Enhancing Credit Fraud Detection in e-Payments through Predictive Analytics using Machine Learning: A Scoping Review

Zenande Nondula and Moses Moyo
Department of Information Systems, Rhodes University, Makhanda, South Africa

nondulazenande@gmail.com
moses.moyo@ru.ac.za

Abstract: The rapid global expansion of e-payment has created new opportunities for sophisticated, evolving financial fraud, leading to substantial financial losses and undermining or eroding customer trust, despite new security efforts. This scoping review examines how the application of predictive analytics, utilising machine learning and data analytics techniques, can enhance credit fraud detection and prevention in e-payments. The Joanna Briggs Institute protocols for scoping reviews were used to identify literature published between 2019 and 2025 from multiple academic databases, resulting in the selection of 30 relevant studies. Data mapping and analysis were applied to the selected studies, enabling insights into how financial institutions can leverage machine learning and data analytics to detect and prevent fraud more effectively across diverse digital payment environments. The review revealed various fraudulent methods, including complex transaction-like fraud, card-not-present fraud in online purchases, account takeover, identity theft, and high-frequency, small-scale fraud targeting vulnerable time windows, with emerging threats in DeFi platforms that pose unique detection challenges and high vulnerability. These findings demonstrate that fraud patterns are increasingly dynamic, adaptive, and designed to blend in with legitimate customer behaviour, making early detection more challenging. The study's findings also highlight that advanced machine learning models, such as ensemble methods, deep learning, neural networks, anomaly detection algorithms, and data analytics methods, can significantly improve real-time fraud detection and outperform traditional rule-based approaches that rely on static thresholds, manual review, or historical assumptions. Despite these benefits, the review highlights persistent issues that limit practical implementation. These include data imbalance, high rates of false positives and false negatives, challenges with model transparency, privacy concerns, and integration challenges with legacy systems. Addressing these technical and operational challenges is therefore essential to enhancing the effectiveness of predictive analytics in safeguarding digital payment ecosystems and supporting a more trusted and resilient digital financial environment, while also informing regulatory compliance, operational risk management, and future research directions on fraud detection in e-payment systems.

Keywords: Credit fraud, Prevention, Detection, Predictive analytics, Machine learning, Data analytics

1. Introduction

E-commerce has evolved and grown greatly since its introduction to the customer and business worlds as a unique approach, providing businesses and consumers worldwide with significant advantages, such as the rise in electronic payment systems [1]. An electronic payment (e-payment) is an e-commerce transaction in which goods or services are purchased over the Internet. In an e-payment system, a monetary value is transmitted electronically between two parties as compensation or consideration for the receipt of goods or services [2]. Easy access to the Internet has promoted online shopping and banking, which require efficient payment methods; hence, the rise of electronic payment systems [3]. E-payment methods play an important role in today's competitive financial society. According to a study [4], EPSs have made payments for goods and services easy and convenient. Four main types of electronic payment systems in use today are credit and debit cards, mobile payment apps, online payment gateways, and digital wallets. Digital credit card payments have become the most prevalent payment option in recent years. This is due to the technological improvements and the introduction of new e-funding options and alternatives, such as e-commerce and phone banking [5]. This is also supported in [6], which states that credit cards are the most used form of payment for online purchases and transactions. This includes Visa and MasterCard. Study [7] singles out user-friendly features as the main benefit of credit cards, as they enable quick and convenient online transactions from any location. Study [8] states that credit card fraud has increased with the introduction of new technology. Banks worldwide prioritise the security and confidence of card payments for their customers. According to studies [9] and [4], credit card fraud is defined as the unauthorised use of credit cards to obtain money or property by fraudulent means. Even though credit cards offer consumers few advantages, they are also linked to issues such as fraud and security [4]. The growth of online purchases indicates that additional work will be needed to guarantee the security of online card payments [10]. Traditional machine learning methods for fraud detection are ineffective because they cannot accurately predict whether a transaction is fraudulent, as fraudsters continually develop new patterns and techniques to evade detection [8]. The rise in e-payment brought significant security and trust challenges [11]. According to a study [12], the internet expands commercial options, and fraudsters are developing increasingly complex and sophisticated methods to commit these crimes. Traditional fraud detection techniques, reliant on rule-based systems or manual reviews, are now inefficient against the complexity of modern e-payment fraud [12]. This implies that relying on traditional fraud-detection methods is no longer viable to protect e-payments. Therefore, proactive methods are necessary, such as predictive analytics enabled by machine learning, which analyses large datasets to detect complex fraud patterns. Machine Learning has emerged as a powerful tool for fraud detection [11]. A proactive strategy is enabled by Machine learning, which predicts and prevents fraudulent activity before it causes serious damage. Study [13] states that in this era of big data, financial institutions are increasingly relying on advanced analytics and machine learning to tackle challenges in the credit card industry. This research study aims to explore the use of predictive analytics and machine learning in addressing e-payment credit card fraud, thereby enhancing detection and prevention and fostering a safer digital payment ecosystem. The article sought to answer the following research questions:

- What are the most common types of fraudulent activities in e-payment systems?
- What strategies do financial institutions use to detect fraudulent activities in e-payment systems?
- How can Machine learning be used to improve the accuracy of fraud detection in online payments?

