Journal of Social Science and Management Studies
Vol. 2, No. 1, Jan - Mar 2026, pp. 1-6
ISSN: 3107-3719, DOI: https://doi.org/10.17051/JSSMS/02.01.01

AI-Driven Fraud Detection Models in Digital Payment Systems

Janaranjjanee BN[1], Dr. S. Vasantha[2]

[1]II YEAR MBA (Finance and Marketing) Saveetha Engineering College, Chennai
Email: janaranjjanee2003@gmail.com
[2]Professor, Department of MBA, Saveetha Engineering College, Chennai
Email: vasanthas@saveetha.ac.in

Article Info

Article history:

Received : 01.02.2026
Revised : 28.02.2026
Accepted : 03.03.2026

Keywords:

Artificial Intelligence (AI),
Fraud Detection,
Digital Payment Systems,
Machine Learning (ML),
Financial Risk Management (FRM),
Financial Technology (FinTech),
Predictive Analytics.

ABSTRACT

Digital payment systems have evolved rapidly, changing the way we carry out financial transactions by allowing consumers to make fast, secure and easily accessible cashless payments. At the same time, the immense increase in volume of electronic transactions created greater exposure to fraud and cyber risk. Traditional rule-based fraud detection techniques are becoming less effective as they don't adapt to new types of fraud or the high volume of real-time transactions. This paper presents a systematic review of the literature and a comparative analytical synthesis of artificial intelligence (AI) and machine learning (ML) based fraud detection methods in digital payment systems. The results from the literature review indicate that AI based methods have been consistently better than all other approaches at detecting fraud, especially in situations where data is heavily imbalanced and transaction behavior is dynamic. Ensemble methods - especially random forest and gradient boosting - consistently outperform rule-based systems for detecting fraud in imbalanced transactional environments. The study results also indicate that AI will improve operational efficiencies, reduce financial losses, and build consumer trust through greater detection of fraudulent activity; and provide a uniform analytical framework for preventing fraud in today's digital financial ecosystems.

1. INTRODUCTION

Digital technologies such as mobile wallets, internet banking, contactless payments, and real-time transfer systems have led to a significant change in how we perform financial transactions as individuals and companies, creating a new way to conduct business. The transition to cashless economies globally has been accelerated by numerous factors, including the development of a range of financial technologies (fintech), the growth in use of smartphones, the increasing availability of the internet, and government efforts to promote increased access to the financial system for all [1, 2].

Digital payment systems have a variety of benefits: Customers can perform transactions in an expeditious manner; businesses can reduce their operational costs; digital payment systems provide visibility into the transaction process; and there is a reduced lag time between transaction and settlement.

As digital transactions have grown, so have their vulnerabilities. Cybercriminals have taken the opportunity to exploit both technological and behavioral flaws in the payment system, resulting in many types of fraudulent activity [3].

Fraud has also evolved with changes in technology. Today's fraud schemes have become much more complex and can take advantage of traditional monitoring techniques, which rely heavily on rules and past history, to detect them. Fraud schemes today use phishing, identity theft, unauthorized access to someone's account, synthetic identities, and transaction manipulation to perpetrate fraud. Traditional fraud detection systems typically have a narrower view of fraud methodology due to their excessive dependence on predefined rules and historical data [4, 5].

The imbalance of fraudulent and legitimate transactions that exist today has created a problem where fraud cases represent only a small fraction of overall payment activity. This creates a complex environment which makes detecting fraud difficult, resulting in numerous false positive alerts that hinder legitimate customer transactions and drive up operational costs (6).

There are now AI and Machine Learning technologies that have been used as transformational solutions to these issues. Instead

of relying on rule-based systems like those in the past, AI models assess an extensive amount of transactional data by identifying hidden correlations and recognizing anomalies in real-time. Additionally, advanced analytics techniques such as ensemble learning and neural networks provide superior predictive performance through their ability to capture nonlinear behavioral patterns in large and complex financial data sets (3), (7).

