iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.83561

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

A Comprehensive Review of Hybrid Deep Learning Models for Real-Time UPI Fraud Detection and Digital Payment Security

Ashish Malik, Jitender Kumar
MTech. Scholar, Assistant Professor, Computer science & Engineering GITAM Kablana Jhajjar

Abstract: ***The emergence of the Unified Payments Interface (UPI) has transformed the digital payment ecosystem by enabling seamless, instant, and interoperable financial transactions across India. Its widespread acceptance has accelerated the shift toward cashless payments and increased the availability of digital financial services for millions of users. However, the rapid growth in transaction volume and user adoption has also created new opportunities for cybercriminals to exploit vulnerabilities within the digital payment infrastructure.Financial fraud associated with UPI platforms has become increasingly sophisticated, involving techniques such as phishing campaigns, fraudulent QR codes, identity impersonation, account hijacking, social engineering attacks, and the misuse of mule accounts. These evolving threats generate complex transaction patterns that are often difficult to detect using conventional rule-based security mechanisms. As fraud strategies continue to change, static detection systems struggle to provide accurate and timely identification of suspicious activities.Recent progress in Artificial Intelligence, Machine Learning, and Deep Learning technologies has significantly enhanced the capability of fraud detection systems. One of these developments has caught a lot of interest from researchers is hybrid deep learning methods that are able to integrate the benefits of several computational models. Several techniques can be combined in a unified approach for enhancing fraud detection, such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Autoencoders, Graph Neural Networks (GNNs), Explainable Artificial Intelligence (XAI), and Federated Learning. These architectures enable real-time analysis, adaptive learning, privacy protection, and efficient management of large-scale transactional data.***

This review is based on the recent research and studies regarding the detection of fraudulent activities in UPI-based payment environment using hybrid deep learning techniques. It offers detailed evaluations of the current models, their strengths and weaknesses, explores current issues and challenges, and suggests areas of future work. These results suggest that hybrid deep learning architectures are promising to improve the security of digital payment systems through better detection accuracy, fewer false alarms, safeguarding sensitive user data, and greater transparency of automated decision-making. Thus, these wise frameworks are a valuable basis for developing safe, reliable, and trustworthy digital financial ecosystems.

Keywords: UPI Fraud Detection, Digital Payment Security, Hybrid Deep Learning, CNN, LSTM, Autoencoder, Graph Neural Networks, Explainable AI, Federated Learning, Financial Cybersecurity.

I. INTRODUCTION

Digital technologies have revolutionized the finance industry and completely reshaped the way financial transactions happen. The Unified Payments Interface (UPI) has become a crucial part of this financial revolution in India, ensuring instant and seamless digital transactions. The National Payments Corporation of India (NPCI), an initiative by the Reserve Bank of India to promote digital payments, created UPI.The National Payments Corporation of India (NPCI) is an initiative by the Reserve Bank of India (RBI) that promotes digital payments, and it developed UPI. It is easy to use, interoperable with financial institutions, always available and has low transaction costs, hence its fast adoption in the country.

UPI's rising popularity has helped propel growth of the digital economy and to reach more people with formal financial services. UPI-based applications are widely adopted by both consumers and businesses to perform various transactions like bill payments, money transfer, subscription payments, online shopping and retail transactions. With the growth of digital transactions, payment platforms are now a part of daily financial activities. However, these systems have also increased the attack surface for the cybercriminals and in turn led to serious security concerns.

Digital payments have been a target of the bad guys for years and years, and the threat environment has changed significantly over the years.

©IJRASET: All Rights are Reserved

Fraudsters use ever-evolving techniques, including misguided phishing, spoofed apps, fake QR codes, SIM swapping, credential theft, account access fraud, social engineering and money laundering via mule accounts. Such malicious actions can lead to significant financial loss and erode consumer confidence in e-payment services. Furthermore, cybercrime is an evolving threat and fraud detection is difficult for current security systems.

Stale fraud signatures, static thresholds and predetermined rules are typical approaches to conventional fraud prevention. These methods can help identify previous attack patterns but are not always able to catch new and/or more complicated attack patterns. Furthermore, due to the large volume and real-time transactions of UPI, the analytical system needs to handle a huge amount of heterogeneous data and process it with minimal delay. This has spurred financial institutions to utilize intelligent, data-driven approaches that leverage Artificial Intelligence (AI) and Machine Learning (ML) for improved fraud detection.

One of the most specialized forms of AI, Deep Learning (DL), has proven to be very capable of deriving meaningful values from high-dimensional and complex data. Deep learning algorithms can be used to identify user behavior patterns, device features, and context, and uncover hidden relationships in the transaction records, which allows them to effectively separate legitimate transactions from fraudulent ones. CNNs, LSTMs, Autoencoders and Graph Neural Networks (GNNs) have all proven successful in financial fraud detection applications.

