AI Based Fraud Detection Models for Digital Payment Security

Ms. Adithya Ramanan[1], Albin Jinu[2], Filna John[3]

[1]Assistant Professor, Department of Computer Science, MG University, Santhigiri College of Computer Sciences, Vazhithala, Kerala, India, 686662

[2,3]Student, Department of Computer Science, MG University, Santhigiri College of Computer Sciences, Vazhithala, Kerala, India,686662

DOI: https://doi.org/10.51584/IJRIAS.2026.11110028

Received: 24 October 2026; Accepted: 29 October 2026; Published: 23 November 2026

ABSTRACT

The rapid growth of digital payments has increased the need for reliable methods of identifying fraudulent transactions. It's hard for traditional rule-based systems to keep up with new ways of attacking and large amounts of transaction data. Using machine learning to detect fraud on digital payment platforms is smarter and more flexible than other methods. Using real-time monitoring and predictive analytics, different supervised and unsupervised learning models can help identify unusual transaction patterns, make detection more accurate, and reduce false positives. Even with these changes, there are still significant problems, such as data imbalance, privacy issues, model interpretability, and difficulty in computing. Explainable AI and advanced learning architectures are two new methods that are making fraud detection systems more reliable and useful in today's financial world.

Index Terms*:* Artificial Intelligence(AI), Digital Payment Security, Fraud Detection, Machine Learning, Anomaly Detection, Deep Learning, Financial Cybersecurity, Predictive Analytics, Data imbalance.

I. INTRODUCTION

Digital payments, including card transactions, mobile wallets, online banking, and instant bank transfers, support convenient and rapid financial activity. At the same time, digital channels expose customers and payment providers to several forms of fraud. Some transactions are initiated by an attacker without the account holder’s permission; in other cases, a customer is deceived into authorising a transfer to a fraudster. These situations differ operationally and should not be treated as one identical classification problem.

Traditional rule-based systems can identify known indicators, such as unusual transaction amounts or repeated failed logins. However, rules may require frequent manual updates and can miss patterns that do not match predefined conditions. Machine-learning models can estimate risk from historical transactions and behavioral signals, while anomaly-detection techniques can flag activity that differs from a learned baseline. A systematic literature review by Ali et al. describes a broad range of machine-learning techniques used in financial-fraud research and highlights continuing issues involving datasets, evaluation, and model selection.

Fraud detection is not simply a question of maximising classification accuracy. Fraud is usually a minority class, so a model can appear accurate while missing many fraudulent transactions. A useful system must balance missed fraud, unnecessary customer interruptions, investigation workload, decision latency, and the value of losses prevented. This paper reviews the main model families and considers how they can be combined in a practical digital-payment security process.

II. OBJECTIVES OF THE STUDY

The main goals of this research are:

1. To define and detect significant fraud occurrences in Internet-based payments.

2. To analyse how AI based models are used to detect and prevent digital payment fraud.

3. To compare various machine learning methods such as supervised and unsupervised and deep learning methods.

4. To assess the most important issues encountered during the implementation of AI-

based fraud detection systems.

5. To investigate the possible future development of AI-based fraud prevention *systems.*

III. METHODOLOGY

The rese1arch employs the qualitative research approach involving secondary data analysis. The study is held as a systematic literature review of the literature in terms of the analysis of the existing academic publications, conference papers, scholarly articles concerning the fraud in the digital payment systems and AI-based techniques of fraud detection. Academic databases were used to find relevant sources using keywords digital payment fraud, credit card fraud detection, machine learning in fraud detection, anomaly detection, and deep learning models. The reviewed studies were used to find out the general types of fraud, AI applications employed, and the main implementation issues. The supervised, unsupervised, and deep learning methods were compared in a comparative analysis to investigate their applicability to various fraud situations. The methodology focuses on the synthesis of the results of the existing research instead of creating or testing a new model and, therefore, gives a broad overview of the AI-driven fraud detection processes in online payment settings.

