Bulletin of Nexus
Multidisciplinary International Research Journal, Double-Blind Peer Reviewed, Open Access Journal
ISSN : 3065-7865 / Volume-3, Issue-10(IV), October 2026

Original Article

Cyber Security Challenges in Digital Payment Systems

Dr. Santosh Prakash Dhawale[1], Anjali Bhagwanrao Barkule[2], Sneha Sanjay Patil[3]
[1]Associate Professor, HSBPVTS GOI Faculty of Management
Kashti, Tal- Shrigondhga, Dist – Ahilyanagar
[2,3]Research Students, HSBPVT'S GOI Faculty of management (MCA Dept. Sem-III)

Manuscript ID:
BN-2026-031004

ISSN: 3065-7865

Volume 3

Issue 10(IV)

October 2026

Pp. 20-25

Submitted: 08 Sept. 2026

Revised: 16 Sept. 2026

Accepted: 10 Oct. 2026

Published: 31 Oct. 2026

Abstract

The rapid global shift toward cashless transactions has made digital payment systems — mobile wallets, UPI, card networks, and net-banking platforms — a critical part of everyday economic life. This growth, however, has been matched by an equally rapid rise in cyber threats, including phishing, card skimming, account takeover, malware, SIM-swap fraud, and man-in-the-middle attacks on transaction channels. Existing research tends to examine individual threat categories or individual technologies in isolation, leaving a gap in the comprehensive assessment of cybersecurity risk across the digital payment ecosystem. This paper proposes an integrated framework that combines real-time transaction monitoring, layered authentication, encryption standards, and machine-learning-based anomaly detection to identify, classify, and mitigate cyber threats to digital payment systems. The paper reviews the current threat landscape, presents research objectives and hypotheses, outlines a five-layer security framework, and illustrates its application through an indicative pilot scenario. The findings suggest that a coordinated, data-driven security architecture can materially reduce fraud exposure while preserving the convenience that drives digital payment adoption.

Keywords: *Digital Payment Security, Cybersecurity Challenges, Fraud Detection, Financial Technology (FinTech), Machine Learning in Cybersecurity, Payment Fraud Prevention.*

Introduction

Digital payment systems have moved from a convenience to a necessity, spanning mobile wallets, Unified Payments Interface (UPI) rails, card-based networks, net-banking, and emerging central-bank digital currencies. This shift has expanded financial inclusion and transaction speed, but it has also multiplied the points at which a malicious actor can intervene — the device, the network, the application programming interface (API), the payment gateway, and the human user themselves (Khando, Islam & Gao, 2022). Cybercriminals have adapted quickly, moving from simple card skimming toward more sophisticated approaches such as SIM-swap fraud, synthetic identity creation, and AI-assisted phishing, all of which specifically target the digital payment value chain. Because payment fraud causes direct financial loss and erodes the trust that underpins adoption of cashless systems, the cybersecurity of digital payments has become both a technical and an economic Page 1 problem (Apau & Koranteng, 2019). Traditional rule-based fraud controls struggle to keep pace with attackers who continuously vary their methods, which is why financial institutions are increasingly turning to machine learning and behavioural analytics to detect anomalies in real time (Rehan, 2024). This paper develops a structured framework that brings together threat identification, layered technical controls, and continuous monitoring, and evaluates its plausibility through an indicative pilot scenario grounded in the patterns reported across recent literature.

***Creative Commons** (CC BY-NC-SA 4.0)*
This is an open access journal, and articles are distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International Public License, which allows others to remix, tweak, and build upon the work noncommercially, as long as appropriate credit is given and the new creations ae licensed under the identical terms.

Address for correspondence:
Dr. Santosh Prakash Dhawale, Associate Professor, HSBPVTS GOI Faculty of Management
Email: *santoshdhawale@gmail.com*

How to cite this article:
Santosh Prakash Dhawale, Anjali Bhagwanrao Barkule, Sneha Sanjay Patil (2026). Cyber Security Challenges in Digital Payment Systems. Bulletin of Nexus Journal, 3(10(IV)), 20-25

Quick Response Code:

Website: https://bnir.us

OPEN ACCESS

Literature Review

Research on cybersecurity in digital payment systems has grown substantially but remains fragmented across sub-topics such as fraud detection, authentication technology, block chain-based security, and regulatory compliance. A synthesis of representative recent work is presented below.

