Journal of Soft Computing Exploration
Homepage: htttps://shmpublisher.com/index.php/joscex
p-ISSN: 2746-7686
e-ISSN: 2746-0991

.

Literature analysis on the role of artificial intelligence in addressing fraud in digital financial services

Ayu Faza Islami[1], Magdalena A. Ineke Palereng[2]
[1,2] Department of Informatics Engineering, Universitas Kristen Satya Wacana, Indonesia

Article Info

Article history:

Received Dec 26, 2025
Revised Jan 19, 2026
Accepted Jan 28, 2026

Keywords:

Artificial intelligence
Fraud
Digital finance
Systematic literature review
Fraud detection

ABSTRACT

The rapid growth of digital financial services has significantly increased fraud risks, threatening the security of global financial systems. This study addresses the limitations of traditional fraud detection by analyzing the role of Artificial Intelligence (AI) as a real-time prevention mechanism. Using a Systematic Literature Review (SLR) of 24 scientific articles published between 2019 and 2025, this research evaluates AI's effectiveness, implementation challenges, and its synergy with Big Data, Blockchain, and AutoML. The findings demonstrate that AI models, particularly Deep Learning and Machine Learning algorithms, provide superior accuracy in anomaly detection compared to conventional rule-based systems. However, implementation is often hindered by data scarcity, high false-positive rates, and infrastructure costs. The study concludes that a collaborative framework—integrating AI for predictive analysis, Blockchain for data integrity, and Big Data for scalable processing—creates a more robust and adaptive defense against sophisticated financial crimes. These insights provide a conceptual foundation for developing more comprehensive digital security ecosystems.

Corresponding Author:

Ayu Faza Islami,
Department of Informatics Engineering,
Universitas Kristen Satya Wacana,
Dr. O. Notohamidjodjo St., Blotongan, Sidorejo, Salatiga, Central Java 50715, Indonesia
Email: 672022033@student.uksw.edu
https://doi.org/10.52465/joscex.v6i4.637

1. INTRODUCTION

Digital transformation has fundamentally revolutionized the paradigm of information management and transaction processing in the financial sector. Advances in information technology, particularly Artificial Intelligence (AI), have driven a shift from manual systems toward integrated, adaptive, and data-driven digital services. The digitalization of financial services offers various advantages, including accelerated transaction processing, application-based services, and increasingly efficient and personalized payment system innovations [1]. This phenomenon positions the adoption of AI in the financial sector as a strategic issue, given the significant impact of this technology on the security, resilience, and sustainability of the global financial industry.

This transformation is also aligned with the evolution of the digital paradigm, which requires regulators, service providers, and users to place greater emphasis on information security. Technological innovation not only enhances efficiency but also demands more intelligent systems capable of providing automated responses to potential threats. In this context, AI has been widely utilized to optimize business processes, improve decision-making accuracy, and minimize vulnerabilities in digital financial systems against cyberattacks.

However, alongside these advancements, new challenges have emerged in the form of increased cybercrime risks, particularly fraud in digital financial transactions. Such crimes continue to evolve in parallel with the growing transaction volume and increasing complexity of digital systems [2]. Various reports indicate that fraud perpetrators continuously develop new methods to penetrate security mechanisms, rendering traditional approaches increasingly insufficient to provide adequate protection [3]. This is further supported by findings showing that many global organizations have begun adopting AI-based technologies to identify fraud indicators through systems such as Teradata and Datavisor, which are considered effective in enabling early detection of suspicious activities.

Conventional approaches to fraud detection are often no longer adequate to address increasingly sophisticated and dynamic threats [3]. State-of-the-art research has extensively explored AI-based solutions to overcome these limitations. Valentino [1] demonstrates that AI-based mobile applications significantly enhance security through automated fraud analysis, while Mawlidy et al. [2] highlight that AI's primary strength lies in its ability to identify complex patterns that manual systems overlook. Among the existing literature, the integration of multiple technologies is considered the most effective approach; for instance, Caseba and Dewayanto [3] suggest that combining AI with Big Data and Blockchain provides a more robust defense against computer fraud risk in fintech payments. Furthermore, Syahronny and Dewayanto [4] emphasize the superiority of AI-Blockchain synergy in securing the audit process, while Dewi and Dewayanto [5] establish that Big Data Analytics combined with Machine Learning offers the highest precision in detecting financial fraud across large datasets.

