IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 11 ISSUE : 02 Print / Issue Publication Date: June 2026

ISSN : 2455-2143

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 02, ISSN No. 2455-2143, Pages 139-143
Published Online June 2026 in IJEAST (http://www.ijeast.com)

A COMPREHENSIVE REVIEW OF UPI FRAUD DETECTION USING MACHINE LEARNING-BASED ANOMALY DETECTION TECHNIQUES

Suchitra Vasantrao Dahiwade
Student
Computer Science and Information Technology,
MBES COEA, Maharashtra, India

Sushil V. Kulkarni
HOD
Computer Science and Information Technology,
MBES COEA, Maharashtra, India

Nitin V. Swami
IT Analyst, TCS,
Hinjewadi Phase-3, Pune,
Maharashtra, India.

Abstract: **The rapid adoption of Unified Payments Interface (UPI) has transformed digital payments by providing instant, secure, and convenient financial transactions. However, the increasing volume of UPI transactions has also led to a significant rise in fraudulent activities, including phishing attacks, account takeovers, identity theft, and transaction manipulation. Traditional rule-based fraud detection systems struggle to identify emerging fraud patterns due to their static nature. Machine Learning (ML) techniques, particularly anomaly detection algorithms, have emerged as effective solutions for identifying suspicious transactions in real-time. This review paper presents a comprehensive analysis of machine learning-based anomaly detection approaches used for UPI fraud detection. Various supervised, unsupervised, and hybrid learning methods are examined, along with datasets, evaluation metrics, challenges, and future research directions. The study highlights the effectiveness of anomaly detection in identifying previously unseen fraud patterns and enhancing the security of digital payment systems.**

Keywords: **UPI Fraud Detection, Machine Learning, Anomaly Detection, Digital Payments, Financial Fraud, Artificial Intelligence, Cybersecurity.**

I. INTRODUCTION

India has witnessed remarkable growth in digital payments through the Unified Payments Interface (UPI), developed by the National Payments Corporation of India. UPI enables users to transfer funds instantly using mobile applications without requiring traditional banking details[1]. The convenience and accessibility of UPI have resulted in billions of monthly transactions[2].

Despite its success, the increasing dependency on digital payments has attracted cybercriminals who exploit system vulnerabilities and user behavior[3,4]. Common UPI frauds include:

- Phishing and social engineering attacks
- QR code scams
- Account takeover attacks
- Fake payment requests
- SIM swap frauds
- Identity theft

.

Traditional fraud detection methods rely on predefined rules and thresholds, making them ineffective against evolving fraud strategies. Machine Learning-based anomaly detection systems offer a dynamic approach by identifying unusual transaction behavior that deviates from normal patterns.

Machine Learning (ML) techniques offer adaptive and data-driven solutions capable of learning transaction patterns and detecting suspicious activities in real time [5]. Among these techniques, anomaly detection has emerged as a promising approach because fraudulent transactions are generally rare and significantly different from legitimate transactions [6].

This review explores recent developments in anomaly detection techniques for UPI fraud detection and evaluates their effectiveness in securing digital payment ecosystems.

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 02, ISSN No. 2455-2143, Pages 139-143
Published Online June 2026 in IJEAST (http://www.ijeast.com)

II. LITERATURE SURVEY

Several researchers have investigated machine learning approaches for detecting financial fraud.

A. Rule-Based Fraud Detection Systems

Earlier fraud detection systems employed static rules based on transaction amount, frequency, and geographical location. Although easy to implement, these systems generate a high number of false positives and cannot adapt to new fraud patterns.

B. Machine Learning-Based Fraud Detection

Researchers have proposed supervised learning algorithms such as:

- Logistic Regression
- Decision Trees
- Random Forest
- Support Vector Machines
- Gradient Boosting

These models require labeled datasets containing both fraudulent and legitimate transactions. While achieving high accuracy, their performance depends heavily on the availability of quality labeled data.