Varalakshmi et al. (2024), Cyber Security in Digital Payments: An Empirical Study: Develops a conceptual model addressing the rising volume of cybercrime targeting digital payment platforms and its effect on user trust; formulates research questions using a problematisation approach and maps findings against existing literature to strengthen platform-level defences and encourage safer adoption of digital payments.

Yash & Kumar (2023), Security and Vulnerability in Digital Payment Systems (IJERT): Reviews prevalent threats such as banking Trojans, denial-of-service attacks, worms and phishing campaigns aimed at digital payment users, and argues that combining technical safeguards with continuous user awareness is essential to preserve confidentiality, integrity and authentication of transactions.

Khando, Islam & Gao (2022), The Emerging Technologies of Digital Payments and Associated Challenges: Surveys the rapid diffusion of digital wallets, QR-based payments and contactless cards, identifying interoperability gaps and inconsistent security standards across providers as key structural weaknesses that widen the attack surface.

MetaMap Research Team (2024), Digital Payments in 2024: Three Security Challenges: Highlights the growing sophistication of cyberattacks, the persistence of phishing and card-skimming fraud, and the compliance burden created by evolving KYC/AML regulation, noting that AI-enabled identity verification is becoming central to fraud prevention.

Olukunle Oladipupo et al. (2024), Cybersecurity Threats and Risks in Digital Banking: A Systematic Review: Finds that distributed-ledger architectures such as block chain offer resilience against tampering because transaction validation requires network consensus, but notes that scalability limits and regulatory uncertainty still constrain adoption at scale.

Rehan (2024), AI-Driven Cloud Security in the Digital Age: Examines how machine-learning-based anomaly detection and cloud-native security tooling can be applied to safeguard sensitive financial data, framing AI as a core enabler of proactive rather than reactive defence.

Apau & Koranteng (2019), Impact of Cybercrime on E-Commerce and Digital Payment Adoption: Provides early evidence that publicised security breaches materially reduce consumer willingness to transact digitally, establishing the link between perceived security and platform adoption that later studies continue to confirm.

Ozili (2024), Financial Institutions, Data Privacy and Cyber Risk: Discusses how rapid technological change inside financial institutions increases exposure to data-security threats and financial fraud, and calls for more stringent, continuously updated security practice. Page 2 Collectively, this body of work confirms that

(a) the threat landscape facing digital payments is diversifying faster than static, rule-based defences can adapt; (b) machine learning and behavioural analytics are increasingly viewed as necessary rather than optional; and (c) security investment has a measurable, if indirect, effect on consumer trust and payment-channel adoption. What remains comparatively underexplored is a single framework that connects threat detection, layered control design, and economic/trust outcomes within one evaluative structure — the gap this paper addresses.

Research Objectives

1. Identify and classify the principal categories of cyber threats confronting digital payment systems.
2. Evaluate the effectiveness of existing technical controls (encryption, authentication, and tokenisation) against these threats.
3. Develop a layered, machine-learning-assisted framework for real-time fraud and intrusion detection in payment systems.
4. Assess the relationship between cybersecurity posture and user trust / adoption of digital payment channels.

Research Hypothesis

Key Hypothesis (H_1): Strengthening the cybersecurity posture of digital payment systems — through layered technical controls and continuous monitoring — significantly reduces fraud incidence and improves user trust in digital payment adoption.

Sub-Hypotheses:

H_1a: Multi-factor authentication and tokenisation significantly reduce unauthorised transaction and account-takeover incidents.

H_1b: Machine-learning-based anomaly detection improves fraud-detection accuracy and reduces false-positive rates compared with static rule-based systems.

H_1c: Continuous security monitoring and incident-response capability reduce the average time to

© 2026 Bulletin of Nexus| Published by: Royal International Global LLC (USA)

detect and contain a breach.