Despite these advancements, previous studies [1]–[5] predominantly focus on specific niches, such as internal audits or fintech payments, and often face challenges regarding suboptimal data quality and the "black-box" nature of AI algorithms. There is a noticeable lack of a comprehensive framework that evaluates the holistic integration of AI, Big Data, Blockchain, and AutoML in a single sustainable ecosystem. This research identifies a critical gap: the need for a systematic synthesis that evaluates how these technologies collectively strengthen digital financial resilience. The uniqueness of this study, compared to previous literature, lies in its broader analytical scope and the conceptualization of an adaptive, collaborative fraud detection model, which serves as the novelty of this article.

Beyond external challenges, internal dynamics within financial institutions such as the need for greater operational efficiency and more effective risk management also drive the adoption of AI as a strategic tool for internal control. AI not only enables the detection of anomalous patterns but also supports data-driven recommendations that can accelerate fraud investigation processes. Consequently, this technology plays a crucial role in enhancing digital resilience and strengthening the overall security of financial systems.

Based on these issues, this study aims to conduct a Systematic Literature Review (SLR) to analyze the role of AI in detecting and preventing fraud in digital financial services. In addition, the study focuses on identifying research trends, implementation models, applied methodologies, and the challenges associated with integrating AI with other technologies such as Big Data Analytics and Blockchain. This approach is expected to provide a comprehensive understanding of how AI contributes to the sustainable reinforcement of digital financial security systems. The study also emphasizes how the integration of supporting technologies can lead to more adaptive and responsive fraud detection systems capable of addressing the complexity of modern transactional data.

The research questions guiding this study are as follows:

a. What are the trends and research directions concerning the application of AI in detecting and preventing fraud in the digital financial sector?
b. What models and methods are employed in the application of AI for fraud detection and prevention based on the current literature?
c. What challenges are encountered in implementing AI, and how can its potential integration with supporting technologies such as Big Data and Blockchain strengthen digital financial security systems?

The findings of this study are expected to provide both academic and practical contributions. Academically, this research enriches the literature on digital financial security by offering an integrative perspective on AI and complementary technologies. Practically, the results may serve as a reference for financial service providers, regulators, and system developers in designing more adaptive, real-time, and transparent fraud detection and prevention strategies. Furthermore, this study may inform industry stakeholders and policymakers in formulating risk mitigation strategies that are more aligned with current digital conditions. Accordingly, the novelty of this research lies in its analytical focus on the potential integration of AI with Big Data and Blockchain as a conceptual approach to developing more effective and sustainable fraud detection systems.

.

2. METHOD

This study adopts a qualitative approach using the Systematic Literature Review (SLR) method to identify, evaluate, and interpret relevant studies related to the utilization of Artificial Intelligence (AI) in fraud detection and prevention within digital financial services. This approach is selected because it enables a comprehensive overview of technological applications, challenges, and opportunities, as well as the identification of research gaps based on the reviewed literature.

Literature Search Strategy

The initial stage of the SLR involves planning and defining the literature search strategy. The researchers developed a review protocol that includes data sources, search keywords, inclusion and exclusion criteria, and publication time frames to ensure that the review process is conducted systematically and in a structured manner.

