IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2025

DOI: 10.17148/IARJSET.2025.12927

# Online Payment Security Using AI

**Prof. Miss. Reeta V. Patil*[1], Miss. Shubhangi K. Mahajan[2]**

Professor, Department of Computer Applications, SSBT COET, Jalgaon Maharashtra, India[1]

Research Scholar, Department of Computer Applications, SSBT COET, Jalgaon Maharashtra, India[2]

**Abstract:** The rapid growth of e-commerce, mobile wallets, and digital banking services has changed the way people and businesses conduct financial transactions. While these advancements have increased convenience and accessibility, they have also created significant security risks, such as identity theft, phishing assaults, account takeovers, and large-scale financial crime. Traditional rule-based security systems, while helpful in some cases, are becoming ineffective in fighting fraudsters' developing strategies. In this context, Artificial Intelligence (AI) has emerged as a powerful tool for improving online payment security by enabling intelligent, adaptive, and real-time fraud detection.

AI-powered security models can scan massive volumes of transactional data, user activity, and contextual information to uncover tiny irregularities that traditional detection approaches often miss. Neural networks, random forests, and support vector machines are common machine learning methods used to create predictive models that can accurately distinguish between legal and fraudulent transactions. Unsupervised learning techniques are also used to find hidden patterns and detect previously unknown dangers, while Natural Language Processing (NLP) can help identify phishing emails, phony websites, and suspicious conversations.

The combination of AI and real-time monitoring enables preemptive responses by stopping questionable transactions before they are conducted, reducing financial loss and increasing customer trust. Furthermore, AI systems are constantly learning and adapting to new attack vectors, making them resilient to developing attacks. Future improvements, like explainable AI, federated learning for privacy-preserving fraud detection, and blockchain integration, are projected to improve the security and transparency of online payment systems.

This paper underlines the expanding relevance of Artificial Intelligence in protecting online payments, assesses the efficacy of current AI-based solutions, and underscores the importance of continual innovation in developing strong, scalable, and trustworthy financial systems.

## I. INTRODUCTION

Online payments have become an essential element of modern life, allowing individuals and businesses to execute financial transactions with remarkable convenience and speed. From e-commerce to digital banking, mobile wallets, and peer-to-peer transactions, the quick transition to cashless economies has considerably increased efficiency and convenience. However, this digital transition has resulted in a significant increase in security concerns, such as identity theft, phishing, data breaches, and fraudulent transactions. The surge in sophisticated cyberattacks has highlighted the shortcomings of existing payment security systems, which are frequently rule-based, inflexible, and unable to react to new and evolving attack strategies**.**

Artificial intelligence (AI) is increasingly seen as a transformational tool for addressing these concerns. Unlike traditional approaches, AI-powered systems can analyze massive amounts of real-time data, find hidden trends, and make intelligent judgments to detect and prevent fraudulent activity. Machine learning algorithms, in particular, play an important role in fraud detection by learning from historical transaction data and categorizing actions as legitimate or suspect. AI systems can achieve improved detection accuracy while limiting false positives by utilizing advanced approaches such as neural networks, deep learning, and ensemble models, which are common in older systems.

Furthermore, AI improves payment security by providing continuous monitoring and anomaly detection. For example, user behavior analytics can monitor how people generally engage with digital platforms, identifying any unexpected conduct such as unusual login locations, anomalous spending patterns, or abrupt changes in device use. Natural Language Processing (NLP) improves security by detecting phishing efforts, fraudulent messaging, and harmful websites that aim to deceive visitors. These capabilities enable financial institutions and payment service providers to act proactively, preventing fraud before it occurs rather than reacting after the damage has been done.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2025

DOI: 10.17148/IARJSET.2025.12927

Beyond fraud detection, AI helps to increase trust and user confidence in online payment systems. Real-time decision-making, adaptive risk assessment, and predictive analytics safeguard users while still providing smooth and secure transaction experiences. Furthermore, with advances in explainable AI, federated learning, and blockchain integration, future online payment systems are likely to be even more transparent, resilient, and privacy-preserving.

This article examines the role of artificial intelligence in improving online payment security. It nalyses current dangers and vulnerabilities in digital transactions, investigates AI strategies for detecting and preventing fraud, and identifies future research topics that can improve the security of financial ecosystems. AI can help online payment systems transition to a more safe, intelligent, and trustworthy digital financial ecosystem.

