Applicability Of Industry 4.0 Technologies in Combating Fraud in the Financial System

Jennyfer da Conceição Fonseca Santos, Luciana Paula Reis and June Marques Fernandes
Universidade Federal de Ouro Preto, João Monlevade, Brasil

jennyfer.santos@aluno.ufop.edu.br
lucianapaula@ufop.edu.br
june@ufop.edu.br

Abstract: The increasing digitalization of financial services has brought significant benefits, such as speed and convenience, but it has also increased exposure to sophisticated fraud schemes, including identity theft, card fraud, and money laundering. In this context, Industry 4.0 (I4.0) technologies—particularly Machine Learning (ML) and blockchain—have emerged as strategic tools for enhancing security and mitigating risks in the banking sector. This study aims to examine the applicability of these technologies in detecting and mitigating financial fraud, addressing the following research question: How have blockchain and ML technologies contributed to mitigating different categories of fraud? To answer this question, a Systematic Literature Review (SLR) was conducted using the Scopus and Web of Science databases, focusing on open-access articles published between 2021 and 2025 that were aligned with the research topic. Following the PRISMA protocol, 27 articles were selected and analyzed through bibliometric analysis, content analysis, and mapping of future research directions. The originality of this research lies in the integration of cutting-edge ML and blockchain analyses to mitigate financial fraud, bridging technology, challenges, and gaps. Despite these advances, challenges remain, including data imbalance, the need for model interpretability, and ethical and regulatory concerns. Future research should focus on integrating ML and blockchain, improving algorithms to handle imbalanced datasets, and developing explainable and secure solutions. This study contributes by providing an up-to-date and comprehensive overview of current trends and research gaps in the application of I4.0 technologies to financial security, serving as a foundation for scientific progress and the adoption of these tools by banking institutions.

Keywords: Industry 4.0, Machine learning, Blockchain, Financial system, Fraud prevention

1. Introduction

The increasing digitalization of financial services has brought a series of benefits to both banking institutions and their customers, making transactions faster, more convenient, and more accessible (Chang *et al*., 2022). However, this transformation has also increased the banking sector's vulnerability to increasingly complex frauds, such as identity theft, credit card fraud, advanced money laundering schemes, and data manipulation (Asmar and Tuqan, 2024). According to Btoush *et al*. (2023), cybercrimes related to these transactions pose a constant challenge for financial institutions, which need to invest in more advanced techniques to detect and prevent such crimes.

Industry 4.0 (I4.0) technological innovations emerge as strategic alternatives to strengthen the security and robustness of financial systems against fraud (Ismaeil, 2024). Machine learning (ML), a subset of AI, has been widely used to detect suspicious patterns in transactions, allowing for more accurate and faster identification of fraudulent activities (Asmar and Tuqan, 2024). Approaches such as supervised and unsupervised learning are crucial for improving anomaly detection systems and reducing financial losses (Hilal et al., 2022). Furthermore, recent research indicates that combining graph databases with ML models enhances the identification of unusual behavior, increasing the effectiveness of anti-fraud systems (Patil et al., 2024). By processing large volumes of data in real time, artificial intelligence reduces false positives and improves transaction security, benefiting both customers and financial institutions (Ismaeil, 2024).

The literature identifies ML and blockchain as central to combating financial fraud, including fraudulent banking transactions, identity fraud, credit card fraud, money laundering, and document forgery (Baabdullah *et al*., 2024; El-Chaarani and El-Abiad, 2024; Patil *et al*., 2024). ML stands out for its ability to detect anomalous patterns in real time, while blockchain offers traceability, immutability, and transparency. The integration of these technologies improves detection accuracy, reduces false positives, and enables automated mitigation through smart contracts and collaborative systems, strengthening incident prevention and response in the financial sector (Rabbani *et al*., 2024; Ren *et al*., 2023). Mapping trends, limitations, and application potential contributes to the advancement of academic knowledge at the intersection of I4.0 and fraud prevention.

This article aims to analyze the applicability of I4.0 technologies, with a focus on ML and blockchain, in treating and mitigating the effects of fraud in the banking system. The study begins with the following question: "What is the current progress of academic research related to the application of these technologies in financial fraud

mitigation?" To achieve this objective, this study adopts a Systematic Literature Review (SLR), gathering data through a bibliographic search. The bibliographic search aims to collect, identify, select, and critically evaluate previously published references in various forms of academic and scientific materials (Marconi and Lakatos, 2021).

