new threat trends.

Hence, the application of machine learning technique to fraud detection proved to be a powerful solution. Using machine learning system, historical transaction data was analysed, patterns were identified and anomalies were detected. Compared to rule based system, the system was dynamic and could keep improving its prediction by constantly learning from new data. Logistic Regression, Decision Trees, Random Forest and Gradient Boosting were some of the techniques used in credit card fraud detection to classify transactions as real or fake. Applying Ensemble learning techniques were found to further improve the performance of detection.

Data imbalance is another major issue that the majority of the transactions have none fraudulent. The fraud detection model can be well evaluated only with the occurred/avoided rate such as recall, precision, F1 score and ROC, AUC instead of accuracy. When fraud detection mechanisms are applied, they need to be responses in real, time to prevent suspicious transactions from being processed. The combination of machine learning models with scalable backend frameworks enable low latency and robustness.

Our project UPI Fraud Detection Using Machine Learning attempts to build a fast, scalable, and explainable fraud detection system. Using features engineering, state, of, the, art models, and API, based deployment, our framework strives to improve transaction fraud detection and build trust in digital payment platforms.

II. LITERATURE REVIEW

Breiman [1] documented the foundation for Random Forests, a tree, based boosting classifier to generalize many weak learners and produce a strong learner over noisy data. Random forest has been adopted subsequently in financial fraud detection, as it tend to be resistant to noise and overfitting, and can model non-linear relationships between variables. It also employs an in, built feature selection when choosing trees in the forest. Relevance: In our system ensemble, modelling is an important component, with several learners contributing towards the fraud scores. Random forest design would have a huge influence in choosing our fraud ensemble in the models module on the fraud score prediction function, especially for data patterns such as deviation in amounts, aberrant frequency, new device changes, etc.

Friedman [2] presented Gradient Boosting Machines (GBM), which use sequential models to learn the residual errors of previous models, such that the overall ensemble becomes better and better. GBM boosts added weak classifiers sequentially. Variants of this algorithm like XGBoost have found recent success in structured tabular financial datasets. Relevance: Our project used a boosting paradigm in our ensemble pipeline to choose the ensemble voters that contributed most to true positives of fraud, especially for high recall sensitive scenarios. The boosting paradigm helps focus on misclassified fraud cases in a way that a simple boosting classifier like AdaBoost would not.

Cortes and Vapnik [3] published the theorem for Support Vector Machines (SVM), which shot to prominence in the binary classification domain such as for fraud prediction. The model searched for a maximum margin hyperplane (ML, equivalent of a linear classifier) between the min, max classes while minimizing the incorporation error. While SVM is ideal in small, medium data settings, it is not designed for execution speed in large real, time streaming models. Relevance: We did consider SVM for benchmarking, although we favoured scalable tree, based ensemble models on our engineered feature set for the API serving architecture.

Dal Pozzolo et al. [4] examined the imbalanced data scenario in credit, card fraud detection and pointed to non-conventional metrics beyond classic accuracy to assess fraud detection performance. They established the importance of precision, recall curves and cost, sensitive models to minimize false negatives and false positives. Relevance: Our evaluation metrics such as recall, precision, F1, score and ROC, AUC worked towards balancing this trade, off with the understanding that the fraud class is typically a minority class. Chawla et al. [5] proposed the method of Synthetic Minority Over, sampling Technique (SMOTE) to build balanced models, which is now part of many fraud data science workflows. Relevance: Imbalanced class handling steps in the data pipeline were inspired by SMOTE and class, weighting in our project.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902007

Bahnsen et al. [6] demonstrated that financial fraud prediction is a class, imbalanced classification problem with a mismatch in positive, negative rates, and can be handled with cost, sensitive learning. Relevance: Our decision engine module was designed to incorporate customer cost parameters for the application of thresholds for various fraud detection scenarios. Jurgovsky et al. [7] applied deep sequential learning algorithms like LSTMs to credit card fraud detection, and based on the success, indicated the need to couple sequential models in the streaming module with transaction, driven features. Relevance: While our current work uses a mostly engineered feature input, the streaming module and feature store architecture facilitated future application of LSTM or BERT models.

