

AI in Digital Payments: Security and Fraud Detection

Jenisa Nazareth Benka¹, Aarti Sanjay Gawai²

¹Assistant Professor, Department of Information Technology and Computer Science, D.G. Ruparel College²

Student, Department of Information Technology and Computer Science, D.G. Ruparel

College, Mumbai, Maharashtra, India

jenisabenka08@gmail.com¹, aartigawai1611@gmail.com²

Abstract - The rapid adoption of digital payments has raised the need for robust security and trustworthy fraud detection. This research explores the impact of Artificial Intelligence on digital payment security and fraud detection. The study employs a review-based methodology, reviewing existing research on AI and ML techniques for digital payment fraud detection. The reviewed studies reveal that supervised learning, anomaly detection, Frauddeep learning and hybrid AI models can detect suspicious transactions, detect new fraud, monitor in real time, and decrease false positives. Behavioural analysis and explainable AI make the fraud detection systems more reliable and transparent. The results suggest that AI-based approaches can provide more flexible and efficient fraud detection than traditional rule-based approaches. However, challenges around data quality, privacy, model transparency, regulatory compliance and changing fraud patterns remain important. The study results show that the right implementation of standard artificial intelligence can increase digital payment safety, better fraud detection, and develop secure and trustworthy digital payment systems.

Key Words: Artificial Intelligence, Digital Payments, Fraud Detection, Machine Learning, Payment Security, Anomaly Detection.

1. INTRODUCTION

Online transactional methods have become a crucial component of modern financial transactions as they offer fast, convenient, and accessible ways of transferring money. The way individuals and businesses conduct financial transactions has changed with the increasing use of online banking, mobile wallets, payment applications, cards, and real-time payment platforms. In India, UPI has played a significant role in the expansion of digital payments by allowing quick peer-to-peer and peer-to-merchant transactions.

The proliferation of digital payments, however, has also introduced increased risk of financial fraud and cybersecurity threats. Users and payment systems are attacked by fraudsters using methods such as phishing, QR code manipulation, account takeover, impersonation and social engineering. Moreover, the increasing volume of transactions makes it difficult for conventional fraud detection methods to detect suspicious activities in a timely and accurate manner.

Traditional rule-based systems largely rely on predefined rules and static conditions. These methods can identify known fraud patterns, but can struggle with new and evolving fraud. Artificial Intelligence (AI) and Machine Learning (ML) provide a more flexible solution by analysing transaction data, highlighting abnormal behaviour, and catching suspicious transactions in real time. The different AI and ML techniques studied to improve digital payment fraud detection are supervised learning, anomaly detection, neural networks and hybrid models. These approaches can help to identify both known and emerging fraud patterns and reduce false positive results.

However, issues like data quality, privacy, model transparency, imbalanced datasets and changing fraud patterns still need to be addressed. That is why, in this research, we consider the role of Artificial Intelligence in enhancing the security of digital payments and fraud detection. We consider current AI solutions, their pros and cons, and their capability to ensure higher safety and reliability of the digital payment system.

2. REVIEW OF LITERATURE

Fraud detection in online banking and digital payments is an area of significant interest due to the emergence of digital financial services. It has been established from the review of literature that rule-based fraud detection methods have certain limitations because they rely heavily on pre-defined rules and lack flexibility when faced with emerging fraud patterns.

As the number and complexity of transactions continue to rise in the digital world, machine learning approaches for fraud detection are gaining popularity. Logistic Regression, Decision Tree, Random Forest, and XGBoost are some of the supervised machine learning algorithms that can help detect whether a transaction is fraud or not by analysing past transaction records. There has been analysis of the use of unsupervised learning approaches in scenarios where there is inadequate labelled fraud data.

Unsupervised approaches like Isolation Forest and Autoencoders help in identifying transactions that differ from the usual transaction pattern. This helps in detecting unusual behaviours that have not occurred in the training data. In addition, some research has looked at a combination of supervised classification and anomaly detection approaches. The idea behind this combination is to catch fraud that matches known patterns as well as fraud that does not. The literature review also points to a second important area: analysing behaviour and detecting fraud in real time with AI.

The AI system can analyse transaction characteristics such as the amount of the transaction, transaction frequency, location, device data, merchant information, and the history of transaction behaviour to identify suspicious activity. Real-time detection is very significant in the context of digital payments, as a fraudulent transaction can inflict financial damage on an organisation within a very short time. Explainable Artificial Intelligence (XAI) is another focus area for research, as financial organisations require explanations of why the AI system has categorised a transaction as suspicious.