As technology has progressed, many areas needing research are still being researched. Most studies performed have used credit card fraud data sets from developed nations, therefore limiting their application to the new digital payment environments that feature real-time mobile payments and a wide range of user behaviors. This study will address these gaps by providing a comparative analysis of the available AI traffics fraud detection systems by merging the technological understanding with the practical risk management aspect of the systems.

2. PROBLEM STATEMENT

As more digital payment systems become mainstream, access to finances and the speed at which you can make transactions will improve; however, there is now a greater risk for sophisticated types of financial fraud than ever before. Traditional rule-based systems do not work well with processing the high volume of real-time transactions, and they are often responsible for producing a high number of “false-positive” alerts, resulting in higher operating costs and an overall lower level of customer satisfaction with those systems.

There is currently a significant gap in research on fraud because it mainly focuses on credit card fraud data from developed countries. This research is not helpful in creating context around fraud risk for new emerging digital payments. The need for a comprehensive analytic understanding of how AI can be used to detect fraud and its effectiveness from both a technological and management perspective is very important.

3. RESEARCH OBJECTIVES AND QUESTIONS

3.1 Research Objectives

- To identify fraud risk areas within digital payments.
- To describe limitations of traditional rule-based fraud detection systems in detecting fraud.
- To bring together current empirical evidence regarding artificial intelligence (AI) based fraud detection systems.
- To evaluate the strengths of various machine learning methods for fraud detection.

3.2 Research Questions

RQ1: What limitations exist for traditional fraud detection systems in the area of digital payments?

RQ2: Based on prior empirical research, how do AI-based analytical models allow for improved fraud detection?

4. LITERATURE REVIEW

However, with the emergence of digital financial systems, fraud detection has changed quite a bit. Originally, early methods of detection relied primarily on statistical analysis and monitoring rules. Bolton & Hand noted that, because statistics rely on historical assumptions and use static rules, statistical monitoring methods cannot adapt to rapidly evolving fraud behaviours.

As electronic transactions become more common, research has turned to data mining approaches to improve the ability to detect fraud. A review of the literature conducted by Ngai and others indicated that the use of classification, clustering, or neural network-based techniques resulted in much greater accuracy in identifying fraud than traditional manual monitoring systems.

Machine learning has been a further advance for fraud detection via predictive analytics and adaptive learning. As shown by Bhattacharyya et al., machine learning algorithms are significantly superior to traditional statistical approaches by providing lower rates of false positives as well as improved accuracy in classification for credit card fraud situations. Likewise, Phua et al. noted that machine learning methods work especially well in fraud situations characterised by highly imbalanced data.

As research on ensemble learning methods has progressed, researchers have started to pay attention to them because they are capable of combining multiple predictive models and therefore enhancing the predictive reliability of fraud detection. For instance, Dal Pozzolo et al. [6] demonstrated that ensemble based techniques yield better fraud detection results compared with traditional methods, especially when using skewed datasets with rare fraudulent events.

Recent developments have provided access to deep learning and behavior-based analytical models that can identify sequential and non-linear transaction patterns. Machine learning and deep learning methods have been shown to significantly enhance the effectiveness of automated fraud monitoring by using real-time analytical capabilities (Chen et al., 2010) [10]. Roy and Sun (2013) [11] also stressed that using deep learning architectures increases the accuracy of fraud detection as a result of their capacity to identify complex user behavior across transaction sequences.

Researchers have stated that the implementation of AI enhanced monitoring systems will result in an increase of the efficiency of detecting fraudulent transactions as well as an increase in the level of customer trust in the digital financial services being offered in emerging economies. This suggests that behavioural analytics, and adaptive learning models are increasingly being viewed as critical components of a secure digital payment infrastructure (Kumar and Gupta, 2014) [12].

5. PROPOSED CONCEPTUAL FRAMEWORK

This is a conceptual framework that illustrates how digital payment environments (e.g., mobile payments, online banking), fraud risk environments (e.g., cyber fraud, identity theft, a lot of differences in transaction data), AI analytical models (e.g., logistic regression, decision trees, ensemble methods, neural networks), and organizational performance are related in today's financial systems. The primary components of the framework are to show that the growth in the use of digital payment systems requires a shift away from traditional fraud detection systems to intelligent, data-driven monitoring systems.