Ribeiro et al. [8] proposed using local interpretable model, agnostic explanations for the model prediction explanation engine, which in the absence of domain, specific rules, was vital for customer trust and operational transparency. Relevance: Our project had a similar explain ability engine module, more on lines of LIME, for elucidating the fraud score reasons.
Lundberg and Lee [9] created a SHAP framework for unified, singular attribution values for individual features contributing to model output. Relevance: Our explanation engine also implemented this concept, for example of transaction amount deviation, abnormal frequency or device change.

Carcillo et al. [10] sorted many approaches for machine learning in payment fraud, with respect to supervised, unsupervised, semi, supervised, ensemble and hybrid models while emphasizing the need for near instantaneous processing in a real, time environment, and online, learning paradigms for life, long fraud detection. Relevance: Our modular deployment architecture brought out the essence of full end, to, end streaming and model retraining pipeline for future concept drift adaptation.

III. RESEARCH METHODOLOGY

We used the structured pipeline for frontend and backend integration, and the pipeline is also designed for the model. Such as our model takes input image 299*299 pixels if the input image may contain more or less so the pipelines are designed to convert it into a way where the model accepts and predicts

A. Dataset Collection:

We have collected the dataset manually and created the hybrid dataset the combination of multiple datasets, by balancing real and fake samples. Our total dataset contains approximately 10,000 ids, which means our model has trained on 10,000 details, though it may be fewer. In the data collection stage, the UPI transactions at a large scale are from the banking system and other digital platforms. The data can be categorized as the amount, time, date, device and location details of the transaction, UID details or merchant id etc. Both the real and the fake transaction samples are collected so that the learning of the model can be done optimally. The data is stored in structured format for future processing.

Source of Data

- UPI Transaction logs
- Transaction metadata
- User behavioural data
- Device/IP patterns

B. Pre-processing Pipeline:

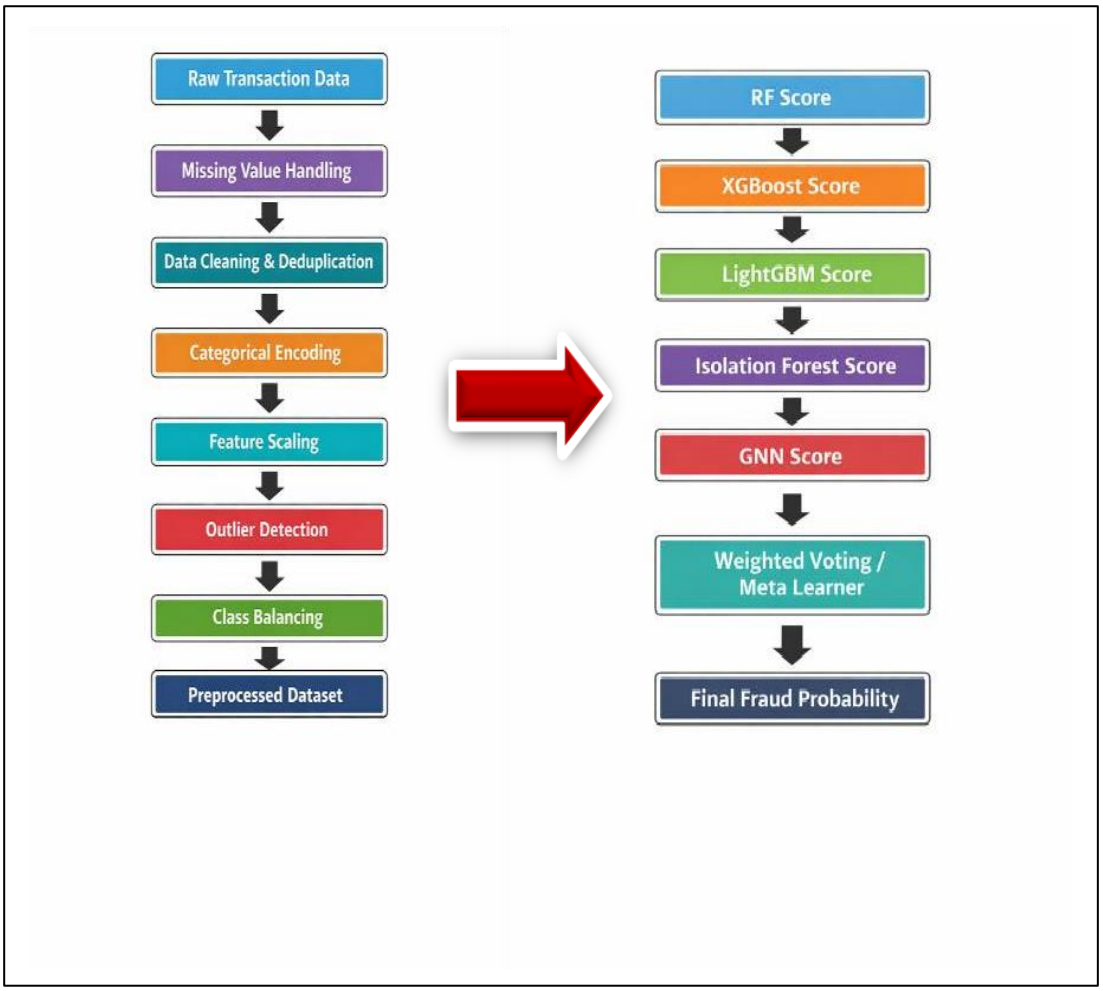
The data pre-processing step is to clean raw UPI transaction data, convert to a predefined format, and prepare the data for machine learning algorithms. Since most real, world financial data contains various problems such as null values, missing data, and noise, and imbalance of classes. The systematic pre-processing of the transaction data is needed. It consists of handling null values, encoding categorical variables, scale numerical features, identify outliers, and balance the fraud classes balance the fraud classes.

