Analysis and Metaphysics
ISSN: 1584-8574, e-ISSN: 2471-0849
Vol 25 (1), 2026
pp. 19–36

Financial Fraud Detection Using Artificial Intelligence in Colombia: A Systematic Literature Review

Deixy Ximena Ramos Rivadeneira[1] , Fabio Emilio Coral Melo[2], Dillan Alexander Cardenas Melo[3]

[1] Universidad CESMAG, Colombia, Email: dxramos@unicesmag.edu.co
[1] Universidad CESMAG, Colombia, Email: dxramos@unicesmag.edu.co
[1] Universidad CESMAG, Colombia, Email: dxramos@unicesmag.edu.co

Abstract

Financial fraud has become one of the main challenges in the financial and accounting sectors due to the increasing sophistication of fraudulent schemes and the rapid digitalization of financial services. In this context, artificial intelligence (AI) has emerged as a strategic solution for improving fraud detection through predictive analytics, anomaly detection, and automated decision-making. This study presents a systematic literature review (SLR) aimed at analyzing the main artificial intelligence techniques applied to financial fraud detection, as well as their benefits, challenges, and future research directions, with particular emphasis on the Colombian context. The review followed the methodological guidelines proposed by Barbara Kitchenham and included studies published between 2020 and 2025 in databases such as Scopus, ScienceDirect, Google Scholar, and Redalyc. A total of 388 records were initially identified, from which 40 studies were selected after applying screening and quality assessment criteria. The findings indicate that machine learning, deep learning, graph-based models, and hybrid architecture are the most widely used approaches for detecting fraud in banking systems, Fintech ecosystems, tax administration, and public procurement processes. The results also reveal significant improvements in anomaly detection, operational efficiency, and real-time monitoring. However, important challenges remain regarding explainability, data accessibility, regulatory frameworks, and the shortage of specialized human talent. Overall, the study highlights the growing relevance of AI-driven fraud detection systems and the need for explainable, scalable, and ethically aligned solutions for future financial environments.

Keywords: Artificial Intelligence; Financial Fraud Detection; Machine Learning; Deep Learning; Systematic Literature Review; Fintech; Explainable AI.

Analysis and Metaphysics
ISSN: 1584-8574, e-ISSN: 2471-0849
Vol 25 (1), 2026
pp. 19–36

Received: 15 February 2026 **Received:** 05 March 2026 **Accepted:** 21 March 2026

1. Introduction

Financial fraud has become one of the most critical challenges in the accounting and business environment, driven by the increasing digitalization of financial operations and the growing sophistication of fraudulent schemes. Traditional rule-based approaches have shown significant limitations in detecting complex and evolving fraud patterns, highlighting the need for more advanced technological solutions [1].

In this context, artificial intelligence (AI) has emerged as a key tool for fraud detection, enabling the analysis of large volumes of data, the identification of anomalous patterns, and the generation of real-time alerts. Techniques such as *Machine Learning* and *Deep Learning* have demonstrated high effectiveness in detecting fraudulent behavior, surpassing traditional systems and significantly reducing detection errors [2].

Furthermore, the integration of artificial intelligence with emerging technologies such as *Blockchain* and advanced analytics has strengthened the security and transparency of financial transactions. These technologies not only support fraud detection but also enable prevention through predictive and adaptive models. However, their implementation presents important challenges, including data quality issues, model interpretability, and the need for specialized human capital [3].

Within this framework, the systematic literature review (SLR) emerges as a rigorous methodology to synthesize existing knowledge, identify research trends, and analyze the main advances in the application of artificial intelligence in financial fraud detection. Recent studies have employed this approach to examine multiple investigations, revealing the exponential growth of AI-based techniques in the financial sector while highlighting both their benefits and limitations [4].

In this sense, the present study aims to analyze, from a systematic perspective, the role of artificial intelligence in the detection, prevention, and management of financial fraud through a comprehensive review of recent scientific literature. The study seeks to identify trends, opportunities, challenges, and research gaps, particularly in emerging contexts such as Colombia, contributing to the strengthening of transparency, efficiency, and trust in accounting and financial systems.

Finally, this article is structured as follows: first, the research problem, research questions, and objectives are presented; second, the theoretical framework and related work are discussed; third, the methodology used for the systematic literature review is described; and finally, the results, discussion, and conclusions derived from the study are presented.

2. Method

This study was conducted using a systematic literature review (SLR) approach, following the methodological guidelines proposed by Barbara Kitchenham. This approach enables a structured, transparent, and reproducible process for identifying, evaluating, and synthesizing existing research.

The methodological design was structured into sequential and interrelated stages, including the formulation of research questions, the development of a search strategy, the selection and screening of studies, the assessment of methodological quality, and the extraction and synthesis of data. This structured process ensured methodological consistency and facilitated the traceability of the review.