C. Anomaly Detection Approaches

Anomaly detection techniques identify deviations from normal transaction behavior. Since fraudulent transactions are rare and continuously evolving, anomaly detection has become increasingly popular in financial security systems.
Common anomaly detection algorithms include:

- Isolation Forest
- Local Outlier Factor (LOF)
- One-Class SVM
- Autoencoders
- K-Means Clustering
- DBSCAN
- Deep Learning-Based Anomaly Detection

Studies indicate that anomaly detection models can identify unknown fraud patterns more effectively than traditional classification methods.

III. OVERVIEW OF UPI FRAUD

UPI fraud refers to unauthorized or deceptive activities performed through the UPI payment ecosystem to gain financial benefits illegally [7].

A. Phishing Fraud: Attackers trick users into revealing sensitive banking credentials through fake websites, emails, or SMS messages [8].
B. QR Code Fraud: Victims are deceived into scanning malicious QR codes, resulting in unauthorized fund transfers [9].
C. Account Takeover: Fraudsters gain access to user accounts through stolen credentials or malware attacks [10].
D. Social Engineering: Attackers manipulate users psychologically to perform unauthorized transactions [11].
E. Device Spoofing: Cybercriminals imitate legitimate devices to bypass authentication mechanisms[12].

3.1. Machine Learning in Fraud Detection

Machine Learning (ML) plays a vital role in detecting fraudulent UPI transactions by learning patterns from historical transaction data and identifying suspicious activities [13]. Based on the availability of labeled data, fraud detection techniques are categorized into three approaches:

a) Supervised Learning

Supervised learning uses labeled transaction records to classify activities as genuine or fraudulent. Algorithms such as Random Forest, Logistic Regression, SVM, and XGBoost are widely used due to their high prediction accuracy when sufficient fraud data is available [14,15].

b) Unsupervised Learning

Unsupervised learning detects anomalies without requiring labeled datasets. Techniques like Isolation Forest, Local Outlier Factor (LOF), One-Class SVM, and clustering methods identify unusual transaction patterns that may indicate fraud [16,17].

c) Hybrid Learning

Hybrid approaches integrate supervised and unsupervised models to enhance detection accuracy. These methods combine anomaly detection with classification techniques, enabling the identification of both known and emerging fraud patterns [18].

IV. ANOMALY DETECTION IN UPI FRAUD DETECTION

Anomaly detection focuses on identifying transactions that significantly differ from normal user behavior [19]. It checks and identifies unusual patterns from the feature data set.
It is also a major task to get the data set to train the algorithm for other types of ML algorithms.
Anomaly detection algorithm now became the one of the most used ML algorithm to detect the frauds in financial transactions as it's continuously improving and tackling the latest introduced types of frauds.
The main thing makes it differs about Anomaly is it maps the multidimensional geometry of routine operational telemetry, an unsupervised neural network can identify sudden topological shifts in data behavior without relying on historical labeled failures.

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 02, ISSN No. 2455-2143, Pages 139-143
Published Online June 2026 in IJEAST (http://www.ijeast.com)

Features Used in Detection:
Important transaction features include:

Feature	**Description**
Transaction Amount	Amount transferred
Transaction Time	Time of transaction
Transaction Frequency	Number of transactions per period
Device Information	Device ID and type
Geographical Location	User location
Merchant Details	Receiver information
IP Address	Network identity
Login Pattern	User access behavior

V. LITERATURE REVIEW

The academic landscape of financial fraud detection has evolved significantly over the past decade, transitioning from basic algorithmic classification to complex, hybrid deep learning architectures. Early breakthroughs focused heavily on maximizing baseline accuracy using ensemble methods. For instance, Bhattacharyya et al. (2011) demonstrated that Random Forest algorithms drastically improved fraud classification accuracy compared to traditional single decision trees by effectively reducing overfitting on tabular transactional data. [24]

However, as datasets grew, researchers realized that raw accuracy was an insufficient metric due to the severe scarcity of fraudulent examples. To address this inherent limitation, Dal Pozzolo et al. (2015) introduced cost-sensitive learning frameworks designed for the effective handling of extreme class imbalance. By assigning higher penalties to missed fraud (false negatives) than to false alarms, their work aligned machine learning objectives directly with real-world financial risk management. [25]