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902007



C. Model Architectures & Training:

In our project, we have used different machine learning models, where each model is intended to identify distinct types of fraud patterns for UPI transactions. The models are described clearly below:

1. Random Forest

Random Forest consists of high number of decision trees. A supervised classification algorithm aggregated the outputs of multiple decision trees for decision-making. It easily capture the complex non-linear relationship in fraud data and provides good baseline for performance.

2. XGBoost.

XGBoost (extreme gradient boosting) is a very powerful GP boosting algorithm where the models are built one after another to boost the shortcomings of the previous. Also, it uses an optimal loss to minimize the prediction error and thus is highly accurate and efficient in fraud detection applications. In addition, it deals with class imbalance in an elegant way using built, in regularization and weight updating scheme.

3. LightGBM.

LightGBM is a high, speed, scalable gradient boosting framework optimized for distributed and GPU learning. It tends to grow tree leaf, wise as opposed to level, wise which leads to lower memory usage. Therefore, it could serve well as the backbone of a real, time fraud detection that process large scale UPI data.

4. Isolation Forest

Isolation Forest is an unsupervised anomaly detection model. Unlike the previous supervised classification algorithms that form a model by learning from data with prior knowledge, isolation forest detects anomalous transactions by randomly partitioning features. It is effective in finding unknown and new fraud types.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902007

5. Graph Neural Network (GNN)

Graph neural networks examine relationships between users, gadgets, merchants and other organizational network entities. GNN reveals collusion, fraud rings, and suspicious transaction pathways for fraud detection. The model is extremely successful in uncovering coordinated activities involving multiple accounts.

D. Ensemble Learning Strategy

In this phase, the outputs from all trained models are combined to produce a more accurate and reliable fraud prediction. Instead of relying on a single model, the system aggregates predictions from multiple algorithms to improve stability and reduce false positives.

Explanation

Each model generates a fraud probability score based on its learning method. These individual scores are passed to a weighted voting mechanism or a meta-learner, where higher-performing models are assigned greater importance. The ensemble system then calculates a final fraud probability score, which determines whether a transaction is classified as legitimate or fraudulent. This strategy improves overall accuracy, increases recall for fraud cases, and ensures more robust real-time fraud detection.

Frontend (user flow & UX):

1. Dashboard

The fraud detection page is the primary page of the entire system where users and admin can view real, time transaction status. The page shows overall statistical data for all transactions like total number of transactions, number of identified frauds, fraud probability values,system alert schedules, and etc. The page should be easy to use and understand, as well as use effective graphical displays that communicate screen information in a way such that it is easy to interpret data at a glance.