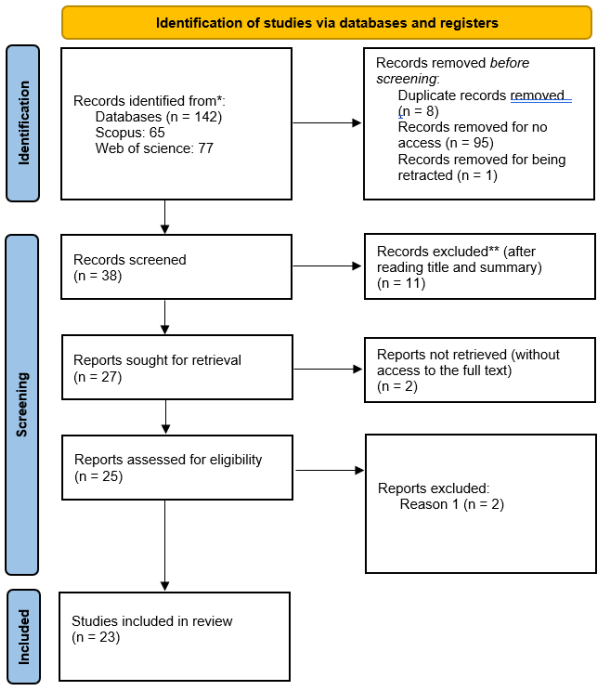
Existing literature predominantly focuses on the use of blockchain or ML for fraud mitigation, without, however, comprehensively exploring the complementarity and synergy between these and other I4.0 technologies. Therefore, this SLR aims to fill this gap by providing a deeper and more up-to-date understanding of the state of research and implementation practices of these technologies in combating banking fraud.

This research is divided into four sections in addition to this brief introduction. Section 2 presents the methodology used to execute and support this work. Section 3 presents the main results and discussions of the analyses performed. Finally, Section 4 presents the final considerations obtained from the research, the limitations of the work, and proposals for future studies.

2. Methodology

The method employed here is theoretical-conceptual, utilizing the SLR tool. SLR is a rigorous methodology that synthesizes scientific evidence from multiple studies, providing a comprehensive and reliable overview of a specific topic (Roever, 2020). To conduct the SLR, the PRISMA principles (Page *et al*., 2021) were used to search for, identify, and select articles for inclusion in the research.

The Scopus and Web of Science databases were selected as data sources, as they are two of the largest and most comprehensive academic databases, containing a wide range of journals from various fields. The search was conducted in the "Title, Abstract, and Keywords" fields, using the keywords "Fraud," "Technologies," "Security," and "Finance." Restrictions were applied to include only articles published between 2021 and 2025, aiming to understand the current discussions on the topic over the past five years. Furthermore, only open access documents were selected for analysis. Figure 1 presents the Prisma flowchart used in the research:



Source: Adapted from Page *et al*. (2021).

Figure 1: PRISMA flowchart for article identification and screening

After conducting the database search and applying the filtering criteria, the search yielded a total of 142 articles. After searching the database, 8 duplicate articles, 95 articles that were not open access, and 1 article that had been retracted by the journal were removed, resulting in 38 selected articles. Subsequently, the titles and abstracts were read to exclude articles that did not fit the research topic, resulting in the exclusion of 11 articles. Subsequently, after reading the full article, 2 articles whose full texts were not found were excluded, as well as 2 articles that were also not aligned with the research topic. The final result of this review was 23 articles.

Three distinct analyses were conducted to understand and synthesize the existing body of knowledge on the topic in question: i) bibliometric analysis, ii) content analysis, and iii) analysis of suggested future work. The bibliometric analysis included identifying and categorizing articles according to various criteria, such as year of publication and first author's country, as well as creating a keyword cloud using VOSviewer software. Content analysis focused on the themes and subthemes discussed in the articles. Finally, analyzing the recommendations for future work described in the articles provides valuable insights into future research directions in this specific field. These combined analyses offer a comprehensive and in-depth understanding of the current state and emerging trends in technologies used to mitigate fraud in financial systems.

