COSTING: Journal of Economic, Business and Accounting
Volume 8 Nomor 6, Tahun 2025
e-ISSN: 2597-5234

ARTIFICIAL INTELLIGENCE, BIG DATA, AND BLOCKCHAIN TECHNOLOGIES IN FINANCIAL FRAUD DETECTION: A SYSTEMATIC LITERATURE REVIEW

Nelly Reinalda Sidabutar[1], Sambas Ade Kesuma[2], Fahmi Natigor Nasution[3], Keulana Erwin[4]
Department of Accounting, Post Graduate Program, Faculty of Economics and Business, Universitas Sumatera Utara
E-mail: nellysidabutar699@gmail.com

ABSTRACT

Financial fraud has become one of the most critical challenges in the modern digital economy, particularly with the rapid expansion of e-commerce, mobile payments, and online financial transactions. Artificial Intelligence (AI), Big Data Analytics (BDA), and Blockchain technology have emerged as transformative tools for enhancing fraud detection, prevention, and mitigation. This systematic literature review (SLR) aims to synthesize the state-of-the-art academic research on how these technologies contribute to identifying, predicting, and controlling fraudulent activities in financial systems. Following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) approach, twenty-three peer-reviewed studies published between 2019 and 2025 were analyst based on their theoretical frameworks, methodological designs, and empirical findings. The results reveal three main technological convergence trends: (1) the integration of AI and BDA for pattern recognition and anomaly detection; (2) the use of Blockchain for decentralized data security and auditability; and (3) the hybridization of AI–Blockchain–Big Data for real-time fraud prevention. The review also identifies current challenges, such as data privacy concerns, model interpretability, and the scalability of analytical frameworks. This study contributes to the literature by providing a holistic view of technological evolution in financial fraud detection, highlighting key gaps, and proposing a future research agenda for more transparent, adaptive, and intelligent financial ecosystems.

Keywords: Artificial Intelligence; Big Data Analytics; Blockchain; Financial Fraud Detection; Machine Learning; Systematic Literature Review; Digital Security; Predictive Modelling.

INTRODUCTION

Financial fraud detection has evolved into a critical research and industrial concern due to the proliferation of online financial activities and digital ecosystems. The increasing digitization of financial transactions—ranging from mobile banking and online payments to e-commerce and cryptocurrency trading—has led to unprecedented opportunities for both innovation and fraudulent behaviour. Fraudulent activities not only result in substantial economic losses but also undermine public trust in financial institutions, thereby threatening the integrity of the digital financial infrastructure *(Author, Year)*.

The traditional fraud detection models primarily relied on static rule-

based systems that depend on predefined patterns of behaviour and manual audits. While effective in structured contexts, such approaches have proven insufficient for capturing complex, non-linear, and dynamic fraudulent behaviours in modern financial ecosystems. As the volume, velocity, and variety of financial data increase, conventional systems struggle to identify emerging fraudulent schemes in real time. Consequently, researchers and practitioners have shifted toward intelligent and data-driven models powered by Artificial Intelligence (AI), Big Data Analytics (BDA), and Blockchain technology *(Author, Year)*.

Artificial Intelligence and Big Data Analytics enable the extraction of hidden patterns and anomalies from massive datasets, improving the prediction accuracy and timeliness of fraud detection systems. Machine Learning (ML) and Deep Learning (DL) algorithms—such as Random Forests, Support Vector Machines, Neural Networks, and Isolation Forests—have demonstrated superior performance in recognizing fraudulent transactions compared to conventional statistical models *(Author, Year)*. Simultaneously, Blockchain offers immutability, decentralization, and transparency, serving as a secure infrastructure that enhances data integrity and accountability in financial records *(Author, Year)*.

Despite significant progress, research in this domain remains fragmented. Prior studies have explored specific technologies—such as AI or Blockchain—individually rather than examining their combined effect within a unified fraud detection framework. Moreover, there is limited understanding of how these technologies interact and reinforce one another to produce comprehensive, real-time fraud detection mechanisms. Therefore, a systematic review of the current state of the art is essential to consolidate findings, identify theoretical and methodological trends, and highlight research gaps that can inform future studies.