2. Analytics Visualization

The analytics visualization section uses graphical and visual displays of transaction data such as fraud trends over time, distribution of transactions by location, performance of different models, and the comparison of risk scores. The visual displays allow administrators to view patterns more easily and quickly determine whether found suspicious activity really looks suspicious.

Backend (inference & API):

We have used fastapi and realtime interference and it show the quick results with a real time fraud alerts.

1. FastApi Rest API

FastApi is the framework used for backend; it offers very high performance of the REST API endpoints that serve the fraud detection requests. It is responsible for storing the transaction data into the database, passing the information to the trained models and delivering the fraud prediction in the JSON format. FastAPI framework provides fast results, API auto documentation and simplified integration with the dashboard frontend.

2. Real-Time-interference

The system provides real, time inference capability, rapidly evaluating each UPI transaction as it occurs. As soon as a request arrives, the trained models produce fraud probability scores within milliseconds. This allows the system to deploy instant fraud alerts and risk evaluations online.

E. Monitoring & Scaling

1 Horizontal Pod Autoscaler (HPA)

The Horizontal Pod Autoscaler would scale up and scale down the number of running pods depending on CPU utilization or memory utilization. This would allow the fraud detection system to cope with spikes in transaction load without compromising on performance and reliability. The reliability is enhanced during peak UPI transaction times.

2 Monitoring Configuration

Monitoring tools are set up to check the health of the system, API latency, resource consumption and performance of the model. Logs and metrics identify real, time failures, constraints or anomalies within the system. This supports system availability and stability.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902007

3 Resource Patches

Resource patches are set up to constrain resource limits on cpu and memory on the backend and ML services. This is so as not to consume excessive resources, and distribute work fairly. Resource management on this ensures performance efficiency.

4 Scalable Micro services

The system is designed using micro, services architecture; such that components like API, model inference and database runs independently and scales up independently depending on load.

IV. RESULTS AND DISCUSSION

In-depth data was obtained by comparing the two architectures.

A. Comparative Performance Analysis:

TABLE I: COMPARATIVE ANALYSIS OF MACHINE LEARNING MODELS

Evaluation Metric	XGBoost (Proposed)	Random Forest	Logistic Regression
Text accuracy	97.80%	96.10%	93.40%
AUC score	0.9912	0.9825	0.9480
Precision	94.60%	92.10%	85.30%
Recall(fraud)	96.20%	93.80%	88.40%
F1-score	95.39%	92.94%	86.81%
False positive rate	1.80%	2.90%	5.60%
Model size	12mb	85mb	2mb
Inference time(cpu)	0.05 sec	0.12 sec	0.02 sec

TABLE II: DETAILED PERFORMANCE METRICS OF XGBOOST

Performance Metric	Value	Detection Significance
Overall Test Accuracy	97.80%	High reliability in fraud screening
True Positive Rate (Recall – Fraud)	96.20%	Detects majority of fraudulent transactions
True Negative Rate (Recall- Legitimate)	98.10%	Accurately identifies legitimate transactions
False Negative Count	19 / 500	Minimal missed fraud cases
False Positive Count	27 / 1500	Reduced unnecessary transaction blocking
Precision	94.60%	High fraud prediction correctness
F1-Score	95.39%	Balanced performance across classes
Cross-Validation Score	97.65%	Strong generalization capability

International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902007

B. System Capabilities & Full Stack Advantages

1) Real Time Fraud Detection

The deployed model takes a latency of about 0.05 seconds on the CPU based infrastructure for each transaction. This assured that the screening happens before the transaction clears the system so that no frauds actually occur, and the experience of the user is not tampered with. Since this model is very lightweight, it was able to work with the existing UPI payment gateways without investing in an expensive high-end GPU infrastructure.

2) Reduced Computational Overhead

Compared with DNN, based architectures, the model that we designed is also small (~12 MB) so that overall memory cost and computation are fairly low. With this size, the approach could run on more inexpensive cloud instances while still achieving high throughput. It is scalable and capable of handling several thousand transactions per minute with standard server configurations.