As fraud patterns grew more dynamic, the limitations of static, supervised models became apparent, prompting a shift toward anomaly detection. Ahmed et al. (2016) provided a comprehensive review of this paradigm, highlighting the unique strengths of unsupervised methods in detecting novel, zero-day fraud patterns without requiring pre-labeled training data. Building on the necessity for operational efficiency, Roy et al. (2018) utilized the Isolation Forest algorithm to achieve effective, real-time anomaly detection. Their approach isolated anomalies directly rather than profiling normal behavior, drastically lowering computational overhead for high-speed streaming data. [26, 27]

The subsequent boom in fintech and mobile applications introduced high-velocity transaction ecosystems. Kumar and Singh (2020) benchmarked multiple machine learning models to deliver enhanced fraud detection tailored specifically to the metadata of digital payment platforms. Yet, as fraudsters developed multi-layered evasion tactics, shallow machine learning architectures began to struggle. Addressing these sophisticated structures, Sharma et al. (2022) deployed deep learning autoencoders. By training neural networks to reconstruct legitimate transaction profiles, they achieved superior detection of highly sophisticated, non-linear fraud patterns based on reconstruction error spikes. [28, 29]

Most recently, the focus of the literature has shifted from pure detection capability to operational viability, specifically minimizing the burden of false alerts on human analysts. Verma et al. (2023) proposed a hybrid machine learning framework that successfully reduced false positive rates significantly. By pipeline-linking unsupervised anomaly filters with downstream supervised classifiers, their approach represents the contemporary state-of-the-art balance between high sensitivity and operational precision. [30]

VI. PERFORMANCE EVALUATION METRICS

Fraud detection systems are evaluated using various performance metrics [31]:

6.1 Accuracy

This metric provides a foundational overview of a model's performance by calculating total correct predictions against all analyzed transactions. However, in fraud detection, a high accuracy percentage can be deeply misleading because legitimate transactions vastly outnumber fraudulent ones. A flawed system can achieve near-perfect accuracy simply by labeling every single transaction as safe while completely missing actual theft. Consequently, relying solely on this figure risks creating a false sense of security while leaving systemic vulnerabilities completely exposed.

6.2 Precision

Precision serves as a critical measure of operational efficiency by calculating the true accuracy of the system's fraud alerts. When a model suffers from low precision, it inundates security teams with false alarms, which wastes valuable investigative resources and causes alert fatigue. Furthermore, high false-alarm rates directly harm the customer experience by mistakenly declining legitimate purchases and frustrating users. Optimizing this metric ensures that when the system flags a transaction as suspicious, there is a high probability that actual fraud is occurring.

6.3 Recall

Recall focuses entirely on the system's sensitivity and its capacity to catch every single bad actor within the dataset. A low recall score means the system is blind to active threats, allowing unauthorized charges to slip through unnoticed and cause direct financial losses. For institutions prioritizing asset protection, maximizing recall is often the primary objective, even if it results in more frequent system

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 11, Issue 02, ISSN No. 2455-2143, Pages 139-143
Published Online June 2026 in IJEAST (http://www.ijeast.com)

checks. Ultimately, this metric reflects how comprehensive a shield the system provides against fraudulent leakage.

6.4 F1-Score

The F1-Score acts as a specialized mathematical compromise that prevents engineers from over-optimizing for either precision or recall alone. By calculating the harmonic mean of those two metrics, it provides a single, unified indicator of a model's real-world viability. This metric is especially valuable during the training phase when developers need to compare different algorithms under highly imbalanced data conditions. A stable, high F1-Score proves that the system maintains a healthy equilibrium between catching thieves and maintaining user convenience.

6.5 ROC-AUC

This metric evaluates a model's core diagnostic power by measuring its performance across every possible operational threshold. It maps the dynamic trade-off between identifying true threats and accidentally triggering false alarms as the system's sensitivity dials are adjusted. A perfect score indicates that the algorithm can flawlessly separate clean transactions from malicious anomalies under any organizational risk tolerance. This comprehensive view helps risk managers select the ideal settings that match their specific corporate security policies.