However, despite the developments in the field of AI-supported fraud detection, there are still some problems and research directions that require more attention. The problem of imbalanced fraud datasets is inherent in many studies, since the number of legitimate transactions is much higher than that of fraudulent ones, and labelled fraud datasets may not be available. There is also a possibility of false positives, since identifying legitimate transactions as fraudulent can be annoying for customers. Moreover, there are such problems as concept drift, computational costs, privacy, and explainability. All told, bringing AI into this space should make fraud detection considerably more effective.

3. METHODOLOGY

This research uses literature review research approach based on secondary data analysis. Ten research articles relating to Artificial Intelligence, Machine Learning, digital payment security and fraud detection have been chosen for further research. The selected research papers consist of research articles about digital payment fraud, UPI security, machine learning techniques, anomaly detection, hybrid systems, deep learning, Explainable AI and emerging AI-based solutions. The main reason for choosing these research papers was to learn about the existing state of development of AI-based techniques for improving digital payment security.

The research papers have been evaluated on the basis of the fraud detection techniques used by them, sources of their data, machine learning algorithms used, methods of security, findings, strengths, weaknesses, and future prospects. The various methodologies such as supervised learning, unsupervised learning, hybrid learning, deep learning, and anomaly detection have been analysed. A comparison has been made between different studies to find out the applications of these methods in classifying and detecting fraudulent transactions.

The methodology also looks at the overall process of fraud detection using AI technology, which involves the processes of collecting transaction data, data preprocessing and preparation, feature extraction or feature engineering, developing and training the model, classification of fraud or detecting anomalies, and creation of fraud alerts. Information related to behavior including transaction amount of transaction, frequency of transactions, transaction location, device information, merchant information, and past transaction records, was also analysed from the studies considered in this analysis. This process was analysed to learn about how transaction information is used as input for fraud detection models.

In the end, the results of the chosen research papers were compared and classified according to main themes associated with the security of digital payments, efficiency of fraud detection, advantages, limitations, and future development. Special emphasis was placed on such problems as imbalanced datasets, scarcity of labelled data, false positives, evolving types of fraud, privacy, transparency, regulatory compliance, and real-time deployment of systems. This comparative analysis of research papers allowed not only finding common results but also identifying gaps that will contribute to future research in developing adaptive, transparent, and scalable AI-based fraud detection for digital payments.

4. BODY OF PAPER

4.1 DigiStal Payments and Security Challenges

With the rise in technology and innovation, digital payment systems have become a vital element of financial transactions. Online banking systems, wallets, cards, and other payment systems have altered the process of sending money. In the Indian context, the Unified Payments Interface (UPI) has been instrumental in making digital payments possible through real-time peer-to-peer transactions. But at the same time, with the rising number of digital transactions, the threat of financial fraud has increased.

There are several ways in which digital payments can be defrauded, for instance, by phishing, QR-code abuse, account takeover, impersonation, merchant fraud, and social engineering. Fraudsters constantly develop new ways to take advantage of users and vulnerabilities within digital payment systems. With the many transactions being made daily, it is challenging to manually detect each suspicious transaction. Thus, there needs to be some security measures in place that will allow detection of any possible fraud activity.

Because of the complexity of fraud nowadays, there is an increased demand for fraud detection techniques to be adaptive. While the traditional method can detect known threats, any changes in the patterns of such threats necessitate an adaptive system to learn about the transaction data and detect abnormal behavior. This has made AI and ML popular for enhancing digital payment security.

4.2 Artificial Intelligence and Machine Learning for Fraud Detection

The current anti-fraud techniques mostly rely on rules and thresholds that are pre-defined by humans. These approaches are good for recognising the patterns that they were designed for; however, they cannot be adapted to new fraud methods. With Machine Learning, transaction patterns can be learned from historical data by the models, which will then be used to recognise abnormal activities. The presented studies reveal that ML algorithms are becoming a popular approach for fraud detection.

In supervised learning algorithms, labelled transaction data is used for classifying whether a transaction is fraudulent or non-fraudulent. Some of the algorithms that are examined for this purpose are the Decision Tree algorithm, Random Forest algorithm, Logistic Regression algorithm, and the XGBoost algorithm. The XGBoost algorithm is specifically effective for detecting financial fraud because it can accommodate complex interactions between transaction attributes and imbalanced datasets. But the problem with the supervised learning model is the availability of labelled fraud data.