2.1 Research Questions

To guide the review process, the following research questions (RQs) were defined:

- RQ1: What types of financial fraud have been addressed using artificial intelligence techniques in Colombia?
- RQ2: Which artificial intelligence methods are most commonly used for financial fraud detection?
- RQ3: What outcomes or benefits have been reported from the application of these techniques?
- RQ4: What research gaps or future research directions can be identified in this field?

These questions were formulated based on the PICO framework, which allows the structured definition of key components in systematic reviews, including population, intervention, and outcomes. This approach facilitated a focused and coherent analysis of the scientific evidence.

2.2 Search Strategy

The search process was designed to ensure comprehensive coverage of relevant scientific literature. To achieve this, four major academic databases were selected due to their recognized quality and international scope: Scopus, ScienceDirect, Google Scholar, and Redalyc.Scopus

- ✓ ScienceDirect
- ✓ Google Scholar
- ✓ Redalyc

Analysis and Metaphysics
ISSN: 1584-8574, e-ISSN: 2471-0849
Vol 25 (1), 2026
pp. 19–36

A structured search string was developed by combining key terms related to financial fraud and artificial intelligence, using Boolean operators (AND, OR) and incorporating synonyms and related concepts to maximize the retrieval of relevant studies. The final search equation was defined as follows:

("financial fraud" OR "financial crime" OR "accounting fraud" OR "fraud detection") AND ("artificial intelligence" OR "machine learning" OR "deep learning")

The application of this search strategy across the selected databases resulted in the identification of 388 records, published between 2020 and 2025 in English and Spanish

2.3 Selection of Studies

The identified studies were subjected to a rigorous screening and filtering process to determine their relevance to the research scope. This process included the removal of duplicate records, the evaluation of titles and abstracts, and the application of predefined inclusion and exclusion criteria.

The inclusion criteria considered peer-reviewed articles published between 2020 and 2025, focused on financial fraud detection using artificial intelligence techniques, with full-text availability and published in English or Spanish. The exclusion criteria involved duplicate records, non-accessible documents, studies lacking scientific rigor, and research not directly related to artificial intelligence applications in fraud detection.

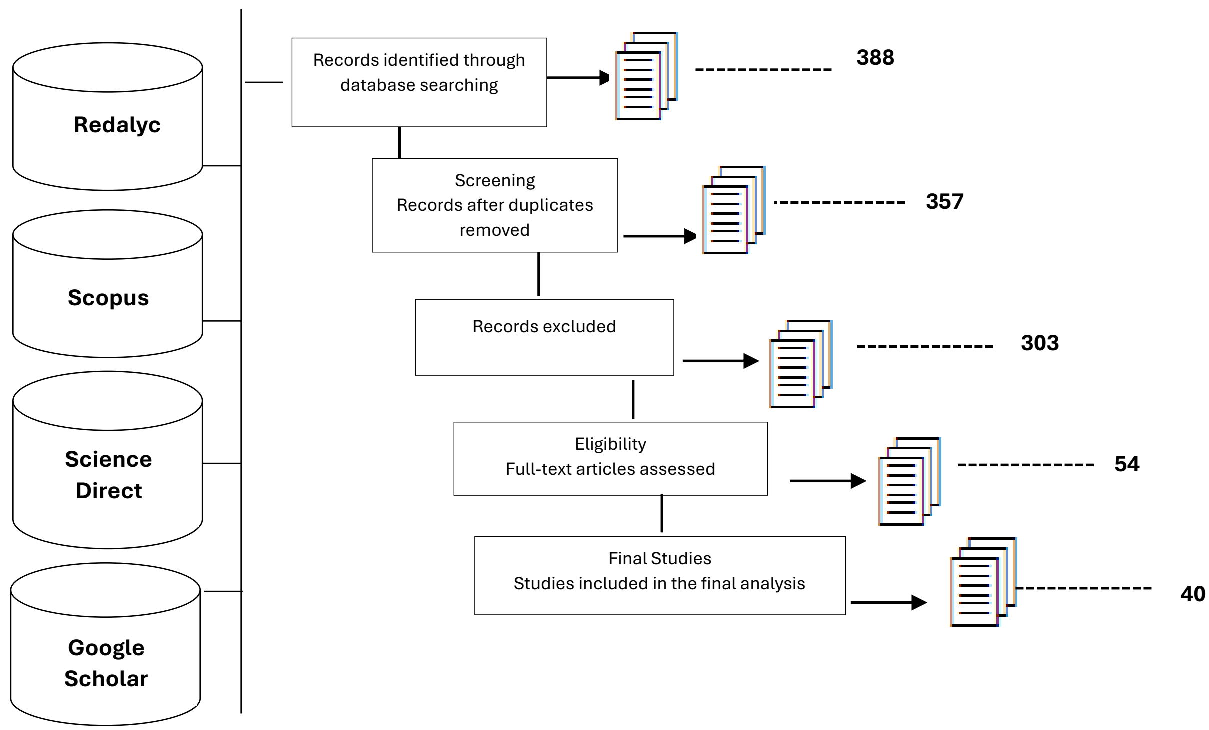
The screening process was supported by Rayyan, which facilitated the identification of duplicates and the preliminary classification of studies. Subsequently, the selected articles were managed using Zotero to ensure systematic organization and traceability.

