Journal of
Risk and Financial Management

MDPI

Systematic Review

AI and Financial Fraud Prevention: Mapping the Trends and Challenges Through a Bibliometric Lens

Luiz Moura [1,*], Andre Barcaui [1] and Renan Payer [2]

[1] Faculdade de Administração e Ciências Contábeis (FACC), Universidade Federal do Rio de Janeiro (UFRJ), Av. Pasteur, 250–sala 242, Praia Vermelha, Urca, Rio de Janeiro 22290-240, Brazil; barcaui@facc.ufrj.br
[2] Departamento de Engenharia de Produção (TEP), Universidade Federal Fluminense (UFF), Rua Passo da Pátria, 156, Bloco D–sala 306, Campus da Praia Vermelha, Niterói 24210-240, Brazil; rpayer@id.uff.br
* Correspondence: lcarlos_moura@facc.ufrj.br

Abstract: This study systematically reviews academic research on artificial intelligence (AI) in financial fraud prevention. Employing a bibliometric approach, we analyzed 137 peer-reviewed articles published between 2015 and 2025, sourced from Scopus, Web of Science, and ScienceDirect. Using Bibliometrix, we mapped the field's intellectual structure, collaboration patterns, and thematic clusters. Research interest has surged since 2019, led mainly by China and India, though the literature is mostly technical, with limited social science engagement. Three main themes emerged: AI-based fraud detection models, blockchain and fintech integration, and big data analytics. Despite growing output, international collaboration and focus on ethical, regulatory, and organizational issues remain limited. These insights provide a foundation for advancing both research and practical AI-driven fraud mitigation.

Keywords: bibliometric review; artificial intelligence; financial fraud prevention; machine learning; fintech

Academic Editor: Thanasis Stengos

Received: 16 April 2025
Revised: 4 June 2025
Accepted: 9 June 2025
Published: 12 June 2025

Citation: Moura, L., Barcaui, A., & Payer, R. (2025). AI and Financial Fraud Prevention: Mapping the Trends and Challenges Through a Bibliometric Lens. *Journal of Risk and Financial Management*, *18*(6), 323. https://doi.org/10.3390/jrfm18060323

1. Introduction

The financial sector has experienced rapid advancements in the application of artificial intelligence (AI) and machine learning (ML) technologies, transforming key areas such as risk management and decision making. One of the most critical applications of AI in this domain is financial fraud detection and prevention. Fraud continues to pose a significant threat, and as fraudsters adapt their tactics, traditional methods become increasingly ineffective, highlighting the need for more sophisticated solutions. AI-powered tools, such as machine learning algorithms and big data analytics, have emerged as essential for real-time fraud detection, enhancing both efficiency and accuracy. Moreover, as fraud patterns constantly evolve, AI-driven detection systems must continually adapt as well. Our review finds that, while some recent studies propose adaptive or online learning algorithms to cope with emerging fraud strategies, this aspect is not yet thoroughly covered in the literature—indicating a crucial gap where academic research is still catching up to rapidly changing fraud tactics.

AI has proven its potential across multiple sectors of the financial industry, including credit risk assessment, customer service optimization, and fraud prevention (Jagtiani & John, 2018; N. Kumar et al., 2019; Hajek & Henriques, 2017; Jullum et al., 2020). Although numerous studies have explored AI's application in areas such as credit scoring, algorithmic trading, and predictive analytics for financial crime prevention (B. S. Kumar & Ravi, 2016; Belanche et al., 2024; Cummings, 2021), the specific role of AI in tackling financial fraud

remains a critical yet underexplored subject. Existing literature has examined various AI models for detecting and preventing fraud, including credit card fraud, money laundering, and insider trading (Kirkos et al., 2007; Ngai et al., 2011), but often lacks a holistic view of the field. Most research tends to focus on isolated aspects, leaving gaps in understanding the broader trends, methodologies, and evolving challenges within the domain of AI-based fraud prevention.