Another way of doing this is through the application of unsupervised learning by finding transactions that are vastly different from the typical behaviour. Unsupervised learning methods like Isolation Forest and Autoencoders can help find out these anomalies even without relying entirely on labelled instances of fraud. For instance, the Isolation Forest method can find anomalies in transaction amounts, frequency, location, and devices used.

Current studies are also interested in AI hybrid models that consist of both supervised and unsupervised approaches. In the case of the supervised approach, one is able to detect the already existing patterns of fraud, whereas in the case of the anomaly detection approach, one is able to detect unusual behaviour that was not detected during the training process.

AI techniques, including Deep Learning, have also been investigated for fraud detection in digital payments. Some of the studies in the selected research papers have examined the use of models like LSTM, CNN, and hybrid models of deep learning to analyse sequential and complicated transaction data. Newer approaches, including LLMs, have been applied for scam detection. However, problems like explainability and computational costs still persist.

Technique	Approach	Main Application
Logistic Regression	Supervised	Fraud classification
Random Forest	Supervised	Transaction classification
XGBoost	Supervised	Known fraud detection
Isolation Forest	Unsupervised	Anomaly detection
Autoencoder	Unsupervised	Abnormal behaviour detection
Hybrid Models	Combined	Known and emerging fraud detection

Table-1: Comparison of AI Techniques Used in Fraud Detection

Various AI techniques have various abilities when it comes to detecting fraudulent transactions. Supervised models are helpful in detecting known fraud cases, but unsupervised models assist in detecting unusual behaviors in transactions. Hybrid models apply the two techniques in order to be able to detect known and emerging cases of fraud. Table 1 shows some of the AI techniques and their application.

4.3 AI-Based Security and Fraud Detection in Digital Payments.

AI-enabled fraud detection systems help secure online payments through the examination of transactions and detecting actions that do not correspond to regular user behavior. When performing such behavioral analysis, a number of factors could be taken into account, including the amount and frequency of the transaction, location, merchant category code, device information, and history of activities.

Real-time fraud detection is very crucial in online payment processing because there could be losses in a small period of time due to fraudulent transactions. Such systems using AI can come up with fraud probabilities or anomaly scores and based on these findings decide whether the transaction is a potential case of fraud or not. There are hybrid systems that can integrate fraud probabilities and anomaly scores.

Explanation of Artificial Intelligence (XAI) is yet another aspect of financial security that relies on artificial intelligence. The financial sector must be able to explain why certain transactions are considered suspicious by their system. One way of achieving this is through the use of algorithms like SHAP, which help in identifying how different attributes of the transaction contribute to the detection of fraud.

The steps involved in AI-based fraud detection are linked and include the first step of the digital payment transaction followed by collecting data on the transaction. After collecting the data, the analysis is conducted to determine the features as well as the abnormal behavior. AI and ML algorithms can predict the fraud probabilities or anomaly scores that will assist in decision making.

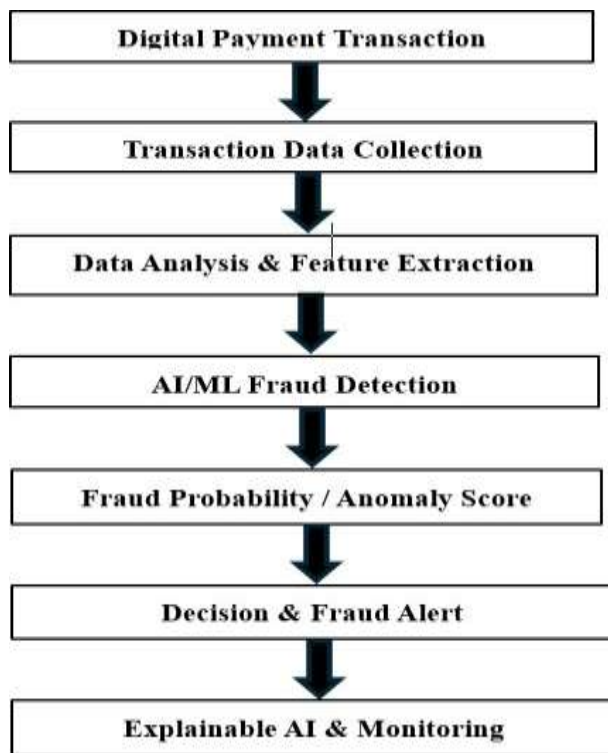


Fig.1. AI-Based Digital Payment Fraud Detection Process

This process is founded upon the architecture presented in the analysed research paper, where supervised learning, anomaly detection, hybrid decision-making, and explainability are employed.

