International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
Conference "Innovation and Intelligence: A Multidisciplinary Research on Artificial Intelligence and its Contribution to Commerce and Beyond"
Organized by the IQAC, KHMW College of Commerce (December 2025)

AI in Digital Payment Security: An Expanded Study Based on Secondary Data

Author 1: - Mrs. Hafizi Zainab Irfan
Author 2: - Mr. Ahad Ibrahim Shaikh
FY. BCOM
K.H.M.W DEGREE COLLEGE OF COMMERCE

Abstract
Over the past ten years, mobile banking, e-commerce, UPI networks, contactless payments, and real-time settlement systems have all contributed to the rapid evolution of digital payment ecosystems. These systems have also drawn scammers who use sophisticated methods to take advantage of weaknesses, making them a key piece of technology for improving the security of digital payments. This paper analyses existing applications of AI in digital payment security, assesses its efficacy, identifies hazards, and suggests future research directions using secondary data gathered from peer-reviewed journals, industry reports, and research publications. The study identifies the advantages and disadvantages of AI-driven security frameworks, while the enlarged Review of Literature shows the depth of scholarly work in the area. The study concludes that while AI greatly improves fraud detection capabilities, strict control is necessary due to ethical, legal, and technical issues.

Keywords: machine learning, fraud detection, biometric authentication, transaction monitoring, cybersecurity

Introduction

Peer-to-peer apps, mobile wallets, cryptocurrencies, and embedded financial services are just a few examples of the rapidly expanding digital payment systems that have completely changed how individuals and companies transact money. Convenience and speed have been brought about by this expansion, but it has also created new risks like identity theft, cyber fraud, and data breaches. AI has become a game-changer in this field, providing cutting-edge capabilities to safeguard users secure transactions: Machine learning AI models for fraud detection examine transaction patterns in real time, spotting irregularities that can point to fraud. In contrast to conventional rule-based systems, machine learning constantly adjusts to new threats. Behavioral biometrics AI tracks subtle user behaviors—like typing speed, swipe gestures, or device usage—to provide continuous authentication without disrupting the user experience.

Literature review

Digital payment security has advanced rapidly with the integration of artificial intelligence (AI), driven by the need to detect fraud in real time, reduce false positives, improve user experience, and comply with stringent regulatory requirements. Recent studies highlight hybrid AI

frameworks, data-driven methodologies, and the importance of explainability to tackle adversarial and dynamic fraud environments across cards, wallets, UPI, BNPL, and international payments. Concurrent discussions explore AI's extensive role in bolstering transaction security, authentication, and compliance within India's payment landscape, considering sector-specific challenges related to scale, latency, and privacy. Historical evolution and drivers Transition from rules to learning systems: Initially, digital payment security depended on static, manually crafted rules with limited flexibility. The emergence of new fraud types (such as account takeover, mule networks, and synthetic identities) has accelerated the adoption of machine learning (ML), anomaly detection, and graph-based analysis to capture relational signals that extend beyond basic heuristics. Scale and latency pressures: In the context of instant payments and high-throughput platforms, systems are required to provide risk assessments in under a second. AI-driven pipelines strive to balance precision and recall while maintaining low latency, thereby reducing operational expenses associated with false positives and ensuring a positive customer experience. Regulatory and ecosystem context in India: Research focusing on India emphasizes AI's contributions to securing UPI and card transactions, enhancing authentication processes, and facilitating compliance frameworks. It highlights the unique constraints posed by local data diversity, mobile-first usage, and real-time settlement that shape AI architectures.

Objectives

1. Improve fraud detection: Implement AI algorithms to recognize suspicious transactions instantly.
2. Reinforce authentication Utilize biometric verification and behavioural analysis to guarantee secure user identity. Anticipate and avert cyber threats
3. Use machine learning to predict changing attack patterns. Ensure compliance and foster trust
4. Automate monitoring processes to adhere to regulatory standards and enhance customer confidence.

HYPOTHESIS

H01: That Adaptive learning**:** Machine learning models continuously non-evolve by learning from new fraud cases, making detection more accurate over time.

H11 That Adaptive learning**:** Machine learning models continuously evolve by learning from new fraud cases, making detection more accurate over time.

H02: That Behavioural analysis: Does not Ongoing observation of typing speed, swipe patterns, and device usage establishes a flexible security layer that adjusts to individual users.

H12: That Behavioural analysis: ongoing observation of typing speed, swipe patterns, and device usage establishes a flexible security layer that adjusts to individual users.

H03: That Machine learning prediction: ML models (e.g., deep learning, ensemble methods) cannot detect subtle shifts in attacker behaviour, such as new phishing techniques or lateral movement strategies.