2. Research Methodology

This article followed the Joanna Briggs Institute (JBI) methodology to guide authors through scoping reviews and followed the PRISMA-ScR reporting criteria [14]. Its goal is to investigate fraud detection and prevention technologies in the e-payment context while addressing associated issues. According to a study [14], the Population, Concept, and Context (PCC) framework is used to create an understandable and appropriate title and inclusion standards for a scoping review. The population consists of electronic payment systems, particularly credit and debit cards, mobile payment apps, digital wallets, and online payment gateways. The concept focused on predictive analytics, data analytics, or machine learning for both fraud detection and fraud prevention. The context focused on global e-payment systems. The PCC framework is presented in Table 1 below.

Table 1: PCC Framework

	Population	Concept	Context
Principal	Electronic payment systems	Predictive analytics, data analytics, or machine learning for fraud detection	Global
Synonym	Online payment platforms	Predictive analytics, data analytics, or machine learning for fraud detection	International

The search string was formulated based on Table 1:

("credit fraud" OR "payment fraud" OR "financial fraud") AND ("e-payment" OR "digital payment" OR "online payment") AND ("predictive analytics" OR "data analytics" OR "machine learning" AND ("fraud detection" OR "fraud mitigation" OR "fraud prevention")

2.1 Eligibility Criteria

This eligibility criterion focuses on ensuring the inclusion of relevant studies on the use of data analytics and machine learning for credit fraud detection in electronic payment systems. The review focused on peer-reviewed literature from 2019 to 2025 and excluded non-English studies, those without full text, or those unrelated to credit fraud. It aims to map current methodological trends to inform future research in this field.

2.2 Information Sources

The scoping review used a comprehensive literature search across several reputable academic databases, including ScienceDirect, EBSCOhost, ACM Digital Library, Scopus, and Google Scholar, to collect academic literature on credit fraud detection, predictive analytics, and machine learning in e-payment systems. Furthermore, grey literature, such as government reports and company white papers, was rigorously searched for current industry insights.

2.3 Selection of Sources of Evidence

The JBI's three-step search technique and the PCC framework, as shown in Table 1, guarantee a methodical approach. Literature searches were conducted between May and June 2025 across databases including ScienceDirect, EBSCOhost, ACM Digital Library, and Scopus, alongside relevant grey literature such as government reports, policy documents, and cybersecurity white papers.

The search strategy involved the following steps:

Step 1: Initial search

An initial limited search was performed using the broad search terms "Credit fraud detection", "Credit fraud prevention", and "e-payments". This stage helped refine the search phrases for further stages.

*Step 2: Focused Search*Search string such as "Credit fraud detection" AND "Credit fraud prevention" AND "e-payment" AND "Predictive analytics" AND "Machine learning" AND "Data analytics was documented for transparency, refined for relevance and coverage.

Step 3: Backward Search

To find additional relevant articles that met the inclusion criteria, the reference lists of all included papers were screened (reverse searching).

2.4 Data Charting Process

A structured charting template guided data extraction and analysis following the JBI scoping review approach. The results were obtained using the search string. This process identified key themes and trends in the application of machine learning and predictive analytics for e-payment credit card fraud detection and prevention. The mapping also incorporated a review of industry practices, regulations, and technological mitigation measures.

2.5 Data Items

The following variables were recorded for every study included in this review:

Author(s), Year of publication, Country of origin, purpose, Study population and sample size, Methods used, Findings.

3. Results

3.1 Selection of Sources of Evidence

The initial search across four databases (Science-Direct, ACM Digital Library, EBSCOhost, Scopus) yielded 345 articles. Following the removal of duplicates and screening of titles, abstracts, and full texts, 18 articles were deemed suitable. To address the scarcity of peer-reviewed literature on the topic, nine articles from grey literature and three from a backward search were included, resulting in a final selection of 30 articles for the review. The selection process is detailed in Figure 1.