A notable gap in the literature is the insufficient number of studies addressing AI's evolution and its effectiveness in financial fraud prevention. Moreover, there is limited engagement from the social sciences and interdisciplinary fields, which limits understanding of critical issues such as algorithmic bias, regulatory challenges, organizational resistance, and the societal impact of AI-driven decisions. Addressing this gap could lead to more responsible and context-aware fraud prevention strategies. Future research would benefit from incorporating insights from behavioral finance, law, and public policy to align technological solutions with ethical and institutional considerations. While works by Ahmed et al. (2022), Goodell et al. (2021), and Lu et al. (2022) have contributed to the broader understanding of AI in finance, they overlook the specific context of fraud detection. Furthermore, these studies fail to systematically examine how academic research aligns with the practical needs of financial institutions facing increasingly sophisticated fraud tactics. This paper aims to fill this gap by expanding on Ahmed et al. (2022), providing a deeper exploration of AI methods in financial fraud prevention, and offering insights into both academic and practical implications.

The primary objective of this study is to map the scientific literature related to the use of AI in the prevention and control of financial fraud. Specifically, the paper seeks to answer the research question: how has the academic debate surrounding AI techniques for preventing financial fraud evolved over time? To address this, the study first conducts a comprehensive bibliometric analysis of the available literature. This analysis will identify key themes, methodologies, and trends in the application of AI to financial fraud detection. The study will then examine the evolution of AI research in financial fraud prevention by analyzing publication patterns and identifying emerging areas of interest. Finally, it will conduct an in-depth analysis of the most influential articles in the field, selecting them based on citation counts and other relevant criteria, to assess their impact on the academic discourse.

This research offers several important contributions to both academic literature and the practice of financial fraud prevention. First, it provides a much-needed synthesis of the current state of AI applications in financial fraud detection, offering a holistic view of the methodologies and techniques employed in this domain. Second, through its bibliometric analysis, the study identifies key trends and research gaps, highlighting areas that require further exploration. Additionally, by linking the findings from academic literature to the practical challenges faced by financial institutions, this paper contributes to a more nuanced understanding of how AI can be effectively utilized to combat financial fraud in real-world scenarios. The insights from this study have the potential to inform future research directions and the development of more effective fraud prevention strategies.

In addition to mainstream financial institutions, recent studies have explored how AI is being implemented in specialized financial environments such as Islamic banking. For example, Hamadou et al. (2024) analyze AI-based tools for fraud detection and compliance in Sharia-compliant financial systems. Their findings highlight how ethical and religious considerations intersect with technological innovations, reinforcing the importance of tailoring AI applications to diverse institutional contexts. Including such perspectives broadens the discussion and emphasizes the need for inclusive, culturally aware research on AI-driven fraud prevention.

Recent advancements highlight the growing need to tackle emerging challenges in fraud detection, including: (i) the continuous evolution of fraud patterns, which demands models capable of adapting dynamically to new fraudulent behaviors (Chen et al., 2025); and (ii) the convergence of AI and blockchain technologies, where smart contracts can autonomously execute preventive actions upon identifying fraud risks. These innovations mark a paradigm shift toward more adaptive and self-sufficient fraud prevention frameworks, leveraging AI's predictive capabilities alongside blockchain's transparency and immutability. For the first challenge, although concept drift in fraud is well-recognized (Chen et al., 2025), relatively few studies in our corpus explicitly propose mechanisms for continuous model updates or online learning to handle this issue. This suggests that academic literature is still developing proactive strategies to ensure AI models remain effective as fraud tactics evolve, underscoring an important avenue for future work.

Building on these developments, AI-driven fraud detection has evolved with the introduction of cloud-optimized Transformer models, enhancing scalability and real-time data processing capabilities (Deng et al., 2025). These models leverage graph self-attention mechanisms to detect complex fraudulent patterns without extensive feature engineering. Moreover, the integration of quantum computing with federated learning has enabled frameworks like QFNN-FFD, which achieve precision rates above 95% while ensuring data privacy (Innan et al., 2024). These advancements signify a shift toward more adaptive and secure fraud detection systems, addressing the growing sophistication of financial fraud schemes.