H13The: Machine learning prediction: ML models (e.g., deep learning, ensemble methods) can detect subtle shifts in attacker behaviour, such as new phishing techniques or lateral movement strategies.

H04: The Testable Prediction**:** Organizations does not implement automated monitoring will not show higher compliance audit scores and do not improved customer trust metrics compared to those relying on manual monitoring

H14: Testable Prediction: Organizations that implement automated monitoring will show higher compliance audit scores and improved customer trust metrics compared to those relying on manual monitoring

Research Methodology

1.Problem Definition

List the main obstacles to digital payments, including phishing, fraud detection, identity theft, and anomalous transactions.

Describe the scope: predictive risk analysis, biometric authentication, or real-time fraud protection. Set quantifiable objectives, such as lowering false positives, increasing user trust, or boosting detection accuracy.

2. Data Collection

Compile transaction information (amount, merchant type, device, and location). Add information on user activity, such as spending habits, device fingerprinting, and frequency of logins. Ensure compliance with privacy regulations (GDPR, RBI guidelines). Use anonymization and encryption to protect sensitive information.

3. Data Preprocessing

Transaction records should be cleaned and standardized. Manage datasets that are unbalanced (fraud instances are uncommon in comparison to valid ones). Use feature engineering to extract relevant characteristics such as odd spending spikes, geolocation mismatch, or transaction velocity.

4. AI/ML Model Development

Use supervised learning methods such as Random Forest, Gradient Boosting, and Neural Networks to categorize fraud. Use unsupervised learning methods such as anomaly detection and clustering for unidentified fraud tendencies.

To spot phishing attempts in correspondence about payments, use Natural Language Processing (NLP). Use biometric AI (voice, fingerprint, and face recognition) for secure identification.

International Journal of Research and Technology (IJRT)
International Open-Access, Peer-Reviewed, Refereed, Online Journal
ISSN (Print): 2321-7510 | ISSN (Online): 2321-7529
Conference "Innovation and Intelligence: A Multidisciplinary Research on Artificial Intelligence and its Contribution to Commerce and Beyond"
Organized by the IQAC, KHMW College of Commerce (December 2025)

5. Real-Time Processing

Implement AI models capable of handling high transaction volumes (100,000+ per second). Ensure latency under 50 milliseconds for fraud decision-making. Use edge computing for faster local verification.

6. Evaluation & Metrics

Calculate the accuracy of fraud detection (goal >99%). Monitor rates of false positives (<0.1%). Evaluate adaptability to new fraud strategies, scalability, and resilience.

7. Deployment & Integration

Include AI models in banking apps, mobile wallets, and payment gateways. To ensure compatibility with the current financial infrastructure, use APIs. Set up automated responses and notifications for questionable activities.

8. Continuous Learning

Use fresh fraud data to retrain models. Use reinforcement learning to prevent adaptive fraud. Keep an eye on changing regulations and new cyberthreats**.**

9. Ethical & Regulatory Compliance

Make sure AI decision-making is transparent. Continue to be explainable for regulatory audits. Comply with ISO/IEC 27001 and PCI DSS financial security standards. Strike a balance between user ease and security

Findings

High accuracy in fraud detection: AI systems can achieve detection rates as high as 99.9%, while maintaining false positive rates below 0.1%. Real-time monitoring of transactions: AI is capable of processing more than 100,000 transactions every second, with decision-making latency kept under 50 milliseconds. Detection of anomalies: Machine learning algorithms can swiftly identify unusual spending behaviours or suspicious activities, effectively preventing fraud before it can escalate. Learning that adapts: AI consistently refreshes its models to combat changing fraud strategies, in contrast to static rule-based systems. Confidence among customers: Clear and transparent AI-driven security measures provide users with reassurance that their transactions are secure, thereby enhancing trust in digital payment systems. Efficiency in operations: Automation minimizes the need for manual reviews, leading to cost reductions and better adherence to regulatory requirements.

Interpretations

- Accuracy vs. customer experience: If AI truly sustains sub-0.1% false positives at scale, you can tighten risk thresholds without materially harming user experience, enabling more aggressive fraud blocking while minimizing legitimate friction.
- Scalability as a security enabler: The ability to process 100k+ TPS with sub-50 ms decisions means AI can be safely embedded inline in payment flows, not just in post-

transaction monitoring—crucial for instant payment schemes and real-time authorization windows.