To further improve detection performance, recent studies have explored hybrid deep learning frameworks that combine multiple algorithms within a unified architecture. These integrated models leverage complementary strengths such as feature learning, sequential pattern recognition, anomaly detection, and relationship analysis to enhance overall effectiveness. Furthermore, the adoption of Explainable Artificial Intelligence (XAI) provides greater transparency in decision-making, while Federated Learning supports privacy-preserving model training across distributed environments. Together, these advancements offer a robust and scalable solution for safeguarding digital payment systems. This review provides a comprehensive examination of hybrid deep learning techniques for UPI fraud detection, discussing their underlying methodologies, practical applications, advantages, challenges, and future research directions aimed at strengthening the security of next-generation digital financial ecosystems.

II. RESEARCH OBJECTIVES

The primary objectives of this review study are as follows:

1) To examine and evaluate the existing hybrid deep learning methodologies employed for detecting fraudulent activities in UPI-based digital payment systems.
2) To investigate the efficiency and effectiveness of real-time fraud detection approaches in enhancing the security and reliability of digital financial transactions.
3) To assess and compare different hybrid deep learning architectures in terms of detection accuracy, computational performance, scalability, robustness, and security capabilities.
4) To explore current challenges, identify research limitations, and highlight potential future directions for the development of advanced intelligent fraud detection frameworks in digital payment ecosystems.

III. UPI FRAUD LANDSCAPE

The Unified Payments Interface (UPI) has been a game-changer in making digital financial transactions more convenient and accessible. The rise of UPI payment systems, though, has also paved the way for cybercriminals to take advantage of vulnerabilities in the system. Fraud on the digital payment platforms has evolved and is now a significant threat to financial institutions, payment service providers and end users. To effectively design detection and prevention mechanisms, it is critical to grasp the different types of UPI fraud.

A. Common Types of UPI Fraud

1) Phishing Attacks

Phishing is one of the most common types of online payment fraud. It's an attack where hackers trick users into giving out personal information like login credentials, banking information, UPI PINs or OTPs on fake websites, emails, SMS or phone calls pretending to be authentic.

2) QR Code Fraud

QR code fraud involves the use of manipulated or counterfeit QR codes to divert payments to unauthorized accounts. Fraudsters often persuade victims to scan malicious QR codes under false pretenses, resulting in unauthorized fund transfers and financial losses.

3) Account Takeover Attacks

An Account Takeover happens when a hacker steals the login information of a user's UPI account from a data breach, malware, phishing or credential theft. Once the access is gained, fraudulent transactions can be carried out without the knowledge of the account holder.

4) SIM Swap Fraud

In SIM swap attacks, fraudsters obtain control of a victim's mobile number by acquiring a duplicate SIM card from a telecom service provider. This enables attackers to intercept OTPs and authentication messages, thereby bypassing security mechanisms and gaining unauthorized access to financial accounts.

5) Mule Account Fraud

Mule accounts are bank accounts used to receive, transfer, or conceal illegally obtained funds. Cybercriminals frequently utilize intermediary accounts to obscure the origin of fraudulent transactions, making financial crime investigations more challenging. The detection of mule accounts has become a critical area of research in modern fraud analytics.

6) Fake UPI Applications

Fraudsters often develop counterfeit mobile applications that imitate legitimate UPI payment platforms. These malicious applications are designed to collect confidential user information, including banking credentials, authentication details, and transaction data, which can subsequently be exploited for fraudulent activities.

The increasing complexity of digital payment fraud highlights the need for intelligent and adaptive security solutions. Recent research emphasizes the importance of behavioral analytics, transaction pattern analysis, and mule account identification as key components of advanced fraud detection frameworks. Consequently, artificial intelligence and hybrid deep learning models are being increasingly adopted to detect suspicious activities, identify emerging fraud patterns, and strengthen the security of UPI-based payment ecosystems.

IV. DEVELOPMENT OF FRAUD DETECTION APPROACHES

The rapid growth of digital financial services and online payment platforms has led to a significant increase in fraudulent activities, compelling researchers and financial institutions to develop more advanced fraud detection mechanisms. As transaction networks become larger and more complex, traditional monitoring methods have gradually evolved into intelligent systems capable of analyzing vast amounts of data and identifying suspicious behavior with greater precision. The progression of fraud detection techniques can be broadly categorized into rule-based systems, machine learning approaches, and deep learning-based solutions.

A. Traditional Rule-Based Detection Methods

Rule-based fraud detection techniques were among the first solutions implemented by banks and financial service providers to combat fraudulent transactions. These systems operate using a collection of predefined conditions established by security experts. Transactions are evaluated against these rules, and any activity that exceeds specified limits or exhibits unusual characteristics is marked for review.

The popularity of rule-based systems stems from their straightforward implementation and transparent decision-making process. Since the criteria for detecting fraud are explicitly defined, security teams can easily understand, modify, and maintain the system. Such methods have been effective in identifying known fraud patterns and enforcing organizational security policies.

However, the effectiveness of rule-based systems decreases in rapidly changing digital environments. Fraudsters continually develop new attack strategies that may not match existing rules. As a result, these systems frequently generate excessive false alarms and fail to detect previously unknown fraud techniques. Their dependence on manually configured rules also limits their flexibility and scalability, making them less effective in handling high-volume digital payment ecosystems.