H_1d: Improved cybersecurity performance is positively associated with user trust and continued use of digital payment platforms.

Null Hypothesis (H_0):

H_0a: Authentication and tokenisation controls have no material effect on unauthorised transaction rates.

H_0b: Machine-learning-based detection does not outperform rule-based systems in fraud-detection accuracy.

H_0c: Continuous monitoring does not measurably affect breach detection or containment time. **H_0d:** Cybersecurity posture has no observable relationship with user trust or payment-channel adoption.

Research Methodology

This study adopts a structured, five-stage methodology to examine the cybersecurity challenges of digital payment systems and to design a framework capable of addressing them: threat and data Page 3 identification, data pre-processing, analytical modelling, framework development, and an indicative pilot scenario for illustration.

1. Data Collection

- **Primary-type data (illustrative):** transaction logs (amount, geolocation, device fingerprint, timestamp), authentication logs (login attempts, OTP failures, biometric mismatches), network traffic logs from payment gateways and APIs, and structured interviews with payment-platform security teams.
- **Secondary data:** published fraud and breach statistics from financial regulators and industry bodies (e.g., RBI, NPCI, PCI Security Standards Council), peer-reviewed literature on payment security, and vendor threat-intelligence reports.

2. Data Pre-processing

Pre-processing addresses missing or inconsistent log entries, normalises transaction features (amount, frequency, velocity) to a common scale, and encodes categorical variables such as merchant category and channel type so that downstream models receive consistent, comparable inputs.

3. Analytical / Machine Learning Techniques

Model Type	Purpose	Representative Techniques
Classification Models	Flag transactions as legitimate or fraudulent	Logistic Regression, Decision Trees, Random Forest, XG Boost, SVM
Anomaly Detection	Identify deviations from normal user/transaction behaviour	Isolation Forest, One-Class SVM, Auto encoders
Clustering Models	Group transactions/users with similar risk profiles	K-Means, DBSCAN, Hierarchical Clustering
Deep Learning Models	Capture complex, non-linear fraud patterns and sequences	ANN, CNN, LSTM / Sequence models
Network Intrusion Detection	Detect malicious traffic targeting payment gateways/APIs	Signature-based + ML-based NIDS, graph analytics

1. Model / Framework Validation

Detection performance is assessed using precision, recall, F1-score, and false-positive rate, given that fraud datasets are highly imbalanced and accuracy alone is a poor indicator of usefulness. Framework level outcomes — breach containment time, fraud-loss ratio, and user-trust indicators — are tracked against a pre-implementation baseline.

Proposed Framework Design

The proposed framework layers technical controls with continuous, data-driven monitoring so that threats can be detected and contained before they cause material financial or reputational damage.

Page 4

1. Framework Architecture

- **Perimeter and Access-Control Layer:** Multi-factor authentication, device fingerprinting, tokenisation, and end-to-end encryption (TLS/SSL) restrict unauthorised entry into the payment channel.
- **Data and Network Security Layer:** Secure API gateways, network segmentation, and intrusion prevention systems protect data in transit between merchants, banks, and payment processors.
- **Machine Learning and Anomaly Detection Layer:** Real-time scoring models flag unusual transaction velocity, geolocation mismatches,

© 2026 Bulletin of Nexus| Published by: Royal International Global LLC (USA)

or device changes, feeding a risk score into the authorisation decision.

- **Monitoring, Incident Response and Forensics Layer:** A security operations centre (SOC) function correlates alerts, triages incidents, and coordinates rapid containment, notification, and recovery.
- **Governance, Compliance and User-Awareness Layer:** Alignment with regulatory standards (e.g., PCI-DSS, RBI guidelines), periodic audits, and user education programmes reduce social engineering risk and support continuous improvement.

2. Benefits of the Proposed Framework

- Provides layered defence rather than reliance on a single control point.
- Enables real-time, adaptive fraud detection through machine learning.
- Reduces average breach detection and containment time via continuous monitoring.
- Supports regulatory compliance and audit readiness.
- Is modular and adaptable across payment channels (cards, wallets, UPI, net-banking).