4.4 Benefits, Challenges and Future Scope of AI in Digital Payment Security.

Several advantages of using artificial intelligence for digital payment security are revealed by the analysed studies. AI allows processing a lot of data from transactions, monitor them in real time, recognize suspicious behavior, and spot both traditional and novel fraud patterns.

The hybrid approach allows combining various types of fraud recognition, and Explainable AI allows increasing transparency and assisting in understanding of the fraud predictions made. Thus, AI-based solutions are more flexible than those relying solely on rules. That said, adopting AI in this space comes with real difficulties. For one, genuine fraud cases make up only a tiny fraction of payment data, so the pool of labelled fraud examples available for training can end up quite small. Second, there can be false positives in the process of using AI models, and changing patterns of fraud can make models outdated. Finally, privacy issues, regulatory compliance, explainability, and computational demands are other problems of using AI in finance.

Future areas of research include building adaptive hybrid models, enhancing explainable AI techniques, and privacy-preserving techniques, and real-time detection techniques. The area of federated learning has also been researched to build fraud detection models where no direct data exchange from the customer takes place at all. Advanced machine learning techniques, such as scam detection using large language models, are some of the other areas of research that might be explored.

5. CONCLUSIONS.

AI and Machine Learning have now become the key technologies to enhance the security of digital payment systems and detect any instances of fraud. The literature review reveals that both supervised learning, unsupervised anomaly detection, deep learning, and hybrid AI systems can be used to detect suspicious behaviour and enable quicker fraud detection. In comparison to the traditionally used rule-based systems, the use of AI is more flexible when it comes to the analysis of large amounts of transaction data.

Various types of AI bring varying strengths when it comes to the detection of frauds. Examples of supervised models include Logistic Regression, Random Forest, Decision Tree, and XGBoost which are helpful when it comes to detecting fraud cases that are already known. Unsupervised learning techniques like Isolation Forest and Autoencoders help in detecting abnormal behavior of transactions. The hybrid approach combines all these techniques to enhance the detection of known and emerging fraud cases. On the other hand, some limitations are presented by the selected studies when it comes to the application of AI to enhance security in digital payments. This is because the reviewed studies have indicated the limitations of unbalanced datasets, the absence of labelled fraud data, high false-positive rates, privacy problems, nonexplainable nature, computational demands, regulation, and constant changes in fraud schemes.

Future research could consider working on creating adaptive hybrid systems, increasing explainability of AI, improving methods that protect privacy, and developing real-time fraud detection tools. Methods such as federated learning and novel AI systems may help to enhance the security of payments without compromising data privacy.

Apart from developing technologies, proper security procedures, regulatory compliance, and user knowledge are also vital. When we pull this all together, AI holds real promise for making digital payments more secure, more reliable, and more efficient. Intelligent fraud detection, explainable decisions, privacy protection, monitoring, and responsible deployment together will make it far easier for financial institutions to stay ahead of fraud and keep digital payments secure enough that users can genuinely rely on them.

ACKNOWLEDGEMENT

This research would not have taken shape without the steady guidance of my teachers, and I am thankful to each of them for it. I am also grateful to my college for giving me the facilities and support I needed to carry this research through to the end. My thanks also go to my classmates and colleagues for their useful suggestions and encouragement. And finally, to everyone whose help, whether they realised it or not, made finishing this research possible.