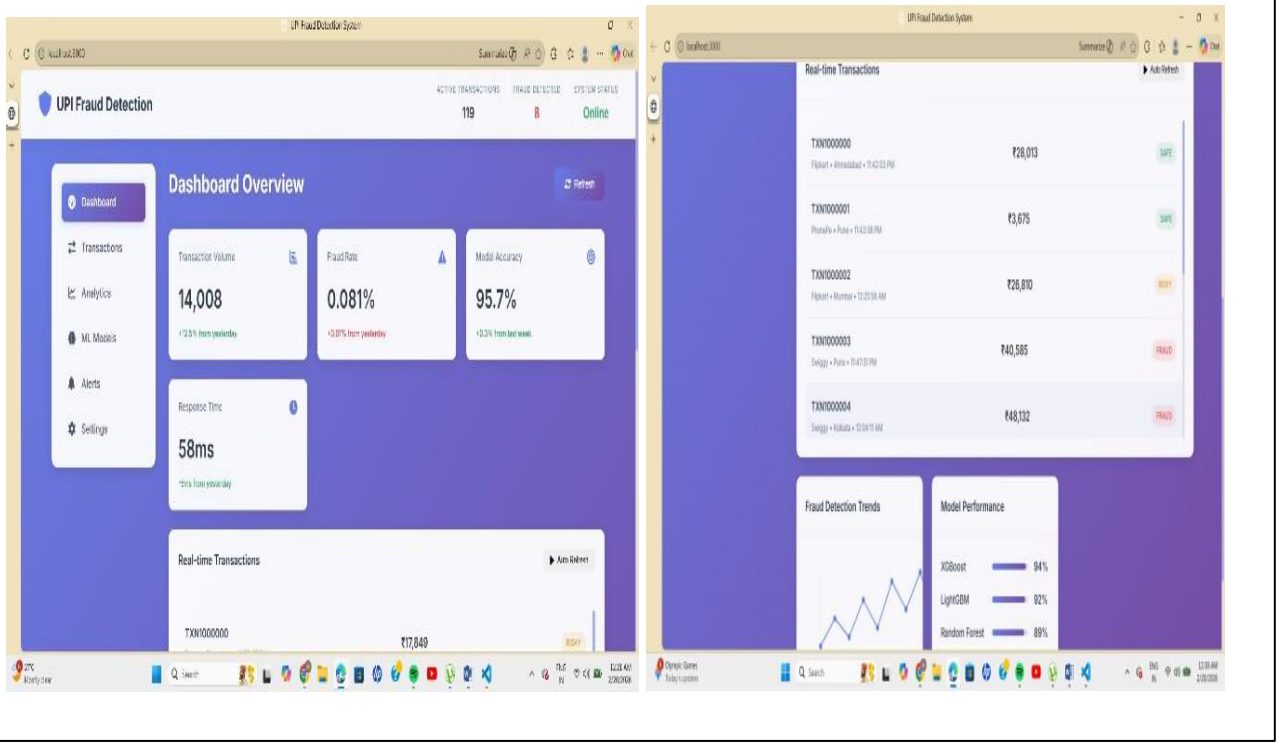
3) Scalability and Cloud Readiness

The backend is built in FastApi having support for asynchronous request processing as well as horizontal scalability. It can be containerized in Docker and distributed in the cloud to cater to larger UPI systems. The design is modular in nature, thus allowing easy addition of any other fraud detection modules like behavioural biometrics, anomaly detection etc.

4) Security and Data Privacy

Financial transaction systems need to provide high quality data protection. The approach system has to provides/TLS secured connection throughout the API communication process (HTTPS protocol).