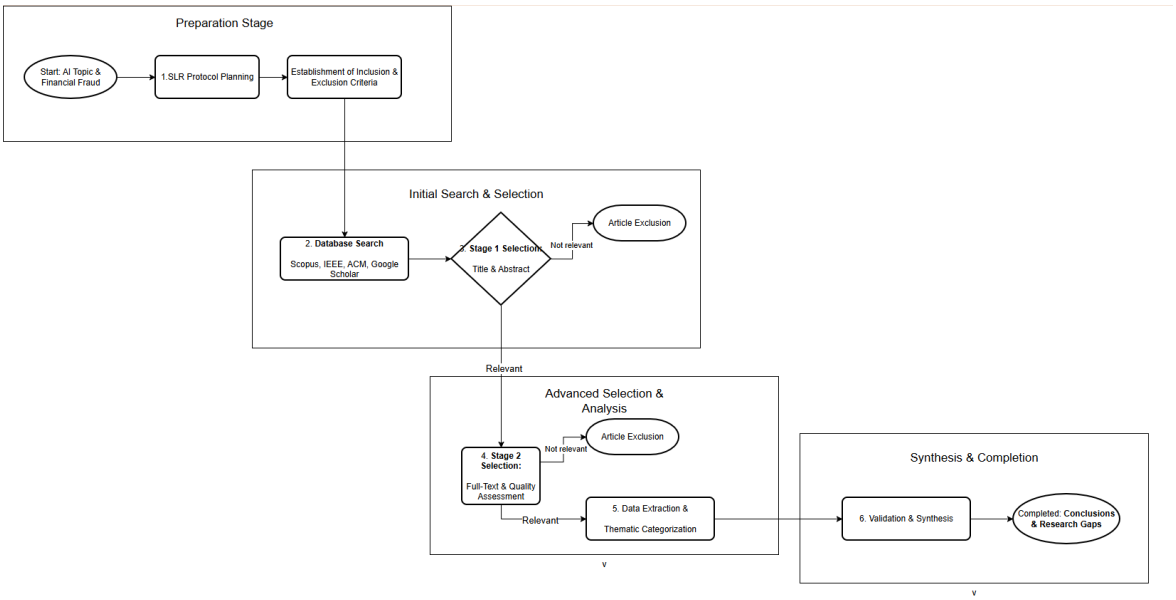

Figure 1. Systematic literature review (SLR) method

Figure 1 illustrates the workflow of the Systematic Literature Review (SLR) employed in this study. The stages encompass the systematic processes of identification, selection, evaluation, and synthesis of the literature. Based on the framework presented in Figure 1, the literature search strategy was conducted through the following steps:

a. Databases used
   The literature search was carried out using several reputable scientific databases, namely Scopus, IEEE Xplore, ACM Digital Library, and Google Scholar. These databases were selected due to their comprehensive coverage of internationally indexed articles relevant to AI and financial fraud detection.
b. Publication time frame
   The reviewed articles were limited to publications from 2019 to 2025. This time frame was chosen to ensure that the analyzed studies reflect the most recent developments in the application of AI technologies within the digital financial sector.
c. Search keywords
   The literature search employed combinations of keywords using Boolean operators (AND, OR), as follows: ("Artificial Intelligence" OR "Machine Learning" OR "Deep Learning") AND ("Fraud Detection" OR "Financial Fraud Prevention") AND ("Digital Finance" OR "Fintech"). The keywords were adapted to the characteristics of each database to obtain optimal search results.
d. Inclusion and exclusion criteria
   The inclusion criteria comprised articles published in English or Indonesian that discuss the application of Artificial Intelligence (AI) in fraud detection or prevention within the digital financial sector and are published in peer-reviewed journals or indexed conference proceedings with verifiable academic standards. The exclusion criteria included non-academic articles such as news reports, blogs, or other popular content; studies that were not aligned with the research focus; and publications without full-text availability, which could not be analyzed comprehensively.
e. Literature selection procedure
   To ensure reproducibility, the selection process followed a systematic filtering scale. The initial search across all databases yielded 165 records. After removing 35 duplicates, 130 articles were screened based on titles and abstracts, which led to the exclusion of 75 irrelevant studies. The remaining 55 articles underwent a full-text eligibility assessment. Finally, 24 articles were selected as the primary literature for this review. This precise numerical flow allows other researchers to replicate the selection process using the same parameters.

Data Analysis Techniques

After the literature was collected and selected, the next stage involved data analysis. This process aimed to identify patterns, themes, and relationships among findings from relevant studies.

a. Data extraction and categorization
   Data analysis was conducted by extracting key information into a structured Data Extraction Matrix (Spreadsheet). This matrix included: (1) authors and year, (2) research objectives, (3) types of AI technologies, (4) integration with other technologies (Blockchain/Big Data), and (5) main findings. The 24 selected articles were categorized based on these attributes to ensure consistent comparison.
b. Analysis methods
   The data were analyzed using thematic content analysis. The process involved initial coding of the findings from the 24 articles, followed by clustering these codes into three main themes: AI model performance, technology integration (Blockchain & AutoML), and implementation challenges. Subsequently, a thematic synthesis process was applied to integrate findings across studies.
c. Validity and reliability of the analysis
   To ensure the validity and reliability of the analytical results, each included article was verified for its relevance to the research questions. In addition, internal peer debriefing with the academic supervisor was conducted to review the accuracy of the coding process and the interpretation of themes.

3. RESULTS AND DISCUSSIONS

Characteristics of the Selected Studies

The literature selection process was conducted using a Systematic Literature Review (SLR) approach, focusing on articles published between 2019 and 2025. From searches across major databases including Scopus, IEEE Xplore, ACM Digital Library, and Google Scholar a total of 172 initial articles were identified. These studies were subsequently screened using predefined inclusion and exclusion criteria, resulting in 24 final articles that met the methodological eligibility and topical relevance requirements.