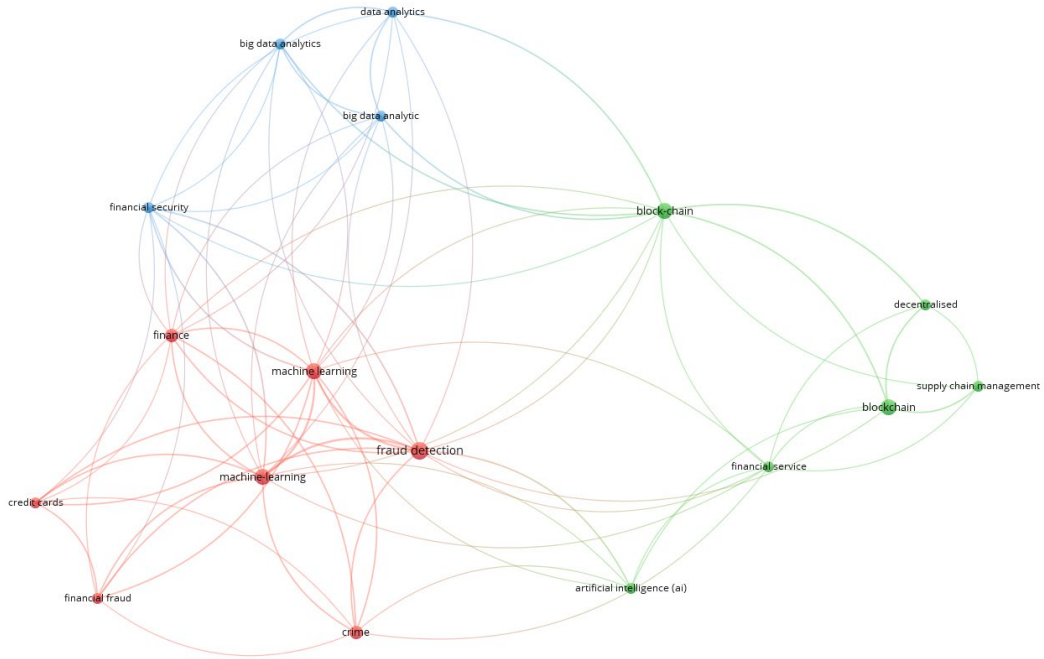
3. Results and Analysis

This section presents the results of the SLR analyses, containing three subsections: bibliometric analysis; content analysis; and analysis of future work.

3.1 Bibliometric Analysis

The analysis of the number of articles published per year reveals an increasing trend in academic production over time. In 2021 and 2023, there was an equal number of publications (4 articles each), while in 2022 there was a significant increase to 6 articles. However, the most significant growth occurred in 2024, with 13 publications, representing a peak in production.

The progressive increase in publications may indicate a growing academic interest in the topic, as well as a greater availability of related research and studies. The increase in publications in 2024 suggests that the topic may be gaining relevance in the scientific community, possibly driven by technological advances or greater awareness of its importance. If this trend continues, it is possible that an even greater volume of articles will be published in the coming years, consolidating the area as a growing field of study. An analysis of articles by the first author's country of origin reveals a heterogeneous distribution across different regions, as shown in the figure. India stands out as the country with the highest number of publications (9), indicating strong academic production in the field. China follows with 3 publications, demonstrating a significant but significantly lower share compared to India. Other countries, such as Saudi Arabia, Romania, the United Arab Emirates, the United States, Malaysia, Nigeria, and the United Kingdom, have a moderate number of publications (2 each), suggesting a significant but less significant share. On the other hand, Brazil appears with only one publication, representing a smaller contribution to the sample analyzed. This distribution may reflect different levels of research investment, academic interest in the topic, or access to resources and incentives for scientific production and publication.



Source: Data tabulated in VOSviewer.

Figure 2: Word Cloud

Word cloud analysis identifies three major thematic clusters that stand out in the literature. The first cluster is directly related to fraud detection in the financial sector, with terms such as fraud detection, ML, crime, financial fraud, credit cards, and finance. This cluster demonstrates that the application of artificial intelligence techniques, especially ML, is central to strategies aimed at combating financial fraud, often associated with transaction security and crime prevention. The second cluster has as its central element the term blockchain, which connects to topics such as financial service, decentralized, supply chain management, and artificial intelligence (AI). This cluster highlights the growing use of blockchain technology not only in the financial sector but also in solutions aimed at decentralizing processes and managing supply chains, reinforcing its role in promoting data security, transparency, and traceability. The third cluster focuses on the terms big data analytics and financial security. This group reflects the importance of large-scale data analysis tools as essential support for financial security, enabling the identification of patterns, the prediction of suspicious behavior, and the generation of insights for risk mitigation.

In general, the topics are strongly interconnected, particularly through the terms fraud detection, ML, blockchain, and financial security. This demonstrates that current research adopts a multidisciplinary approach, integrating emerging technologies to address the challenges related to financial security, fraud detection, and innovation in financial services.