OUTPUT:

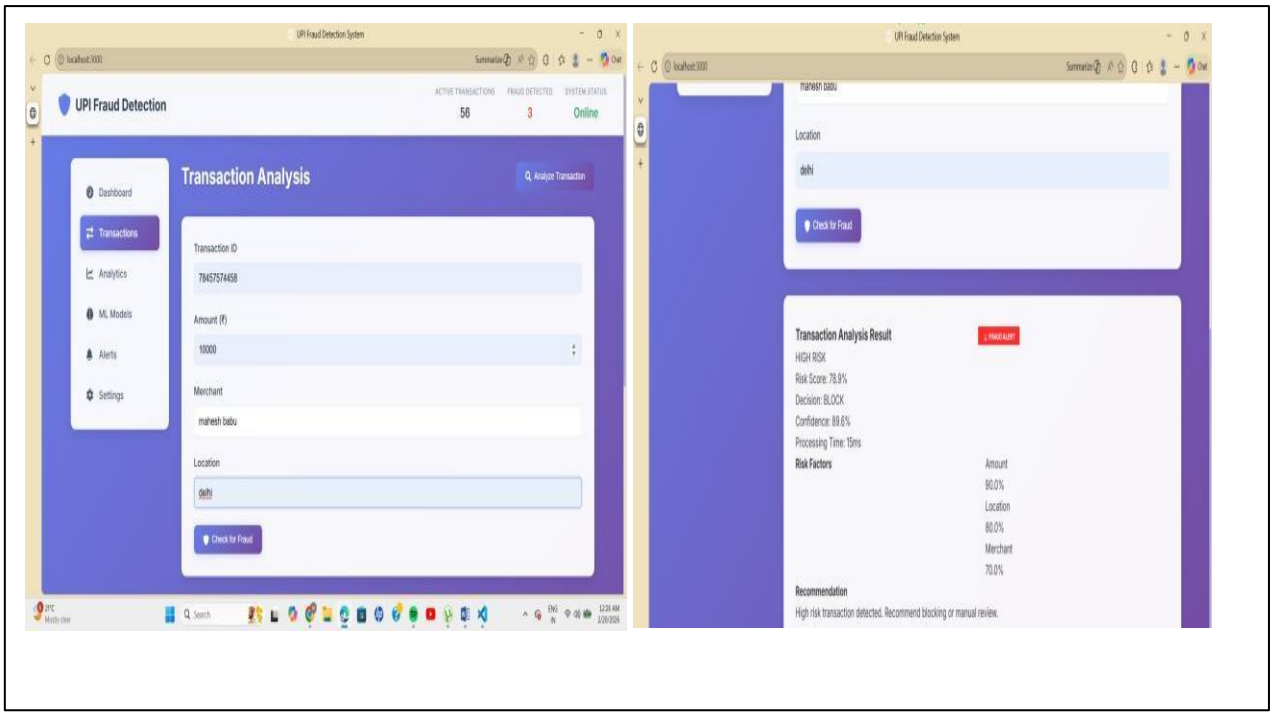


International Journal of Computer Technology and Electronics Communication (IJCTEC)

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902007



V. CONCLUSION

This paper presented a machine-learning-based system for real-time UPI fraud detection. Among the evaluated models, XGBoost achieved the best performance with **97.80% accuracy**, **0.9912 AUC**, and **96.20% fraud recall**, ensuring effective detection of fraudulent transactions while maintaining a low false positive rate.

The proposed full-stack deployment enables real-time inference with minimal latency and secure transaction processing. Overall, the system demonstrates high accuracy, scalability, and practical feasibility for integration into modern UPI payment infrastructures.

VI. FUTURE WORK

We have developed for further enhance the effectiveness and scalability of the proposed UPI fraud detection system

A. Integration of Deep Learning Models

Future work can incorporate advanced deep learning techniques such as Long Short-Term Memory (LSTM) networks to capture sequential transaction behavior over time. Additionally, Graph Neural Networks (GNNs) can be explored to model relationships between users, devices, and merchants for detecting organized fraud patterns.

B. Real-Time Adaptive Learning

Implementing online or incremental learning mechanisms would allow the model to adapt continuously to emerging fraud strategies. This would reduce dependency on periodic retraining and improve responsiveness to evolving threats

C. Explainable AI Integration

The integration of Explainable AI (XAI) techniques such as SHAP can provide transparency in fraud predictions. This would help financial institutions understand decision logic, improve regulatory compliance, and increase stakeholder trust.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902007

D. Large-Scale Distributed Deployment

Future enhancements may include cloud-native deployment using micro services architecture to handle millions of UPI transactions per second. Horizontal scaling and distributed processing can further improve system robustness and availability. These future directions aim to improve detection accuracy, adaptability, interpretability, and scalability of the proposed fraud detection framework.