At the start of the framework, there is a digital payment ecosystem (e.g., mobile payments, internet banking, real-time transaction processing), which includes all forms of electronic payments. With this growth, there is a fraud risk ecosystem that results in an increase in fraud risks due to cybercrime (e.g., cyber fraud), identity theft, behavioral anomalies, and an enormous amount of data that show few instances of fraud compared to the total number of transactions.

Additionally, groups of AI and machine learning models are the core analysis component of the framework. Analysis can be performed using sophisticated analytical models such as logistic regression, decision trees, ensemble methods, and neural networks to analyze large amounts of transaction data. With these analytical models, the following analytic capabilities can be developed: behavioral pattern analysis; outlier detection; real-time analysis; and a much better way of handling imbalanced data.

As a result of these innovations in technology, there is both an effect on management and finance including decreases in the amount of money lost, increases in how efficient operations are, improved ability to manage risk, and improved trust from customers. This illustrates that the addition of AI-driven fraud detection systems will help create a secure and sustainable digital financial ecosystem.

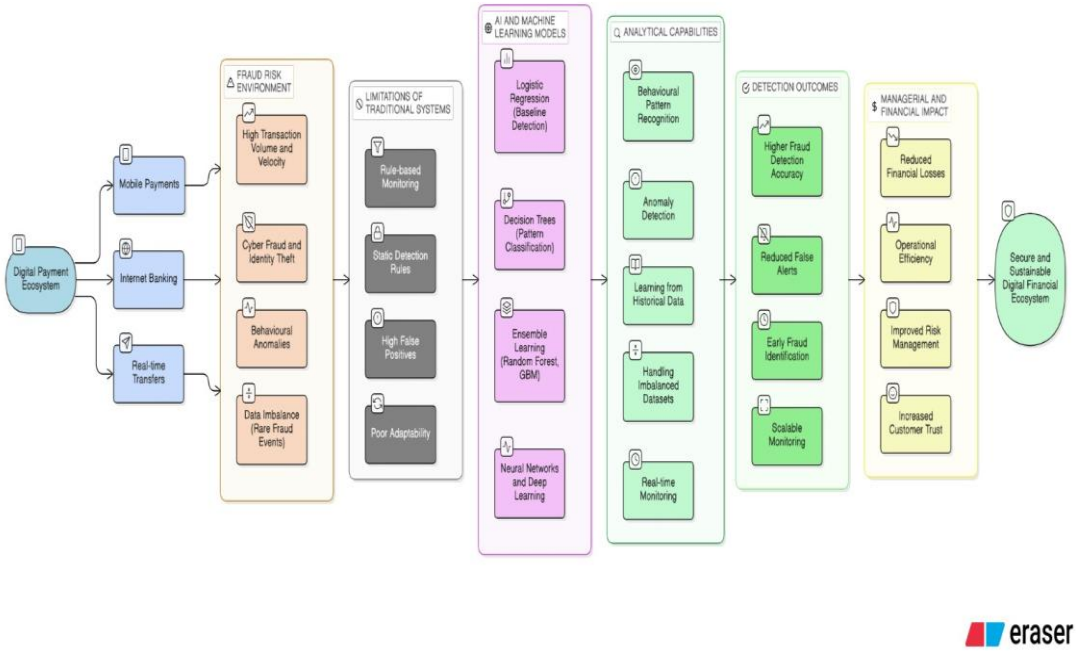


Fig. 1. AI-driven fraud detection conceptual framework.

6. RESEARCH METHODOLOGY

A systematic review of the literature and comparative analytical research methods were used to identify artificial intelligence (AI) fraud detection models for digital payment systems. The synthesis of information from peer reviewed academic journals, conference proceedings, and industry-specific reports published from 2002 to 2023 was done on the basis of secondary empirical

data collection with no primary data or algorithmic implementation being performed.

The criteria for selection of studies in the synthesis involved three specific criteria: (1) the study had to provide empirical or comparative evaluation results of AI or machine learning (ML) based fraud detection or classification methods; (2) studies must also consider digital payment or financial transaction environments; and (3) only studies employing some combination of statistical, ensemble, or deep learning methodologies for their analyses will be included in the review, in order to capture the findings across all fraud detection methods examined.