## II. IMPORTANCE

**1. Fraud Prevention**
AI recognizes anomalous spending patterns, location mismatches, and many failed attempts, minimizing the likelihood of fraud.
**2. Real-time Protection**
Unlike manual inspections, AI works instantly, preventing fraudulent transactions before they occur.
**3. Improved Accuracy**
Machine learning reduces false positives (blocking genuine users) and false negatives (missing actual fraud).
**4. Enhanced User Trust**
Secure transactions boost trust in online banking, e-commerce, and mobile wallets.
**5. Cost Reduction**
Preventing fraud protects banks, businesses, and customers from financial losses and chargebacks.
**6. Adaptive Security**
AI constantly learns from new cyberattack patterns, strengthening systems over time.
**7. Stronger Authentication**
Biometric AI (facial, fingerprint, voice) provides an extra layer of security in addition to passwords and PINs.
**8. Regulatory Compliance**
Helps financial organizations comply with security standards and government regulations.

**Applications On Online Payment Security Using AI**
1. Debt and Credit Card Fraud Prevention: Real-time monitoring and detection of suspicious transactions.
2. Secures mobile payment apps with AI-powered authentication and anomaly detection.
3. Banking Transactions: Identifies suspicious activity in online banking platforms.
4. E-commerce Payment Security: Monitors online transactions to avoid identity theft and fraudulent accounts.
5. Blockchain Transactions: AI detects anomalous transactions to prevent cryptocurrency fraud.

**The Role of AI in Online Payment Security**

**1. Fraud Detection** - Artificial intelligence algorithms can detect questionable transactions by monitoring user activity patterns and detecting irregularities.
**2. Real-time Monitoring** - Machine learning models continuously monitor transaction flows to detect and prevent fraud.
**3. User Authentication** - Biometric AI approaches (facial recognition, voice recognition, fingerprint matching) provide additional security levels.
**4. Risk Scoring** - AI calculates risk rankings to each transaction, lowering false positives while increasing accuracy.
**5. Adaptive Security** - AI systems learn from new fraud schemes and evolve over time without operator involvement.

**Scope of AI in Online Payment Security**

The scope of AI in this industry is quickly rising due to the increasing online transactions and cyber concerns.

**1. E-Commerce and Online Banking**
AI-powered fraud detection enables secure shopping and online banking.

**2. Mobile Wallets and UPI Transactions**
As mobile payment acceptance grows, AI will play an important role in securing microtransactions and peer-to-peer transfers.

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2025

DOI: 10.17148/IARJSET.2025.12927

**3. Cryptocurrency and Blockchain Security**
AI can detect suspicious wallet activity, phishing attempts, and bitcoin scams.

**4. Regulatory Compliance**
AI ensures compliance with DSS, GDPR, and RB requirements by monitoring data privacy and security.

**5. Personalized Security**
AI systems can tailor security checks to specific user behavior, balancing safety and ease.

**6. Future advancements**
Integration with Quantum AI for enhanced encryption.
Generative AI is used to simulate and test advanced threats.
AI-powered identity verification for cross-border transactions.

## III. LITERATURE SURVEY

**1.Overview**
AI and machine learning research for online payment security has transitioned from rule-based systems to ML/DL pipelines that reduce false positives through feature engineering, supervised/unsupervised learning, and real-time scoring (Btoush et al., 2023; Chen et al., 2025).

**2. Supervised Training for Fraud Scoring**
Supervised classifiers such as Logistic Regression, Random Forest, SVMs, and boosting ensembles are still commonly utilized in conjunction with imbalance-handling algorithms like SMOTE or cost-sensitive learning (Dal Pozzolo et al., 2015; Jurgovsky et al., 2018).

**3. Deep Learning and Temporal Models**
Sequential models (RNNs, LSTMs, GRUs, and Transformers) capture temporal fraud patterns more successfully, however they have interpretability concerns. GAN-based techniques also show potential (Fiore et al., 2019; Chen et al., 2025).

**4. Unsupervised & Anomaly Detection**
Unsupervised models like clustering, autoencoders, and isolation forests detect unique or uncommon fraud and are frequently coupled with supervised models in hybrid designs (Ahmed et al., 2016 survey).

**5. NLP for Phishing & Social Engineering**
Phishing and malicious messaging detection relies on NLP algorithms ranging from lexical analysis to transformers, with promising findings for phishing identification (Salloum et al., 2021).

**6. Privacy-Preserving & Federated Learning**
Federated learning allows for multi-institution fraud detection without centralizing data, while challenges with non-IID distributions and communication persist (Yang et al., 2019; Abdul Salam et al., 2024).