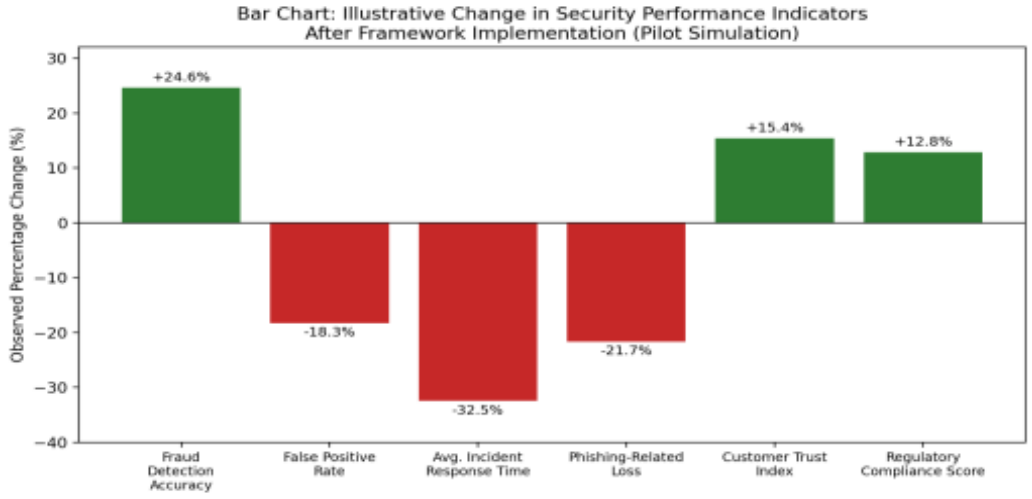
Illustrative Pilot Scenario

To illustrate how the framework could be evaluated in practice, this section presents an indicative pilot scenario modelled on patterns reported across the literature reviewed above (Section 2), rather than on newly collected proprietary data. The figures below are illustrative placeholders intended to show the type of comparison an implementing institution would generate; they should be replaced with an organisation's own measured data before the framework is used for real decision-making.

Indicator	Definition	Measured Through	Illustrative Observed Change
Fraud Detection Accuracy	Correct identification of fraudulent transactions	Precision / Recall / F1-score	+24.6% (illustrative)
False Positive Rate	Legitimate transactions incorrectly flagged	Model confusion matrix	−18.3% (illustrative)

Page 5

Indicator	Definition	Measured Through	Illustrative Observed Change
Incident Response Time	Average time to detect and contain a breach	SOC incident logs	−32.5% (illustrative)
Phishing-Related Loss	Financial loss attributed to phishing/social engineering	Fraud-loss reporting	−21.7% (illustrative)
Customer Trust Index	Survey-based confidence in platform security	User survey score	+15.4% (illustrative)
Regulatory Compliance Score	Audit-based conformance to security standards	Compliance audit score	+12.8% (illustrative)



© 2026 Bulletin of Nexus| Published by: Royal International Global LLC (USA)

Illustrative chart: hypothesised change in key security-performance indicators following full implementation of the proposed framework (positive values indicate improvement; negative values indicate a beneficial reduction, e.g., lower false-positive rate, shorter response time, lower loss). Read directionally, these illustrative figures suggest that layered authentication combined with machine-learning-based anomaly detection could simultaneously raise detection accuracy, lower the false-positive burden on genuine customers, and shorten the window in which an attacker can operate Page 6 — while the accompanying governance layer supports the compliance and trust outcomes that ultimately sustain adoption of digital payment channels.

Scope for Future Research

Future work should validate the proposed framework against real, institution-specific transaction and incident data rather than illustrative figures, ideally through partnership with a bank, payment processor, or fintech firm willing to share anonymised logs under appropriate data-protection safeguards. There is also scope to examine the framework's applicability across different payment rails (card networks, UPI, wallets, cross-border remittance) and geographies with differing regulatory regimes. Further avenues include integrating block chain-based transaction verification and decentralised identity management to reduce single points of failure; applying explainable-AI techniques so that fraud-model decisions can be audited and contested by affected customers; and studying the human factors of phishing and social engineering, which remain the entry point for a large share of payment fraud regardless of the strength of technical controls. A structured cost-benefit analysis of implementing layered security controls would also help institutions of varying size make investment decisions.