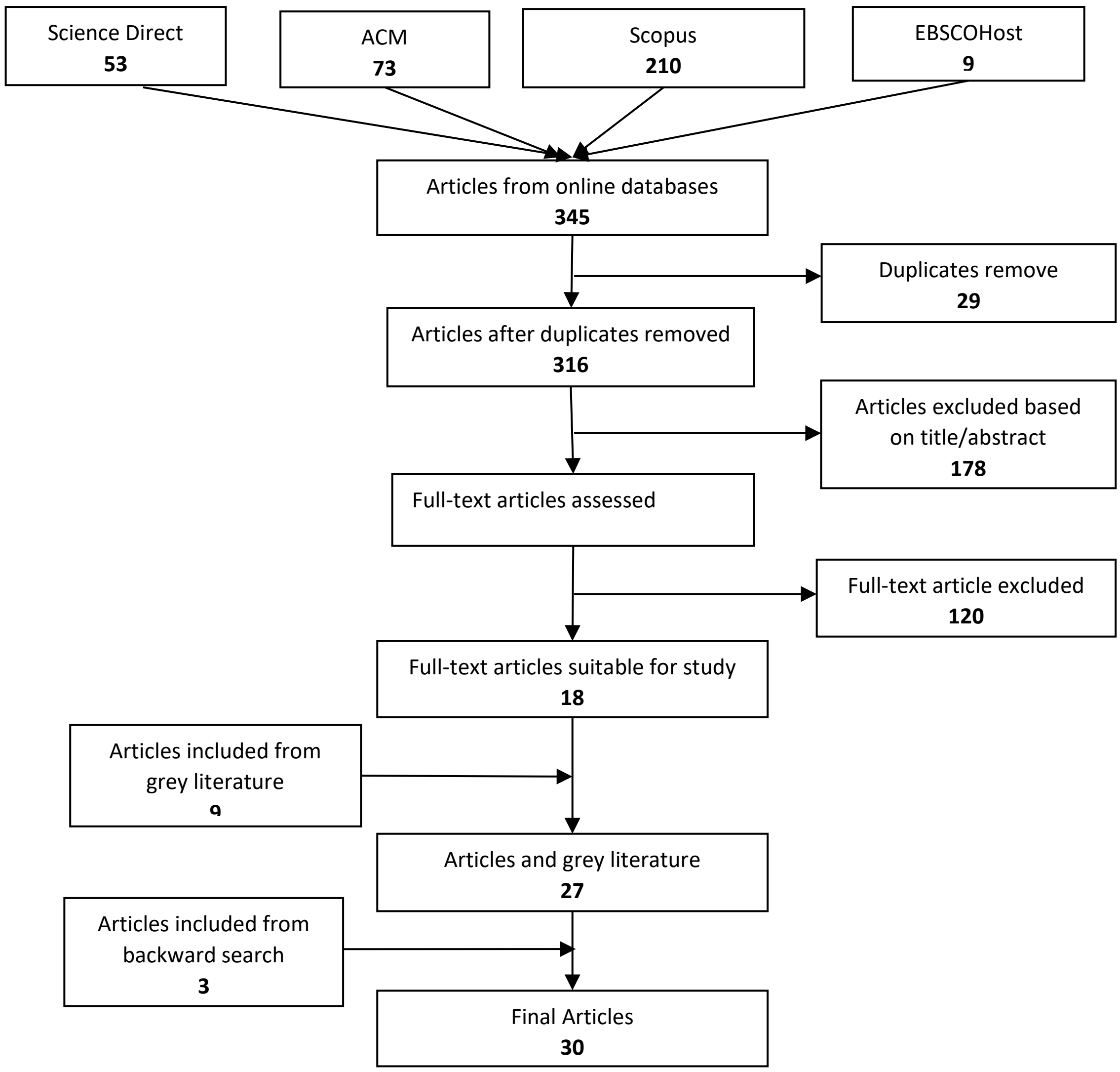

Figure 1: PRISMA-ScR diagram

3.2 Characteristics of Sources of Evidence

Figures 2 and 3 below visually represent the main data elements from the data mapping table, including publication date and country of publication. These visualisations were created using Microsoft Excel.

3.2.1 Distribution of literature sources by dates of publication

The articles were categorised by year of publication to examine the trends in the discussions of the issues addressed in this study. The results are illustrated in Figure 2.

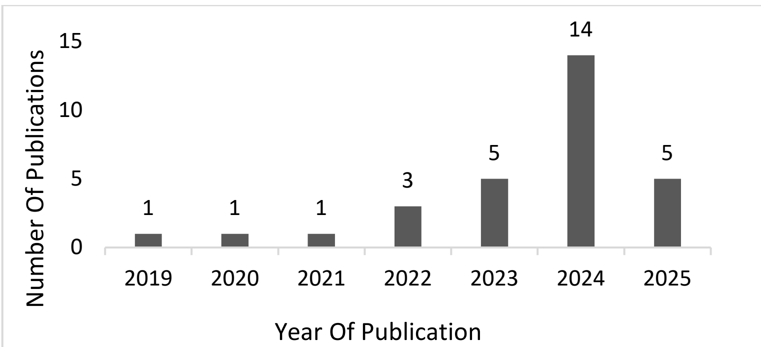

Figure 2: Distribution of literature sources by dates of publication

The results in Figure 2 show relatively low and stable publication output between 2019 and 2021, followed by a gradual increase in 2022 and 2023. The number of publications increased dramatically in 2024, before dropping in 2025. This trend indicates growing research interest over time, reaching its peak in 2024.