B. Machine Learning-Oriented Fraud Detection

The limitations of static rule-based approaches encouraged the adoption of machine learning techniques for fraud identification. Unlike conventional methods, machine learning models learn behavioral patterns directly from historical transaction data and use this knowledge to distinguish legitimate activities from fraudulent ones. Popular algorithms used in this domain include Decision Trees, Random Forests, Support Vector Machines (SVM), Logistic Regression, and Extreme Gradient Boosting (XGBoost).

Machine learning systems offer greater adaptability because they can uncover complex relationships hidden within large datasets. By analyzing user behavior and transaction characteristics, these models can detect suspicious activities that may not be represented by predefined rules.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Their ability to improve through continuous exposure to new data contributes to higher detection effectiveness and better responsiveness to changing fraud patterns.

Despite these advantages, machine learning models often require extensive feature engineering. Domain specialists must identify and construct meaningful features that accurately represent transaction behavior. The success of the model is therefore closely linked to the quality of these engineered features. Furthermore, many traditional machine learning algorithms have difficulty modeling sequential transaction patterns and long-term behavioral dependencies, which are important for detecting sophisticated financial fraud.

C. Deep Learning Approaches for Fraud Detection

Advances in artificial intelligence have accelerated the adoption of deep learning techniques for fraud prevention and risk management. Deep learning models can automatically learn complex feature representations from raw data, reducing the reliance on manual feature extraction. Common architectures employed in fraud detection include Artificial Neural Networks (ANNs), Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), Long Short-Term Memory (LSTM) networks, Gated Recurrent Units (GRUs), and Autoencoders.

These models are particularly effective when dealing with large-scale and high-dimensional financial datasets. Their capability to learn hidden structures and behavioral patterns enables them to identify fraudulent transactions with a high degree of accuracy. Deep learning techniques can simultaneously capture spatial relationships among transaction attributes and temporal dependencies across transaction sequences, making them highly suitable for real-time fraud monitoring systems.

Nevertheless, deep learning models are associated with several challenges. Their complex internal structures often reduce transparency, making the reasoning behind predictions difficult to interpret. Additionally, training deep neural networks requires substantial computational resources, including powerful processors, large memory capacity, and significant training time. To address these concerns, recent research has increasingly focused on hybrid deep learning frameworks that integrate multiple learning techniques. Such models aim to achieve improved detection performance while enhancing interpretability, efficiency, and scalability in modern digital payment environments.

V. HYBRID DEEP LEARNING MODELS FOR UPI FRAUD DETECTION

The increasing complexity of fraudulent activities in digital payment ecosystems has necessitated the development of advanced fraud detection techniques capable of handling diverse transaction patterns and evolving attack strategies. While individual machine learning and deep learning models have demonstrated significant potential, their standalone implementation often faces limitations in terms of accuracy, adaptability, and interpretability. To address these challenges, researchers have increasingly adopted hybrid deep learning frameworks that integrate multiple algorithms within a unified architecture. By combining the strengths of different models, hybrid approaches enhance fraud detection performance, improve anomaly identification, and support real-time decision-making in UPI-based payment systems.

A. CNN-LSTM Hybrid Model

The CNN-LSTM hybrid architecture is one of the most widely adopted approaches for financial fraud detection. This model combines the feature extraction capabilities of Convolutional Neural Networks (CNNs) with the sequential learning strengths of Long Short-Term Memory (LSTM) networks.

In this framework, the CNN component automatically extracts meaningful features from transaction data and identifies localized behavioral patterns that may indicate suspicious activities. These extracted features are subsequently processed by the LSTM network, which analyzes temporal dependencies and transaction sequences over time. The integration of spatial and temporal learning enables the model to capture complex fraud behaviors that may not be detectable through individual algorithms.

As a result, CNN-LSTM models typically achieve higher detection accuracy, facilitate real-time transaction monitoring, and significantly reduce false-positive alerts. These characteristics make them particularly suitable for high-volume digital payment environments such as UPI.

B. Autoencoder-LSTM Hybrid Model

The Autoencoder-LSTM model combines unsupervised anomaly detection with sequence learning to identify fraudulent transactions. Autoencoders are trained to learn the normal behavioral patterns of legitimate transactions by reconstructing input data with minimal error. Transactions that produce unusually high reconstruction errors are considered potential anomalies.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The LSTM component further enhances the detection process by examining transaction sequences and temporal relationships between activities. This combination allows the model to identify subtle deviations from normal behavior while simultaneously considering transaction history and user activity patterns.

The Autoencoder-LSTM framework is particularly effective for detecting previously unseen fraud scenarios and zero-day attacks, where labeled fraud examples may not be available during training. Consequently, it provides a robust solution for adaptive fraud detection in dynamic digital payment ecosystems.

C. GNN-LSTM Hybrid Model

Graph Neural Network (GNN) and LSTM integration represents an advanced approach for modeling complex relationships within financial transaction networks. GNNs are designed to analyze interconnected entities such as users, bank accounts, devices, merchants, and transaction channels. By representing these entities as nodes and their interactions as edges, the model can uncover hidden relationships associated with fraudulent activities.

The LSTM component complements the graph structure by analyzing transaction timelines and capturing temporal behavioral changes. Together, these models provide a comprehensive understanding of both relational and sequential transaction patterns.

