International Journal of
Science, Architecture, Technology and Environment

Securing the Cashless Economy: A Systematic Review of Payment Fraud Typologies, AI-Driven Countermeasures, and Socio-Economic Implications

Divya Mangesh Jakhal[1*], Sandhya Kaprawan[2]

[1]*MS Cyber Security, Dept. of Information Technology, Mumbai University, Kalina, Mumbai, India*

[2]*Assistant Professor, Dept. of Information Technology, Mumbai University, Kalina, Mumbai, India*

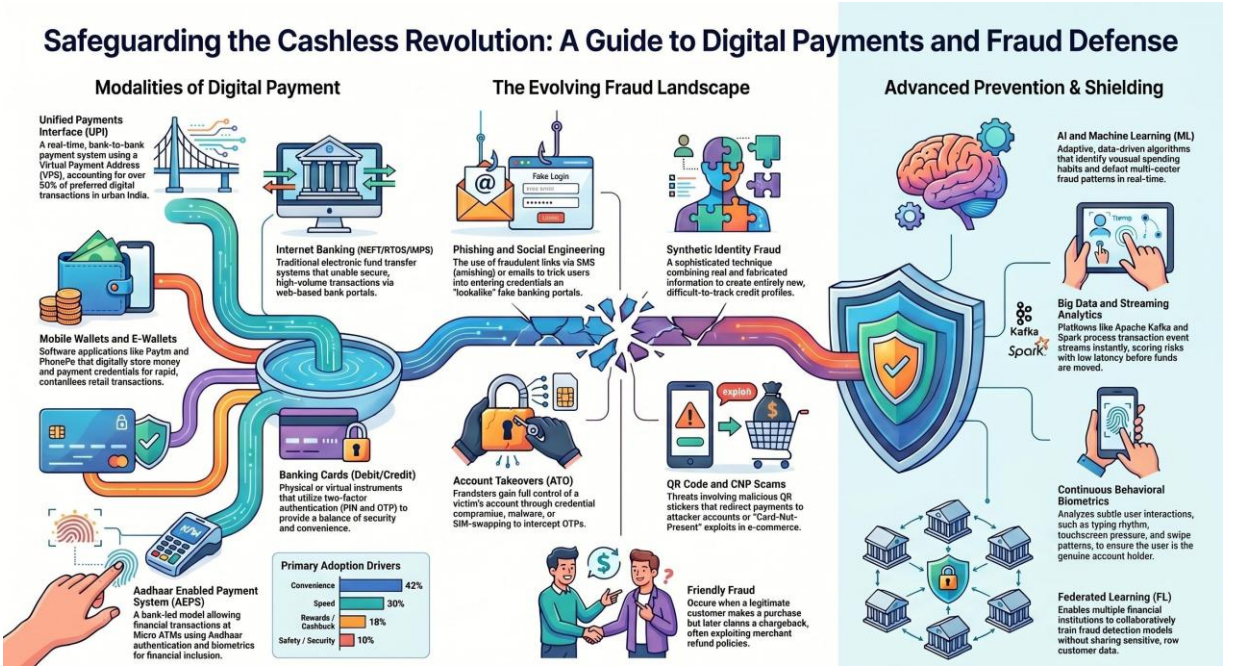
[*]*Corresponding author, divyajakhal657@gmail.com*

DOI: https://doi.org/10.63680/ijsate062603.15

Abstract

As technologies evolve, the mode of payment has shifted from cash to digital. The cashless economy boosted by innovations like the Unified Payments Interface (UPI) in India and mobile banking globally has opened new avenues for payment fraud. Cybercriminals are advancing their tactics— including social engineering, synthetic identities, account takeovers (ATO), and dynamic QR code manipulation — rendering traditional rule-based detection systems incompetent due to rigidity, slow processing speeds, and high false-positive rates. This paper presents a Systematic Literature Review (SLR) to understand payment fraud typologies and analyse how next-generation countermeasures mitigate these frauds. Our synthesis reveals that hybrid architectures integrating Machine Learning (ML), Artificial Intelligence (AI), CNNs, and RNNs demonstrate superior detection accuracy. Persistent challenges include data imbalance, algorithm opacity, and strict data privacy regulations for AML and KYC compliance. We highlight the need for Explainable AI (XAI) tools — LIME and SHAP — and Federated Learning frameworks to enable privacy-preserving collaboration between financial institutions.

Keywords: Digital Payments, UPI, Financial Fraud, Machine Learning, Cyber Security, Explainable AI (XAI), Federated Learning, Deep Reinforcement Learning, Fraud Risk Management



1. Introduction

A. The Digital Payment Revolution

The global financial domain has experienced a massive shift toward a cashless economy. In India, this transition was accelerated by the 2016 demonetization policy and the COVID-19 pandemic [1,2]. The Unified Payments Interface (UPI) rapidly positioned India as a global leader in real-time payments, handling more than 640 million transactions per day and accounting for 85% of all digital transactions in the country [3,4,36].