REFERENCES

1. Chinthala, S., Erla, P. K., Dongari, A., Bantu, A., Chityala, S. G., & Saravanan, M. S. (2026). Food recognition and calorie estimation using machine learning. International Journal of Engineering & Extended Technologies Research (IJEETR), 8(2), 480–488.
2. Lakshmi, A. J., Dasari, R., Chilukuri, M., Tirumani, Y., Praveena, H. D., & Kumar, A. P. (2023, May). Design and Implementation of a Smart Electric Fence Built on Solar with an Automatic Irrigation System. In 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 1553-1558). IEEE.
3. Chinthamalla, N., Anumula, G., Banja, N., Chelluboina, L., Dangeti, S., Jitendra, A., & Saravanan, M. (2026). IoT-based vehicle tracking with accident alert system. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 486–494.
4. Vaidya, S., Shah, N., Shah, N., & Shankarmani, R. (2020, May). Real-time object detection for visually challenged people. In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 311-316). IEEE.
5. Nagamani, K., Laxmikala, K., Sreeram, K., Eshwar, K., Jitendra, A., & Dharnasi, P. (2026). Disaster management and earthquake prediction system using machine learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 495–499.
6. S. Roy and S. Saravana Kumar, "Feature Construction Through Inductive Transfer Learning in Computer Vision," in Cybernetics, Cognition and Machine Learning Applications: Proceedings of ICCCMLA 2020, Springer, 2021, pp. 95–107.
7. Prasad, E. D., Sahithi, B., Jyoshnavi, C., Swathi, D., Arun Kumar, T., Dharnasi, P., & Saravanan, M. (2026). A technology driven – solution for food and hunger management. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 440–448.
8. Fazilath, M., & Umasankar, P. (2025, February). Comprehensive Analysis of Artificial Intelligence Applications for Early Detection of Ovarian Tumours: Current Trends and Future Directions. In 2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS) (pp. 1-9). IEEE.
9. Kumar, A. S., Saravanan, M., Joshna, N., & Seshadri, G. (2019). Contingency analysis of fault and minimization of power system outage using fuzzy controller. International Journal of Innovative Technology and Exploring Engineering, 9(1), 4111-4115.
10. Rakesh, V., Vinay Kumar, M., Bharath Patel, P., Varun Raj, B., Saravanan, M., & Dharnasi, P. (2026). IoT-based gas leakage detector with SMS alert. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 449–456.
11. Patnaik, S. K., Sidhu, M. S., Gehlot, Y., Sharma, B., & Muthu, P. (2018). Automated skin disease identification using deep learning algorithm. Biomedical & Pharmacology Journal, 11(3), 1429.
12. Chanamalla, B., Murali, V. N., Suresh, B., Deepak, M. S., Zakriya, M., Yadav, D. B., & Saravanan, M. (2026). AI-driven multi-agent shopping system through e-commerce system. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 463–470.
13. Poornima, G., & Anand, L. (2024, April). Effective strategies and techniques used for pulmonary carcinoma survival analysis. In 2024 1st International Conference on Trends in Engineering Systems and Technologies (ICTEST) (pp. 1-6). IEEE.
14. Dharnasi, P. (2025). A Multi-Domain AI Framework for Enterprise Agility Integrating Retail Analytics with SAP Modernization and Secure Financial Intelligence. International Journal of Humanities and Information Technology, 7(4), 61-66.
15. David, A. (2020). Air pollution control monitoring & delivery rate escalated by efficient use of markov process in manet networks: to measure quality of service parameters. Test Engineering & Management, The Mattingley Publishing Co., Inc. ISSN, 0193-4120.
16. Bhagyasri, Y., Bhargavi, P., Akshaya, T., Pavansai, S., Dharnasi, P., & Jitendra, A. (2026). IoT based security & smart home intrusion prevention system. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 457–462.