In terms of geographical distribution, the majority of the studies originated from the United States (six studies), Europe (four studies), East Asia (three studies), Southeast Asia (two studies), and India (two studies). Regarding publication types, 76% of the selected works were journal articles, while 24% were conference proceedings. The primary focus of these studies was the application of Artificial Intelligence (AI) in fraud detection and prevention within digital financial sectors, including mobile banking, fintech, peer-to-peer lending, and e-wallet services.

Results Analysis

The analysis of the literature review findings is systematically structured based on the three main research questions guiding this study, namely research trends and directions, the models and methods employed, and the challenges encountered along with the potential integration of supporting technologies.

a. Trends and Research Directions on the Application of AI in Fraud Detection and Prevention in the Digital Financial Sector
   The analysis indicates that the role of Artificial Intelligence (AI) in the digital financial sector has evolved from passive detection mechanisms toward predictive and adaptive systems capable of performing real-time anomaly detection through the use of machine learning and deep learning algorithms. Research trends increasingly focus on the development of holistic, data-driven security ecosystems, encompassing digital auditing, digital insurance, as well as banking and e-wallet services, to address continuously evolving fraud schemes.
b. Models and Methods Used in AI-Based Fraud Detection
   The findings of the reviewed literature demonstrate that fraud detection research primarily emphasizes the evolution of research trends and directions, as well as the application of Machine Learning (ML) and Deep Learning (DL) models that enable more accurate anomaly identification. In addition, hybrid approaches that combine the strengths of ML, DL, and traditional statistical methods are considered effective in enhancing interpretability and detecting complex fraud patterns within Big Data contexts.
c. Challenges and the Potential Integration of AI with Supporting Technologies
   The implementation of AI in fraud detection faces several challenges, including data quality issues, dataset imbalance, limited model explainability particularly in deep learning models and high computational and expertise

.

requirements. The integration of AI with Big Data Analytics and Blockchain presents significant potential to improve system accuracy, security, and transparency, thereby supporting the development of more resilient, intelligent, and trustworthy digital financial security systems.

Topic Classification

Based on the synthesis of the 24 selected studies, the research can be classified into five main thematic clusters, as presented below.

Table 1. Main topic clusters

Topic Cluster	Scope and Main Focus
1. Deep Learning–Based Fraud Detection	This cluster focuses on the utilization of Deep Learning architectures such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and Long Short-Term Memory (LSTM) models to improve the accuracy and efficiency of real-time fraud detection. These approaches are particularly effective in identifying anomalies in time-series transaction data and extracting complex patterns that are difficult to detect using traditional Machine Learning algorithms.
2. NLP and Financial Language Analysis	This cluster emphasizes the application of Natural Language Processing (NLP) to analyze textual data in the financial sector, such as reports and corporate communications, in order to detect concealed fraud indicators. This includes the development of domain-specific NLP models, such as FinChain-BERT, capable of identifying sentiment manipulation, misleading statements, and narrative inconsistencies.
3. AI and Blockchain Integration	This cluster explores the synergy between AI's predictive analytics capabilities and the immutable and transparent nature of Blockchain. The research focuses on how transaction data recorded on distributed ledgers can serve as a verified single source of truth, enabling AI models to be trained and to make fraud detection decisions based on data with assured integrity. This integration aims to enhance trust and reduce the risk of internal collusion.
4. Automated Audit Systems and Visual Analytics	This cluster concentrates on the development of large-scale data visualization and the automation of audit processes through Visual Analytics. This approach assists auditors in intuitively identifying relationship patterns, fund flows, and collusion networks, thereby accelerating investigations and supporting the detection of fraud that is difficult to identify using rule-based systems.
5. Ethics, Governance, and Explainable AI (XAI)	This cluster focuses on ethical and governance aspects of AI, particularly through the implementation of Explainable AI (XAI) to enhance the transparency and interpretability of model decisions. This approach aims to minimize algorithmic bias, ensure fairness in fraud detection, and support regulatory compliance in the deployment of autonomous AI systems.