REFERENCES

- [1] J. Bari, R. Pawar, I. Holkar, and R. Dekate, "Strengthening Digital Payment and Security using AI, Big Data, and Cybersecurity in India," *Advanced International Journal for Research*, vol. 7, no. 2, 2026. <https://doi.org/10.63363/aijfr.2026.v07i02.4814>
- [2] D. Dahiphale et al., "Enhancing Trust and Safety in Digital Payments: An LLM-Powered Approach," 2024. <https://doi.org/10.48550/arXiv.2410.19845>
- [3] A. B. Lahari, K. K. Kumar, B. Neelima, K. Raghu, and K. P. Varsh, "Digital Payment Fraud Detection Using Machine Learning," *International Journal for Multidisciplinary Research*, vol. 8, no. 2, 2026. <https://www.ijfmr.com/researchpaper.php?id=73671>
- [4] V. Chang et al., "Digital payment fraud detection methods in digital ages and Industry 4.0," *Computers and Electrical Engineering*, vol. 100, Art. No. 107734, 2022. <https://doi.org/10.1016/j.compeleceng.2022.107734>
- [5] M. Sorinola and K. Hamed, "Machine Learning for Digital Payment Fraud Detection in Financial Institutions: A Review of Methods, Explainability, and Performance," *Cureus Journal of Computer Science*, 2026. <https://doi.org/10.7759/s44389-026-00149-0>
- [6] L. Koduru, "Harnessing AI to Enhance Security in Digital Payments: Detection of High-Risk Users and Mitigation of Financial Crime," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 12, no. 17s, pp. 918–927, 2024. <https://www.ijisae.org/index.php/IJISAE/article/view/7626>
- [7] A. Shivarudraiah, "AI-Powered Threat Detection in Digital Payments: Addressing Cyber Fraud," *International Journal of Artificial Intelligence, Data Science, and Machine Learning*, vol. 3, no. 4, pp. 19–26, 2022. <https://doi.org/10.63282/3050-9262.IJAIDSML-V3I4P103>
- [8] S. M. S. Shaikh and G. N. A., "AI Based Transaction Anomaly and Fraud Detection System," *International Research Journal on Advanced Engineering Hub*, vol. 4, no. 3, pp. 1160–1169, 2026. <https://doi.org/10.47392/IRJAEH.2026.0164>
- [9] N. B. Chakka and S. S. Saheb, "A Hybrid Autoencoder-XGBoost Framework for High-Performance UPI Fraud Detection," *Proceedings of Engineering and Technology Innovation*, vol. 33, pp. 93–105, 2026. <https://doi.org/10.46604/peti.2026.16002>
- [10] A. Davitaia, "Artificial Intelligence and machine learning in fraud detection for digital payments," *International Journal of Science and Research Archive*, vol. 15, no. 3, pp. 714–719, 2025. <https://doi.org/10.30574/ijrsra.2025.15.3.1784>
- [11] A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," *Journal of Network and Computer Applications*, vol. 68, pp. 90–113, 2016. <https://doi.org/10.1016/j.jnca.2016.04.007> 2026.
- [12] N. F. Ryman-Tubb, P. Krause, and W. Garn, "How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark," *Engineering Applications of Artificial Intelligence*, vol. 76, pp. 130–157, 2018. <https://doi.org/10.1016/j.engappai.2018.07.008> (ScienceDirect)
- [13] A. Ali, S. Abd Razak, S. H. Othman, T. A. E. Eisa, A. Al-Dhaqm, M. Nasser, T. Elhassan, H. Elshafie, and A. Saif, "Financial fraud detection based on machine learning: A systematic literature review," *Applied Sciences*, vol. 12, no. 19, Art. no. 9637, 2022. <https://doi.org/10.3390/app12199637> (MDPI)
- [14] K. G. Al-Hashedi and P. Magalingam, "Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019," *Computer Science Review*, vol. 40, Art. no. 100402, 2021. <https://doi.org/10.1016/j.cosrev.2021.100402>

- [15] L. Hernandez Aros, L. X. Bustamante Molano, F. Gutierrez-Portela, J. J. Moreno Hernandez, *et al.*, “Financial fraud detection through the application of machine learning techniques: A literature review,” *Humanities and Social Sciences Communications*, vol. 11, Art. no. 1130, 2024. <https://doi.org/10.1057/s41599-024-03606-0>
- [16] “Credit card fraud detection in the era of disruptive technologies: A systematic review,” *Journal of King Saud University Computer and Information Sciences*, 2022. <https://doi.org/10.1016/j.jksuci.2022.11.008>
- [17] T. Awosika, R. M. Shukla, and B. Pranggono, “Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection,” arXiv, 2023. <https://doi.org/10.48550/arXiv.2312.13334> (arXiv)
- [18] X. Sha, “Research on financial fraud algorithm based on federal learning and big data technology,” arXiv, 2024. <https://doi.org/10.48550/arXiv.2405.03992> (arXiv)
- [19] A. Sawaika, S. Krishna, T. Tomar, D. P. Suggisetti, A. Lal, T. Shrivastav, N. Innan, and M. Shafique, “A privacy-preserving federated framework with hybrid quantum-enhanced learning for financial fraud detection,” arXiv, 2025. <https://doi.org/10.48550/arXiv.2507.22908> (arXiv)
- [20] P. Panth and N. Nigam, “Scalable and verifiable federated learning for cross-institution financial fraud detection,” arXiv, 2026. <https://doi.org/10.48550/arXiv.2604.23437> (arXiv)