3.2 Content Analysis

The selected studies cover a wide range of application areas. They investigate issues such as cybersecurity in the financial sector, fraud detection in banking transactions, and the use of emerging technologies to improve financial crime monitoring and prevention systems.

3.2.1 Fraud in the financial system

Fraud is defined as an intentional act of deception aimed at obtaining an undue advantage or causing harm to third parties. It is characterized as a non-violent crime, but highly damaging in the economic and corporate context (Kulmie *et al*., 2024). The literature identifies two main groups of frauds: internal and external.

Internal fraud in the banking sector is a complex and multifaceted problem, committed by employees or managers within the organization, often exploiting flaws in internal control and corporate governance systems (El-Chaarani and El-Abiad, 2022; Kyrychenko *et al*., 2021; Bonsu *et al*., 2018). These frauds can be especially damaging because they involve the use of insider privileges to divert resources or compromise the organization's integrity. They occur due to factors such as a lack of effective anti-fraud policies, inadequate training, insufficient compensation, and inexperienced personnel (Kulmie *et al*., 2024; Bonsu *et al*., 2018).

External frauds are committed by individuals or groups outside the financial institution and can include a wide variety of attacks, many of which exploit technological vulnerabilities or psychologically manipulate victims (Taher *et al*., 2024; Btoush *et al*., 2023). Attacks range from direct data theft to more complex methods such as phishing and social engineering, which involve psychologically manipulating users to obtain confidential information (Taher *et al*., 2024). Cyberfraud with credit cards is one of the most prevalent forms, costing banking institutions billions of dollars annually and involving the unauthorized use of a card or its information to carry out fraudulent transactions (Baabdullah *et al*., 2024; Charizanos *et al*., 2024). Furthermore, practices such as money laundering and identity theft pose ongoing risks that exploit flaws in internal control systems and corporate governance (Kulmie and Ibrahim, 2024). Regarding the most frequently discussed types of fraud, general banking transactions lead, being addressed in sixteen papers (Baabdullah *et al*., 2024; Ghrib *et al*., 2024; Patil *et al*., 2024; Rabbani *et al*., 2024; Wei and Lee, 2024; Chang *et al*., 2022; Aljofey *et al*., 2022; Kyrychenko *et al*., 2021; Ileberi *et al*., 2021). Next, identity fraud was discussed in 10 articles (Ali *et al*., 2024; Asmar and Tugan, 2024; Ismaeil, 2024), reflecting growing concern about the risks associated with the theft and misuse of personal data. Credit card fraud and money laundering are also among the most discussed topics, each appearing in 9 studies (El-Chaarani and El-Abiad, 2024; Patil *et al*., 2024; Wijaya *et al*., 2024). With the advancement of I4.0, financial fraud detection requires new technological paradigms to respond to growing risks. I4.0 technologies emerge as strategic solutions to strengthen the security and resilience of financial systems against fraud (Ismaeil, 2024).

3.2.2 Technologies to combat fraud

With the advancement of I4.0, financial fraud detection requires new technological paradigms to respond to growing risks. Technologies such as AI, ML, big data, and blockchain have shown promise for detecting these frauds and preventing cyberattacks (Patil *et al*., 2024). The articles analyzed for this systematic literature review

reveal a clear predominance of ML use, present in 21 articles. Blockchain also stands out, present in 20 studies, frequently combined with ML, Federated Learning (FL) (ML technique that collaboratively trains models across different institutions or devices, without sharing the raw data, ensuring privacy and security), or data mining techniques, especially in cases requiring transparency and immutability, such as money laundering and distributed denial-of-service (DDoS) attacks (Ahmed and Alabi, 2024; Baabdullah *et al*., 2024; Wei and Lee, 2024; Aljofey *et al*., 2022; Chang *et al*., 2022). On the other hand, emerging technologies or those with more specific uses, such as FL, graph technologies, deep learning, biometrics, and data balancing techniques, appear less frequently, indicating a still incipient adoption trend or potential implementation challenges.

Detection-focused approaches predominate over mitigation strategies. The literature has shown greater interest in the application of technologies capable of identifying anomalous patterns, suspicious behavior, or early signs of irregularities (Ahmed and Alabi, 2024; Gaikwad *et al*., 2023; Ren *et al*., 2023; Aljofey *et al*., 2022; Ashfaq *et al*., 2022; Chang *et al*., 2022). In contrast, mitigation strategies appear less systematically (Ali *et al*., 2024; Asmar and Tugan, 2024; Kyrychenko *et al*., 2021), suggesting a gap in the structuring of mechanisms capable of containing the impacts of fraud or adapting organizational processes in the face of already materialized threats (El-Chaarani and El-Abiad, 2024; Khan *et al*., 2023). Table 1 presents the applications for ML and blockchain, technologies that appear most frequently in the literature.