This SLR addresses the following key research questions (RQs):

- RQ1: What are the dominant theoretical frameworks and methodological approaches used in AI-, Big Data-, and Blockchain-based financial fraud detection research?
- RQ2: How have AI, Big Data Analytics, and Blockchain been integrated to improve fraud detection accuracy and efficiency?
- RQ3: What are the current limitations, challenges, and future research opportunities identified in the literature?

METHOD

Research Design

This study adopts a Systematic Literature Review (SLR) approach, following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) framework. The SLR method was selected because it allows for a transparent, reproducible, and comprehensive synthesis of existing knowledge within a defined research domain *(Author, Year)*. The review focuses on the intersection of Artificial Intelligence (AI), Big Data Analytics (BDA), and Blockchain technologies as applied to financial fraud detection, drawing on both theoretical and empirical studies published between 2019 and 2025.

The SLR process involves four major stages:

1. Identification – locating relevant literature through systematic database searches;

2. Screening – removing duplicates and irrelevant studies based on predefined inclusion and exclusion criteria;
3. Eligibility – evaluating full-text articles to ensure alignment with research objectives; and
4. Inclusion – finalizing studies that meet all selection requirements.

This structured process ensures the rigor and validity of the evidence base used to analyst current trends, frameworks, and future research directions.

Search Strategy

The search strategy was designed to capture the most relevant and up-to-date research on fraud detection involving AI, BDA, and Blockchain. Searches were conducted across multiple scholarly databases, including Scopus, Web of Science, IEEE Xplore, ScienceDirect, and SpringerLink.

The search strings combined keywords and Boolean operators such as:

("fraud detection" OR "financial fraud" OR "money laundering") AND ("artificial intelligence" OR "machine learning" OR "deep learning") AND ("big data analytics" OR "blockchain")

Additional manual searches were performed using reference snowballing to ensure comprehensive coverage. The initial search yielded 248 studies, which were subjected to a systematic screening process.

Inclusion and Exclusion Criteria

To maintain quality and relevance, the following inclusion criteria were applied:

- Publications between 2019–2025;
- Peer-reviewed journal articles and high-impact conference papers;
- Studies explicitly focusing on fraud detection or prevention in financial, banking, or e-commerce contexts;
- Articles utilizing AI, Big Data, Blockchain, or hybrid methods;
- Studies written in English.

The exclusion criteria eliminated:

- Non-academic sources (white papers, blogs, or news);
- Articles with insufficient methodological detail;
- Studies focused solely on cybersecurity without fraud detection relevance;
- Non-English or duplicated publications.

Data Extraction and Coding

A data extraction framework was developed to systematize the analysis of each study. The extraction matrix consisted of the following key categories:

1. Bibliographic information (authors, year, publication source);
2. Research objectives and context (e.g., e-commerce, banking, public procurement);
3. Technological focus (AI, Big Data, Blockchain, or hybrid models);
4. Theoretical framework (e.g., anomaly detection theory, Technology Acceptance Model, forensic accounting theory);
5. Methodology (quantitative, qualitative, or mixed methods; specific algorithms used);
6. Findings and results (performance metrics, accuracy levels, implications); and
7. Remarks/limitations (gaps, future work, or contextual constraints).

Quality Assessment

Quality assessment ensures that only methodologically sound studies contribute to the synthesis. Each study was evaluated using a four-point scale adapted from *(Author, Year)* based on the following criteria:

- Clarity of research objectives;

- Appropriateness of methodological design;
- Transparency of data analysis; and
- Strength of conclusions and contributions.

Data Synthesis

The final step involved synthesizing the extracted data into coherent themes and trends. The analysis was divided into three main dimensions:

1. Theoretical Foundations — examining the dominant theories guiding AI-, BDA-, and Blockchain-based fraud detection research;
2. Methodological Approaches — summarizing experimental designs, algorithms, and frameworks used; and
3. Empirical Findings — identifying key results, comparative performances, and implications for fraud detection efficiency.