The study selection process is illustrated in Figure 1, which summarizes the identification, screening, and inclusion phases.

Analysis and Metaphysics
ISSN: 1584-8574, e-ISSN: 2471-0849
Vol 25 (1), 2026
pp. 19–36

Figura 1

Proceso de búsqueda, filtrado y selección de los estudios



From the initial 388 records identified, 31 were removed due to duplication or incomplete information. After the screening phase, 303 studies were excluded for not meeting the inclusion criteria. Subsequently, a stricter full-text assessment was conducted, applying additional quality criteria such as methodological rigor, relevance, and clarity of results.

As a result, 40 studies were selected for the final analysis.

2.4 Quality assessment

The methodological quality of the selected studies was evaluated using a set of criteria aimed at assessing their scientific validity and relevance. These criteria included source credibility, research clarity, methodological rigor, contextual relevance, and consistency in data analysis.

Each of the 54 selected articles was thoroughly reviewed to ensure compliance with these standards, allowing the construction of a robust and reliable evidence base for the study.

2.5 Data extraction and synthesis of results

Data extraction was conducted systematically, focusing on key variables such as the type of financial fraud addressed, the artificial intelligence techniques employed, the results obtained, and the limitations identified in each study. The extracted data were organized into a structured database, facilitating comparison and classification.

The synthesis of results was performed using a qualitative approach, enabling the identification of patterns, emerging trends, and research gaps in the application of artificial intelligence for financial fraud detection.

3. Results and discussion

This section presents the main findings derived from the systematic review, followed by a critical discussion that contrasts the results with existing literature and highlights their implications for future research and practice.

3.1 Types of Financial Fraud Addressed Using Artificial Intelligence in Colombia

Administration the selected studies reveals that the application of artificial intelligence (AI) in Colombia is concentrated on a set of well-defined financial fraud typologies, primarily associated with the banking sector, Fintech ecosystems, public administration, and tax control systems. These findings indicate that AI adoption is not homogeneous but rather aligned with high-risk domains characterized by large volumes of transactional data and complex relational structures [5].

In the context of transactional and credit fraud within Fintech and digital ecosystems, the literature highlights threats such as account takeover (ATO), fraudulent account creation through bots, and the misuse of stolen credit cards in digital wallets. These fraud modalities have been effectively addressed through advanced machine learning and deep learning techniques, particularly graph-based models that capture relationships between users, devices, and transactions. Studies demonstrate that Graph Neural Networks (GNNs) significantly improve fraud detection performance by modeling relational dependencies beyond traditional tabular data [6].

Similarly, recent research emphasizes that fraud in digital financial platforms is increasingly characterized by network-based behavior, where fraudulent actors operate in coordinated structures. In this sense, graph-based learning approaches allow the identification of hidden connections and suspicious clusters, outperforming classical classification models [7].

Analysis and Metaphysics
ISSN: 1584-8574, e-ISSN: 2471-0849
Vol 25 (1), 2026
pp. 19–36

Furthermore, the integration of AI into tax administration systems has enabled the transition from reactive auditing to predictive and preventive control models, allowing early detection of suspicious behaviors and improving the efficiency of fiscal oversight [8].

Regarding fraud in public procurement and corruption-related activities, the literature identifies patterns such as contract overpricing, collusion between contractors, and misallocation of public funds. These types of fraud are typically detected through large-scale data integration from public information systems combined with predictive analytics models. Studies highlight that machine learning techniques, particularly classification and clustering algorithms, are effective in detecting irregularities in public contracts and identifying high-risk relationships between entities [9].

In the case of internal banking fraud, financial institutions have implemented data mining and classification models to detect anomalous behavior among employees and operational processes. These approaches focus on identifying deviations from historical transaction patterns and preventing operational losses. Recent studies confirm that supervised learning models, such as decision trees and ensemble methods, remain highly effective for internal fraud detection in structured financial environments [10]. Additionally, AI-based behavioral analytics have shown strong capabilities in identifying suspicious transaction sequences and unusual user interactions in real time, reducing the operational impact of fraudulent activities in Fintech and digital payment platforms. These approaches improve fraud prevention by detecting anomalous user behavior patterns before financial losses occur [11]

Furthermore, recent evidence suggests that financial institutions are increasingly adopting AI-driven monitoring systems due to the limitations of traditional auditing approaches in detecting dynamic and sophisticated fraud schemes. AI-based fraud detection models enable continuous monitoring of transactional activities and improve the identification of abnormal financial behaviors in digital banking environments [12].