Table 1: Applications of ML and blockchain

Technology	Applications	Authors
Machine Learning (ML)		
Supervised Learning	It uses algorithms such as Logistic Regression, Random Forest, and Convolutional Neural Networks (CNN) to detect card fraud, classify transactions, and correct data imbalances. It is also used to identify accounting fraud and suspicious behavior in real time.	Ileberi et al. (2024); Ismaeil (2024); Wijaya et al. (2024), Lokanan e Sharma (2022), Stojanovic e Bozic (2022)
Unsupervised Learning	It uses algorithms such as SVM, HMM, and Autoencoders to classify transactions, detect temporal patterns, model sequences of fraudulent actions, and generate synthetic data for training.	Asmar e Tuqan (2024), Hilal et al. (2022)
Hybrid ML Techniques	They combine multiple algorithms (e.g., CNN, RNN, LSTM) to detect complex and sequential patterns, especially in time series, and map connections between users and transactions.	Patil et al. (2024), Wei e Lee (2024), Ren et al. (2023)
Federated Learning	It allows multiple participants to collaborate on model training without sharing their raw data, ensuring privacy. It is combined with techniques such as SVM and neural networks.	Rabbani et al. (2024), Ahmed e Alabi (2024)
Blockchain		
Blockchain (isolated)	Ensures the traceability and integrity of financial records through its immutable nature, which helps reduce corruption, money laundering, and human error.	Kulmig et al. (2024), Abad-Segura et al. (2024)
Blockchain + ML / Deep Learning	The combination enhances high-precision fraud detection by analyzing patterns in large volumes of transaction data, including temporal anomalies.	Aldabam e Hamdi (2024), Gałkoyad et al. (2023)
Blockchain + Federated Learning	Creates collaborative models for real-time fraud detection while maintaining the privacy of participating financial institutions' data.	Rabbani et al. (2024), Baabdullah et al. (2024)
Blockchain + Other Technologies	When combined with GBDT, it improves accuracy on imbalanced data. With the Zero Trust model, it offers continuous authentication. Combined with mobile protection, it combats phishing and vishing.	Paşek e Sharma (2024), Njoya et al. (2023), Ren et al. (2023)

Source: The authors.

ML focuses on the development of algorithms and computational models capable of learning patterns from data, without being explicitly programmed for a specific task (Asmar and Tuqan, 2024; Ismaeil, 2024). It has been widely applied in cybersecurity, financial fraud detection, banking transaction analysis, and data protection, demonstrating the ability to handle large volumes of information and identify complex patterns that are difficult to detect manually (Asmar and Tuqan, 2024; Wei and Lee, 2024; Gaikwad *et al*., 2023). These systems use historical data to "learn" and improve their performance over time, becoming increasingly accurate in tasks such

as classification, prediction, and anomaly detection (Ileberi and Sun, 2024; Wijaya *et al*., 2024). Algorithms can be supervised (trained with labeled data), unsupervised (identify patterns in unlabeled data), or semi-supervised (combine both approaches) (Ismaeil, 2024; Hilal *et al*., 2022). Furthermore, the integration of ML techniques with technologies such as blockchain and federated learning has further expanded their applications, ensuring greater security, privacy, and efficiency in financial and technological systems (Rabbani *et al*., 2024; Ren *et al*., 2023).

The use of blockchain to monitor and record financial transactions offers a transparent and secure platform, enabling collaboration between financial institutions without the need to exchange sensitive data. This offers advantages related to transaction traceability and reduced corruption and money laundering (Rabbani *et al*., 2024). However, when used in isolation, it fails to detect complex fraud patterns and is limited to post-facto auditing (Kulmie *et al*., 2024). The integration of blockchain with ML/deep learning significantly expands its potential, enabling highly accurate fraud detection (Gałkowad *et al*., 2023).