3.1 Conceptual Foundation of Machine Learning in Fraud Detection

Artificial Intelligence (AI) boosts fraud detection within digital payment systems by providing an opportunity to analyze financial transactions on the basis of data and react to it. In contrast to conventional rule-based frameworks, which are based on the pre-established conditions, AI frameworks are trained on the basis of the vast amount of historical data to detect suspicious activity. The techniques of supervised learning follow the principles of labelled datasets to classify transactions as well as fraudulent or legitimate, whereas unsupervised learning methods identify concealed patterns and irregularities without labels. The approaches enable systems to detect ongoing and new patterns of fraud. Predictive analytics and anomaly detection are some of the essential elements of AI-fraud prevention. Fraudulent transactions are also few relatives to normal transactions; thus, this means the anomaly detection techniques are aimed at detecting an abnormality in the transactions. Also, predictive models are used to estimate the likelihood of fraud in the future by examining the past. But changes in strategy of fraud also cause concept drift, which evolves with time. AI systems respond to this issue by providing continuous learning processes, which enables flexibility and sustainability in the changing digital worlds.

IV. TYPES OF FRAUD IN DIGITAL PAYMENT SYSTEMS

Online payment systems have made money much more convenient, yet at the same time,they have provided a platform on which all kinds of fraud can be perpetrated. Online transactions, authentication methods, and user behavior can be used by the fraudsters tocarry out unauthorized operations. As discussed below, the most prevalent forms of fraud in online payment settings are:

4.1 Credit Card Fraud

One of the most common digital payment fraud is credit card fraud. It happens when the card information is stolen and used by an unauthorized person to complete the transactions without the permission of the cardholder. This would include physical theft of cards, skimmers or even data theft leading to leakage of card details. The large amount of online and offline transactions is a significant issue that financial institutions are struggling to deal with in real time to detect fraudulent patterns.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue XI November 2026

4.2 Card Not Present Fraud

Card-Not-Present (CNP) fraud is when a real card is not needed in the transaction like online shopping, mobile payments and phone-based payments. Merchants will not be able to physically check the card and the fraudsters use the stolen card information to purchase without authorization. This form of fraud has increased due to the quick development of the e-commerce system and hence it is a significant issue in the area of security in terms of digital payments.

4.3 Account Takeover Fraud

Account takeover fraud is a type of fraud where attackers illegally access the financial account of a user by stealing a user login or credential using phishing or malware or data breaches. After gaining access, the fraudster will be able to transfer funds, alter account information or conduct unwarranted transactions. This form of fraud is especially risky with the digital wallet and online banking facility as user authentication is at the heart of security.

4.4 Phishing and Electronic Payment Fraud.

Phishing and electronic payment fraud, are fraudulent methods of deceiving the person into disclosing sensitive information like passwords, OTPs, or card information. There is also the practice of fraudsters making fraudulent websites, emails, or messages that appear to be real financial institutions. Along with the growth of digital communication channels, phishing attacks have become more sophisticated, and they are a significant threat to the users of digital payments.

V.AI BASED FRAUD DETECTION TECHNIQUES

Digital payment systems are also important in preventing and detecting fraud using artificial intelligence techniques. These models detect suspicious behavior by using transactional and behavioral data in real time. The key AI-powered models that are applied in credit card fraud, card-not-present fraud, account takeover, and phishing- related fraud detection are described below.

5.1 Supervised Learning Models

The supervised learning models are trained on labelled data in which we have transactions that are classified as fraudulent or legitimate. These models are very effective in the detection of familiar fraud patterns and they are prevalent in financial institutions.

5.1.1 Logistic Regression

Logistic Regression is usually applied when the classification is binary in fraud detection and the transactions are classified into fraud and legitimate. It approximates the risk of fraud with regards to attributes like transaction volume, frequency, and location. It is highly interpretable and simple to use; therefore, it can be a benchmark model of credit card fraud detection.