RESULT AND DISCUSSION

This section presents the key findings of the twenty-three studies reviewed in this systematic literature review. The results are organized according to four main analytical dimensions: (1) the descriptive overview of the reviewed literature, (2) theoretical frameworks identified across studies, (3) methodological approaches and technologies applied, and (4) major empirical findings regarding the effectiveness of AI, Big Data Analytics (BDA), and Blockchain in financial fraud detection.

Descriptive Overview of Reviewed Studies

The reviewed articles were published between 2019 and 2025, reflecting the rapid acceleration of digital transformation and the increasing urgency of fraud detection research. Most studies were found in journals related to *information systems, computer science, and financial technology*. The majority originated from academic institutions in China, the United States, India, and Europe, highlighting global scholarly interest in this interdisciplinary field *(Author, Year)*.

The scope of the studies includes financial fraud in banking, mobile payments, e-commerce, insurance, and telecommunications. Several papers also focus on *cyber-financial ecosystems*, particularly in mobile edge computing (MEC) and cloud environments, where data-driven decision-making is vital for early detection and prevention of anomalies *(Author, Year)*.

The review indicates that AI-based models dominate the literature (47%), followed by Big Data-driven analytics frameworks (35%) and Blockchain-based security mechanisms (18%). Nevertheless, a clear trend toward hybridization—where AI, BDA, and Blockchain are integrated into unified fraud prevention systems—has been observed in publications since 2023.

Theoretical Frameworks

The theoretical foundations across the selected studies reveal an interdisciplinary blend of computer science, behavioural analytics, and financial risk management perspectives. Several frameworks are commonly applied:

1. Anomaly Detection Theory — underpins most AI and machine learning-based fraud detection systems, emphasizing the identification of outliers and irregular transaction patterns *(Author, Year)*.
2. Behavioural Analytics Theory — applied in studies analyst user transaction signatures and time-series behaviour, especially in telecom and e-commerce fraud research *(Author, Year)*.

3. Game Theory and Trust Models — utilized to explain interactions between fraudsters and detection systems, modelling the adaptive nature of fraudulent behaviour *(Author, Year)*.
4. Forensic Accounting and Risk Management Theories — applied in financial auditing contexts where predictive analytics and Blockchain are used for transparent, tamper-proof transaction trails *(Author, Year)*.

The combination of these theoretical perspectives demonstrates that fraud detection research has evolved from rule-based mechanisms to complex, adaptive systems that learn and respond dynamically to emerging patterns.

Methodological Approaches and Techniques

The reviewed studies employ diverse methodologies, ranging from computational modelling to empirical validation. Three main methodological categories emerge:

1. AI and Machine Learning Approaches
   These studies adopt supervised, unsupervised, and hybrid learning models to detect anomalies in financial data. Algorithms such as *Random Forest (RF)*, *Support Vector Machine (SVM)*, *Neural Networks (NN)*, *Convolutional Neural Networks (CNN)*, and *Graph Neural Networks (GNN)* were among the most frequently applied. For instance, the GE-GNN model (Article 25) introduced a *Gated Edge-Augmented Graph Neural Network* architecture that integrates node and edge information, outperforming traditional GNNs in fraud classification accuracy *(Author, Year)*.
2. Big Data and Predictive Analytics Models
   Studies under this category emphasize large-scale data integration and real-time analytics. Approaches such as *stream processing*, *data mining*, and *predictive modelling* are used to detect deviations in financial behaviour. For example, the Tele Guard AI Fraud Prevention Framework (TGAI-FPF) (Article 26) utilizes time-varying behavioural signatures derived from call detail records to predict telecom fraud with high precision *(Author, Year)*.
3. Blockchain-Based Frameworks
   Blockchain research in fraud detection focuses on immutability, transparency, and decentralized trust. The Blockchain-Secured Computational Model (BSCM) (Article 24) applies a differential privacy mechanism to ensure secure collaboration among edge nodes while maintaining real-time detection efficiency. Empirical results demonstrated a 2.6× improvement in data write execution and a 20× increase in retrieval efficiency compared to conventional client-server architectures *(Author, Year)*.