ML complements the immutability of blockchain by enabling the joint analysis of on-chain data (recorded on the network) and off-chain data (such as banking histories or digital interactions). While blockchain ensures the traceability and integrity of transactions, it cannot, by itself, identify hidden patterns of fraud (Ismaeil, 2024; Asmar and Tuqan, 2024; Wei and Lee, 2024; Gaikwad et al., 2023; Ren et al., 2023; Rabbani et al., 2024; Ahmed and Alabi, 2024). In this sense, ML algorithms, such as recurrent neural networks and hybrid methods, are capable of correlating multiple sources of information, detecting anomalous behaviors and sophisticated fraud schemes that exploit gaps between the internal and external environments of the blockchain (Ren et al., 2023; Gaikwad et al., 2023; Wei and Lee, 2024). This integration expands predictive and preventive capabilities, allowing complex attacks to be identified before they consolidate.

The analyzed literature highlights significant advances in the use of I4.0 technologies to combat financial fraud, with an emphasis on ML techniques (Patil *et al*., 2024; Wijaya *et al*., 2024; Gaikwad *et al*., 2023) and blockchain-based solutions (Baabdullah *et al*., 2024; Rabbani *et al*., 2024). Recent studies highlight the predominance of approaches aimed at automated fraud detection, particularly by identifying behavioral patterns and anomalies in banking transactions, using algorithms such as Random Forest, XGBoost, and convolutional neural networks (Asmar and Tuqan, 2024; Wijaya *et al*., 2024). Despite the sophistication of these approaches, there is a significant gap in strategies aimed at mitigating and responding to fraud. Most studies focus on predictive models aimed at detection, but do not delve into the practical implications of adopting these technologies within the banking environment (El-Chaarani and El-Abiad, 2024; Kyrychenko *et al*., 2021). Furthermore, although some research mentions the integration of ML with blockchain to improve security and traceability (Gaikwad *et al*., 2023; Ren *et al*., 2023), the applicability of these systems in concrete operational contexts still lacks robust empirical evidence.

Another critical point concerns the scarcity of empirical studies based on real data from financial institutions. Much of the academic literature uses public or simulated databases, limiting understanding of the operational and regulatory barriers involved in the practical application of these technologies (Lescano-Delgado, 2023; Stojanović *et al*., 2021). Furthermore, there is little articulation between different types of fraud and the specificity of the most appropriate technological solutions for each case (Kulmie *et al*., 2024; Chang *et al*., 2022).

3.3 Directions for Future Research

The reviewed studies point to several opportunities for future research in financial fraud detection, ranging from the application of new technologies to overcoming methodological, technical, and ethical challenges. One of the main directions in Stojanović and Božić's (2022) research involves expanding the risk assessment architecture in fraud detection systems, considering broader cyber threats and vulnerabilities. Furthermore, the implementation of new security properties would contribute to strengthening the reliability of anomaly detection-based systems in the financial sector.

Another relevant aspect concerns the improvement of ML algorithms, particularly in addressing data imbalance in fraudulent transaction sets, which can compromise detection effectiveness. Strategies such as data augmentation and the development of robust adversarial countermeasure models are indicated as promising avenues for strengthening predictive accuracy (Ashfaq *et al*., 2022). Furthermore, testing ML algorithms from other domains and collecting new financial datasets can improve the applicability of these solutions (Stojanović *et al*., 2021).

Methodologically, combining neural networks with decision tree-based techniques, such as Gradient Boosting Decision Trees (GBDT), has been identified as a promising alternative for dealing with highly sparse data (Ren *et*

al., 2023). Furthermore, hyperparameter tuning and careful feature selection can optimize model training time without compromising detection accuracy (Ileberi and Sun, 2024).

Beyond the technical challenges, the application of AI in financial security raises ethical and regulatory concerns. Issues such as algorithmic bias, data privacy, and regulatory compliance need to be examined to ensure that the implementation of these solutions occurs in a fair and transparent manner (Asmar and Tuqan, 2024). Financial institutions should invest in high-quality data and strategies that ensure the reliability of AI-based systems, in addition to adapting to emerging regulations (Ismaeil, 2024).

Finally, future research could focus on developing testable hypotheses about fraudster behavior in the financial market, exploring interdisciplinary approaches that integrate criminological theories with ML techniques (Lokanan and Sharma, 2022). It is also crucial to compare different ML-based cybersecurity methods to assess their effectiveness in real-world scenarios (Asmar and Tuqan, 2024).

4. Final Considerations

This study provided a detailed analysis of the current state of research on the application of technologies to financial fraud mitigation, highlighting advances, emerging trends, and future directions for the field. Through SLR, it was possible to identify a growing academic production on the topic, with a significant increase in publications starting in 2024, reflecting the growing interest and relevance of these technologies in the financial sector.