Five commonly reported family of models utilized in the comparative evaluation framework were: Logistic Regression, Decision Trees, Random Forest, Gradient Boosting, and Neural Networks. Measurements of evaluation included accuracy of fraud detection, adaptability to class imbalance, scalability of computation used for detecting fraud, and ability of the method to operate. The approach was designed to be a conceptual synthesis of knowledge rather than an experimental benchmarking study with the primary contribution from this research being improvement of managers' and strategists' understanding of AI and ML based fraud detection in digital payment environments.

Table 1. Comparison of AI-Based Fraud Detection Models

Model	Key Strengths	Limitations	Best Application
Logistic Regression	Interpretable; computationally efficient baseline	Poor nonlinear pattern detection; sensitive to outliers	Baseline fraud scoring
Decision Trees	Captures nonlinear relationships; transparent	Prone to overfitting; poor on imbalanced data	Rule extraction and audit
Random Forest	High accuracy; robust to imbalance; low variance	Reduced interpretability; computationally intensive	High-volume transaction monitoring
Gradient Boosting	Superior AUC; handles imbalance well	Hyperparameter sensitive; slow training	Real-time fraud prediction
Neural Networks	Captures complex behavioral patterns; deep feature learning	Black-box; requires large training data	Behavioural anomaly detection

7. RESULTS AND DISCUSSION

This study bases its findings on a comparative synthesis of previously conducted empirical research into AI-based fraud detection systems. Evidence across various studies indicates that machine learning-based approaches consistently outperform traditional rule-based monitoring systems when used within a dynamic digital payment environment.

Logistic regression models are commonly cited as a reliable baseline approach but have limited capabilities for detecting complex fraud patterns. Decision tree models improve the classification process by accounting for nonlinear relationships between features and observations, while ensemble learning methods, such as random forest and gradient boosting, have been shown to perform better when the data set is highly imbalanced. Neural network-based models are able to further enhance detection capabilities by being able to recognize complex behavioral transaction patterns; however, interpretability of results continues to be a challenge.

7.1 Key Findings

- Many studies report better performance on detecting fraud by using ensemble learning methods compared to classical statistical or rule-based methods.
- Current literature highlights that increased recall rates are essential in order to increase fraud detection capabilities; this is especially true with significantly skewed datasets.
- Techniques using behavioral pattern recognition to determine predictive ability show improvement of predictive capability through their ability to detect multi-faceted and evolving transaction anomalies.
- Artificial intelligence (AI) based analytic models are able to provide scalability and continual monitoring support in high volume digital payment markets.

In summary, the synthesized findings support both ensemble learning techniques and behavior-based analytic techniques as the most valid methodologies being employed today for the detection of fraud in digital payments, as supported by findings published by Dal Pozzolo et al. [6] and Roy and Sun [11].

8. MANAGERIAL AND FINANCIAL IMPLICATIONS

Past research and studies demonstrate that organizations who utilize artificial intelligence for fraud detection have many operational/financial benefits. In the case of fraud, if detected quickly, direct financial loss through the flow of fraudulent activity can be prevented prior to the completion of any fraud transaction. By automating the transaction monitoring process, organizations can increase their operational efficiency by decreasing reliance on manual review processes and increasing the ability to implement proactive risk measures.

A strong data-driven decision support system within the enterprise risk management framework allows the banking and financial services industry to have a more dynamic response to changing patterns of risk or fraud. The reduction and elimination of false-positive forecasts are also essential to enhancing consumer confidence and trust in digital/online payment solutions, which leads to stronger customer loyalty and improved service delivery.

As such, in conjunction with the totality of the evidence presented in current research, banks and financial technology companies should deploy AI-driven fraud detection systems that incorporate a variety of model-based predictive and/or ensemble modeling techniques in combination with various forms of behavioral analytics. These models will assist these companies to improve their abilities to prevent and/or detect fraudulent transactions.