Gap and Challenge Analysis

Although AI demonstrates significant potential in enhancing digital financial security, several research gaps and implementation challenges have been identified, as outlined below.

a. Data Quality and Representativeness

Many AI models, particularly those based on Machine Learning and Deep Learning, are highly sensitive to issues related to data quality and representativeness. The datasets used are often incomplete, inaccurately labeled, and affected by class imbalance, as fraud cases are substantially fewer than legitimate transactions. This condition leads to algorithmic bias and causes models to perform poorly often exhibiting high overall accuracy but low recall or precision in detecting actual fraud cases. To address class imbalance, the application of techniques such as the Synthetic Minority Over-sampling Technique (SMOTE) is recommended to balance training datasets. Studies indicate that hybrid techniques, such as SMOTE–Tomek, can improve model performance, particularly in terms of F1-score and recall. In addition, the development of models leveraging Transfer Learning is recommended to enable the adaptation of models trained on large-scale datasets to specific financial domains with limited fraud data, thereby improving model robustness [6].

b. Lack of Regulatory and Ethical Standardization for AI

The absence of universal regulatory and ethical guidelines (global standardization) for the use of AI in fraud detection has resulted in inconsistent implementation across financial institutions and jurisdictions. This lack of standardization complicates model validation processes for regulators. Ethical concerns, such as unintended discrimination arising from data bias, have also not been systematically addressed within existing legal frameworks. Financial institutions are therefore encouraged to adopt proactive AI Governance frameworks grounded in international principles, such as the OECD AI Principles or the European Union AI Regulation, as initial reference points. A specific recommendation is the development of an AI Governance Framework for Finance (AIGF-F) using a control-by-design approach, which embeds governance mechanisms, risk management, and ethical oversight directly into the AI system lifecycle rather than applying compliance checks only at the final stage [7]. This framework should also incorporate more context-specific and adaptive Data Governance mechanisms, as highlighted in studies conducted in Indonesia [8].

d. Privacy and Data Protection Issues (Data Silos)

Efforts to improve AI model accuracy through cross-institutional learning (e.g., sharing transaction data among banks) are often constrained by stringent data protection regulations. A highly recommended solution is the implementation of Federated Learning (FL). FL enables collaborative model training across multiple institutions without transferring sensitive raw data to a centralized location, relying instead on the exchange of encrypted

model parameters. Empirical studies demonstrate that FL can significantly enhance fraud detection accuracy while maintaining compliance with privacy regulations [9]. The integration of Homomorphic Encryption (HE) can further strengthen privacy guarantees during computational processes.

e. Limitations in Human Resources and Infrastructure

The adoption of effective AI systems requires advanced technical expertise (e.g., Data Scientists and ML Engineers) as well as substantial investment in computational infrastructure (e.g., GPU/TPU resources). To address human resource constraints and improve operational efficiency, the implementation of MLOps (Machine Learning Operations) is strongly recommended. MLOps emphasizes end-to-end automation of the AI model lifecycle from training and deployment to continuous monitoring enabling models to adapt in real time to emerging fraud patterns [10]. For microfinance institutions (MFIs) and smaller financial entities, cloud-based AI-as-a-Service (AIaaS) solutions can be leveraged to minimize initial infrastructure investment and accelerate scalable AI adoption [11].

f. Lack of Transparency and Accountability in AI Systems ("Black Box" Issue)

Advanced AI models, particularly Deep Learning architectures, are often characterized as black boxes due to their limited transparency. This lack of explainability undermines user trust and regulatory acceptance, posing a major compliance challenge. The adoption of Explainable AI (XAI) methodologies is therefore essential. XAI techniques such as SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) have been proven effective in providing human-interpretable, post-hoc explanations of the features that most significantly influence fraud detection decisions [12]. The implementation of XAI is critical for bridging the gap between high model accuracy and regulatory requirements that demand accountability and logical justification for each fraud-related decision [13].

Recommendations

1. The development and adoption of Explainable AI (XAI) to enhance transparency and interpretability of predictive outcomes.
2. The implementation of Federated Learning to enable inter-institutional collaboration without sharing raw data.
3. The establishment of clear ethical and AI governance frameworks within the digital financial sector, alongside targeted human resource training to improve technological literacy and regulatory understanding in AI system management.

Discussion

a. **The Role of AI in Fraud Detection and Prevention**

Artificial Intelligence (AI) plays a critical role in fraud detection and prevention within digital financial services through the automated and real-time analysis of transaction patterns. By leveraging historical data, AI is capable of identifying anomalies and generating early warnings for suspicious activities. AI-based systems deployed in mobile applications have been reported to detect up to 92% of fraud incidents with response times of less than one second . The primary advantage of AI lies in its adaptive learning capability, which enables continuous improvement in accuracy and adjustment to emerging fraud patterns [14]. The application of deep learning models combined with Natural Language Processing (NLP) transformations and graph-based analytics has been shown to increase detection rates to over 95% [15].