VII. CHALLENGES IN UPI FRAUD DETECTION

Detecting fraud in the Unified Payments Interface (UPI) is a complex balancing act. Because UPI processes billions of instant, low-value transactions, AI and rule-based systems face four distinct hurdles:

7.1 Data Imbalance

- **The Problem:** Fraudulent transactions make up a tiny fraction (often \(< 0.1\%\)) of total UPI traffic.[32]
- **The Challenge:** Machine learning models trained on this skewed data struggle to learn fraud patterns. Instead of identifying fraud, they become biased toward predicting "legitimate" for almost every transaction.
- **The Fix:** Engineers use synthetic data generation (like SMOTE) and algorithmic weighting so the system pays equal attention to legitimate and fraudulent examples.

7.2 Evolving Fraud Patterns

- **The Problem:** Scammers constantly adapt. They shift from basic phishing to advanced remote-access scams, money muling, and QR code manipulation.[33]
- **The Challenge:** Traditional static rule engines become obsolete quickly. Models must adapt continuously to identify novel "zero-day" attack vectors before significant funds are lost.
- **The Fix:** Deployment of self-learning AI models and neural networks that update their threat definitions in real-time as new attack signatures emerge.

7.3 Real-Time Detection Requirements

- **The Problem:** UPI payments are instantaneous. Users expect payments to clear in a matter of seconds.[34]
- **The Challenge:** Complex fraud detection algorithms (like deep learning) require heavy computational power, which introduces latency. If a security check takes too long, the UPI system fails the transaction's strict timeout window.
- **The Fix:** Utilizing lightweight machine learning models and edge computing to execute risk-scoring protocols in milliseconds while the payment is actively processing.

7.4 Privacy and Security Concerns

- **The Problem:** UPI transactions move highly sensitive financial and personal data.[35]
- **The Challenge:** Building highly accurate fraud models usually requires large, centralized datasets. This creates a risk of data breaches and violates strict financial privacy laws (like India's DPDP Act).
- **The Fix:** Modern systems rely on privacy-preserving machine learning. Techniques like **Federated Learning** allow the model to learn from user behavior without the raw transaction data ever leaving the bank's secure servers.

VIII. RESEARCH GAPS

Existing studies reveal several limitations:

- Lack of publicly available UPI-specific fraud datasets [36].
- Limited application of advanced deep learning techniques.
- High false positive rates in anomaly detection systems.
- Insufficient research on explainable AI for fraud detection.
- Need for federated learning approaches to preserve privacy [37, 38].

IX. CONCLUSIONS

UPI has become the backbone of India’s digital payment ecosystem, but its rapid adoption has also increased fraud risks. Machine learning-based anomaly detection techniques offer a robust solution for identifying suspicious transactions that traditional rule-based systems often miss. Techniques such as Isolation Forest, Local Outlier Factor, One-Class SVM, and Autoencoders have demonstrated promising results in detecting fraudulent behavior. Despite significant advancements, challenges such as class imbalance, evolving fraud strategies, and privacy concerns remain. Future research should focus on developing intelligent, explainable, and privacy-preserving fraud detection systems capable of operating efficiently in real-time UPI environments.