This hybrid architecture is particularly valuable for identifying mule accounts, uncovering organized fraud networks, and supporting anti-money laundering (AML) initiatives. Its ability to detect coordinated fraudulent activities makes it highly effective in large-scale financial systems.

D. Federated Deep Learning Framework

The growing concern for data privacy and regulatory compliance has led to the adoption of Federated Deep Learning frameworks in fraud detection applications. Unlike traditional centralized learning approaches, federated learning enables multiple institutions to collaboratively train machine learning models without sharing raw customer data.

In this framework, model parameters are exchanged between participating organizations while sensitive transaction information remains within local environments. This decentralized training mechanism enhances privacy protection and reduces the risk of data breaches.

Federated deep learning offers several advantages, including improved compliance with data protection regulations, reduced privacy-related concerns, and the ability to leverage collective intelligence across multiple banks and financial institutions. Such collaborative learning approaches can significantly strengthen fraud detection capabilities while preserving customer confidentiality.

E. Explainable Hybrid AI Models

Although deep learning models provide exceptional predictive performance, their decision-making processes are often difficult to interpret. To address this limitation, researchers have incorporated Explainable Artificial Intelligence (XAI) techniques into hybrid fraud detection frameworks.

Popular explainability methods include SHapley Additive exPlanations (SHAP), Local Interpretable Model-Agnostic Explanations (LIME), and attention-based mechanisms. These techniques provide insights into the factors influencing fraud predictions and enable stakeholders to understand the reasoning behind model decisions.

The integration of explainability enhances transparency, facilitates regulatory compliance, and increases trust among financial institutions and customers. Explainable hybrid AI models support informed decision-making while maintaining the high detection accuracy required for modern digital payment security systems.

Overall, hybrid deep learning architectures represent a significant advancement in UPI fraud detection by combining feature extraction, temporal analysis, anomaly detection, relationship modeling, privacy preservation, and explainability within a unified framework. These capabilities position hybrid models as a promising solution for securing next-generation digital payment ecosystems.

VI. COMPARATIVE STUDY OF EXISTING MODELS

Various machine learning and deep learning techniques have been applied to detect fraudulent transactions in UPI-based payment systems. Traditional models such as Random Forest offer fast processing and easy interpretation but have limited ability to analyze sequential transaction behavior. Deep learning models, including CNN and LSTM, provide improved performance by learning complex patterns from transaction data. CNN is effective for feature extraction, whereas LSTM excels in capturing temporal dependencies.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Autoencoders are widely used for anomaly detection by identifying deviations from normal transaction patterns. However, they may involve higher computational complexity. Hybrid architectures such as CNN-LSTM and GNN-LSTM combine the advantages of multiple models, resulting in better fraud detection accuracy and enhanced capability to identify complex fraudulent activities. Federated Deep Learning improves privacy by enabling collaborative learning without sharing sensitive customer data, while Explainable AI (XAI)-based hybrid models enhance transparency and trust in decision-making.

Table 1: Comparison of Fraud Detection Models

Model	Strengths	Limitations	Accuracy
Random Forest	Fast and interpretable	Weak sequential analysis	85–92%
CNN	Effective feature extraction	Limited temporal learning	90–95%
LSTM	Strong sequence modeling	High computational cost	92–97%
Autoencoder	Efficient anomaly detection	Reconstruction complexity	90–96%
CNN-LSTM	Combines spatial and temporal learning	Complex training process	95–98%
GNN-LSTM	Detects fraud networks and relationship	Graph construction overhead	94–98%
Federated DL	Preserves data privacy	Communication overhead	93–97%
Hybrid XAI Model	Improves explainability and trust	Additional processing requirement	94–98%

The comparison shows that hybrid deep learning models generally achieve higher accuracy and better adaptability than standalone approaches, making them highly suitable for real-time UPI fraud detection and digital payment security.

VII. RESEARCH GAPS

Despite significant advancements in artificial intelligence and deep learning-based fraud detection systems, several challenges remain unresolved in the field of UPI fraud detection. Existing studies highlight a number of research gaps that limit the effectiveness, scalability, and practical deployment of current solutions.

1) Limited Availability of Public Datasets: The lack of publicly accessible and standardized UPI fraud datasets restricts the development, training, and benchmarking of advanced fraud detection models.
2) Class Imbalance Issues: Fraudulent transactions represent only a small fraction of total transactions, creating highly imbalanced datasets that can negatively affect model performance and detection accuracy.
3) Insufficient Model Interpretability: Many deep learning models operate as black-box systems, making it difficult to understand and justify their predictions in real-world financial applications.
4) High Computational Complexity: Advanced deep learning architectures often require substantial processing power, memory, and training time, which can hinder real-time implementation.
5) Data Privacy and Security Concerns: Centralized learning approaches may expose sensitive financial information, raising concerns regarding data protection, privacy, and regulatory compliance.
6) Limited Information Sharing Across Institutions: The absence of effective mechanisms for collaborative fraud intelligence sharing among banks and payment service providers reduces the ability to identify large-scale fraud networks.
7) Detection of Emerging Fraud Techniques: Existing models often struggle to recognize newly evolving fraud strategies and previously unseen attack patterns, affecting their adaptability in dynamic payment environments.