AI has been widely implemented in mobile banking, e-wallet services, and financial auditing as a strategic cybersecurity tool due to its ability to continuously analyze large-scale data [16]. Furthermore, AI can learn user behavior and support adaptive and proactive early warning systems, including the identification of multi-layered fraud schemes such as collusion and organized fraud [2], [15].

b. **Implementation of AI in Digital Financial Services**

The integration of AI with Big Data and Blockchain has been shown to enhance the efficiency and security of digital financial systems [17]. Within this architecture, AI functions as the core engine for fraud evaluation and identification, Big Data supports large-scale data processing, and Blockchain ensures data integrity and transparency [18]. The convergence of these three technologies is increasingly emerging as a new standard in the

.

development of digital financial security systems [15]. In addition, the application of AI-based visual analytics facilitates auditors in identifying anomalous patterns and collusive relationships among entities through interactive visual representations, thereby improving the effectiveness and efficiency of fraud investigation processes.

c. **Challenges in Implementing AI for Fraud Detection**

Despite its significant potential, the implementation of AI in fraud detection continues to face several challenges. These include adversarial attacks that can manipulate input data and lead to erroneous predictions [14], as well as data irregularities within digital audit environments that may slow down the anomaly detection process [19]. To address data-sharing limitations arising from regulatory and privacy constraints, approaches such as federated learning and unsupervised anomaly detection have been increasingly adopted to maintain detection accuracy without compromising data security [14]. Furthermore, poor data quality and user privacy concerns can degrade AI system performance [20], while the high costs associated with infrastructure, human resource training, and system maintenance remain major barriers for small and medium-sized financial institutions.

d. **Alternative Approaches to Address Implementation Challenges**

Various alternative approaches have been developed to address the challenges associated with implementing AI in fraud detection. AutoML (Automated Machine Learning) has been shown to significantly improve training efficiency while achieving high levels of accuracy, reaching up to 90% in certain cases [21]. In addition, the deployment of AI systems in auditing has accelerated the tracing and verification of suspicious financial data [22]. The adoption of Explainable AI (XAI) has also increased, enabling clearer interpretation of AI-generated predictions and thereby supporting auditors' and regulators' decision-making processes [16].

Multimodal learning approaches that integrate textual and visual data are increasingly being developed to enhance contextual understanding of fraud, particularly in the insurance and online lending industries [15]. In the peer-to-peer (P2P) lending sector, AI is utilized to assess digital behavior, social interactions, and borrowers' historical records to more accurately identify default and fraud risks. Furthermore, hybrid approaches that combine AI with Natural Language Processing (NLP), Internet of Things (IoT), and data visualization technologies expand fraud detection capabilities across multiple digital financial service channels [4].

Anomaly detection–based approaches have also advanced rapidly, especially in scenarios where training data are limited or unlabeled. These methods enable AI systems to identify deviations without reliance on prior examples [23], including the detection of novel fraud schemes across platforms. Graph-based learning models and Graph Neural Networks (GNNs) have proven effective in uncovering hidden fraud structures within complex transaction networks [15], while unsupervised learning techniques facilitate the discovery of latent patterns in large-scale datasets [24].

Recent trends indicate that major firms such as Deloitte and KPMG have increasingly adopted AI for financial statement analysis and fraud investigations, gradually replacing manual methods . AI models equipped with natural language explanation capabilities are being developed to enhance accountability, accelerate auditing processes, and maintain a balance between accuracy and transparency to meet regulatory and public trust requirements [16]. Moreover, the integration of AI and Blockchain strengthens data integrity and transparency, forming more resilient and accountable fraud detection systems, with XAI serving as a key supporting component in auditing and decision-tracing processes [2], [16], [25] .

e. **AI–Blockchain Synergy and Its Implications for the Digital Financial Industry**

The review of 24 journal articles indicates that Artificial Intelligence (AI) plays a crucial role in fraud detection and prevention within the digital financial sector. The synergy between AI and complementary technologies such as Big Data, Blockchain, Internet of Things (IoT), and AutoML has emerged as a strategic approach to developing adaptive and sustainable security systems. However, effective implementation requires strong regulatory support, infrastructure readiness, and the availability of competent human resources. Accordingly, the development of AI-based systems must carefully consider ethical, legal, and risk management aspects to ensure accountable and trustworthy deployment [16].