5.1.2 Decision Tree

Decision Trees categorize transactions through splitting information on the basis of feature conditions. They are simple to interpret and assist identify the pattern of rule- based fraud, thus are applicable in the identification of suspect card handling and out of the ordinary login activities in the case of account takeover.

5.1.3 Random Forest

Random Forest is an ensemble learning technique which is an integration of several decision trees aimed at detecting better and minimizing overfitting. It works effectively on skewed data that occur frequently in credit card fraud and card-not-present fraud detection.

ISSN No. 2454-6194 | DOI: 10.51584/IJRIAS |Volume XI Issue XI November 2026

5.1.4 Support Vector Machine (SVM)

The Support Vector machines are used to categorize the transactions by determining the best line between fraud and genuine transactions. SVM is useful in the high-dimensional data setting and can be used extensively to identify sophisticated frauds.

5.2 Unsupervised and Anomaly Detection Models

When there is a small amount of labelled data, there is the use of unsupervised models.Such methods are used to detect abnormalities in normal transactions hence can be applied to detect new and unknown types of frauds.

5.2.1 K-Means Clustering

K-Means clusters the transactions according to similar patterns. The transactions that do not belong to normal clusters can be signs of an attempt to commit fraud, especially in cases of account takeover and phishing.

5.2.2 Single-Class Support Vector Machine.

One-Class SVM is applied to detect anomalies by gaining knowledge of the usual transactions and detecting anomalies. It is especially applicable in the situation when fraudulent examples are limited.

5.3 Deep Learning Models

Deep learning methods can also encode complex and nonlinear transactions patterns over large data sets, hence it can be applicable in detection of advanced forms of fraud.

5.3.1 Artificial Neural Networks (ANN).

ANN models are the models that imitate the behavior of a network of neurons to analyze the behavior of transactions. They are successful in detecting fraudulent concealed patterns in both credit cards and digital payment platforms.

5.3.2 Deep Neural Networks (DNN)

Deep Neural Networks have several hidden layers which represent intricate data associations. They improve the fraud detection accuracy in large-scale online payment service providers and keep up with changing fraud techniques.

VI. IMPLEMENTATION AND SUSTAINABILITY

The effective adoption of AI-related fraud detection software in online payment systems needs a strong technology infrastructure and real-time monitoring solutions. Banks incorporate machine learning algorithms with real-time transaction processing systems to determine risk scores in real-time then approve or decline the transaction. These systems also make use of massive transaction volumes, secure data pipes, and scalable computing to guarantee the effective model performance. The accuracy of models requires regular retraining, especially when the trends of fraud change at a high rate. The sustainability of AI based fraud detection requires flexibility, cost effectiveness and compliance with regulations. The continual learning models allow systems to revise detection systems without developing them entirely. Nevertheless, the high cost of maintenance of large datasets and complex models can augment computational expenses. Sustainability in the long term also entails having privacy of data, transparency and adherence to financial regulations. Thus, the introduction of explainable and resource- efficient models of AI is vital in ensuring confidence and stability of operations within digital payment ecosystems.

VII. CHALLENGES FACED

Though AI-created models are very effective in detecting fraud in digital payment systems, there are numerous obstacles limiting their performance. The imbalance of the data is one of the main aspects because the

percentage of fraud transactions is very low in comparison with the total transaction. Such an imbalance may result in biased models

that emphasize legitimate transactions thus lowering the sensitivity of fraud detection. The other significant challenge is concept drift whereby the trends of fraud keep changing with time. Models that are trained using historical data can be not as effective because new strategies of fraud can appear. Also, the false positive rates might be high, which is also harmful to customer experience as it will be blocking real transactions. The issue of model interpretability is also an issue, especially in deep learning systems that can be considered a black box that makes it harder to regulate and more challenging to be transparent.