B. The Problem: Rising Financial Fraud

The increase in digital transaction volume has introduced significant vulnerabilities: a marked escalation in cyber-enabled financial fraud [5,6]. Sophisticated attacks — Account Takeovers (ATO), phishing, synthetic identity creation, and malicious QR code manipulation — have overwhelmed traditional rule-based detection systems, which struggle to scale, miss novel fraud tactics, and generate high false-positive rates [7,9,10].

C. Solution: Advanced Countermeasures

The financial sector is pivoting to dynamic, data-driven technologies. AI, ML, and Deep Learning models process huge real-time data streams, spot hidden anomalies, and automatically adapt to new fraud patterns [11,12,13]. Integrating continuous behavioural biometrics and big data streaming creates a multi-layered security architecture that authenticates users instantly without slowing down payments [14].

D. Research Objectives

This review defines three core research objectives:

- RO1 (Fraud Drivers): Identify and analyse drivers of new fraud typologies.
- RO2 (Model Efficacy): Evaluate hybrid ML model performance in practice.
- RO3 (Regulatory Gaps): Identify legal and regulatory blind spots in current systems.

II. Background: Evolving Threat Landscape

Cybercriminal networks now operate like professional organizations, using automated tools and coordinated teams to exploit system weaknesses. Modern payment fraud has shifted from pure technical penetration toward exploiting human behaviour and the speed of instant payment settlements [5,6].

A. Social Engineering & Phishing

Social engineering acts as the foundational mechanism for modern digital payment fraud. Fraudsters leverage psychological pressure to precipitate high-velocity victim decision-making [1]. The most common methods include phishing (malicious SMS/email links) and vishing (phone calls impersonating banking authorities to steal OTPs or PINs) [7,4]. Criminals now use deepfake technology for "CEO Fraud" and audio cloning for advanced Business Email Compromise (BEC), making scams virtually indistinguishable from reality [14].

B. ATO and Synthetic Identities

Account Takeover (ATO) uses credentials stolen via data breaches or phishing to gain unauthorized access, after which attackers lock out the legitimate holder and drain funds [9,6]. Synthetic identity fraud combines real identification markers (e.g., a legitimate SSN) with fabricated demographic parameters to create profiles that bypass standard KYC checks, enabling long-term credit misuse [11,14].

C. UPI & QR Code Scams

Because UPI transactions complete in 1–2 seconds, investigators have no time to intervene [7,9]. Fraudsters physically paste malicious QR stickers over legitimate merchant codes, diverting payments into mule accounts. Users are also manipulated into entering their UPI PIN under the false belief that they are receiving money, resulting in unauthorized debits.

D. E-Commerce & Card Fraud

Card-Not-Present (CNP) fraud exploits the absence of physical card verification during online checkout. Criminals also target the credit lifecycle — activation fraud and limit-upgrade scams — leading to unauthorized withdrawals [14,16].

III. State-of-the-Art Technological Countermeasures

Traditional rule-based frameworks — with their static rules, predefined criteria, and legacy architectures — generate high false-alert rates or miss zero-day scams entirely [11,17]. The financial industry is shifting toward dynamic, data-driven security architectures.

A. AI and Machine Learning

Machine learning has transformed fraud detection by automating complex transactional data analysis [12,10]:

- Supervised Learning: Random Forests, XGBoost, CNNs, and RNNs trained on annotated datasets to map known adversarial signatures with high precision [18,19,20].
- Unsupervised Learning: Autoencoders and Isolation Forests analyse unlabelled streams and flag transactions deviating from baseline behaviour [20,22].
- Deep Reinforcement Learning (DRL): Deep Q-Networks interact with the live payment environment, dynamically optimizing detection policies against zero-day anomalies [11,23].
- Hybrid Models: Combining supervised and unsupervised frameworks to cross-verify telemetry, mitigating both known and zero-day threats in a single low-latency stream [9,14].

B. Big Data & Streaming Analytics

Apache Kafka and Spark Streaming process millions of events concurrently, correlating live transactions against global threat intelligence with millisecond latency — cutting the criminal's operational window to near zero [24,25].

C. Biometric Authentication & Device Intelligence

- Physical Biometrics: Facial recognition, fingerprint scanning, and palm vein mapping provide robust resistance against credential forgery and deepfake-driven presentation attacks [13,25].
- Behavioural Biometrics: Keystroke dynamics, touchscreen pressure, and micro-swipe vectors continuously authenticate users in the background, detecting anomalous interaction patterns even after successful login [11,17].
- Device Intelligence: Tracking device fingerprints, IP addresses, and network logs flags requests from malicious IPs, new devices, or multiple locations in rapid succession [20,23].