Addressing these research gaps is essential for developing more accurate, explainable, privacy-preserving, and scalable fraud detection frameworks for next-generation UPI payment systems.

VIII. PROPOSED HYBRID FRAMEWORK

To address the limitations of existing fraud detection approaches, a comprehensive hybrid deep learning framework is proposed for real-time UPI fraud detection and digital payment security. The framework integrates advanced deep learning techniques, explainable artificial intelligence, and privacy-preserving mechanisms to enhance fraud detection accuracy while ensuring transparency and data security.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The proposed architecture consists of six major layers: Data Collection Layer, Preprocessing Layer, Hybrid Deep Learning Layer, Explainability Layer, Privacy Layer, and Decision Engine. These layers work collaboratively to analyze transactional, behavioral, and contextual information for identifying fraudulent activities in real time.

A. Data Collection Layer

This layer gathers information from multiple sources to create a comprehensive transaction profile. The collected data include:

- Transaction records and payment history
- Device fingerprint information
- User behavioral patterns and activity logs
- Network and communication metadata

The integration of diverse data sources enables the framework to capture behavioral, transactional, and environmental characteristics associated with fraudulent activities.

B. Preprocessing Layer

The collected data undergo preprocessing to improve data quality and model performance. Key operations include:

- Data cleaning and normalization
- Feature extraction and feature engineering
- Handling missing values and outliers
- Data balancing using SMOTE (Synthetic Minority Oversampling Technique)

This layer ensures that the data are suitable for effective model training and analysis.

C. Hybrid Deep Learning Layer

The core fraud detection module combines multiple deep learning models to leverage their complementary strengths:

- CNN (Convolutional Neural Network): Extracts significant transaction features and behavioral patterns.
- LSTM (Long Short-Term Memory): Captures temporal dependencies and sequential transaction behavior.
- Autoencoder: Identifies anomalies by learning normal transaction patterns.
- GNN (Graph Neural Network): Models relationships among users, devices, accounts, and transactions.

The integration of these models enables accurate detection of both known and previously unseen fraud patterns.

D. Explainability Layer

To improve transparency and interpretability, the framework incorporates Explainable AI techniques such as:

- SHAP (SHapley Additive Explanations)
- Attention-based mechanisms

These techniques provide meaningful explanations for fraud predictions and assist analysts in understanding model decisions.

E. Privacy Preservation Layer

To protect sensitive financial information, the framework employs privacy-preserving technologies, including:

- Federated Learning for decentralized model training
- Differential Privacy for safeguarding user data

This layer ensures compliance with privacy regulations while enabling collaborative fraud intelligence.

F. Decision Engine

The final layer evaluates model outputs and generates actionable insights through:

- Fraud score computation
- Transaction risk assessment
- Real-time alert generation and management

Based on the generated risk level, transactions can be approved, flagged for review, or blocked automatically.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Proposed Framework Diagram