FUTURE SCOPE

The future trends of AI-based fraud detection are directed towards enhancing the flexibility, precision, and privacy. Such approaches as federated learning allow training models together with other institutions without the exchange of sensitive customer information and increase privacy protection. Those models that integrate supervised and unsupervised methods are likely to enhance the detection of the known and emerging pattern of fraud. Moreover, explainable AI (XAI) is being developed to make the process of fraud detection decision-making more transparent, allowing the financial institutions to comply with regulatory requirements. Real-time systems of continuous learning that keep models updated will also be of great importance in countering the changing fraud schemes in dynamic digital payment settings.

CONCLUSION

The fast development of the digital payment systems has greatly increased the danger of financial fraud, and the use of the classical rule-based detection approach can no longer be relevant in the contemporary settings. This paper reviewed the most relevant forms of digital payment fraud namely credit card fraud, card-not-present fraud, account takeover and phishing-related fraud and has discussed how Artificial Intelligence can be used to overcome these difficulties. Deep learning models and unsupervised anomaly detection, and supervised learning are important to detect suspicious patterns and improve the accuracy of real-time fraud detection. Although AI-based systems are much more flexible and efficient, issues like imbalance in the data, concept drift, and model interpretability are still influential. Constant improvements of adaptive and explainable AI algorithms are necessary to enhance the mechanisms of preventing fraud and to provide secure digital financial ecosystems.

REFERENCES

1. A. Ali, S. A. Razak, S. H. Othman, T. A. Eisa, A. A. Al-Dhaqm, M. Nassar, T.Ellahassan, H. Elshafie, and A. Saif, "Financial fraud detection based on machine
2. learning: A systematic literature review," Applied Sciences, vol. 12, no. 19, Art. no. 9637, 2022.
3. S. Omar, A. Ngadi, and H. H. Jebur, "Machine learning techniques for anomaly detection: An overview," International Journal of Computer Applications, vol. 79, no. 2,Oct. 2013.
4. S. Teker, D. Teker, and I. Orman, "Digital payment systems: A future outlook," Press Academia Procedia, vol. 15, no. 1, p. 175, 2022. https://doi.org/10.17261/Pressacademia.2022.1613
5. G. K. Patra, S. K. Rajaram, N. Boddapati, and C. Kuraku, "Advancing digital payment systems: Combining AI, big data, and biometric authentication for enhanced security," SSRN Electronic Journal, Sep. 2024. https://ssrn.com/abstract=4945882
6. K. RamaKalyani and D. UmaDevi, "Fraud detection of credit card payment system by genetic algorithm," International Journal of Scientific & Engineering Research, vol. 3, no. 7, Jul. 2012.
7. I. D. Mienye and N. Jere, "Deep learning forcredit card fraud detection: A review of algorithms, challenges, and solutions," IEEE Access, 2024.
8. S. Makki, Z. Assaghir, Y. Taher, R. Haque, M.-S. Hacid, and H. Zeineddine, "An
9. experimental study with imbalanced classification approaches for credit card fraud detection," IEEE Access, vol. 7, pp. 1–13, 2019.

10. M. Di Martino, F. Decia, J. Molinelli, and A. Fernández, "Improving electric fraud detection using class imbalance strategies," Instituto de Ingeniería Eléctrica, Facultad de Ingeniería, Universidad de la República, Montevideo, Uruguay, 2020
11. C. Wang, S. Chai, and H. Zhu, "OpenDrift: Online evolving fraud detection for open-category and concept-drift transactions," in 2023 IEEE International Conference, 2023.
12. H. Abbassi, A. Berkaoui, S. Elmendili, and Y. Gahi, "End-to-End Real-time Architecture for Fraud Detection in Online Digital Transactions," Int. J. Adv. Comput. Sci. Appl., vol. 14, no. 6, 2023.
13. M. Tabiaa and A. Madani, "The Deployment of Machine Learning in eBanking: A Survey," in Proc. 2019 Third Int. Conf. Adv. Comput., 28–30 Oct. 2019.
14. A. Rehman et al., "Enhancing credit card fraud detection: An ensemble machine learning approach," Big Data Cogn. Comput., 2024.