The literature highlights that the use of ML has proven highly effective in detecting anomalous patterns in financial transactions, while blockchain technology stands out as a robust solution for ensuring the transparency and security of transactions. However, despite these advances, studies have also revealed persistent challenges, such as data imbalance in transaction sets, the need for greater interpretability of AI models, and the ethical and regulatory issues involved in the application of these technologies.

Directions for future research indicate that the development of new ML techniques, improving model interpretability, and exploring the use of blockchain in permissioned networks will be fundamental to advancing the field. Furthermore, it is essential that future research integrate interdisciplinary approaches, considering the ethical, regulatory, and practical aspects of implementing these technologies in financial institutions. In short, the application of blockchain and ML to financial fraud mitigation offers great potential to transform the security of banking systems, but continued investment in research that addresses technical and ethical challenges is necessary, promoting increasingly effective and fair solutions.

The main contribution of this study is to provide a comprehensive and up-to-date overview of the use of I4.0 technologies in financial fraud mitigation, highlighting emerging trends and technological advances. The study also offers a critical reflection on the integration of these technologies in the financial sector, contributing to a deeper understanding of cybersecurity in the banking context.

This research has limitations related to the method used. These limitations stem from the search terms selected and the inclusion/exclusion criteria of the articles, which may result in bias on the part of the researchers and the possible exclusion of other relevant work. For future research, we suggest including new terms that can encompass different aspects of the research topic, such as potential benefits and implementation barriers. Furthermore, we suggest considering the applicability of these technologies in different contexts and types of financial institutions.

Acknowledgements

The authors would like to thank the Universidade Federal de Ouro Preto (UFOP/Brazil) (www.ufop.br), the Pró-Reitoria de Pesquisa, Pós-graduação e Inovação (PROPPI), the Conselho Nacional de Desenvolvimento Cientifico e Tecnológico (CNPq), the Coordenação de Aperfeiçoamento de Pessoal de Nivel Superior (Capes), and the Fundação de Amparo à Pesquisa do Estado de Minas Gerais (FAPEMIG), for their support during the development of this research.

Ethics Statement: This research did not involve human or animal participants, nor did it collect sensitive data that required approval from a research ethics committee. Therefore, ethics approval was not considered necessary for this study.

AI Use Statement: In the creation of this article, artificial intelligence tools were used.

AI tools, specifically Google Gemini and GPT-4, were employed to rephrase sentences for clarity, check grammar and spelling, and summarize sections of the literature. All final content and conclusions presented are the responsibility of the authors.

References

Ahmed, A. A., and Alabi, O. (2024). Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: A systematic review. *IEEE Access*.

Ali, G., Mijwil, M. M., Buruga, B. A., and Abotaleb, M. (2024). A comprehensive review on cybersecurity issues and their mitigation measures in FinTech.

Aljofey, A., Rasool, A., Jiang, Q., and Qu, Q. (2022). A feature-based robust method for abnormal contracts detection in ethereum blockchain. *Electronics*, *11*(18), 2937.

Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., and Hameed, I. A. (2022). A ML and blockchain based efficient fraud detection mechanism. *Sensors*, *22*(19), 7162.

Asmar, M., and Tuqan, A. (2024). Integrating ML for sustaining cybersecurity in digital banks. *Heliyon*, *10*(17).

Baabdullah, T., Alzahrani, A., Rawat, D. B., and Liu, C. (2024). Efficiency of Federated Learning and Blockchain in Preserving Privacy and Enhancing the Performance of Credit Card Fraud Detection (CCFD) Systems. *Future Internet*, *16*(6), 196.

Bonsu, O. A. M., Dui, L. K., Muyun, Z., Asare, E. K., and Amankwaa, I. A. (2018). Corporate fraud: Causes, effects, and deterrence on financial institutions in Ghana. *European Scientific Journal*, *14*(28), 315-335.

Btoush, E. A. L. M., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., and Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. *PeerJ Computer Science*, *9*, e1278.

Chang, V., Di Stefano, A., Sun, Z., and Fortino, G. (2022). Digital payment fraud detection methods in digital ages and Industry 4.0. *Computers and Electrical Engineering*, *100*, 107734.

Charizanos, G., Demirhan, H., & İçen, D. (2024). An online fuzzy fraud detection framework for credit card transactions. Expert Systems with Applications, 252, 124127.

El-Chaarani, H., and El-Abiad, Z. (2024). The impact of public legal protection on the internal corporate governance efficiency in banking sector. *Journal of Economic and Administrative Sciences*, *40*(3), 482-515.