The structure of the paper is as follows: Section 2 outlines the methodology used for the bibliometric analysis and data sources, the treatment of the data, article selection criteria, and the categorization process. Section 3 presents the results of the analysis, focusing on trends, influential studies, and further analysis. Finally, Section 4 concludes the paper by discussing the implications of the findings and suggesting directions for future research. This structure facilitates a comprehensive examination of AI's role in financial fraud prevention.

2. Materials and Methods

2.1. Methodology

This study employs a quantitative approach due to its bibliometric nature, which involves the systematic measurement of scientific knowledge production and dissemination (Araújo, 2006). Quantitative research employs deductive reasoning and statistical methods to analyze numerical data, ensuring replicability and objectivity (Gerhardt & Silveira, 2009). Bibliometrics applies statistical techniques to quantify patterns in scholarly communication (Quevedo-Silva et al., 2016) and facilitates the examination of academic output within a specific field, enabling the mapping of research communities, the identification of scholarly networks, and an understanding of underlying research trends (Chueke & Amatucci, 2015).

2.2. Data Collection

For data collection, the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) methodology (Moher et al., 2015) was adapted to include four key stages: identification, screening, eligibility, and inclusion (Figure 1). In the identification stage, the population, intervention, comparison, outcomes, and context (PICOC) protocol was used to define the search string ("Financial Fraud" AND "Artificial Intelligence" OR "Machine Learning") in keywords, titles, and abstracts (Navarrete et al., 2018). A total of 1,085 records were retrieved from three prominent databases: Scopus (468 articles), Web of Science (191 articles), and ScienceDirect (426 articles). Scopus, Web of Science, and ScienceDirect were selected for their extensive coverage of high-impact journals and

advanced search capabilities, ensuring a comprehensive and rigorous dataset (Chadegani et al., 2013; Mongeon & Paul-Hus, 2016).