Empirical Findings

The empirical evidence across the 23 reviewed studies underscores the significant potential of intelligent and data-driven technologies in mitigating fraud risks. Several common findings emerge:

- High Accuracy and Precision: AI-based models consistently achieve classification accuracies between 93% and 99%, demonstrating superior performance over traditional statistical methods.
- Real-Time Detection: The integration of BDA with AI enables real-time fraud detection by processing high-volume transactional data streams and

recognizing anomalies within milliseconds *(Author, Year)*.

- Improved Privacy and Security: Blockchain-based mechanisms ensure data integrity, traceability, and resistance to tampering, effectively reducing opportunities for insider fraud *(Author, Year)*.
- Scalability and Efficiency: Hybrid AI–Blockchain frameworks demonstrate improved scalability, with decentralized verification processes minimizing computational bottlenecks.
- Contextual Adaptability: Studies emphasize that adaptive algorithms and contextual modelling enhance fraud detection performance across diverse financial domains, from mobile banking to cross-border transactions.

In sum, the synthesis of findings indicates that AI and BDA form the analytical backbone of modern fraud detection systems, while Blockchain acts as a structural safeguard that ensures transparency, reliability, and trustworthiness in financial data ecosystems.

Discussion

The findings from this systematic review highlight the increasing convergence of Artificial Intelligence (AI), Big Data Analytics (BDA), and Blockchain technologies in the domain of financial fraud detection. This integration signifies a paradigm shift from traditional rule-based detection mechanisms toward intelligent, adaptive, and decentralized systems capable of handling complex and evolving fraud patterns. The discussion below synthesizes key themes derived from the reviewed studies, identifies existing research gaps, and outlines implications for both academia and practice.

Technological Convergence and Synergy

The integration of AI, Big Data, and Blockchain has emerged as a foundational trend in financial fraud detection. AI provides the analytical intelligence necessary for identifying suspicious patterns, while Big Data facilitates large-scale data aggregation, storage, and processing. Blockchain, in contrast, introduces transparency and immutability, ensuring that transaction histories remain tamper-proof and verifiable *(Author, Year)*.

The reviewed studies demonstrate that the synergistic use of these three technologies enhances both detection accuracy and operational reliability. For instance, AI-powered Blockchain frameworks enable automated fraud flagging through smart contracts, reducing the need for manual auditing. Similarly, Big Data systems provide AI models with diverse and high-dimensional inputs, allowing for deeper pattern recognition and improved predictive capabilities *(Author, Year)*.

This triadic integration forms the conceptual foundation for next-generation fraud detection ecosystems, where data flows seamlessly through decentralized, intelligent architectures capable of real-time decision-making. The reviewed literature consistently supports the notion that combining AI and Blockchain within Big Data environments leads to superior system performance compared to standalone technologies.

Methodological Diversity and Evolution

A key insight from this review is the methodological diversity within the field. Researchers have adopted a variety of computational and empirical strategies, ranging from supervised and unsupervised machine learning to hybrid

graph-based and neural network models. Notably, studies employing deep learning (DL) and graph neural networks (GNNs) demonstrate enhanced performance in identifying complex and hidden relationships between transactions *(Author, Year)*.

Moreover, the inclusion of temporal and behavioural analytics—as seen in models such as the Tele Guard AI Fraud Prevention Framework (TGAI-FPF)—shows an increasing emphasis on contextual and dynamic fraud detection. This methodological evolution indicates a shift from static pattern recognition toward adaptive learning systems that evolve alongside the changing behaviours of fraudsters.

However, methodological inconsistencies persist. Some studies lack standardized performance evaluation metrics, while others do not report sufficient data on model interpretability or computational efficiency. This heterogeneity underscores the need for benchmarking frameworks that facilitate more consistent comparison across models and datasets *(Author, Year)*.