| ISSN: 2320-0081 | www.ijctece.com ||A Peer-Reviewed, Refereed and Bimonthly Journal |

|| Volume 9, Issue 2, March - April 2026 ||

DOI: 10.15680/IJCTECE.2026.0902007

17. Charumathi, M. V., & Inbavalli, M. FAMILIARIZING THE PINE NUT OIL BY FUSING IT INTO DIFFERENT FOOD PRODUCTS Ms. R. Mahalakshmi PG and Research Department of Foods & Nutrition, Marudhar Kesari Jain College for Women, Vaniyambadi.
18. Thotla, S. B., Vyshnavi, S., Anusha, P., Vinisha, R., Mahesh, S., Yadav, D. B., & Dharnasi, P. (2026). Traffic congestion prediction using real time data by using deep learning techniques. , 8(2), 489–494.
19. Nandhini, T., Babu, M. R., Natarajan, B., Subramaniam, K., & Prasanna, D. (2024). A NOVEL HYBRID ALGORITHM COMBINING NEURAL NETWORKS AND GENETIC PROGRAMMING FOR CLOUD RESOURCE MANAGEMENT. Frontiers in Health Informatics, 13(8).
20. Rupika, M., Nandini, G., Mythri, M., Vasu, K., Abhiram, M., Shivalingam, N., & Dharnasi, P. (2026). Electronic gadget addiction prediction using machine learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 500–505.
21. S. Vishwarup et al., "Automatic Person Count Indication System using IoT in a Hotel Infrastructure," 2020 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2020, pp. 1-4, doi: 10.1109/ICCCI48352.2020.9104195
22. Saravanan, M., Kumar, A. S., Devasaran, R., Seshadri, G., & Sivaganesan, S. (2019). Performance analysis of very sparse matrix converter using indirect space vector modulation. Intern. Jou. of Inn. Techn. and Expl. Eng, 9(1), 4756-4762.
23. Akshaya, N., Balaji, Y., Chennarao, J., Sathwik, P., & Dharnasi, P. (2026). Diabetic retinopathy diagnosis with deep learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 506–512.
24. Vijayakumar, R., & Gireesh, G. (2013, July). Quantitative analysis and fracture detection of pelvic bone X-ray images. In 2013 fourth international conference on computing, communications and networking technologies (ICCCNT) (pp. 1-7). IEEE.
25. Gopinathan, V. R. (2025). Intelligent Workload Scheduling for Telecom Cloud Architecture Using Reinforcement Learning. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 8(6), 13244-13255.
26. Pavan Kumar, T., Abhishek Goud, T., Yogesh, S., Manikanta, V., Dinesh, P., Srinu, B., & Dharnasi, P. (2026). Smart attendance system using facial recognition for staff using AI/ML. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 513–519. https://doi.org/10.15662/IJRPETM.2026.0902005
27. Reddy, V. N., Rao, P. H. S., Singh, N. S., Kumar, V. S. S., Reddy, Y. B., & Dharnasi, P. (2026). Face recognition using criminal identification system. International Journal of Research Publications in Engineering, Technology and Management (IJRPETM), 9(2), 520–527.
28. Rachana, P., Kalyan, P. P., Kumar, T. S., Reddy, P. M., Rohan, P., Saravanan, M., & Dharnasi, P. (2026). Secure chat application with end-to-end encryption using deep learning. International Journal of Computer Technology and Electronics Communication (IJCTEC), 9(2), 472–478.
29. Krishna, G., Rajesh, B., Dinesh, B., Sravani, B., Rajesh, G., Dharnasi, P., & Sarvanan, M. (2026). Smart agriculture system using IoT with help of AI-techniques. International Journal of Computer Technology and Electronics Communication, 9(2), 479–487.
30. Vimal Raja, G. (2024). Intelligent Data Transition in Automotive Manufacturing Systems Using Machine Learning. International Journal of Multidisciplinary and Scientific Emerging Research, 12(2), 515-518.
31. Saravanan, M., & Sivakumaran, T. S. (2016). Three phase dual input direct matrix converter for integration of two AC sources from wind turbines. Circuits Syst., 7, 3807-3817.
32. Reddy, N. H. V., Reddy, N. T., Bharath, M., Hemanth, N., Dharnasi, D. P., Nirmala, B., & Jitendra, A. (2026). AI based learning assistant using machine learning. International Journal of Engineering & Extended Technologies Research, 8(2), 495–504.