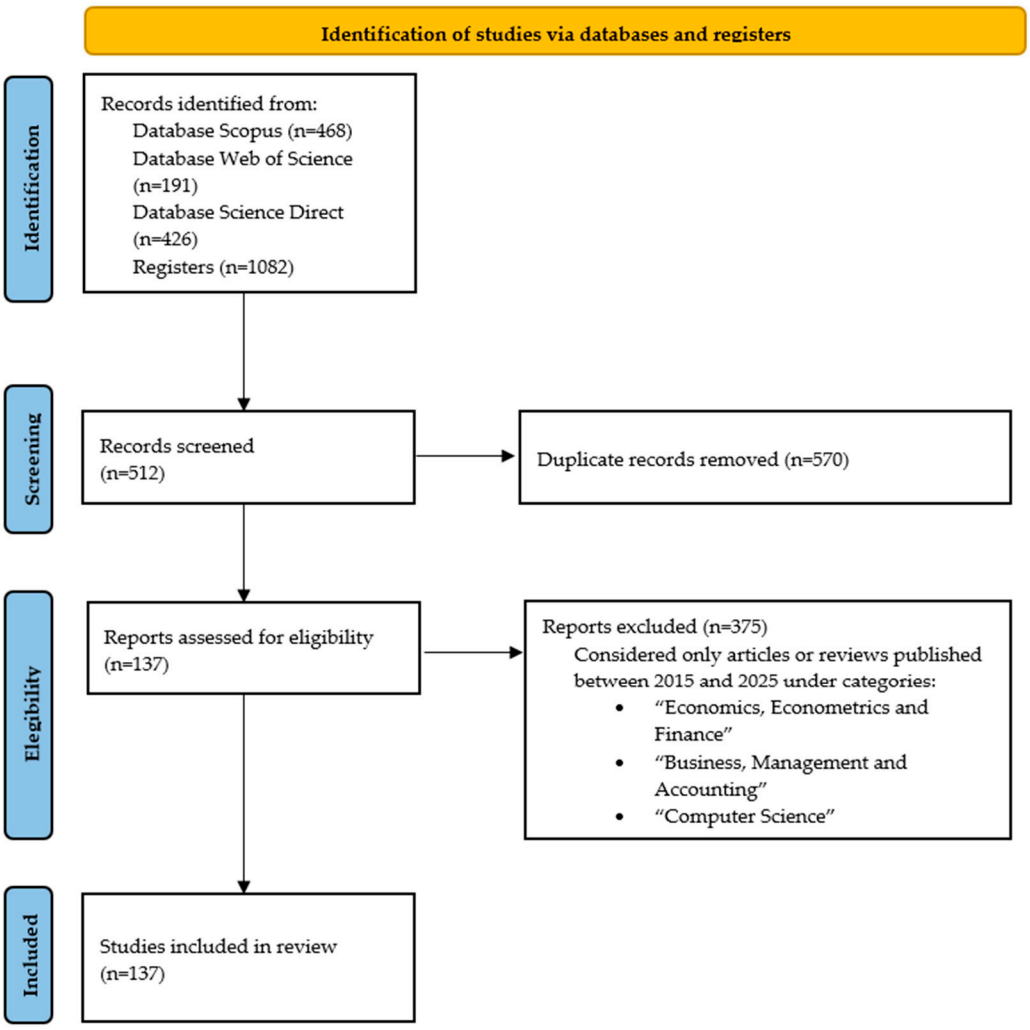

Figure 1. PRISMA flowchart (Page et al., 2021).

In the screening phase, duplicate entries across databases were removed, resulting in a total of 512 unique articles. The eligibility stage involved a comprehensive assessment of the articles' alignment with the research scope, leading to the inclusion of 137 articles in the final review. Only articles or reviews published in journals under the "Economics, Econometrics and Finance", "Business, Management and Accounting", or "Computer Science" categories and available for download were considered. Additionally, only articles published between 2015 and 2025 were included to ensure the research was up to date and aligned with the latest academic contributions in the field. This review was registered in a public registry with Open Science Framework (associated project osf.io/axty2/Registration DOI https://doi.org/10.17605/OSF.IO/KH7E6).

2.3. Analysis Framework

The metadata of the 137 articles (Figure 1) that made up the bibliographic database were analyzed with the help of the Bibliometrix software (Aria & Cuccurullo, 2017) and the biblioshiny application, which offers a web interface to Bibliometrix (Secinaro et al., 2020). The analysis was conducted based on three macro aspects: general trends, journals, and authors. First, the general analysis focused on examining the number of publications per year, providing a temporal overview of scientific production on the topic over time.

This helped identify potential trends and variations in academic interest, as suggested by Merigó et al. (2018). Additionally, the frequency of keywords over the years was analyzed to uncover trends and variations in academic discourse. Finally, the number of publications per country was assessed to offer a geographical overview of the academic output, as highlighted by Ahmed et al. (2022).

To identify the most relevant journals, Bradford's Law was used to identify core journals that contribute most significantly to the field, allowing for a targeted analysis of key publication sources (Chueke & Amatucci, 2015). Furthermore, Lotka's Law will be employed to analyze author productivity, evaluating whether article output is concentrated among a few researchers or more evenly distributed across a larger pool of contributors, as indicated by Araújo (2006).

In addition, the biblioshiny application made it possible to obtain an overview of the most explored research topics, the topics that still need to be further explored and deepened, the development of research topics over time, and which topics still need to be addressed holistically, within the scope of the application of artificial intelligence for the prevention of financial fraud.

3. Results

3.1. General Information

The bibliometric database comprises 137 articles from 92 distinct sources, covering the period from January 2015 to January 2025. On average, each article has received 26.36 citations, suggesting a growing academic interest in the field, with a total of 454 contributing authors. The collaboration index indicates an average of 3.57 authors per paper, reflecting a moderate level of co-authorship.