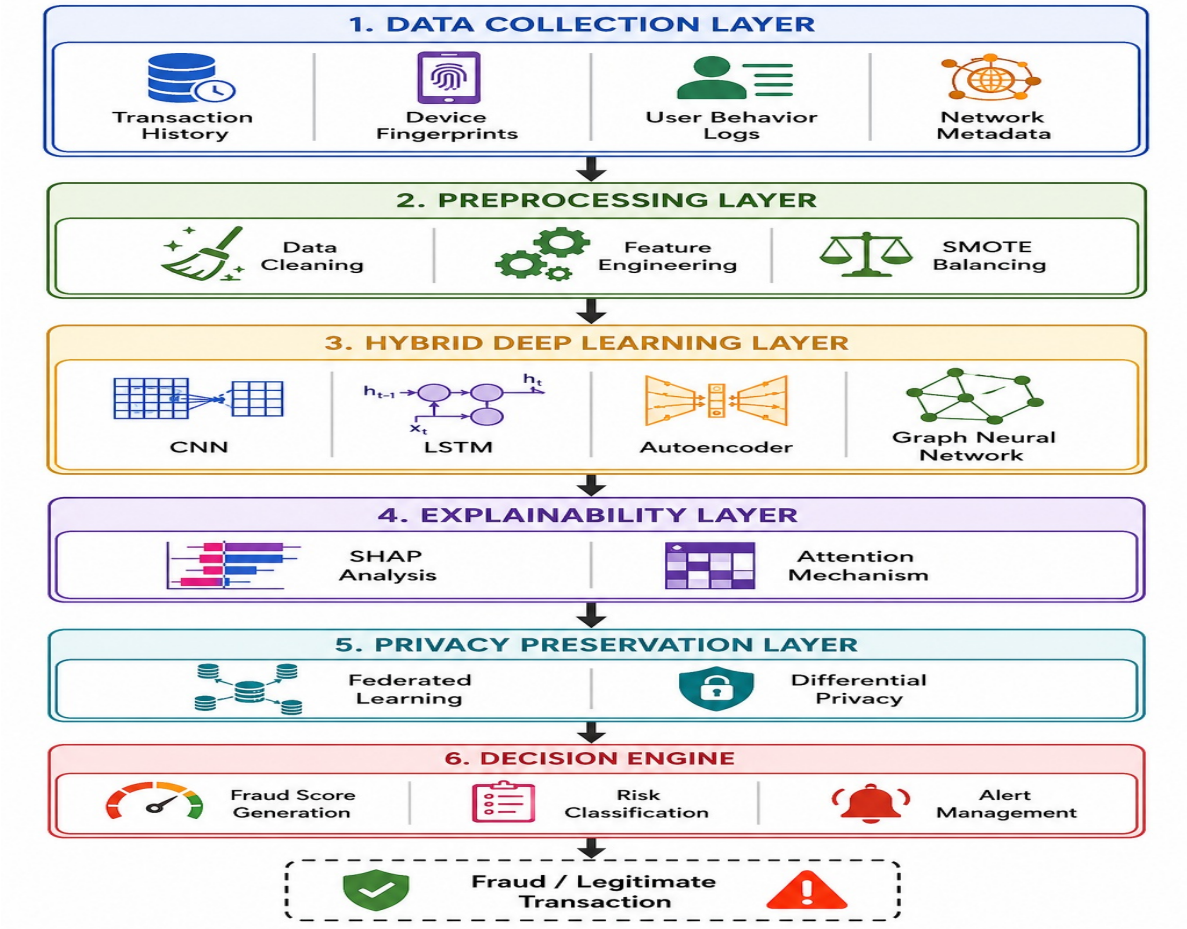


Figure 1: Proposed Privacy-Preserving Hybrid Deep Learning Framework for Real-Time UPI Fraud Detection and Digital Payment Security

The proposed framework combines behavioral analysis, temporal learning, anomaly detection, relationship modeling, explainability, and privacy preservation within a unified architecture. By integrating these components, the framework provides a scalable, accurate, and secure solution for next-generation UPI fraud detection and digital payment protection.

IX. APPLICATIONS

The proposed hybrid deep learning framework can be applied across various domains of digital payment security to improve fraud prevention, transaction monitoring, and financial risk management. Its major applications are summarized in Table 2.

Table 2: Applications of the Proposed Hybrid Fraud Detection Framework

Application Area	Description
Real-Time UPI Fraud Detection	Identifies and prevents fraudulent transactions during payment processing.
Digital Wallet Security	Protects digital wallets from unauthorized access and suspicious activities.
Mobile Banking Protection	Enhances the security of mobile banking transactions through continuous monitoring
Anti-Money Laundering (AML)	Detects suspicious fund transfers and financial laundering activities.
Account Takeover Prevention	Recognizes abnormal user behavior and prevents unauthorized account access.
Transaction Risk Assessment	Evaluates transaction risk levels and generates fraud risk scores.
Financial Crime Investigation	Assists investigators in identifying fraud patterns and criminal networks.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

Application Area	Description
Intelligent Payment Monitoring	Enables continuous monitoring of payment activities to detect emerging threats.

The versatility of the proposed framework makes it suitable for banking institutions, fintech companies, payment gateways, and digital financial service providers seeking to strengthen security and reduce fraud-related losses.

X. FUTURE SCOPE

The field of UPI fraud detection continues to evolve, creating opportunities for the development of more intelligent, secure, and adaptive fraud prevention systems. Future research should focus on integrating advanced technologies to enhance detection accuracy, privacy protection, and real-time decision-making capabilities.

Key future research directions include:

1) Federated Explainable Deep Learning to combine privacy preservation with transparent decision-making.
2) Blockchain-Based Fraud Detection for secure and tamper-resistant transaction monitoring.
3) Graph Transformer Networks (GTNs) to improve the analysis of complex transaction relationships and fraud networks.
4) Multimodal Fraud Analytics by integrating transaction, behavioral, device, and network data.
5) Quantum-Resistant Security Solutions to safeguard payment systems against future quantum computing threats.
6) AI-Driven Scam and Phishing Detection for identifying fraudulent communications and social engineering attacks.
7) LLM-Assisted Fraud Investigation to support automated fraud analysis and decision support systems.
8) Deepfake Fraud Prevention Mechanisms to counter emerging identity spoofing and synthetic media attacks.
9) Self-Adaptive Learning Frameworks capable of continuously learning and responding to new fraud patterns.
10) Edge AI-Based Fraud Detection for low-latency analysis and real-time transaction monitoring.

The integration of Large Language Models (LLMs), Federated Learning, Graph Neural Networks (GNNs), and privacy-preserving artificial intelligence is expected to play a significant role in the development of next-generation digital payment security solutions. These advancements will contribute to building more robust, scalable, explainable, and resilient fraud detection systems for future UPI ecosystems.

XI. CONCLUSION

The rapid expansion of Unified Payments Interface (UPI) transactions has significantly increased the demand for intelligent and robust fraud detection mechanisms. Traditional rule-based security systems are becoming inadequate for addressing the growing complexity and constantly evolving nature of financial fraud. As cybercriminals employ increasingly sophisticated attack strategies, there is a critical need for adaptive, data-driven approaches that can identify fraudulent activities accurately and in real time.