Moreover, recent studies have identified a growing increase in fraud associated with cryptocurrency transactions and decentralized financial ecosystems (DeFi). These fraud schemes include money laundering, phishing attacks, fraudulent token operations, and illicit crypto-asset transfers. Artificial intelligence techniques, particularly anomaly detection models and blockchain analytics, have demonstrated strong capabilities in tracking suspicious transactional behaviors and identifying irregular patterns within decentralized financial networks [13] .

Another emerging area involves fraud related to digital identity theft and synthetic identities in online financial services. Fraudsters increasingly combine stolen and artificially generated personal information to bypass authentication systems and access banking or credit services. In response, AI-based biometric verification systems and behavioral analytics models have become critical tools for detecting identity inconsistencies and preventing unauthorized financial access in digital platforms Additionally, the literature highlights the increasing use of artificial intelligence for detecting insurance fraud and fraudulent claims within digital financial ecosystems [14]. Machine learning algorithms and predictive analytics models enable the identification of anomalous claim patterns, suspicious customer behaviors, and inconsistencies in financial documentation. These approaches contribute to reducing operational losses and improving the efficiency of fraud investigation processes in insurance and risk management sectors [15].

Furthermore, recent literature highlights the growing relevance of artificial intelligence in detecting fraud associated with electronic commerce and online payment systems. Fraudulent activities such as transaction laundering, fake merchants, and unauthorized payment operations have increased alongside the expansion of digital commerce platforms. In response, AI-driven fraud detection systems supported by real-time analytics and behavioral profiling have demonstrated strong capabilities in identifying abnormal purchasing patterns and suspicious payment behaviors, improving transaction security and reducing financial risk exposure in online financial ecosystems [16].

3.2 Artificial Intelligence Methods Used in Financial Fraud Detection

The analysis of the selected studies indicates that financial fraud detection using artificial intelligence is primarily based on machine learning (ML) and deep learning (DL) techniques, whose selection depends on data availability, labeling conditions, and the complexity of fraud patterns. The literature reveals a clear methodological classification into supervised learning, unsupervised learning, deep learning, natural language processing, and hybrid models [17].

In the case of supervised learning, this approach remains the most widely used due to the availability of labeled datasets, where transactions are previously classified as legitimate or fraudulent. Algorithms such as Random Forest, Support Vector Machines (SVM), logistic regression, and ensemble methods (e.g., XGBoost and AdaBoost) are frequently applied due to their robustness and interpretability. Recent studies confirm that ensemble models significantly improve predictive performance in fraud detection tasks, achieving higher accuracy and lower false-positive rates compared to single models [18]

Similarly, large-scale evaluations demonstrate that Random Forest and gradient boosting methods outperform traditional statistical approaches in high-dimensional financial datasets, particularly in credit card fraud detection scenarios [19]

In contrast, unsupervised learning techniques have gained relevance in contexts characterized by data imbalance or lack of labeled information, which is common in fraud detection. Methods such as K-Means, DBSCAN, Isolation Forest, and One-Class SVM enable anomaly detection by identifying deviations from normal behavior patterns. Recent research highlights that anomaly detection models are particularly effective for identifying unknown or emerging fraud schemes [20] Furthermore, studies indicate that combining clustering techniques with anomaly detection significantly enhances the ability to detect hidden fraud structures in large transactional datasets

Regarding deep learning approaches, these techniques have become increasingly relevant in complex financial environments involving Big Data and real-time processing. Architectures such as Recurrent Neural Networks (RNN) and Long Short-Term Memory (LSTM) are particularly effective for modeling temporal sequences and detecting evolving fraud patterns over time. Additionally, autoencoders are widely used for anomaly detection through reconstruction error analysis, while Artificial Neural Networks (ANN) enable the extraction of complex nonlinear features [21]

Another important methodological approach is Natural Language Processing (NLP), which focuses on analyzing unstructured data such as financial reports, emails, and contracts. NLP techniques enable the detection of linguistic anomalies, semantic inconsistencies, and suspicious communication patterns associated with fraud. Recent research highlights the use of large language models (LLMs) and text mining techniques to identify manipulation in financial disclosures and detect insider trading signals [22].

3.3 Benefits and Outcomes of Artificial Intelligence in Financial Fraud Detection

The systematic review reveals that the implementation of artificial intelligence (AI) in financial fraud detection within the Colombian context has generated significant improvements in accuracy, efficiency, and decision-making capabilities across multiple sectors.