Gaikwad, V., Meher, K., Dass, R., Jonista, A. S., D'Souza, J., and Victor, R. (2023). Fraud Detection Using ML and Blockchain. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(6s), 584-590.

Ghrib, T., Khaldi, Y., Pandey, P. S., and Abusal, Y. A. (2024). Advanced Fraud Detection In Card-Based Financial Systems Using A Bidirectional Lstm-Gru Ensemble Model. *Applied Computer Science*, *20*(3), 51-66.

Hilal, W., Gadsden, S. A., and Yawney, J. (2022). Financial fraud: a review of anomaly detection techniques and recent advances. *Expert systems With applications*, *193*, 116429.

Ileberi, E., and Sun, Y. (2024). Advancing Model Performance With ADASYN and Recurrent Feature Elimination and Cross-Validation in ML-Assisted Credit Card Fraud Detection: A Comparative Analysis. *IEEE Access*.

Ileberi, E., Sun, Y., and Wang, Z. (2021). Performance evaluation of ML methods for credit card fraud detection using SMOTE and AdaBoost. *Ieee Access*, *9*, 165286-165294.

Ismaeil, M. K. A. (2024). Harnessing AI for Next-Generation Financial Fraud Detection: A DataDriven Revolution. *Journal of Ecohumanism*, *3*(7), 811-821.

Khan, H. U., Malik, M. Z., Nazir, S., and Khan, F. (2023). Utilizing bio metric system for enhancing cyber security in banking sector: A systematic analysis. *Ieee Access*, *11*, 80181-80198.

Kyrychenko, V., Soldatenko, O. A., Gorokhovska, O. V., Voloshyna, M. O., and Maksymova, L. O. (2021). Fraud in the banking system of Ukraine: ways to combat taking into account foreign experience. *Amazonia Investiga*, *10*(45), 208-220.

Kulmie, D. A., and Ibrahim, M. S. (2024). Bank corporate governance: Shield against fraud. *Journal of Ecohumanism*, *3*(3), 1917-1932.

Lescano-Delgado, M. (2023). Avances en el uso de inteligencia artificial para la mejora del control y la detección de fraudes en organizaciones. *Revista Científica de Sistemas e Informática*, *3*(1), e494-e494.

Lokanan, M. E., and Sharma, K. (2022). Fraud prediction using ML: The case of investment advisors in Canada. *ML with Applications*, *8*, 100269.

Marconi, M. A., and Lakatos, E. M. (2017). Fundamentals of Scientific Methodology. 8th ed. São Paulo, SP: Atlas. 346.

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., ... and Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *bmj*, *372*.

Patil, A., Mahajan, S., Menpara, J., Wagle, S., Pareek, P., and Kotecha, K. (2024). Enhancing fraud detection in banking by integration of graph databases with ML. *MethodsX*, *12*, 102683.

Rabbani, H., Shahid, M. F., Khanzada, T. J. S., Siddiqui, S., Jamjoom, M. M., Ashari, R. B., ... and Nooruddin, M. (2024). Enhancing security in financial transactions: a novel blockchain-based federated learning framework for detecting counterfeit data in fintech. *PeerJ Computer Science*, *10*, e2280.

Ren, Y., Ren, Y., Tian, H., Song, W., and Yang, Y. (2023). Improving transaction safety via anti-fraud protection based on blockchain. *Connection Science*, *35*(1), 2163983.

Roever, L. (2020). Practical guide to systematic reviews and meta-analysis.

Stojanović, B., and Božić, J. (2022). Robust financial fraud alerting system based in the cloud environment. *Sensors*, *22*(23), 9461.

Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., ... and Runevic, J. (2021). Follow the trail: ML for fraud detection in Fintech applications. *Sensors*, *21*(5), 1594.

Taher, S. S., Ameen, S. Y., & Ahmed, J. A. (2024). Advanced fraud detection in blockchain transactions: An ensemble learning and explainable ai approach. *Engineering, Technology & Applied Science Research*, *14*(1), 12822-12830.

Wei, S., and Lee, S. (2024). Financial anti-fraud based on dual-channel graph attention network. *Journal of Theoretical and Applied Electronic Commerce Research*, *19*(1), 297-314.

Wijaya, M. G., Pinaringgi, M. F., and Zakiyyah, A. Y. (2024). Comparative Analysis of ML Algorithms and Data Balancing Techniques for Credit Card Fraud Detection. *Procedia Computer Science*, *245*, 677-688.