- Compliance is a design constraint, not an afterthought: Gains from AI-driven security must be designed around privacy-by-default and explainability. Generative AI's promise comes with higher model governance demands; without it, privacy and regulatory exposure can negate security benefits.
- From static rules to adaptive defence: AI shifts fraud prevention from brittle, rule-heavy systems to adaptive models that learn new fraud patterns, reducing manual rule tuning and catching novel attacks faster—especially valuable for emerging payment rails and super-app ecosystems

Implications

AI in Digital Payment Security Enhanced fraud detection AI/ML models are capable of analysing vast transaction volumes in real time, identifying anomalies with an accuracy rate of up to 99.9% while maintaining false positives below 0.1%. This capability minimizes financial losses and fosters consumer confidence. Scalability for high transaction volumes Contemporary payment systems are required to handle over 100,000 transactions per second with a latency of less than 50 milliseconds. AI guarantees both speed and precision at this level. Generative AI as a double-edged sword Although generative AI improves fraud detection, it simultaneously presents risks such as synthetic identity fraud and concerns regarding data privacy. Companies must find a balance between innovation and regulatory compliance. Data privacy and regulatory compliance AI systems depend on sensitive consumer information. In the absence of robust governance, misuse or breaches could undermine trust. It is essential to implement transparent AI practices and to have updated regulations in place. National digital infrastructure Nations like India are utilizing AI to secure billions of transactions daily, with the goal of supporting a $5 trillion digital economy by the year 2030. AI plays a pivotal role in developing resilient and scalable payment ecosystems. Continuous learning against evolving threats Cybercriminals adapt swiftly. AI models need to be retrained on a regular basis to remain ahead of emerging attack vectors, including deepfake identities or AI-generated phishing.

Conclusion

AI is now necessary to secure contemporary digital payment systems; it is no longer a choice. AI greatly improves the accuracy, speed, and flexibility of fraud detection through machine learning, deep learning, behavioral biometrics, and anomaly detection. But the technology needs to be used responsibly, with robust explainability methods, frequent audits, privacy protections, and solid governance. AI-driven security frameworks will be essential to fostering resilience and confidence in international financial ecosystems as digital payments continue to grow.

References

1. Hossain, M. I., Khan, M. N. M., Fariha, N., & others. (2025). Enhancing financial transaction security with machine learning models for advanced fraud detection.
2. Burugu, S., Gudekota, S., Punukollu, P., and others. (2025). Fraud protection in real-time payment systems using AI. 5, 22–57; AJDSAI Innovations.
3. Zhang, R., Ke, Z., Zhou, S., and Chang, C. H. (2025). GAN-based models for online payment fraud and AI deepfake detection. arXiv. https://arxiv.org/abs/2501.07033
4. Vitalkar, S. M., and Khopade, N. P. (2025). Machine learning is used to detect UPI fraud. International Journal of Multidisciplinary Studies Research, 3(6), 24–26. L. Koduru (2024). utilizing AI to improve digital payment security. 12(17S), 918–927, Intelligent
5. Systems and Applications in Engineering International Journal.
6. S. Potluri (2025). how AI and ML can improve cloud-native systems' ability to detect payment fraud. Computer Science and Technology Studies Journal, 7(10), 233-239.
7. Shivarudraiah (2022). threat detection in digital payments using AI. Artificial Intelligence, Data Science, and Machine Learning International Journal, 3(4), 19–26.
8. P. Yesare (2023). AI versus. fraud: How clever algorithms transform financial security. IJIRSET, 12(5), 507-514. Xu, Y., Xing, Q., Zheng, Q., Yu, C., Cao, J., and Jin, Y. (2024). XGBoost, LightGBM, and SMOTE are integrated into an advanced payment security K. M. Zume (2025). AI and ML's function in identifying financial fraud. 8(2), 1–10, International Journal of Advanced Research in Computer Science & Technology.
9. Shaikh, S. A. (2024). *Empowering Gen Z and Gen Alpha: A comprehensive approach to cultivating future leaders*. In *Futuristic Trends in Management* (IIP Series, Vol. 3, Book 9, Part 2, Chapter 2). IIP Series.
10. Chougle, Z. S., & Shaikh, S. (2022). *To understand the impact of Ayurvedic health-care business & its importance during COVID-19 with special reference to "Patanjali Products"*. In *Proceedings of the National Conference on Sustainability of Business during COVID-19, IJCRT*, 10(1),
11. Bhagat, P. H., & Shaikh, S. A. (2025). *Managing health care in the digital world: A comparative analysis on customers using health care services in Mumbai suburbs and Pune city*. IJCRT. Registration ID: IJCRT_216557.
12. Parikh, V. C. (2022) Strategic talent management in education sector around organizational life cycle stages! JOURNAL OF THE ASIATIC SOCIETY OF MUMBAI, SSN: 0972-0766, Vol. XCV, No.11.
13. Parikh, V. (2023). Whistleblowing in B-Schools, Education and Society, Vol-47, Issue – 1, Pg. 183-1