9. CONCLUSION

Digital payment systems provide consumers with more access to financial products than ever before, but they also introduce sophisticated fraud risks. Rule-based methods of monitoring are often inadequate because they cannot adapt quickly to changing fraud schemes and respond quickly enough to prevent the occurrence of new types of fraud.

This paper synthesizes the conclusions of previous empirical research on AI-based fraud detection methods in digital payment ecosystems. The findings from the analysis indicate that AI-based models, especially using ensemble learning methods, are better suited for detecting fraud than previously demonstrated by traditional monitoring systems; they allow for the detection of behavioural patterns and address issues associated with data imbalance.

AI-based monitoring systems improve operational processes, enhance risk management practices, and build trust with customers from a managerial standpoint. Therefore, this research points to the fact that integrating artificial intelligence into fraud detection processes will significantly enhance the safety and sustainability of an evolving digital financial ecosystem.

10. LIMITATIONS AND FUTURE RESEARCH

10.1 Limitations

- The analysis relies on secondary academic and industry sources rather than primary empirical data.
- Findings depend on methodologies and datasets used in prior studies, which may vary across research contexts.
- The study does not include real-time system implementation or experimental validation.

10.2 Future Research Directions

- Conducting empirical investigations using real-time digital payment datasets from diverse transaction environments.
- Integrating Explainable Artificial Intelligence (XAI) techniques to improve model transparency and managerial interpretability.
- Exploring advanced deep learning architectures such as Long Short-Term Memory (LSTM) networks and hybrid analytical models for sequential fraud detection.
- Performing cross-country comparative studies to understand regional variations in digital payment fraud patterns.

ACKNOWLEDGMENT

The author thanks the institution and reviewers for their constructive feedback and support in developing this manuscript.

REFERENCES

1. World Bank, "Global Findex Database: The Global Financial Inclusion Database," World Bank Group, Washington, D.C., 2022.
2. Bank for International Settlements (BIS), "Annual Economic Report: Digital Payments and Financial Stability," BIS, Basel, Switzerland, 2023.
3. G. Kou, Y. Peng, and G. Wang, "Evaluation of clustering algorithms for financial risk analysis using MCDM methods," Inf. Sci., vol. 275, pp. 1–12, 2021.
4. E. W. T. Ngai, Y. Hu, Y. H. Wong, Y. Chen, and X. Sun, "The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature," Decis. Support Syst., vol. 50, no. 3, pp. 559–569, 2011.
5. A. Abdallah, M. A. Maarof, and A. Zainal, "Fraud detection system: A survey," J. Netw. Comput. Appl., vol. 68, pp. 90–113, 2016.
6. A. Dal Pozzolo, O. Caelen, R. Johnson, and G. Bontempi, "Calibrating probability with under-

sampling for imbalanced classification," IEEE Symp. Series Comput. Intell. (SSCI), pp. 159–166, 2017.
7. C. Phua, V. Lee, K. Smith, and R. Gayler, "A comprehensive survey of data mining-based fraud detection research," Artif. Intell. Rev., vol. 34, no. 1, pp. 1–14, 2010.
8. R. J. Bolton and D. J. Hand, "Statistical fraud detection: A review," Stat. Sci., vol. 17, no. 3, pp. 235–255, 2002.
9. S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," Decis. Support Syst., vol. 50, no. 3, pp. 602–613, 2011.
10. C. Chen, J. Li, and Y. Huang, "Machine learning methods for financial fraud detection," IEEE Access, vol. 6, pp. 35323–35334, 2018.
11. A. Roy and J. Sun, "Deep learning for fraud detection in financial transactions," J. Big Data, vol. 9, no. 1, 2022.
12. P. Kumar and R. Gupta, "Digital payment adoption and fraud risk in emerging economies," Int. J. Financ. Stud., vol. 9, no. 3, 2021.
13. T. Dahlberg, J. Guo, and J. Ondrus, "A critical review of mobile payment research," Electron. Commer. Res. Appl., vol. 14, no. 5, pp. 265–284, 2015.
14. Reserve Bank of India, "Report on Currency and Finance: Towards a Digital and Clean Energy Economy," RBI, Mumbai, India, 2023.