In the domain of tax and customs fraud, the application of unsupervised and predictive models has achieved high levels of precision in anomaly detection, reaching rates close to 98%. These approaches have enabled tax authorities to automate risk analysis processes and identify complex concealment structures, such as hidden financial networks and tax evasion schemes. In Colombia, the integration of AI into systems such as electronic invoicing platforms and fiscal information systems has strengthened the capacity to process large volumes of data and detect irregular patterns, contributing to increased tax collection and reduced evasion [23].

Regarding fraud in public procurement and fiscal control, the evidence indicates a substantial improvement in the efficiency of oversight entities. The use of predictive analytics, pattern recognition, and large-scale data integration has allowed the early identification of high-risk contracts, cost overruns, and anomalous relationships between contractors. Unlike traditional audit approaches based on sampling, AI-driven systems enable the evaluation of the entire dataset, significantly enhancing the detection of irregularities and increasing institutional productivity[24].

In the banking and private financial auditing sector, AI has contributed to reducing the time required for financial reviews and improving responsiveness to suspicious transactions. By leveraging data mining techniques and classification models, organizations are now capable of analyzing the complete universe of financial transactions rather than limited samples [25]. This shift has enabled the detection of anomalies such as fictitious suppliers, irregular accounting records, and unusual behavioral patterns, resulting in lower operational costs and improved fraud prevention capabilities.

Similarly, in digital financial ecosystems, including Fintech platforms and electronic wallets, AI-based approaches have demonstrated strong predictive performance. Graph-based deep learning models, particularly Relational Graph Convolutional Networks (R-GCN), have proven effective in detecting fraud in high-volume environments by analyzing relationships between users, devices, and transaction [26] . These models are especially valuable in identifying risks associated with new users who lack historical data, allowing fraud detection even before the first transaction occurs. Performance metrics reported in the literature, such as AUC values close to 0.80, confirm the superiority of these approaches over traditional models [27].

Furthermore, recent studies indicate that AI-based fraud detection systems have significantly improved real-time monitoring capabilities in financial institutions. Through the integration of streaming analytics and automated alert mechanisms, organizations can now identify suspicious activities almost instantly, reducing response times and minimizing financial losses associated with

Analysis and Metaphysics
ISSN: 1584-8574, e-ISSN: 2471-0849
Vol 25 (1), 2026
pp. 19–36

fraudulent transactions. These intelligent monitoring systems also contribute to strengthening operational resilience and improving risk management processes in dynamic digital environments [15].

Another important benefit identified in the literature is the reduction of false-positive rates in fraud detection processes. Traditional rule-based systems frequently generate large volumes of incorrect alerts, increasing operational costs and reducing auditing efficiency. In contrast, machine learning and hybrid AI models are capable of learning complex transactional behaviors and distinguishing legitimate operations from suspicious activities with greater precision. This improvement not only optimizes resource allocation but also enhances customer experience by reducing unnecessary transaction interruptions [28]

In addition, the adoption of artificial intelligence has facilitated the transition toward data-driven auditing and continuous financial supervision models. AI technologies enable the automated analysis of large-scale financial datasets, improving transparency, traceability, and institutional decision-making processes. Recent evidence suggests that these capabilities strengthen strategic planning and support proactive fraud prevention mechanisms, particularly in highly digitalized financial ecosystems and public administration environments [29].

3.4 Research Gaps and Future Directions

Despite the progress achieved by institutions such as the tax authority and fiscal control agencies, the adoption of artificial intelligence (AI) for financial fraud detection in Colombia remains at an early stage of maturity. The literature reveals the existence of structural gaps that require immediate attention from both academia and policymakers[30].

One of the most critical challenges relates to regulatory frameworks and algorithmic ethics. Current evidence highlights the absence of robust regulations guiding the use of AI and emerging technologies such as blockchain in auditing and fiscal control processes. This regulatory gap increases the risk of algorithmic bias and potential violations of data protection principles. In this context, the development of ethical governance frameworks and explainable AI (XAI) mechanisms is essential to ensure transparency, accountability, and legal validity of algorithmic decisions [31].

Another significant limitation concerns data accessibility and the lack of empirical impact evaluation. There are considerable barriers to accessing reliable public data on the actual implementation and effectiveness of AI-based fraud detection systems. Furthermore, empirical

Analysis and Metaphysics
ISSN: 1584-8574, e-ISSN: 2471-0849
Vol 25 (1), 2026
pp. 19–36

studies measuring the real impact of these technologies on fraud reduction remain scarce. This situation highlights the need for rigorous research supported by standardized performance metrics that enable transparent and comparable evaluations [32] .

From a technical perspective, system integration challenges also represent a major barrier. Many organizations struggle to adapt legacy accounting and financial systems to modern data-driven architectures, limiting the effective implementation of automated and continuous auditing models. These constraints are not only technological but also financial, as the transition requires significant investment in infrastructure and system redesign [33].