3.2.2 Distribution of literature sources by country of publication

This result illustrates the number of reviewed articles on credit fraud detection and prevention using predictive analytics, organised by country of publication.

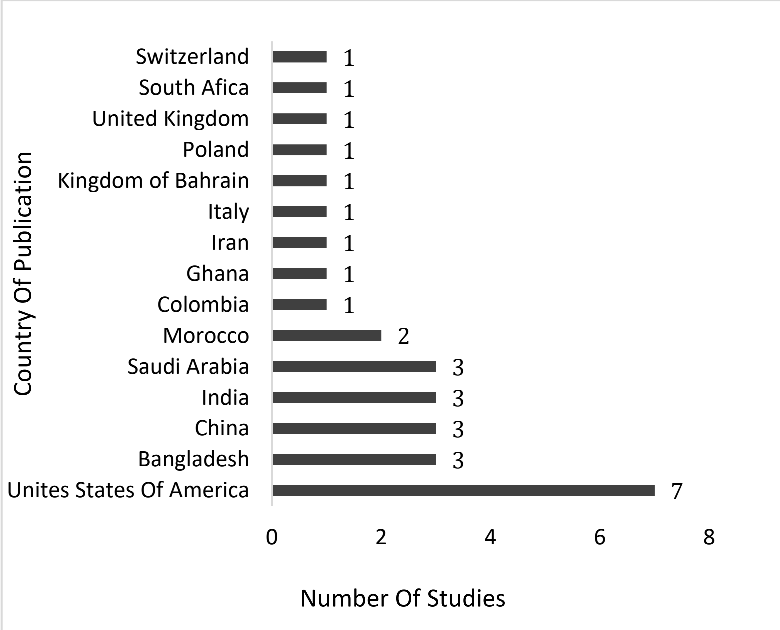

Figure 3: Distribution of literature sources by country of publication

Figure 3 shows that the United States contributed the most studies (7 of 30), followed by Saudi Arabia, India, China, and Bangladesh (three each), and Morocco (two), while other countries contributed one each. This distribution indicates a concentration of research in a few regions, highlighting geographical gaps, while also confirming that credit fraud is a global concern.Table 2: Study classification by research purpose in machine learning fraud detection

Table 2: Study classification by research purpose in machine learning fraud detection

Purpose of the study	Studies (Author & Year)	Count
Develop/enhance a specific machine learning model/framework for credit card fraud detection	[15];[16];[17];[18];[19];[20];[21];[22]	8
Enhance security in online financial transactions	[33];[34];[35];[36];[37];[38]	6
Create a real-time fraud detection system	[23];[24];[25]	3
Address data imbalances in fraud detection	[26];[27];[28]	3
Analyse research trends using bibliometrics	[41];[42];[43]	3
Explore the general application of ML/AI for fraud detection	[29];[30]	2
Enhance operational frameworks and predictive performance	[30];[31]	2
Implement a secure, privacy-preserving collaborative system	[32]	1
Develop a scalable platform for digital finance fraud	[39]	1
Compare the efficacy of specific ML techniques	[40]	1

The results in Table 2 categorise the 30 reviewed studies by their primary research purpose, facilitating the identification of key research clusters and trends. The largest category (8 studies) focuses on developing and refining machine learning models for credit card fraud detection, including real-time systems and methods to address data imbalance. This structured overview clarifies prevailing methodological approaches and highlights prominent areas for future investigation in the field.

4. Discussions

The findings of the study have 3 themes, and each has associated sub-themes

4.1 Summary of Evidence

4.1.1 Theme 1: Types of fraudulent activities

Financial fraud ranges from complex, transaction-like schemes to high-frequency small-scale fraud and rising threats in cryptocurrency and blockchain systems.

4.1.2 Complex, transaction-like fraud behaviours

The study found that sophisticated fraud techniques, particularly those involving identity theft and the misuse of credit card details, are increasingly challenging to detect because they mimic legitimate user behaviour over time, often involving a series of seemingly legitimate actions that culminate in the execution of the fraud. This finding is supported by [29], who emphasise the complexity of such operations. According to a study [15], the shopping category accounted for the most fraudulent transactions (1.19%), followed by groceries (0.73%), miscellaneous (0.36%), transportation (0.28%), and home care (0.16%). Fraudsters employ fraudulent techniques to conduct transactions using others' credit card details. Study [26] states that credit card fraud can occur through several forms, including theft, application fraud, use of fake cards, non-receipt of issued cards (NRI), and online fraud and card-not-present fraud, which only requires access to card data rather than the cardholder's physical presence.

4.1.3 Emerging fraud in decentralised systems (DeFi)

The study found that the decentralised, high-volume characteristics of e-commerce platforms significantly contribute to the development and rapid growth of sophisticated fraud threats. According to a study [32], the e-payment environment creates several vulnerabilities for fraudsters to exploit due to the lack of centralized oversight and the high volume of continuous transactions. The finding emphasises the adaptable and persistent nature of fraudulent activities in current financial systems that function under decentralised frameworks, making identification and prevention more difficult.