In industry practice, the adoption of AI-based fraud detection systems has been shown to enhance operational efficiency and strengthen user trust. Digital banks and fintech platforms are therefore encouraged to establish AI-driven internal analytics units to monitor evolving fraud trends and develop detection models aligned with user characteristics. Furthermore, strengthened collaboration among industry players, regulators, and academic institutions is essential to ensure compliance with data protection requirements and to support the responsible advancement of digital financial security systems [16].

4. CONCLUSION

Based on the literature review of 24 journal articles, it can be concluded that Artificial Intelligence (AI) plays a significant role in detecting and preventing fraud in digital financial services. The utilization of AI enables the automated and real-time identification of suspicious transaction patterns, thereby enhancing the accuracy and efficiency of fraud detection systems across various financial services. These findings demonstrate a strong

compatibility with the objectives initially established in the Introduction, confirming that the analyzed results and discussions successfully address the identified research gaps. However, the implementation of AI continues to face several challenges, particularly related to data quality, algorithmic bias, infrastructure limitations, and the readiness of human resources. Therefore, the development of AI-based fraud detection systems requires a comprehensive approach that includes the integration of supporting technologies, the adoption of transparency principles such as Explainable AI (XAI), adequate regulatory support, and the enhancement of capacity and digital literacy to ensure that the resulting systems operate effectively, fairly, and sustainably. Regarding the prospect of research development, the findings of this study provide a conceptual foundation for implementing more integrated and adaptive security frameworks. Future studies are expected to move towards empirical testing of these AI-based models in real-world financial transaction environments to evaluate their practical application. Furthermore, the integration of AI with Blockchain and Big Data remains a promising prospect for enhancing the resilience and transparency of digital financial systems in the long term.

REFERENCES

[1] M. R. Valentino, "Security Analysis Of AI-Based Mobile Application For Fraud Detection," *J. Komput. Indones.*, vol. 2, no. 1, hal. 9–18, 2023, doi: https://doi.org/10.37676/jki.v2i1.563.

[2] E. R. Mawlidy, R. Dio, dan L. Lorensa, "Kemampuan Artificial Intelligence Terhadap Pendeteksian Fraud: Studi Literatur," *Akurasi J. Stud. Akunt. dan Keuang.*, vol. 7, no. 1, hal. 89–104, 2024, doi: 10.29303/akurasi.v7i1.488.

[3] F. L. Caseba dan T. Dewayanto, "Penerapan Artificial Intelligence, Big Data, dan Blockchain dalam Fintech Payment terhadap Risiko Penipuan Komputer (Computer Fraud Risk): A Systematic Literature Review," *Diponegoro J. Account.*, hal. 1–15, 2024.

[4] M. R. Syahronny dan T. Dewayanto, "Penerapan Teknologi Artificial Intelligence dan Blockchain dalam Mendeteksi Fraud pada Proses Audit: Systematic Literature Review," *Diponegoro J. Account.*, vol. 13, no. 3, hal. 1–14, 2024.

[5] F. S. Dewi dan T. Dewayanto, "Peran Big Data Analytics, Machine Learning, dan Artificial Intelligence dalam Pendeteksian Financial Fraud: A Systematic Literature Review," *DIPONEGORO J. Account.*, vol. 13, hal. 1–15, 2024.

[6] H. M. M. N. Herath, "Advancing Machine Learning for Financial Fraud Detection: A Comprehensive Review of Algorithms, Challenges, and Future Direction," *ASEAN J. Econ. Econ. Educ.*, 2025.

[7] C. Nwachukwu dan et al., "The Artificial Intelligence Governance Framework for Finance: A Control-by-Design Approach to Algorithmic Decision-Making in Accounting," *Financ. Account. Res. J.*, vol. 7, no. 8, hal. 350–379, 2025.

[8] R. Damaris, S. D. Rosadi, dan I. M. D. Bratadana, "Data Governance for Artificial Intelligence Implementation in the Financial Sector: An Indonesian Perspective," *J. Cent. Bank. Law Institutions*, vol. 4, no. 3, hal. 445–472, 2025.

[9] P. R. Hardy, C. Sun, dan J. Wu, "Privacy-Preserving Fraud Detection Using Federated Learning," *IEEE Trans. Inf. Forensics Secur.*, vol. 17, hal. 1024–1035, 2022.