D. Blockchain & Smart Contracts

Blockchain's decentralized, immutable ledger prevents transaction record alteration. Smart Contracts automate transaction rules, ensuring funds transfer only when strict pre-defined security conditions are met — highly reliable for cross-border payment security [17,26].

IV. Thematic Synthesis & Research Gaps

A. Static ML to Adaptive Deep Learning

RNNs achieve up to 95.8% accuracy on known patterns [18,27], but supervised models suffer from "concept drift" — as fraudsters continuously innovate, historical datasets lose predictive value. DRL and hybrid AI architectures address this by dynamically updating detection strategies against live payment data [11,23,28].

B. Data Sparsity & Class Imbalance

Actual fraud constitutes a minuscule fraction of transaction volume, causing models to be biased toward legitimate-transaction predictions and generating high false-positive rates [29]. Solutions include SMOTE for over-sampling [30], cost-sensitive learning, and Fuzzy Logistic Regression for algorithm-level class-imbalance management [20,30].

C. Accuracy vs. Interpretability

Deep learning's "black box" nature conflicts with GDPR's requirement for transparent automated decisions [32]. The XAI-RNN-SGRU framework incorporates LIME to explain neural network predictions — identifying specific factors such as unusual login behaviour or abnormal transaction frequency that led to a flagged transaction [11,18].

D. Privacy-Preserving Collaboration

Federated Learning combined with Homomorphic Encryption allows each institution to train models locally on

encrypted data, sharing only updated model parameters with a central server — enabling collaborative improvement across institutions without exposing sensitive PII [18,32,33].

V. Legal, Regulatory & Socio-Economic Governance

A. Liability & Consumer Vulnerability

European regulations (PSR, PSD3) now provide conditional refund rights to consumers affected by Authorized Push Payment (APP) fraud [34]. India's RBI has introduced customer protection rules, though researchers note that heavy proof requirements still favour financial institutions [4]. Literature also highlights psychological impacts on victims — anxiety, shame, and isolation — particularly among the elderly and those with limited digital literacy [5].

B. Surveillance vs. Data Privacy

Advanced anomaly detection requires processing highly sensitive data — geolocation, typing patterns, and device telemetry — creating conflict with individual privacy rights. Patel and Gupta demonstrate that opaque AI-driven risk-scoring directly compromises India's DPDP Act guarantees [4], while Europe faces similar tensions under GDPR [32]. The literature recommends Privacy by Design principles and Algorithmic Impact Assessments [13,34].

C. Digital Forensics Challenges

Instant payment settlement eliminates the forensic window. Evidence traverses multiple entities with inconsistent formats; regulatory deficiencies allow companies to overwrite critical telemetry; and automated cross-border fund transfers complicate asset recovery [6,9]. A unified cross-border framework mandating forensic-ready telemetry and standardized data retention windows for all PSPs is urgently needed [9].

VI. Conclusion & Future Directions

A. Conclusion

Traditional rule-based detection systems can no longer handle complex fraud such as synthetic identities, social engineering, and deepfakes [14,22]. Hybrid ML architectures — supervised and unsupervised combined — paired with millisecond-latency data processing infrastructure provide demonstrably superior detection without disrupting legitimate customers [10,11,20,24]. However, imbalanced training data, opaque algorithms, and forensic roadblocks remain critical bottlenecks [9,18]. Effective fraud mitigation requires a holistic socio-technical approach: cutting-edge AI anchored by empathetic consumer protection, transparent algorithmic accountability, and harmonized cross-border legal standards [15,24,34].

B. Future Research Directions

- Adaptive DRL: Continuous Online Learning and Deep Q-Network frameworks that dynamically update without manual retraining [11,23].
- Federated Learning + Differential Privacy: Enable global fraud model collaboration across institutions without exposing raw personal data [18,32,33].
- Graph Neural Networks (GNNs): Map relational linkages between accounts, devices, and IPs to detect organized fraud rings missed by single-transaction analytics [9,11].
- XAI & Algorithmic Fairness: Refine SHAP and LIME tools for high-speed environments to auto-generate legally defensible rationales for account-flagging decisions [11,15,18].
- Standardized Forensic Telemetry: Define mandatory secure log retention frameworks and rapid cross-border

evidence preservation mechanisms across all PSPs [6,9].

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship and publication of this article.

Funding

The author received no financial support for the research, authorship and publication of this article.

References

[1] "A Review Research on Online Financial Frauds in India," The USA Journals, Vol. 5, Issue 1, 2023.

[2] N. Priya and J. Ahmed, "A Survey on Digital Payments Security," IJCTT, Vol. 69, Issue 8, pp. 26–34, 2021.