4.1.4 High-frequency, small-scale fraud

The study [15] found that fraudulent transactions occur most frequently between 22:00 GMT and 04:00 GMT, a period when most victims are asleep and less likely to check their accounts. This finding highlights a high-frequency, opportunistic strategy employed by fraudsters, who exploit vulnerable time windows to increase the likelihood of successful transactions while reducing the chances of immediate detection.

4.1.5 Theme 2: Detection strategies by financial institutions

Machine learning enhances fraud detection by leveraging advanced models to identify complex patterns and enabling real-time monitoring and anomaly detection for quick threat responses.

4.1.6 Machine learning methods

The study found that traditional fraud detection methods struggle to handle the massive volumes of data generated by modern digital payment systems, necessitating the use of advanced technologies such as machine learning to analyse large datasets and extract meaningful insights [30]. Most studies employ machine learning, with a strong focus on ensemble learning approaches due to their higher performance in fraud detection tasks. Study [17] developed a stacking ensemble model incorporating support vector machine (SVM), K-nearest neighbors (KNN), and extreme learning machine (ELM) algorithms, which consistently outperformed other models across all evaluation metrics, demonstrating robustness in handling imbalanced datasets. Study [39] further states that GBM is highly effective at fraud detection because it can learn from complex transaction data and improve accuracy over time. According to a study [30], ensemble methods like XGBoost and Random Forest are more effective than other machine learning models at balancing false positives and negatives. However, these techniques also encounter various challenges. However, studies also highlighted several challenges that the above-mentioned machine learning techniques tend to face. Although the stacking ensemble method showed superior fraud detection performance compared to individual machine learning techniques, it has limitations, including the dataset's sole focus on China, potential overfitting to historical patterns, and a lack of integration with unstructured data [39]. According to a study [30], ensemble approaches improve predictive performance but complicate model interpretation and cause high computational costs, limiting scalability and speed. Additionally, training these models on imbalanced datasets without sufficient balancing can result in overfitting. However, studies highlighted several challenges likely to be encountered when machine learning is used: adversarial attack, a malicious entity actively attempting to modify the behavior of machine learning models [45]. This occurs when fraudsters study how data-driven fraud detection systems operate and then design fraudulent transactions that can evade detection [45]. A study [46] confirms that ML models are vulnerable to adversarial machine learning (AML) attacks.

4.1.7 Optimisation techniques

The study found that a hybrid technique combining Competitive Swarm Optimisation (CSO) for feature selection and Deep Convolutional Neural Networks (DCNN) for classification considerably enhances financial fraud detection, outperforming benchmarks in accuracy and precision on large datasets [24]. Furthermore, [39] state that the Sequential Bandwidth Weighting (SBW) algorithm enhances the performance of the gradient boosting machine (GBM) by reducing false positives and improving scalability for fraudulent transaction classification. These findings show that advanced hybrid ML algorithms are reliable and effective for real-time fraud detection in digital financial systems. However, SBW-GBM faces computational complexity, low interpretability, reliance on labeled data, and scalability issues with heterogeneous [39].

4.1.8 Theme 3: Role of machine learning in enhancing fraud detection

Machine learning enhances fraud detection by analysing vast datasets, detecting hidden patterns, and responding to new fraud strategies. Predictive models can detect anomalies in real time while reducing false positives, making fraud prevention more effective.

4.1.9 Advanced machine learning

The study found that Gradient Boosting Machines (GBMs) play an important role in financial risk management by identifying patterns in historical data and forecasting potential risks with high accuracy. According to a study [39], GBMs improve forecast precision iteratively by minimizing errors at each step, and the Sequential Bandwidth Weighting (SBW) technique increases GBM efficiency by hyperparameter tuning. In addition, study [18] highlights deep learning algorithms as effective methods for reducing fraud in financial transactions, leveraging large financial datasets via deep multi-layer artificial neural networks. Study [18] states that deep learning is a subset of machine learning that employs complex ANNs inspired by the structure and function of the human brain and operating on supervised learning principles. The DNN also demonstrated strong performance in spotting complex, non-linear fraudulent patterns [38].

4.1.10 Real-time monitoring detection

The study found that organisations can identify fraudulent activity in real time by processing enormous amounts of transaction data using big data technologies and powerful analytics [27]. Study [35] states that big data supports real-time fraud by processing and analysing transactions as they occur. This strategy enables rapid detection and response to fraudulent activity, hence improving the overall security and integrity of financial systems. Study [34] states that the combination of real-time analytics and machine learning enables rapid response to suspicious behaviour. However, relatively few studies have addressed this topic, highlighting a research gap on the use of big data analytics for real-time fraud detection.