In addition, a critical gap is observed in professional training and organizational culture. The successful adoption of AI requires advanced technical competencies in areas such as data analytics, programming, and cybersecurity. However, the current workforce in accounting and auditing often lacks these skills, which generates resistance to technological change and slows down digital transformation processes. Addressing this issue requires the modernization of academic programs and the incorporation of emerging fields such as digital forensic accounting and data-driven auditing [34].

Overall, the findings suggest that the main barriers to AI adoption in Colombia extend beyond technological limitations and are primarily rooted in regulatory, institutional, and human factors. There is a clear mismatch between the rapid evolution of digital technologies and the slower adaptation of legal frameworks and educational systems [35].

From a future research perspective, it is essential to prioritize the development of explainable and trustworthy AI models, particularly in public sector applications, where transparency and accountability are critical. Additionally, further empirical studies are needed to evaluate the efficiency, cost-effectiveness, and real-world impact of AI solutions in fraud detection. Achieving this will require greater collaboration between academia, government, and industry, as well as the reduction of data access restrictions that currently hinder rigorous scientific analysis[36].

Furthermore, recent studies emphasize that one of the emerging challenges in AI-based fraud detection is the increasing vulnerability of intelligent systems to adversarial attacks and cyber manipulation techniques. Fraudsters are progressively adapting their strategies to evade automated detection mechanisms, which creates the need for more resilient, adaptive, and self-learning fraud detection architectures capable of responding to evolving cyber-financial threats [37]. In this context, future research should focus on the development of robust AI security frameworks that combine fraud analytics with cybersecurity and real-time threat intelligence systems [38]

Another important research gap concerns the limited incorporation of sustainability and social responsibility principles into AI-driven financial control systems. Current fraud detection models are primarily oriented toward predictive performance, while ethical implications, social impact, and responsible AI governance remain insufficiently explored. Recent literature highlights the importance of integrating fairness, transparency, and human-centered approaches into financial AI ecosystems to reduce discriminatory outcomes and strengthen institutional trust in automated auditing processes [39].

Finally, the literature suggests that future advances in financial fraud detection will increasingly depend on interdisciplinary collaboration between computer science, accounting, law, cybersecurity, and data governance. The complexity of modern fraud schemes requires integrated analytical approaches capable of combining technical innovation with regulatory compliance and organizational adaptability. Consequently, future research should prioritize the creation of collaborative frameworks that facilitate secure data sharing, cross-sector interoperability, and the development of standardized methodologies for evaluating AI-based fraud detection systems [40]

Conclusions

This systematic literature review demonstrates that artificial intelligence has become a key tool for financial fraud detection, improving the accuracy, speed, and efficiency of auditing and risk management processes. The findings reveal that machine learning, deep learning, graph-based models, and hybrid architectures are the most widely used approaches, particularly in banking systems, Fintech platforms, tax administration, and public procurement oversight.

The review also shows that AI enables the analysis of large-scale transactional data, facilitating the early identification of anomalous behaviors and complex fraud networks. In Colombia, both public and private institutions are progressively adopting predictive analytics and automated fraud detection systems, contributing to more proactive and data-driven control mechanisms.

Despite these advances, important challenges remain, including limited regulatory frameworks, restricted access to quality datasets, integration difficulties with legacy systems, and the lack of explainable and transparent AI models. Additionally, the shortage of specialized human talent continues to limit the effective adoption of these technologies.

Overall, the evidence suggests that the future of financial fraud detection will increasingly depend on explainable, hybrid, and real-time AI models capable of adapting to evolving fraud schemes. Future research should therefore focus on improving model transparency, standardizing evaluation methods, and strengthening collaboration between academia, government, and industry.

References

[1] K. V. Srinivasa, "Machine Learning for Fraud Detection in Financial Transactions," *Int. J. Sci. Technol.*, vol. 16, no. 1, pp. 1–9, 2025, doi: 10.71097/ijsat.v16.i1.3727.

[2] Y. Chen, C. Zhao, Y. Xu, C. Nie, and Y. Zhang, "Deep Learning in Financial Fraud Detection: Innovations, Challenges, and Applications," *Data Sci. Manag.*, Aug. 2025, doi: 10.1016/j.dsm.2025.08.002.

[3] N. Uddin, "Role of AI in Preventing Financial Crime: A Comprehensive Analytical Review," *J. Econ. Criminol.*, p. 100200, Oct. 2025, doi: 10.1016/j.jeconc.2025.100200.

[4] Olawale Olowu *et al.*, "AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity," *GSC Adv. Res. Rev.*, vol. 21, no. 2, pp. 227–237, Nov. 2024, doi: 10.30574/gscarr.2024.21.2.0418.