**7. Explainable AI (XAI) and Regulation**
Explainability is crucial for detecting financial fraud; techniques such as SHAP, LIME, and interpretable ML models promote compliance and analyst trust (Molnar, 2020).

**8. Blockchain and Complementary Technologies**
Blockchain enables immutable records and auditability in payment systems, but scalability and privacy concerns limit its direct application in fraud detection (Casino et al., 2019).

**9. Datasets, Metrics, and Practical Issues**
Public datasets, such as the UCI/Kaggle credit card dataset, are typical benchmarks, although production systems experience label latency, drift, and imbalance. AUC-PR metrics are preferred over accuracy (Dal Pozzolo et al., 2015).

**10. Open Problems & Future Directions**
Future research needs focus on online learning, privacy-utility trade-offs, explainability, multimodal fusion, and adversarial robustness in fraud detection (Shokri et al., 2017; Chen et al., 2025).

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2025

DOI: 10.17148/IARJSET.2025.12927

## IV. METHODOLOGY (RESEARCH METHODS)

AI systems can detect unexpected patterns and potential risks that traditional approaches may miss using machine learning algorithms and real-time data processing. This proactive approach reduces financial and reputational damage while recognizing and preventing fraudulent actions.

**Key Components of Methodology**

**1. Research Design**

The findings show that AI considerably increases real-time fraud detection and adaptability to changing fraud patterns when compared to traditional rule-based systems. However, ethical concerns, algorithmic prejudice, data privacy difficulties, and system vulnerabilities all impede wider implementation

**2. Data Collection method**

In the digital age, online payments have become an essential component of e-commerce, banking, and financial activities. However, as the number of digital transactions has grown, so have security issues like phishing, identity theft, card fraud, and unauthorized access. Artificial intelligence (AI) plays an important role in improving online payment security, particularly through intelligent data collection techniques.

**3. Research Tools & Instruments**

Online payment systems are extremely sensitive to fraud, phishing, identity theft, and cyber-attacks. Artificial intelligence (AI) offers improved solutions for detecting fraud, anomalies, and ensuring transaction security. To gather, evaluate, and validate data in this field of research, appropriate tools and equipment are required.

**4. Sampling Procedure**

In research, the sampling technique specifies how participants, data sources, or systems are drawn from a larger population in order to appropriately reflect the study. A study on online payment security utilizing AI must include real-world scenarios, security threats, and user experiences.

**5. Data Analysis Techniques**

E-commerce, mobile wallets, and digital banking are all contributing to the rapid growth of online payment systems. However, this expansion has attracted cybercriminals who use weaknesses to commit fraud, identity theft, and unlawful transactions. Traditional security measures (such as passwords and OTPs) are frequently insufficient. Artificial intelligence (AI) combined with data analysis techniques improves online payment security by detecting fraud patterns, abnormalities, and threats in real-time.