X. REFERENCES

[1]. NPCI, "Unified Payments Interface Product Overview," 2024.
[2]. Reserve Bank of India, "Annual Report on Digital Payments," 2024.
[3]. RBI Cyber Security Framework for Digital Banking, 2023.
[4]. Ngai, E.W.T., Hu, Y., Wong, Y.H., Chen, Y., and Sun, X., "The Application of Data Mining Techniques in Financial Fraud Detection," Decision Support Systems, 2011.
[5]. Aggarwal, C.C., Data Mining: The Textbook, Springer, 2015.
[6]. Chandola, V., Banerjee, A., and Kumar, V., "Anomaly Detection: A Survey," ACM Computing Surveys, 2009.
[7]. NPCI Fraud Awareness Report, 2023.
[8]. Kumar, R., and Gupta, A., "Phishing Attacks in Digital Payment Systems," IJCSIT, 2021.
[9]. CERT-In Security Advisory on QR Code Fraud, 2023.
[10]. RBI Banking Fraud Report, 2023.
[11]. Sharma, P., "Social Engineering Threats in Online Banking," IJCA, 2022.
[12]. Singh, V., and Patel, K., "Digital Payment Fraud Trends in India," Springer, 2022.
[13]. Bishop, C.M., Pattern Recognition and Machine Learning, Springer, 2006.
[14]. Han, J., Kamber, M., and Pei, J., Data Mining Concepts and Techniques, Morgan Kaufmann, 2012.
[15]. Breiman, L., "Random Forests," Machine Learning, 2001.
[16]. Ahmed, M., Mahmood, A.N., and Hu, J., "A Survey of Network Anomaly Detection Techniques," Journal of Network and Computer Applications, 2016.
[17]. Aggarwal, C.C., Outlier Analysis, Springer, 2017.
[18]. Phua, C., Lee, V., Smith, K., and Gayler, R., "A Comprehensive Survey of Data Mining-Based Fraud Detection Research," 2010.
[19]. Chandola, V., Banerjee, A., and Kumar, V., 2009.
[20]. Liu, F.T., Ting, K.M., and Zhou, Z.H., "Isolation Forest," ICDM, 2008.
[21]. Breunig, M.M., Kriegel, H.P., Ng, R.T., and Sander, J., "LOF: Identifying Density-Based Local Outliers," SIGMOD, 2000.
[22]. Schölkopf, B., Platt, J.C., Shawe-Taylor, J., Smola, A.J., and Williamson, R.C., "Estimating the Support of a High-Dimensional Distribution," Neural Computation, 2001.
[23]. Hinton, G.E., and Salakhutdinov, R.R., "Reducing the Dimensionality of Data with Neural Networks," Science, 2006.
[24]. Bhattacharyya, S., et al., "Data Mining for Credit Card Fraud Detection," Decision Support Systems, 2011.
[25]. Dal Pozzolo, A., et al., "Calibrating Probability with Undersampling for Unbalanced Classification," IEEE Symposium Series, 2015.
[26]. Ahmed, M., et al., "Survey of Anomaly Detection Techniques," 2016.
[27]. Roy, A., et al., "Financial Fraud Detection Using Isolation Forest," IEEE, 2018.
[28]. Kumar, S., and Singh, R., "Machine Learning for Digital Payment Fraud Detection," IJITEE, 2020.
[29]. Sharma, N., et al., "Deep Learning-Based Fraud Detection in Financial Systems," IEEE Access, 2022.
[30]. Verma, P., et al., "Hybrid Machine Learning Framework for Fraud Analytics," Springer, 2023.
[31]. Fawcett, T., "An Introduction to ROC Analysis," Pattern Recognition Letters, 2006.
[32]. He, H., and Garcia, E.A., "Learning from Imbalanced Data," IEEE TKDE, 2009.
[33]. Whitrow, C., et al., "Transaction Aggregation as a Strategy for Credit Card Fraud Detection," Data Mining and Knowledge Discovery, 2009.
[34]. Jurgovsky, J., et al., "Sequence Classification for Credit Card Fraud Detection," Expert Systems with Applications, 2018.
[35]. European Union GDPR Guidelines, 2022.
[36]. OECD Digital Payment Security Report, 2023.
[37]. Kairouz, P., et al., "Advances and Open Problems in Federated Learning," Foundations and Trends in Machine Learning, 2021.
[38]. Zhou, C., et al., "Graph Neural Networks: A Review of Methods and Applications," AI Open, 2020.

IJEAST

INTERNATIONAL JOURNAL

OF ENGINEERING APPLIED SCIENCE AND TECHNOLOGY

ABOUT IJEAST

International journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high - quality research paper in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED

All submission are rigorously peer reviewed to ensure quality.

OPEN ACCESS

Free and unrestricted access to research for all.

GLOBAL REACH

Connecting researchers and Professionals worldwide.

TIMELY PUBLICATION

We Ensure a swift and efficient publication process.

For more information, visit our website

www.ijeast.com

editor@ijeast.com

www.ijeast.com

India

2455-2143