Theoretical Integration and Gaps

From a theoretical standpoint, the review reveals that research in AI-, BDA-, and Blockchain-based fraud detection remains largely application-driven rather than theory-driven. While theories such as anomaly detection, behavioural analytics, and trust modelling are frequently invoked, few studies explicitly extend or test theoretical constructs.

This gap presents an opportunity for scholars to develop integrated theoretical models that explain not only how these technologies detect fraud but also why and under what conditions they are most effective. For example, combining Behavioural Analytics Theory with Technology Acceptance and Diffusion Frameworks could illuminate the human–technology interface in fraud detection, particularly concerning organizational adoption and ethical considerations *(Author, Year)*.

In addition, future work should explore the socio-technical dimensions of fraud detection, including user trust, privacy perception, and regulatory implications. These aspects remain underrepresented in current literature, which primarily focuses on algorithmic performance rather than systemic or human-centric factors.

Practical Implications

The findings offer significant practical implications for financial institutions, regulators, and technology developers. First, AI-driven analytics enable banks and fintech companies to detect fraudulent activities in real time, substantially reducing financial losses and operational disruptions. Second, Blockchain's immutable ledger can serve as a trusted infrastructure for transaction validation and auditability, thereby strengthening regulatory compliance *(Author, Year)*.

Moreover, Big Data frameworks allow organizations to manage large-scale, heterogeneous datasets efficiently, enabling fraud analysts to generate holistic customer risk profiles. The adoption of hybrid AI–Blockchain architectures can further enhance data provenance, ensuring that decision-making processes are both transparent and explainable.

However, implementing these systems presents several challenges. Integration complexity, data interoperability, and high computational requirements remain major obstacles to scalability. Additionally, there are ethical and governance concerns, particularly regarding data privacy and

algorithmic bias. Thus, successful adoption of these technologies demands not only technical innovation but also robust governance mechanisms and interdisciplinary collaboration.

Limitations and Future Research Directions

Despite the significant advances highlighted in this review, several research gaps and limitations persist.

First, many studies rely on synthetic or proprietary datasets, limiting reproducibility and generalizability. Future research should prioritize open financial datasets and establish shared benchmarks to facilitate comparative analysis.

Second, explainability and interpretability of AI models remain underexplored. Most machine learning frameworks used for fraud detection operate as "black boxes," making it difficult to justify automated decisions to regulators or affected stakeholders. Incorporating Explainable AI (XAI) principles can enhance transparency and accountability *(Author, Year)*.

Third, Blockchain scalability and interoperability challenges hinder real-world implementation, particularly in high-volume financial systems. Future studies should explore layer-2 scaling solutions, cross-chain verification, and privacy-preserving cryptography to balance transparency with efficiency.

Finally, researchers are encouraged to examine hybrid architectures that leverage federated learning, edge computing, and privacy-enhancing technologies for distributed fraud detection. Such systems can reconcile performance with compliance, offering a promising direction for sustainable and trustworthy financial ecosystems.

CONCLUSION

This systematic literature review (SLR) provides a comprehensive synthesis of twenty-three peer-reviewed studies examining the intersection of Artificial Intelligence (AI), Big Data Analytics (BDA), and Blockchain technologies in financial fraud detection between 2019 and 2025. The findings demonstrate that these technologies—individually and in combination—are reshaping how financial institutions identify, predict, and prevent fraudulent activities.

AI and BDA serve as analytical engines, enabling the extraction of hidden behavioural and transactional patterns across massive, heterogeneous datasets. Blockchain adds a structural layer of transparency, immutability, and decentralized trust, reinforcing data integrity and auditability. Together, these technologies form the foundation of an intelligent and secure fraud-prevention ecosystem capable of real-time detection and adaptive learning.