This review explores the potential of hybrid deep learning frameworks in enhancing the security of digital payment systems. By combining advanced technologies such as Convolutional Neural Networks (CNNs), Long Short-Term Memory (LSTM) networks, Autoencoders, Graph Neural Networks (GNNs), Explainable Artificial Intelligence (XAI), and Federated Learning, these models offer a comprehensive and effective solution for fraud detection. The integration of multiple deep learning techniques improves detection performance, strengthens anomaly identification capabilities, enables real-time transaction monitoring, and enhances the protection of sensitive financial data.

In addition, the incorporation of explainability and privacy-preserving methodologies addresses key concerns related to transparency, regulatory compliance, and user confidence. These features are essential for building trustworthy fraud detection systems that can operate effectively in modern financial environments. The study further highlights the necessity of scalable and adaptive architectures capable of responding to emerging fraud patterns and evolving cybersecurity threats.

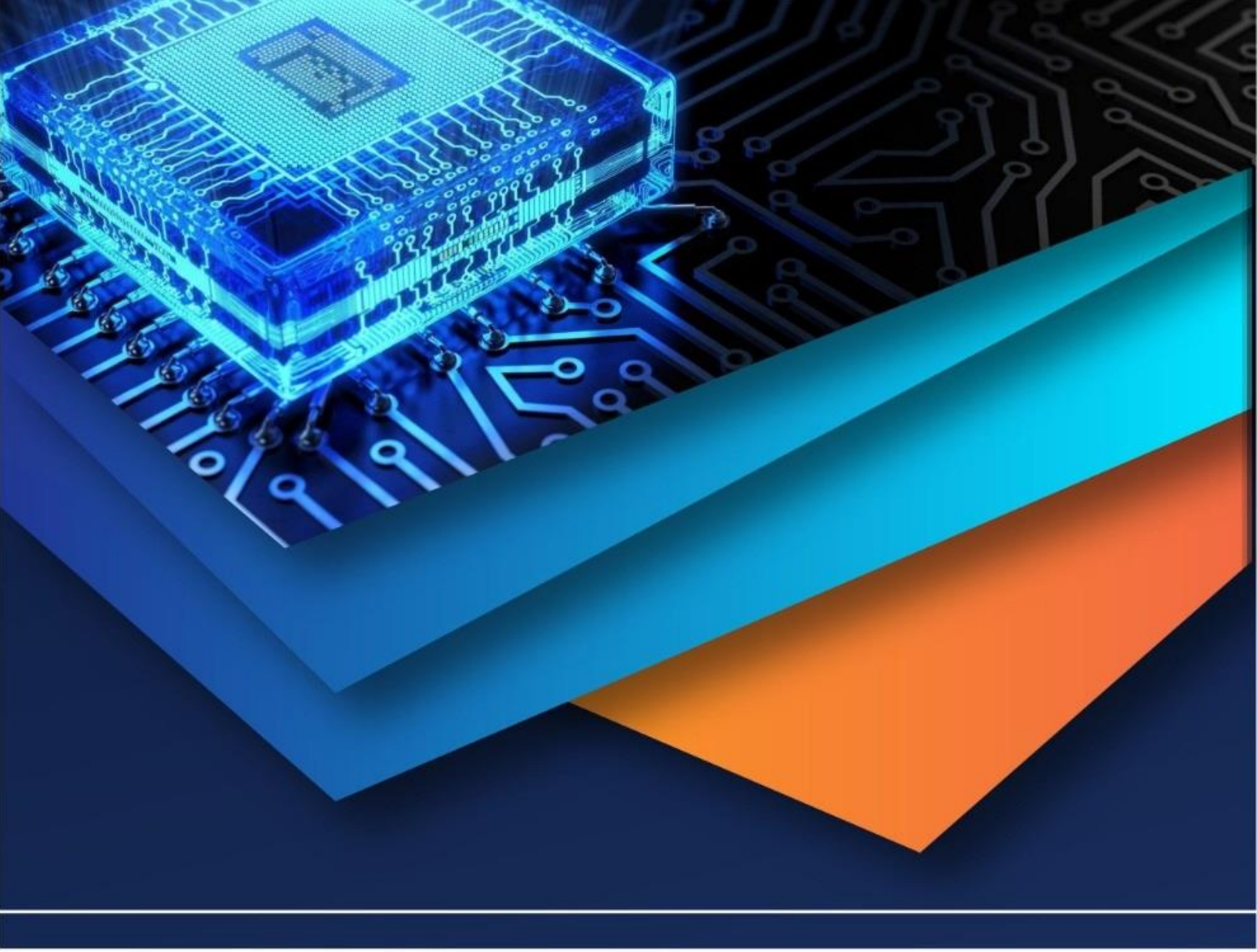
Overall, privacy-preserving and explainable hybrid deep learning frameworks provide a strong foundation for securing next-generation digital payment ecosystems. Their ability to analyze transactional behavior from temporal, behavioral, and relational perspectives makes them highly effective in detecting fraudulent activities within UPI networks. Continued advancements and research in this domain will be instrumental in improving the security, reliability, and trustworthiness of digital financial services in the future.

