Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

A Smart AI Framework for BFSI Fraud Prediction

Mohanapriya M, Divya R, Deeksha G S, Deepak Jogi K, Karthik R
Department of Computer Science and Engineering
Sambhram Institute of Technology, Bengaluru
Visvesvaraya Technological University India

Abstract **- The exponential growth of digital payment infrastructures has intensified the complexity and frequency of financial fraud, necessitating intelligent and automated detection mechanisms. This project proposes a smart machine learning–based fraud detection framework for real-time monitoring of Unified Payments Interface (UPI) transactions within the BFSI sector. A heterogeneous dataset containing both legitimate and fraudulent transactions is utilized for advanced feature engineering, normalization, and dimensionality reduction to extract high-impact discriminative features. The model is trained using historical transaction data and evaluated using standard performance metrics such as precision, recall, F1-score, ROC-AUC, and accuracy. Key attributes including transaction amount, temporal behavior, payer–payee relationships, geospatial indicators, and device fingerprints are incorporated, with higher emphasis on time-series features to capture sequential fraud patterns. The optimized hybrid model is integrated into the UPI framework for real-time inference and transaction scoring. An automated alert and response mechanism is deployed to enable prompt intervention, risk mitigation, and effective fraud containment.**

Keywords: Machine Learning, Fraud Detection, BFSI, UPI Transactions, Anomaly Detection, Cybersecurity

I. INTRODUCTION

Financial fraud is one of the most critical challenges faced by the Banking, Financial Services, and Insurance (BFSI) sector due to the rapid growth of digital payment systems. Fraudsters continuously exploit system vulnerabilities, resulting in significant financial losses and reputational damage. Traditional rule-based and manual fraud detection methods are ineffective in handling the scale, speed, and complexity of modern transactions.

Artificial Intelligence (AI) and Machine Learning (ML) techniques have emerged as effective solutions by learning hidden patterns from large-scale transaction data. These models enable automated anomaly detection, adaptive learning, and near real-time fraud prediction, significantly improving detection accuracy and operational efficiency.

II. LITERATURE SURVEY

Early fraud detection systems relied on static rule-based mechanisms and manual verification, which were limited to known fraud patterns and suffered from high falsepositive rates. Recent studies demonstrate improved accuracy using ML algorithms such as Logistic Regression, Decision Trees, Random Forest, and Support Vector Machines. Ensemble models like Random Forest and XGBoost show superior performance on highdimensional and non-linear data.

To capture sequential fraud behavior, deep learning techniques such as Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks have been widely adopted. Although effective, these models require large datasets and high computational resources, motivating the need for hybrid approaches that balance accuracy and efficiency.

III. IMPLEMENTATION

The proposed **PAYSAFE-X** framework adopts a hybrid fraud detection architecture combining ensemble ML models with deep learning.

1. **Data Ingestion and Integration:** Transaction data from heterogeneous BFSI sources is collected and unified into a common schema, ensuring consistency across transaction amount, timestamp, sender/receiver IDs, device metadata, and location attributes.

2. **Data Pre-processing**: Duplicate and incomplete records are removed. Missing values are handled through statistical imputation. Categorical attributes are encoded using label and one-hot encoding, while numerical features are normalized using Min-Max scaling.
3. **Handling Class Imbalance:** SMOTE is applied only to training data to address class imbalance and improve fraud pattern learning without test data bias.

4. **Feature Engineering:** Features are categorized into transactional, behavioural, and temporal attributes to capture both instantaneous anomalies and evolving fraud patterns.

5. **Model Training:** Random Forest and XGBoost analyze static features, while an LSTM network captures temporal dependencies. Hyperparameter tuning and cross-validation are applied to optimize performance.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

IV. RESULTS AND CONCLUSION

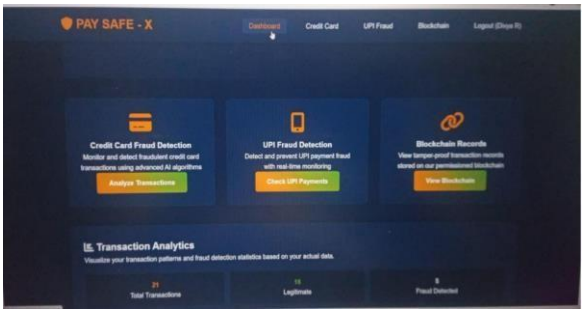
The Smart AI Framework for BFSI Fraud Prediction demonstrates the effectiveness of combining Machine Learning (ML) and Deep Learning (DL) techniques to combat financial fraud in modern digital ecosystems. Through the integration of multiple datasets, advanced feature engineering, and hybrid modelling, the system achieves high detection accuracy while maintaining extremely low latency during real-time predictions.
The results show that:

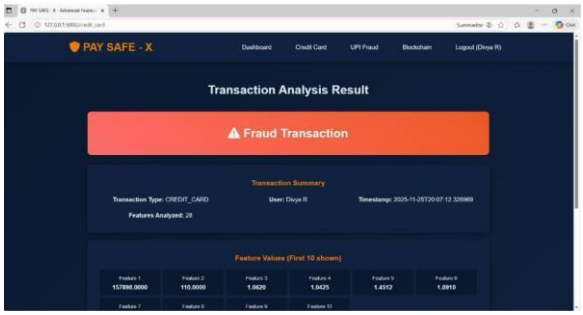
- The hybrid approach of Random Forest, XGBoost, and LSTM provides superior performance compared to single-model systems.
- The framework effectively detects both common and previously unseen fraud patterns, making it highly adaptable to the evolving nature of financial threats.
- The model's prediction speed of <15 milliseconds ensure seamless integration into banking workflows, payment gateways, and mobile financial applications.

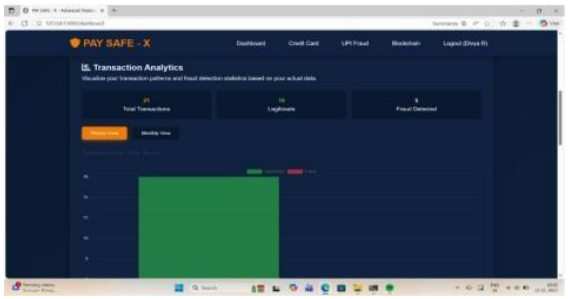
Furthermore, the deployment architecture using Flask/FastAPI and Docker ensures that the framework can be easily integrated into existing infrastructures with minimal modifications. Overall, this project validates the potential of AI-based fraud detection systems in delivering fast, accurate, scalable, and secure solutions, marking a significant step forward in fraud prevention and financial risk management

The proposed PAYSAFE-X fraud detection framework demonstrates strong performance in accurately identifying fraudulent transactions across integrated BFSI datasets. The hybrid AI approach, combining Random Forest, XG Boost, and LSTM models, achieves high precision and recall, effectively reducing false positives while maintaining robust fraud detection capability. The ensemble decision mechanism enhances model reliability and improves detection of complex and previously unseen fraud patterns. Experimental evaluation using standard metrics such as precision, recall, F1-score, and ROC-AUC confirms the superiority of the proposed system over traditional rulebased and single-model approaches. Additionally, the optimized real-time prediction pipeline processes each transaction in approximately 15 milliseconds, meeting near-real-time operational requirements. Overall, the results validate the system's effectiveness, scalability, and suitability for deployment in modern BFSI fraud prevention environments.

Contributes an equal proportion of samples to the dataset. This balanced distribution is important for Cryptographic algorithm detection because it prevents the model from becoming biased toward any Particular algorithm.







By training on an evenly distributed dataset, the classifier is able to fairly learn Features from both legacy algorithms (such as MD5 and SHA1) and modern cryptographic schemes (such as bcrypt and Argon2). This balance ensures consistent detection performance across all algorithm Types.

This project successfully developed a **smart AI-driven fraud detection framework** for the BFSI sector to address the growing challenges of financial fraud in digital transactions. By integrating **ensemble machine learning models (Random Forest and XGBoost)** with a **deep learning LSTM model**, the system effectively detects both static transaction anomalies and sequential fraud patterns.

The use of **multiple real-world datasets**, along with advanced **data preprocessing and feature engineering techniques**, enhanced the robustness and generalization capability of the proposed framework. Performance evaluation using metrics such as **precision, recall, F1-score, and ROC-**

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 01 , January - 2026

AUC demonstrates that the hybrid approach achieves high detection accuracy while significantly reducing false positives. Moreover, the system is optimized for **near-real-time transaction processing**, enabling rapid fraud prediction and proactive intervention with minimal computational overhead. The proposed framework is scalable, reliable, and suitable for deployment in realworld BFSI environments.