Table 3: Comparison of Real-Time and Batch Processing in Fraud Detection

Feature	Real-Time Processing	Batch Processing	Cyber Defence implications
Timing [47]	Runs continuously with very low delay	Runs after transactions at set times	Real-time stops fraud instantly; batch may miss urgent threats
Detection Speed[48]	Instant detection	delayed detection	Real-time lowers fraud risk
Adaptability to new patterns [48]	Able to identify novel fraud patterns in real-time	Limited, it requires retraining	Real-time adapts to emerging threats

Table 3 compares real-time and batch processing approaches in fraud detection, focusing on key aspects such as timing, detection speed, and adaptability. It highlights that real-time processing enables instantaneous identification and response to fraudulent activity and can quickly adapt to new fraud patterns, whereas batch processing functions with delays and necessitates retraining to recognise emerging risks. The comparison emphasises the importance of real-time solutions in enhancing cyber defence by mitigating fraud risk and improving responsiveness.

5. Conclusion

In conclusion, although advanced machine learning and deep learning models have greatly improved financial fraud detection through accurate, real-time analysis and increased recognition of complex fraud patterns, numerous limitations persist. Challenges such as data volume and velocity, processing delays, data privacy concerns, and the need for continuous model updates increase system complexity and cost. Concerns with data imbalance, model transparency, scalability, and inconsistencies among datasets undermine the trustworthiness and generalisability of findings. Despite these constraints, the study highlights important practical and theoretical contributions in enhancing fraud detection through advanced analytics. Future research should focus on developing scalable, real-time big data frameworks and integrating proactive techniques, machine learning, and data analytics to better anticipate and prevent evolving fraud strategies.

Ethics Declaration: This study does not need an ethics clearance since the data used are purely from existing studies obtained through synthesis from different sources. It is a scoping review.

AI Declaration: ChatGPT and Grammarly were used to help with sentence construction, data analysis, and written content refinement. Outputs were reviewed and edited to ensure originality and compliance with academic standards.

References

E. M. Al-dahasi, R. K. Alsheikh, F. A. Khan, and G. Jeon, “Optimizing fraud detection in financial transactions with machine learning and imbalance mitigation”.

J. K. Afriyie et al., “A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions,” Decision Analytics Journal, vol. 6, p. 100163, Mar. 2023, doi: 10.1016/j.dajour.2023.100163.

H. Abbassi, S. El Mendili, and Y. Gahi, “Real-Time Online Banking Fraud Detection Model by Unsupervised Learning Fusion,” HighTech. Innov. J., vol. 5, no. 1, pp. 185–199, Mar. 2024, doi: 10.28991/HIJ-2024-05-01-014.

H. M. Alzoubi, M. T. Alshurideh, B. A. Kurdi, K. M. K. Alhyasat, and T. M. Ghazal, “The effect of e-payment and online shopping on sales growth: Evidence from the banking industry,” 10.5267/j.ijdns, vol. 6, no. 4, pp. 1369–1380, 2022, doi: 10.5267/j.ijdns.2022.5.014.

Omogbeme Angela, Iyabode Atoyebi, Adesola Soyele, and Emmanuel Ogunwobi, “Enhancing fraud detection and prevention in fintech: Big data and machine learning approaches,” World J. Adv. Res. Rev., vol. 24, no. 2, pp. 2301–2319, Nov. 2024, doi: 10.30574/wjarr.2024.24.2.3617.

M. Akouhar, A. Abarda, M. El Fatini, and M. Ouhssini, “Enhancing credit card fraud detection: the impact of oversampling rates and ensemble methods with diverse feature selection,” reks, vol. 2025, no. 1, pp. 85–101, Feb. 2025, doi: 10.32620/reks.2025.1.06.

M. Azim Mim, N. Majadi, and P. Mazumder, “A soft voting ensemble learning approach for credit card fraud detection,” Heliyon, vol. 10, no. 3, p. e25466, Feb. 2024, doi: 10.1016/j.heliyon.2024.e25466.

Z. Bezhovski, “The Future of the Mobile Payment as Electronic Payment System,” 2016.

R. Bin Sulaiman, V. Schetinin, and P. Sant, “Review of Machine Learning Approach on Credit Card Fraud Detection,” Hum-Cent Intell Syst, vol. 2, no. 1–2, pp. 55–68, Jun. 2022, doi: 10.1007/s44230-022-00004-0.

Felix Adebayo Bakare, Jide Omojola, and Augustine Chibuzor Iwuh, “Blockchain and decentralized finance (DEFI): Disrupting traditional banking and financial systems,” World J. Adv. Res. Rev., vol. 23, no. 3, pp. 3075–3089, Sep. 2024, doi: 10.30574/wjarr. 2024.23.3.2968.

S. R. Byrapu Reddy, P. Kanagala, P. Ravichandran, D. R. Pulimamidi, P. V. Sivarambabu, and N. S. A. Polireddi, “Effective fraud detection in e-commerce: Leveraging machine learning and big data analytics,” Measurement: Sensors, vol. 33, p. 101138, Jun. 2024, doi: 10.1016/j.measen.2024.101138.