[5] Prabin Adhikari, Prashamsa Hamal, and Francis Baidoo Jnr, "Artificial Intelligence in fraud detection: Revolutionizing financial security," *Int. J. Sci. Res. Arch.*, vol. 13, no. 1, pp. 1457–1472, Sep. 2024, doi: 10.30574/ijsra.2024.13.1.1860.

[6] H. Yang, Z. Shukur, and S. Sahran, "A Review of Artificial Intelligence for Financial Fraud Detection," *Appl. Sci.*, vol. 16, no. 4, p. 1931, Feb. 2026, doi: 10.3390/app16041931.

[7] M. Z. H. George, M. K. Alam, and M. T. Hasan, "MACHINE LEARNING FOR FRAUD DETECTION IN DIGITAL BANKING: A SYSTEMATIC LITERATURE REVIEW," *ASRC Procedia Glob. Perspect. Sci. Scholarsh.*, vol. 03, no. 01, pp. 37–61, Jan. 2023, doi: 10.63125/913ksy63.

[8] A. A. Compagnino *et al.*, "An Introduction to Machine Learning Methods for Fraud Detection," *Appl. Sci.*, vol. 15, no. 21, p. 11787, Nov. 2025, doi: 10.3390/app152111787.

[9] K. O. Alotaibi, "A Financial Fraud Detection Model Using Artificial Intelligence," *Eng. Technol. Appl. Sci. Res.*, vol. 16, no. 1, pp. 31579–31584, Feb. 2026, doi: 10.48084/etasr.15892.

[10] 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.

[11] T. Sodnomdavaa and G. Lkhagvadorj, “Financial Statement Fraud Detection Through an Integrated Machine Learning and Explainable AI Framework,” *J. Risk Financ. Manag.*, vol. 19, no. 1, p. 13, Dec. 2025, doi: 10.3390/jrfm19010013.

[12] . Mani, A. S., D. V., and D. R., “Financial Fraud Detection in Transactions Using AI,” in *Proceedings of the 1st International Conference on Research and Development in Information, Communication, and Computing Technologies*, SCITEPRESS - Science and Technology Publications, 2025, pp. 515–521. doi: 10.5220/0013868500004919.

[13] T. Fawcett and F. Provost, “Adaptive Fraud Detection,” *Data Min. Knowl. Discov.*, vol. 1, no. 3, pp. 291–316, Sep. 1997, doi: 10.1023/A:1009700419189.

[14] R. J. Bolton and D. J. Hand, “Statistical Fraud Detection: A Review,” *Stat. Sci.*, vol. 17, no. 3, Aug. 2002, doi: 10.1214/ss/1042727940.

[15] 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, Feb. 2011, doi: 10.1016/j.dss.2010.08.006.

[16] I. L. S. Russo, H. S. Bernardino, and H. J. C. Barbosa, “Knowledge discovery in multiobjective optimization problems in engineering via Genetic Programming,” *Expert Syst. Appl.*, vol. 99, pp. 93–102, Jun. 2018, doi: 10.1016/j.eswa.2017.12.008.

[17] A. Faccia, “Explainable AI (XAI) in Auditing: Bridging the Gap Between Predictive Fraud Models and Regulatory Standards,” *J. Risk Financ. Manag.*, vol. 19, no. 5, p. 311, Apr. 2026, doi: 10.3390/jrfm19050311.

[18] C. Gallent Torres, A. Zapata González, and J. L. Ortego Hernando, “El impacto de la inteligencia artificial generativa en educación superior: una mirada desde la ética y la integridad académica,” *Reli. - Rev. Electrónica Investig. y Evaluación Educ.*, vol. 29, no. 2,

Dec. 2023, doi: 10.30827/relieve.v29i2.29134.

[19] . Mani, A. S., D. V., and D. R., "Financial Fraud Detection in Transactions Using AI," vol. 1, pp. 515–521, 2025, doi: 10.5220/0013868500004919.

[20] T. A. Siddquee, "AI in Banking Risk Management and Fraud Detection in Preventing Financial Crimes and Optimizing Credit Decisions," *Int. J. Soc. Sci. Res. Rev.*, vol. 8, no. 8, pp. 391–404, Aug. 2025, doi: 10.47814/ijssrr.v8i8.2889.

[21] Z. Li, G. Zhang, and Y. Wang, "Flash-oriented Coded Storage: Research Status and Future Directions," *ACM Trans. Storage*, vol. 21, no. 1, pp. 1–37, Jan. 2025, doi: 10.1145/3708995.

[22] H. Nathasya, "Fraud Detection using Machine Learning," *Edu Res. Indones. Inst. Corp. Learn. Stud.*, vol. 5, no. 1, pp. 70–80, 2024, doi: 10.14293/PR2199.000647.v1.

[23] B. Bigliardi, V. Dolci, S. Filippelli, B. Pini, A. Petroni, and L. Tagliente, "Circular Economy in the Food Supply Chain: A literature review," *Procedia Comput. Sci.*, vol. 232, pp. 3024–3033, 2024, doi: 10.1016/j.procs.2024.02.118.