REFERENCES

[1] N. B. Chakka and S. S. Saheb, “Mobile Payment Fraud Detection in UPI Through Machine Learning Techniques: A Systematic Review,” International Journal of Research and Analytical Reviews, vol. 12, no. 2, pp. 115–128, 2025.

[2] J. Kumar and N. Rani, "Optimized Machine Learning and Deep Learning Approaches for Effective Detection of Fraud in UPI Transactions," International Journal of Scientific Advances and Technology, vol. 5, no. 3, pp. 45–58, 2025.
[3] T. Sekhar and G. V. 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, pp. 89–98, 2026.
[4] S. Sahu, A. Mishra, and R. Sharma, "Detection of Mule Accounts and Fraudsters in UPI Transactions Using Artificial Intelligence Techniques," IRE Journals, vol. 9, no. 1, pp. 112–121, 2026.
[5] L. Sen, "UPI Fraud Detection and Prevention: Emerging Trends and Challenges," SSRN Electronic Journal, pp. 1–15, 2026.
[6] Y. Qin, J. Yang, and Z. Wang, "Real-Time Fraud Detection in Enterprise Payment Ecosystems Using Deep Learning," Journal of Computational Engineering and Information Management, vol. 8, no. 2, pp. 45–60, 2026.
[7] M. Z. H. George, M. K. Alam, and M. T. Hasan, "Machine Learning for Fraud Detection in Digital Banking: A Systematic Literature Review," arXiv preprint arXiv:2510.05167, 2025.
[8] V. Jurgovsky, M. Granitzer, S. Ziegler, S. Calabretto, P. Portier, L. He-Guelton, and O. Caelen, "Sequence Classification for Credit Card Fraud Detection," Expert Systems with Applications, vol. 100, pp. 234–245, 2018.
[9] A. Roy, J. Sun, R. Mahoney, L. Alonzi, S. Adams, and P. Beling, "Deep Learning Detecting Fraud in Credit Card Transactions," in Proc. Systems and Information Engineering Design Symposium (SIEDS), 2018, pp. 129–134.
[10] B. Baesens, V. Van Vlasselaer, and W. Verbeke, Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques. Hoboken, NJ, USA: Wiley, 2015.
[11] D. Pumsirirat and L. Yan, "Credit Card Fraud Detection Using Deep Learning Based on Autoencoder and Restricted Boltzmann Machine," International Journal of Advanced Computer Science and Applications, vol. 9, no. 1, pp. 18–25, 2018.
[12] S. Fiore, F. De Santis, A. Perla, P. Zanetti, and F. Palmieri, "Using Generative Adversarial Networks for Improving Classification Effectiveness in Credit Card Fraud Detection," Information Sciences, vol. 479, pp. 448–455, 2019.
[13] T. N. Kipf and M. Welling, "Semi-Supervised Classification with Graph Convolutional Networks," in International Conference on Learning Representations (ICLR), 2017.
[14] P. Velickovic et al., "Graph Attention Networks," in International Conference on Learning Representations (ICLR), 2018.
[15] A. Vaswani et al., "Attention Is All You Need," in Advances in Neural Information Processing Systems, vol. 30, pp. 5998–6008, 2017.
[16] A. Dosovitskiy et al., "An Image is Worth 16×16 Words: Transformers for Image Recognition at Scale," in International Conference on Learning Representations (ICLR), 2021.
[17] H. B. McMahan et al., "Communication-Efficient Learning of Deep Networks from Decentralized Data," in Proc. 20th International Conference on Artificial Intelligence and Statistics (AISTATS), 2017, pp. 1273–1282.
[18] C. Dwork, "Differential Privacy," in International Colloquium on Automata, Languages and Programming, 2006, pp. 1–12.
[19] S. Lundberg and S. Lee, "A Unified Approach to Interpreting Model Predictions," in Advances in Neural Information Processing Systems, vol. 30, pp. 4765–4774, 2017.
[20] M. T. Ribeiro, S. Singh, and C. Guestrin, "Why Should I Trust You? Explaining the Predictions of Any Classifier," in Proc. ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016, pp. 1135–1144.
[21] R. Chalapathy and S. Chawla, "Deep Learning for Anomaly Detection: A Survey," arXiv preprint arXiv:1901.03407, 2019.
[22] N. Carlini et al., "The Role of Federated Learning in Privacy-Preserving Financial Analytics," IEEE Security & Privacy, vol. 20, no. 4, pp. 48–56, 2022.
[23] S. Wang, T. Tuor, T. Salonidis, K. Leung, C. Makaya, T. He, and K. Chan, "Adaptive Federated Learning in Resource-Constrained Edge Computing Systems," IEEE Journal on Selected Areas in Communications, vol. 37, no. 6, pp. 1205–1221, 2019.
[24] J. Devlin, M. W. Chang, K. Lee, and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," in Proc. NAACL-HLT, 2019, pp. 4171–4186.
[25] OpenAI, "GPT-4 Technical Report," arXiv preprint arXiv:2303.08774, 2023.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)