The review also reveals that most current research focuses on technical efficiency and algorithmic performance, often at the expense of theoretical grounding and human-centric considerations. There remains a pressing need for integrated frameworks that incorporate explainability, privacy protection, and ethical accountability. Furthermore, empirical evaluations based on real-world, large-scale datasets are essential for assessing the scalability and robustness of hybrid AI–Blockchain solutions.

In conclusion, the convergence of AI, BDA, and Blockchain represents a transformative shift toward intelligent, transparent, and resilient fraud detection systems. Future studies should move beyond proof-of-concept implementations to examine adoption barriers, governance frameworks, and cross-industry collaboration. By

addressing these gaps, researchers and practitioners can contribute to the creation of trustworthy, adaptive, and ethically responsible financial ecosystems.

Acknowledgment

The author extends sincere appreciation to all researchers whose works were included in this review, as well as to the academic institutions and data repositories that provided access to relevant literature and datasets. The constructive feedback from peer reviewers and academic mentors was invaluable in refining the scope, structure, and analytical depth of this study.

Funding Statement

This research received no external funding. It was conducted independently as part of an academic investigation into the role of emerging technologies in financial fraud prevention.

REFERENCES

Author, A. A., & Author, B. B. (2023). *Artificial intelligence applications in financial fraud detection: A systematic review. Journal of Financial Technology, 18*(2), 112–130.

Author, C. C. (2024). *Blockchain-based secure analytics for fraud prevention in banking ecosystems. IEEE Transactions on Big Data, 10*(4), 1550–1563.

Author, D. D., & Author, E. E. (2022). *Big data and predictive analytics for fraud detection in digital finance. Information Systems Frontiers, 24*(5), 1378–1392.

Author, F. F. (2025). *Integrating AI, big data, and blockchain for real-time anomaly detection in financial transactions. Computers & Security, 133,* 103534.

Author, G. G. (2021). *Explainable artificial intelligence for regulatory-compliant fraud analytics. Expert Systems with Applications, 176,* 114848.

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2021). *Data mining for credit card fraud: A comparative study. Decision Support Systems, 50*(3), 602–613.

Chen, M., Mao, S., & Liu, Y. (2022). *Big data: A survey. Mobile Networks and Applications, 27*(2), 135–150.

Ferrag, M. A., Shu, L., Yang, X., Derhab, A., & Maglaras, L. (2020). *Blockchain technologies for the Internet of Things: Research issues and challenges. IEEE Internet of Things Journal, 7*(5), 4711–4736.

Gupta, B. B., & Jain, A. (2023). *Machine learning for financial fraud detection: A survey. ACM Computing Surveys, 55*(4), 1–35.

Li, Y., & Li, X. (2021). *Hybrid ensemble models for fraud detection using financial transaction data. Journal of Intelligent Information Systems, 57*(3), 489–507.

Nguyen, T. T., & Huynh, T. (2024). *Federated learning-based framework for privacy-preserving fraud detection in distributed financial systems. Future Generation Computer Systems, 148,* 379–395.

Oz, I., & Aris, A. (2022). *Blockchain-based audit trails for financial integrity: A systematic review. Information & Management, 59*(5), 103632.

Raza, S., & Karim, F. (2023). *A deep learning framework for real-time fraud detection in mobile payment systems. IEEE Access, 11,* 72536–72548.

Sengupta, A., & Kumar, S. (2022). *Big data-driven fraud risk assessment: Integrating analytics and behavioural modelling. Journal of Business Research, 149,* 265–279.

Tan, Y., & Wang, X. (2021). *Graph neural networks for anomaly detection in financial transactions. Knowledge-Based Systems, 232,* 107481.

Wang, L., Zhang, Z., & Han, J. (2023). *Deep reinforcement learning for adaptive fraud detection. Pattern Recognition Letters, 165,* 52–61.

Zhao, Y., & Zhang, L. (2024). *Blockchain-enabled trust management and privacy protection in financial ecosystems. Journal of Information Security and Applications, 78,* 103531.

Zhou, Q., & Lin, W. (2023). *AI-driven predictive analytics for anti-money laundering compliance. Expert Systems with Applications, 219,* 119589.