[24] S. Park, J. Ban, and S. Doh, "Hybrid Reaching Law of Sliding Mode Position-Sensorless Speed Control for Switched Reluctance Motors," *Electronics*, vol. 14, no. 3, p. 577, Jan. 2025, doi: 10.3390/electronics14030577.

[25] X. Chen, C. Liu, B. Lin, J. Lai, and D. Miao, "AHA-3WKM: The optimization of K-means with three-way clustering and artificial hummingbird algorithm," *Inf. Sci. (Ny).*, vol. 672, p. 120661, Jun. 2024, doi: 10.1016/j.ins.2024.120661.

[26] H. Vadher *et al.*, "EEG-based biometric authentication system using convolutional neural network for military applications," *Secur. Priv.*, vol. 7, no. 2, Mar. 2024, doi: 10.1002/spy2.345.

[27] A. Matsui, R. Ishibashi, and L. Meng, "Optimizing Loss Functions for You Only Look Once Models: Improving Object Detection in Agricultural Datasets," *Computers*, vol. 14, no. 2, p. 44, Jan. 2025, doi: 10.3390/computers14020044.

[28] J. West and M. Bhattacharya, "Intelligent financial fraud detection: A comprehensive review," *Comput. Secur.*, vol. 57, pp. 47–66, Mar. 2016, doi: 10.1016/j.cose.2015.09.005.

[29] W. N. Dilla, "Can Avatars Fight Fraud? How Virtual Business Environments Facilitate Learning More About Fraud Investigation and Prevention," *J. Inf. Syst.*, vol. 27, no. 2, pp. 127–130, Dec. 2013, doi: 10.2308/isys-10371.

[30] A. Barredo Arrieta *et al.*, "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," *Inf. Fusion*, vol. 58, pp. 82–115, Jun. 2020, doi: 10.1016/j.inffus.2019.12.012.

[31] N. Mehrabi, F. Morstatter, N. Saxena, K. Lerman, and A. Galstyan, "A Survey on Bias and Fairness in Machine Learning," *ACM Comput. Surv.*, vol. 54, no. 6, pp. 1–35, Jul. 2022, doi: 10.1145/3457607.

[32] R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, F. Giannotti, and D. Pedreschi, "A Survey of Methods for Explaining Black Box Models," *ACM Comput. Surv.*, vol. 51, no. 5, pp. 1–42, Sep. 2019, doi: 10.1145/3236009.

[33] P. Kairouz and H. B. McMahan, "Advances and Open Problems in Federated Learning," *Found. Trends® Mach. Learn.*, vol. 14, no. 1–2, pp. 1–210, Jun. 2021, doi: 10.1561/2200000083.

[34] Y. K. Dwivedi *et al.*, "Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy," *Int. J. Inf. Manage.*, vol. 57, p. 101994, Apr. 2021, doi: 10.1016/j.ijinfomgt.2019.08.002.

[35] A. Jobin, M. Ienca, and E. Vayena, "The global landscape of AI ethics guidelines," *Nat. Mach. Intell.*, vol. 1, no. 9, pp. 389–399, Sep. 2019, doi: 10.1038/s42256-019-0088-2.

[36] A. De Luca and M. Irigoitia, "Uso de la Técnica de Transfer Learning en Machine Learning para la Clasificación de Productos en el Banco Alimentario de La Plata," 2021. [Online]. Available: http://bancoalimentario.org.ar

[37] R. Spencer, P. Sindall, K. M. Hammond, S. J. Atkins, M. Quinn, and J. J. McMahon, "Changes in Body Mass and Movement Strategy Maintain Jump Height Immediately after Soccer Match," *Appl. Sci.*, vol. 13, no. 12, p. 7188, Jun. 2023, doi: 10.3390/app13127188.

[38] M. N. I. Shibbir, H. Rahman, M. S. Ferdous, and F. Chowdhury, "Evaluating the security of CAPTCHAs utilized on Bangladeshi websites," *Comput. Secur.*, vol. 140, p. 103774, May

2024, doi: 10.1016/j.cose.2024.103774.

[39] E. Strubell, A. Ganesh, and A. McCallum, “Energy and Policy Considerations for Deep Learning in NLP,” in *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, Stroudsburg, PA, USA: Association for Computational Linguistics, 2019, pp. 3645–3650. doi: 10.18653/v1/P19-1355.

[40] R. Charef, E. Ganjian, and S. Emmitt, “Socio-economic and environmental barriers for a holistic asset lifecycle approach to achieve circular economy: A pattern-matching method,” *Technol. Forecast. Soc. Change*, vol. 170, p. 120798, Sep. 2021, doi: 10.1016/j.techfore.2021.120798.