## V. DIAGRAM

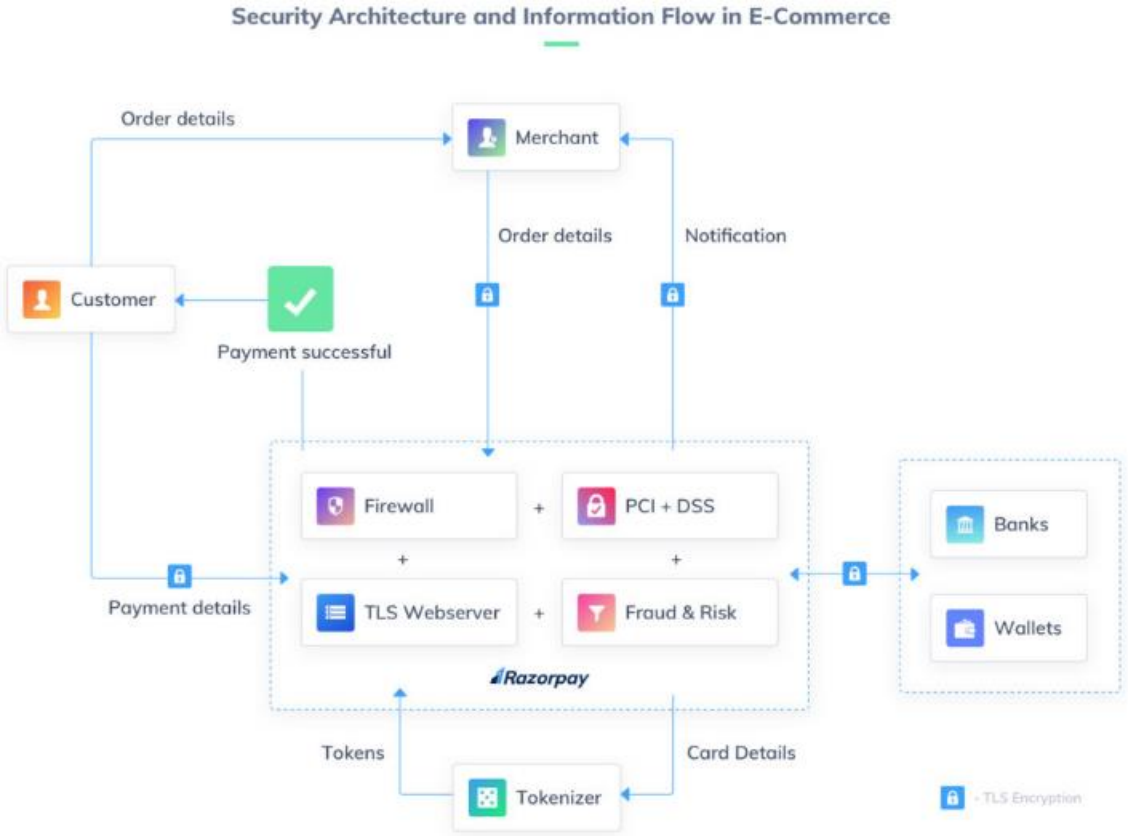

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 9, September 2025

DOI: 10.17148/IARJSET.2025.12927




## VI. RESULTS

AI in Payment Transactions: How It Works. AI systems monitor every stage of a payment transaction to detect fraud and automate payment processing. They use data points from previous transactions to determine whether a payment was successful. The system examines history, location, and amount to detect unusual behaviour.

## VII. CONCLUSION

Artificial Intelligence (AI) has emerged as a transformative tool in enhancing online payment security. By leveraging machine learning, anomaly detection, and predictive analytics, AI systems can effectively identify fraudulent transactions, reduce cyber threats, and protect sensitive financial information in real time. The integration of AI not only strengthens trust between consumers and financial institutions but also ensures a seamless and secure digital payment experience. As online transactions continue to grow, AI-driven security solutions will remain essential in mitigating risks, improving efficiency, and fostering confidence in the digital economy.

## REFERENCES

[1]. Btoush, E. A. L. M., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). *A systematic review of literature on credit card cyber fraud detection using machine and deep learning.* PeerJ Computer Science, 9:e1278.
https://pmc.ncbi.nlm.nih.gov/articles/PMC10280638/

[2]. Rojan, Z. (2024). *Financial Fraud Detection Based on Machine and Deep Learning: A Review.* Indonesian Journal of Computer Science, 13(3).
https://ijcs.net/ijcs/index.php/ijcs/article/view/4059

[3]. Chen, Y., Zhao, C., Xu, Y., Nie, C., & Zhang, Y. (2025). *Year-over-Year Developments in Financial Fraud Detection via Deep Learning: A Systematic Literature Review (2019-2024).* ArXipreprint.
https://arxiv.org/abs/2502.00201

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License

DOI: 10.17148/IARJSET.2025.12927

[4]. Salloum, S. A., Gaber, T., Vadera, S., & Shaalan, K. (2021). *Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey.* Procedia Computer Science, 189, 19–28.
https://www.sciencedirect.com/science/article/pii/S1877050921011741

[5]. Tong, L., Ji, S., Li, B., & Wang, T. (2022). *Federated Learning for Financial Applications.* MDPI Data, 7(2), 38.
https://www.mdpi.com/2504-2289/6/2/38

[6]. Guidotti, R., Monreale, A., Ruggieri, S., Turini, F., Giannotti, F., & Pedreschi, D. (2018). *A Survey of Methods for Explaining Black Box Models.* arXiv preprint.
https://arxiv.org/abs/1802.01933

[7]. Kshetri, N. (2017). *Blockchain's Roles in Strengthening Cybersecurity and Protecting Privacy.* Telecommunications Policy, 41(10), 1027–1038.
https://www.sciencedirect.com/science/article/pii/S0267364917303336

[8]. Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G. (2015). *Calibrating Probability with Undersampling for Unbalanced Classification.* In *Computational Intelligence, 2015 IEEE Symposium* (pp. 159–166).
https://link.springer.com/chapter/10.1007/978-3-319-17290-3_25

© IARJSET This work is licensed under a Creative Commons Attribution 4.0 International License 