G. Charizanos, H. Demirhan, and D. İçen, “An online fuzzy fraud detection framework for credit card transactions,” Expert Systems with Applications, vol. 252, p. 124127, Oct. 2024, doi: 10.1016/j.eswa.2024.124127.

S. Chitta, S. M. Yellepeddi, S. Thota, and A. K. P. Venkata, “Decentralized Finance (DeFi): A Comprehensive Study of Protocols and Applications,” vol. 5, 2019.

V. Chang, B. Ali, L. Golightly, M. A. Ganatra, and M. Mohamed, “Investigating Credit Card Payment Fraud with Detection Methods Using Advanced Machine Learning,” Information, vol. 15, no. 8, p. 478, Aug. 2024, doi: 10.3390/info15080478.

S. Dai, “Research on Detecting Credit Card Fraud Through Machine Learning Methods,” in Proceedings of the 2022 2nd International Conference on Business Administration and Data Science (BADS 2022), vol. 11, V. Fernández-Viagas, B. K. Kandel, C. Valmohammadi, and H. Mallick, Eds., in Atlantis Highlights in Computer Sciences, vol. 11. , Dordrecht: Atlantis Press International BV, 2023, pp. 1030–1037. doi: 10.2991/978-94-6463-102-9_107.

C. Dong and S. Xiao, “Enhancing financial fraud detection in digital finance applications through machine learning algorithms and real-time data analytics,” Journal of Computational Methods in Sciences and Engineering, p. 14727978251352131, Jun. 2025, doi: 10.1177/14727978251352131.

K. G. Dastidar, O. Caelen, and M. Granitzer, “Machine Learning Methods for Credit Card Fraud Detection: A Survey,” IEEE Access, vol. 12, pp. 158939–158965, 2024, doi: 10.1109/ACCESS.2024.3487298.

European Central Bank, Ed., Third report on card fraud. Frankfurt am Main: European Central Bank, 2014. doi: 10.2866/67559.

Ezekiel Onyekachukwu Udeh, Prisca Amajuoyi, Kudirat Bukola Adeusi, and Anwulika Ogechukwu Scott, “The role of big data in detecting and preventing financial fraud in digital transactions,” World J. Adv. Res. Rev., vol. 22, no. 2, pp. 1746–1760, May 2024, doi: 10.30574/wjarr. 2024.22.2.1575.

Faculty of Sciences IPSS, University Mohammed V, Rabat, Morocco, I. Benchaji, S. Douzi, and B. E. Ouahidi, “Credit Card Fraud Detection Model Based on LSTM Recurrent Neural Networks,” JAIT, vol. 12, no. 2, pp. 113–118, 2021, doi: 10.12720/jait. 12.2.113-118.

J. Femila Roseline, G. Naidu, V. Samuthira Pandi, S. Alamelu Alias Rajasree, and Dr N. Mageswari, “Autonomous credit card fraud detection using machine learning approach☆,” Computers and Electrical Engineering, vol. 102, p. 108132, Sep. 2022, doi: 10.1016/j.compeleceng.2022.108132.

L. Fernandes, “FRAUD IN ELECTRONIC PAYMENT TRANSACTIONS: THREATS AND COUNTERMEASURES,” Management Review, 2013.

R. K. Gupta et al., “Enhanced framework for credit card fraud detection using robust feature selection and a stacking ensemble model approach,” Results in Engineering, vol. 26, p. 105084, Jun. 2025, doi: 10.1016/j.rineng.2025.105084.

L. Hernandez Aros, L. X. Bustamante Molano, F. Gutierrez-Portela, J. J. Moreno Hernandez, and M. S. Rodríguez Barrero, “Financial fraud detection through the application of machine learning techniques: a literature review,” Humanit Soc Sci Commun, vol. 11, no. 1, p. 1130, Sep. 2024, doi: 10.1057/s41599-024-03606-0.

S. K. Hashemi, S. L. Mirtaheri, and S. Greco, “Fraud Detection in Banking Data by Machine Learning Techniques,” IEEE Access, vol. 11, pp. 3034–3043, 2023, doi: 10.1109/ACCESS.2022.3232287.

A. Hassan, Z. Shukur, and M. K. Hasan, “An Efficient Secure Electronic Payment System for E-Commerce”.

E. Ileberi, Y. Sun, and Z. Wang, “A machine learning based credit card fraud detection using the GA algorithm for feature selection,” J Big Data, vol. 9, no. 1, p. 24, Dec. 2022, doi: 10.1186/s40537-022-00573-8.

C. James, “Predictive Analytics in Financial Fraud Detection and Prevention.

T. Karthikeyan, M. Govindarajan, and V. Vijayakumar, “An effective fraud detection using competitive swarm optimization based deep neural network,” Measurement: Sensors, vol. 27, p. 100793, Jun. 2023, doi: 10.1016/j.measen.2023.100793.