Overall, this project highlights the effectiveness of **hybrid AI models** in modern fraud detection systems and provides a strong foundation for future advancements in real-time, intelligent, and secure financial transaction monitoring.

V. FUTURE SCOPE

The Smart AI Framework for BFSI Fraud Prediction offers strong foundational capabilities for detecting financial fraud, but there are several avenues where the system can be further enhanced. Financial crime is continuously evolving, and advanced technologies can make fraud detection even more adaptive, reliable, and secure. The following future enhancements can significantly strengthen the framework:

1. Blockchain Integration for Secure Data Logging

The integration of blockchain technology can be employed to securely record transaction logs, fraud detection alerts, and machine learning model predictions in a tamper-proof and immutable distributed ledger. By leveraging the decentralized and cryptographic properties of blockchain, the integrity and authenticity of sensitive transactional data can be preserved. This approach enhances system transparency and auditability by enabling verifiable and traceable records of all transactions and detection events. Additionally, blockchain-based logging prevents unauthorized data manipulation and improves trust among financial institutions and regulatory authorities. Such an immutable logging mechanism also strengthens regulatory compliance by ensuring adherence to data security and audit requirements. Blockchain-enabled secure logging is particularly beneficial for high-risk transactions, dispute resolution, and forensic investigations, where data integrity and non-repudiation are critical.

2. Real-Time Dashboards for Monitoring

The development of real-time monitoring dashboards using advanced data visualization tools such as Power BI, Grafana, or Tableau enables effective supervision of transactional activities and fraud detection outcomes. These dashboards provide live transaction monitoring, visual representation of fraud alerts, and real-time insights into machine learning model performance. Additionally, user behavior analytics, risk scoring metrics, and fraud trend analysis are displayed to support informed decision-making. By presenting complex data in an intuitive and interactive format, the dashboards allow fraud analysts and financial administrators to promptly identify suspicious activities and take immediate corrective actions, thereby improving response time and enhancing overall system effectiveness.

3. Expansion to Insurance and Loan Fraud Detection

While the current system primarily focuses on transaction-level fraud detection, the proposed artificial intelligence framework can be extended to address a broader range of financial fraud scenarios. By incorporating additional domain-specific datasets, the model can be adapted to detect insurance claim fraud, loan application fraud, identity theft patterns, and account takeover behaviors. The inclusion of customer profile data, claim histories, credit information, and behavioral attributes enables more comprehensive risk assessment across multiple financial services. This expansion allows the framework to support various segments of the Banking, Financial Services, and
Insurance (BFSI) sector, enhancing fraud prevention capabilities and improving overall security and operational efficiency.

4. Mobile Application Integration

A dedicated mobile application can be developed to extend the fraud detection system's accessibility and responsiveness. The mobile platform can provide instant fraud alerts, administrative notifications, and real-time transaction monitoring capabilities. It also enables authorized personnel to review suspicious transactions and initiate customer verification and approval mechanisms directly through the application. This mobile integration allows banking staff and administrators to manage fraud incidents efficiently while on the move, thereby improving response time and operational flexibility.

5. Reinforcement Learning for Adaptive Fraud Detection

Reinforcement Learning (RL) techniques can be incorporated to enhance the adaptability and intelligence of the fraud detection system. Unlike static models, RL-based approaches enable continuous learning from new transaction patterns and evolving attacker strategies. By dynamically updating detection policies based on feedback and outcomes, the system can automatically adapt to emerging fraud behaviors, reduce dependence on manual rule updates, and improve self-learning capabilities. This adaptive learning mechanism enhances long-term detection accuracy, system robustness, and resilience against sophisticated and previously unseen fraud attacks.

REFERENCES

[1] Mahbuba Yesmin Turaba et al. "Fraud Detection During Financial Transactions Using Machine Learning and Deep Learning Techniques" in IEEE Oct 2022".

[2] Seyedeh Khadijeh Hashemi et al., "Fraud Detection in Banking Data by Machine Learning Techniques", in IEEE Dec2022.

[3] Mr. Sunil S Mhamane and Mr. L.M.RJ Lobo "Internet Banking Fraud Detection Using HMM", in IEEE July 2012.

[4] Pradheepan Raghavan and Neamat El Gayar "Fraud Detection using Machine Learning and Deep Learning", in IEEE Feb 2020.

[5] G.Jaculine Priya and Dr.S.Saradha "Fraud Detection and Prevention Using Machine Learning Algorithms: A Review", in IEEE 2021