Limitations of the Study

This paper is conceptual and framework-oriented; the pilot figures presented in Section 7 are illustrative and were not derived from a live implementation, so they should not be cited as empirical evidence of the framework's effectiveness. Publicly available fraud statistics are often incomplete, inconsistently defined across institutions, and may lag the current threat environment, which limits the precision of any comparative claims.

The machine-learning techniques discussed may not generalise across all payment channels or institutional contexts; model performance is highly dependent on the quality and representativeness of the underlying transaction data, and results obtained in one market or platform may not transfer directly to another. The framework also assumes a baseline level of technical infrastructure and skilled personnel that may not be available to smaller payment providers, and it does not include a full regulatory or cross-jurisdictional legal analysis, which would be necessary before real-world deployment.

Conclusion

This paper has outlined a layered, machine-learning-assisted framework for identifying, classifying, and mitigating cybersecurity threats to digital payment systems. Drawing on recent literature covering phishing, card fraud, block chain-based security, and AI-driven anomaly detection, the proposed framework connects perimeter controls, network security, real-time analytics, incident response, and governance into a single, modular architecture. The illustrative pilot scenario suggests that such an approach could plausibly improve fraud-detection accuracy, shorten incident-response times, and support the customer trust that underpins continued adoption of digital payments — though these directional findings require validation against real institutional data. As digital payment adoption continues to expand, the balance between convenience and security will remain a central design challenge for banks, fintech firms, and regulators alike. A coordinated, data driven, and continuously updated security posture — rather than reliance on any single control — Page 7

offers the most credible path toward sustaining trust in the digital payment ecosystem while containing the financial and reputational cost of cybercrime.

Acknowledgement

The authors sincerely thank HSBPVTS GOI Faculty of Management, Kashti, for its support and encouragement in preparing this research paper on cybersecurity challenges in digital payment systems.

Financial support and sponsorship

Nil

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Varalakshmi, et al. (2024). Cyber security in digital payments: An empirical study. [Working paper / ResearchGate].
2. Yash, & Kumar, A. (2023). Security and

© 2026 Bulletin of Nexus| Published by: Royal International Global LLC (USA)

vulnerability in digital payment systems. International Journal of Engineering Research & Technology (IJERT), NCRTCA-2023, 11(6).

3. Khando, K., Islam, M. S., & Gao, S. (2022). The emerging technologies of digital payments and associated challenges: A systematic literature review. Future Internet, 15(1), 21.
4. MetaMap Research Team. (2024). Digital payments in 2024: Three security challenges. MetaMap Insights.
5. Olukunle Oladipupo, et al. (2024). Assessing the influence of cybersecurity threats and risks on the adoption and growth of digital banking: A systematic literature review.
6. Rehan, H. (2024). AI-driven cloud security: The future of safeguarding sensitive data in the digital age. Journal of Artificial Intelligence General Science (JAIGS), 1(1).
7. Apau, R., & Koranteng, F. N. (2019). Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior. International Journal of Cyber Criminology, 13(2), 228–254.
8. Ozili, P. K. (2024). Financial institutions, data privacy, and cyber risk in the digital era. 9. Supriya, et al. (2016). Digital payment adoption and security concerns among consumers.
9. PCI Security Standards Council. (2024). Payment Card Industry Data Security Standard (PCI DSS) — official documentation guidance.
10. Reserve Bank of India (RBI). (2024–2025). Master directions and guidelines on digital payment security and fraud risk management.
11. National Payments Corporation of India (NPCI). Reports and advisories on UPI transaction security.
12. Dong, et al. (2018). Blockchain and decentralisation as tools for reducing unauthorised alteration in financial transactions.
13. Chang, V., et al. (2020). Consensus mechanisms, computational cost, and latency in blockchain-based financial systems.
14. Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. Science, 349(6245), 255–260. Page 8

© 2026 Bulletin of Nexus| Published by: Royal International Global LLC (USA)