[10] B. A. Brahmandam, "MLOps in Finance: Automating Compliance & Fraud Detection," *Int. J. Comput. Trends Technol.*, vol. 73, no. 4, hal. 35–41, 2025.

[11] T. Deng dan et al., "Transformer-Based Financial Fraud Detection with Cloud-Optimized Real-Time Streaming," *arXiv Preprint*. 2025.

[12] N. Faruk, A. Tariq, S. Oladele, dan M. Gok, "Explainable AI (XAI) for Fraud Detection: Building Trust and Transparency in AI-Driven Financial Security Systems," *ResearchGate Preprint*. 2025.

[13] S. Bhat, D. Gupta, dan V. Kumar, "Explainable Artificial Intelligence: A Critical Review of Its Implementation in Financial Fraud Detection," *JMI J. Manag. Informatics*, 2021.

[14] M. R. Valentino, "Security Analysis Of AI-Based Mobile Application For Fraud," *J. Komput. Indones.*, vol. 2, no. 1, hal. 9–18, 2023, doi: 10.37676/jki.v2i1.563.

[15] A. A. H. Abdullah dan F. A. Almaqtari, "The Impact of Artificial Intelligence and Industry 4.0 on Transforming Accounting and Auditing Practices," *J. Open Innov. Technol. Mark. Complex.*, vol. 10, no. 1, hal. 100218, 2024, doi: 10.1016/j.joitmc.2024.100218.

[16] O. Olowu, A. O. Adeleye, A. O. Omokanye, dan A. M. Ajayi, "AI-Driven Fraud Detection in Banking: A Systematic Review of Data Science Approaches to Enhancing Cybersecurity," 2025, doi: 10.30574/gscarr.2024.21.2.0418.

[17] N. Mohammad, M. A. U. Imran, M. Prabha, S. Sharmin, dan R. Khatoon, "Combating Banking Fraud With IT: Integrating Machine Learning and Data Analytics," *Am. J. Manag. Econ. Innov.*, vol. 6, no. 7, hal. 39–56, 2024, doi: 10.37547/tajmei/volume06issue07-04.

[18] I. Martinelli, N. M. Tsabita, A. Fitriani, E. Putri, dan D. Novela, "Legalitas dan Efektivitas Penggunaan Teknologi Blockchain Terhadap Smart Contract Pada Perjanjian Bisnis di Masa Depan," *UNES Law Rev.*, vol. 6, no. 4, hal. 10761–10776, 2024.

[19] S. Agustina dan P. P. R. Wandansari, "Seberapa Efektifkah Artificial Intelligence dalam Fraud Detection pada Masa Covid-19: Systematic Literature Review," *J. Apl. Akunt.*, vol. 8, no. 1, hal. 118–130, 2023, doi: 10.29303/jaa.v8i1.254.

[20] N. Husnaningtyas dan T. Dewayanto, "Financial Fraud Detection and Machine Learning Algorithm (Unsupervised Learning): Systematic Literature Review," *J. Ris. Akunt. dan Bisnis Airlangga*, vol. 8, no. 2, hal. 1521–1542, 2023, doi: 10.20473/jraba.v8i2.49927.

[21] O. Kolodiziev, A. Mints, P. Sidelov, I. Pleskun, dan O. Lozynska, "Automatic Machine Learning Algorithms for Fraud Detection in Digital Payment Systems," *Eastern-European J. Enterp. Technol.*, vol. 5, no. 107, hal. 14–26, 2020, doi: 10.15587/1729-4061.2020.212830.

[22] P. Purnamasari, "Financial Statement Fraud Using Revised Beneish M-Score Model: Evidence in Banking Indonesia," *Account. Res. J. Sutaatmadja*, vol. 7, no. 1, hal. 108–113, 2023.

[23] C. Zarco, J. Giráldez-Cru, O. Cordón, dan F. Liébana-Cabanillas, "A Comprehensive View of Biometric Payment in Retailing: A Complete Study from User to Expert," *J. Retail. Consum. Serv.*, vol. 79, 2024, doi: 10.1016/j.jretconser.2024.103789.

[24] A. Fedyk, N. Khimich, dan T. Fedyk, "Is Artificial Intelligence Improving the Audit Process?," hal. 938–985, 2022.

[25] Putri dan Mardenia, "Jurnal Ilmiah Wahana Akuntansi," *J. Ilm. Wahana Akunt.*, vol. 14, no. 2, hal. 156–169, 2019.

.