[3] O. A. Bello et al., "Machine Learning Approaches for Enhancing Fraud Prevention," Int. J. Management Technology, Vol. 10, No. 1, pp. 85–108, 2023.

[4] L. Patel and P. Gupta, "Balancing Code and Constitution," Int. J. Adv. Sig. Img. Sci., Vol. 12, No. S2, 2026.

[5] P. Kumar, "AI-Powered Fraud Prevention in Digital Payment Ecosystems," J. Inf. Systems Engineering and Management, Vol. 9(4), 2024.

[6] A. Davitaia, "AI and ML in Fraud Detection for Digital Payments," Int. J. Science and Research Archive, Vol. 15(03), 2025.

[7] "Cyber Enabled Financial Fraud in the Digital Payments Era," Review of Int. Geographical Education, Vol. 11(12), 2021.

[8] P. Wadkar et al., "Cybersecurity Challenges in Digital Payments: A UPI Fraud Case Study," IJSATE, Vol. 2, Issue 10, 2025.

[9] M. Bharadwaj and B. N. Rajarajeshwari, "Digital Forensics Challenges in UPI Fraud," Proc. First Int. Conf. on Advances in Forensics and Cyber Technologies, 2026.

[10] U. K. A. Sethupathy, "Fraud Detection Mechanisms in Virtual Payment Systems," IJCTEC, Vol. 7, Issue 2, 2024.

[11] "Fraud Detection in eCommerce Payment Systems: The Role of Predictive AI."

[12] A. Patel and S. K. Malve, "ML for Fraud Detection in Digital Payment Systems," IJIUEM, Vol. 4, Issue 3, 2025.

[13] M. Agrawal, "Revolution of Digital Payment in India."

[14] A. P. Nanda, K. K. Veluri, and D. Beura, "Role of AI in Enhancing Digital Payment Security," African J. Biomedical Research, Vol. 27, No. 3s, 2024.

[15] A. Rohilla, "Strengthening Financial Resilience: A Holistic Approach," 2024.

[16] A. Kale and S. Viswanathan, "Global Surge in Banking Frauds," IJAMS, Vol. 4, No. 4, 2025.

[17] "Analysing the Economic Impact of Credit Card Fraud."

[18] S. Ghosh, "A Novel Framework Using XAI-RNN-SGRU," IEEE Access, 2025.

[19] A. Sharma and H. Babbar, "ML-Driven Detection and Prevention of Cryptocurrency Fraud," IEEE IRMKM, 2023.

[20] G. Charizanos et al., "An Online Fuzzy Fraud Detection Framework,"

Expert Systems with Applications, vol. 252, 2024.

[21] N. Singh et al., "AI and IoT in Digital Payments," IRJMETS, Vol. 07, Issue 03, 2025.

[22] A. A. Alex-Omiogbemi, "Advances in Cybersecurity Strategies for Financial Institutions," FARJ, Vol. 6, Issue 12, 2024.

[23] A. Smith and K. R. Lee, "Advancing Digital Payment Systems Combining AI and Big Data," J. Financial Technology, 2022.

[24] T. J. Olorunlana, "Harnessing Technology for Effective Fraud Detection,"

IJSATE, Vol. 2, Issue 6, 2025.

[25] N. Abid, "Improving Accuracy of Online Payment Fraud Detection with ML Models," IJISRT, Vol. 9, Issue 12, 2024.

[26] S. R. Mallreddy, "Enhancing Cloud Data Privacy through Federated Learning," IJRDO-JCSE, vol. 9, no. 8, pp. 15–22, 2023.

[27] A. C. Bahnsen et al., "Example-Dependent Cost-Sensitive Decision Trees," Expert Systems with Applications, 42(19), 6609–6619, 2015.

[28] A. Dal Pozzolo et al., "Learned Lessons in Credit Card Fraud Detection,"

Expert Systems with Applications, 41(10), 4915–4928, 2014.

[29] R. Sharma and A. Sharma, "Combatting Digital Financial Fraud through Deep Learning," ICSCSS, 2024.

[30] N. V. Chawla et al., "SMOTE: Synthetic Minority Over-Sampling Technique," JAIR, 16, 321–357, 2002.

[31] Q. Yang et al., "Federated Machine Learning: Concept and Applications,"

ACM TIST, 10(2), 1–19, 2019.

[32] Regulation (EU) 2016/679 — General Data Protection Regulation, OJ L119/1.

[33] "Trust to Exploitation: Legal Implications of Payment Fraud," Åbo Akademi University.

[34] D. Kp, "Digital Payment Systems: Perception and Concerns," Int. J. Applied Research, pp. 1118–1122, 2017.

[35] M. Hasan and M. Fardous, "Advanced Computing-Enabled Secure Financial Information Systems," AJATES, 2022.

[36] Press Information Bureau of India. https://www.pib.gov.in