S. Lyeonov, V. Draskovic, Z. Kubaščikova, and V. Fenyves, “Artificial intelligence and machine learning in combating illegal financial operations: Bibliometric analysis,” HT, vol. 20, no. 2, pp. 325–360, Sep. 2024, doi: 10.14254/1795-6889.2024.20-2.5.

D. T. Mosa, S. E. Sorour, A. A. Abohany, and F. A. Maghraby, “CCFD: Efficient Credit Card Fraud Detection Using Meta-Heuristic Techniques and Machine Learning Algorithms,” Mathematics, vol. 12, no. 14, p. 2250, Jul. 2024, doi: 10.3390/math12142250.

M. Nasr, M. Farrag, and M. Nasr, “E-PAYMENT SYSTEMS RISKS, OPPORTUNITIES, AND CHALLENGES FOR IMPROVED RESULTS IN E-BUSINESS,” IJICIS, vol. 20, no. 1, pp. 1–20, Jun. 2020, doi: 10.21608/ijicis.2020.31514.1018.

O. Owen and L. Morgan, “Integrating Machine Learning and Data Analytics for Enhanced Fraud Detection Systems”.

T. H. Pranto, K. T. A. Md. Hasib, T. Rahman, A. B. Haque, A. K. M. N. Islam, and R. M. Rahman, “Blockchain and Machine Learning for Fraud Detection: A Privacy-Preserving and Adaptive Incentive-Based Approach,” IEEE Access, vol. 10, pp. 87115–87134, 2022, doi: 10.1109/ACCESS.2022.3198956.

T. Paladini, F. Monti, M. Polino, M. Carminati, and S. Zanero, “Fraud Detection under Siege: Practical Poisoning Attacks and Defense Strategies,” ACM Transactions on Privacy and Security, vol. 26, no. 4, Oct. 2023, doi: 10.1145/3613244.

E. Polytarchos, “Credit Card Fraud Detection Through Deep Learning and Real-Time Data Streams: A Comparison and New Directions,” FinTech and Sustainable Innovation, 2025, doi: 10.47852/bonviewfsi52026108

J. Parker and L. Mitchell, “Predictive Analytics and Machine Learning for Fraud Detection and Risk Management in Digital Banking”.

K. Patel, “Credit Card Analytics: A Review of Fraud Detection and Risk Assessment Techniques,” IJCTT, vol. 71, no. 10, pp. 69–79, Oct. 2023, doi: 10.14445/22312803/IJCTT-V71I10P109.

M. D. J. Peters et al., “Updated methodological guidance for the conduct of scoping reviews,” 2020.

A. Rizky, A. Gunawan, M. A. Komara, and M. Madani, “Optimization of Machine Learning Algorithms for Fraud Detection in E-Payment Systems”.

Viraj Soni, “Fraud Detection in Credit Card Transactions: A Machine Learning Approach,” jes, vol. 20, no. 11s, pp. 3938–3954, Nov. 2024, doi: 10.52783/jes.8318.

S. Subramanian, “Fort-Trust: Safeguarding online transactions by machine learning,” Salud, Ciencia y Tecnología - Serie de Conferencias, vol. 3, p. 1026, Jul. 2024, doi: 10.56294/sctconf20241026.

Md. A. Talukder, M. Khalid, and M. A. Uddin, “An integrated multistage ensemble machine learning model for fraudulent transaction detection,” J Big Data, vol. 11, no. 1, p. 168, Nov. 2024, doi: 10.1186/s40537-024-00996-5.

A. A. Taha and S. J. Malebary, “An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine,” IEEE Access, vol. 8, pp. 25579–25587, 2020, doi: 10.1109/ACCESS.2020.2971354.

A. Tella and I. Abdulmumin, “Predictors of Users’ Satisfaction with E-payment System: a Case Study of Staff at the University of Ilorin, Nigeria,” vol. 48, no. 4, 2015.

E. C. Victor, A. I. Godspower, and A. O. Samuel, “Comparative Study of Real-Time and Batch Processing Approaches in Machine Learning-Based Fraud Detection for Financial Institutions,” IAA Journal of Scientific Research, vol. 12, no. 2, pp. 60–70, Aug. 2025, doi: 10.59298/IAAJSR/2025/1226070.00.

P. Vanini, S. Rossi, E. Zvizdic, and T. Domenig, “Online payment fraud: from anomaly detection to risk management,” Financ Innov, vol. 9, no. 1, p. 66, Mar. 2023, doi: 10.1186/s40854-023-00470-w.

C. Zhao, X. Sun, M. Wu, and L. Kang, “Advancing financial fraud detection: Self-attention generative adversarial networks for precise and effective identification,” Finance Research Letters, vol. 60, p. 104843, Feb. 2024, doi: 10.1016/j.frl.2023.104843.