Figure 2 presents the annual distribution of publications, revealing an average growth rate of 23.11%. The findings indicate that research on the application of artificial intelligence and machine learning in financial fraud prevention has gained significant traction since 2021. This aligns with recent studies emphasizing the acceleration of AI applications in finance during the post-pandemic digital transition (Biswas et al., 2024; Zhu et al., 2024).

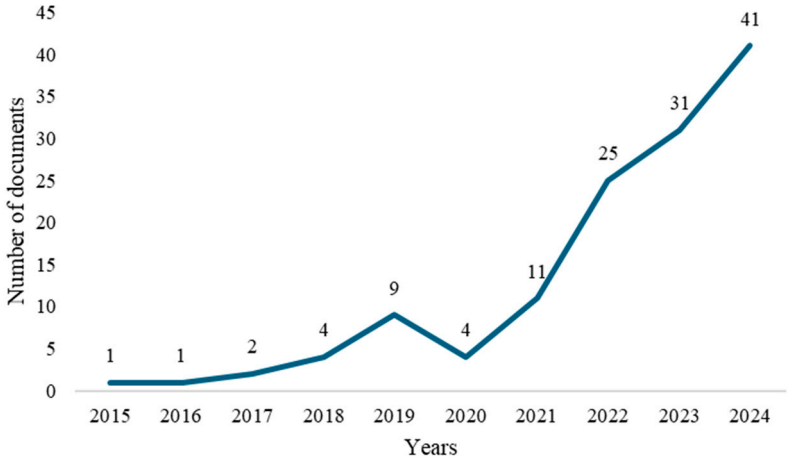

Figure 2. Financial Fraud, AI, and ML in literature growth.

The concentration of publications in recent years highlights both the critical nature of the subject and the growing academic interest in this area. Notably, the financial sector has progressively integrated these technologies into fraud prevention strategies since 2021, marking a pivotal shift in industry practices (Xia et al., 2024).

3.2. Most Relevant Sources

Identifying the most influential publication sources is crucial for understanding the dissemination of knowledge in this field. Figure 3 highlights the eight journals contributing at least three articles to the bibliographic database. Among them, *IEEE Access* and *Expert Systems with Applications* stand out as the primary sources, with 15 and 7 publications, respectively.

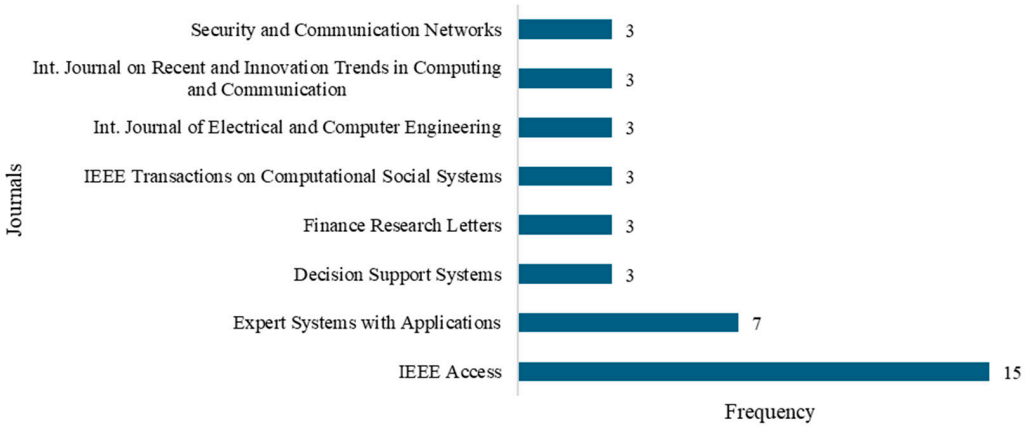

Figure 3. Most relevant scientific sources.

A key aspect of bibliometric analysis is Bradford's Law (Bradford, 1985), which categorizes journals based on their publication volume by dividing them into three sections, each representing one-third of the total publications. The first section, comprising the journals listed in Figure 2, contains the most productive sources in the field. Notably, Bradford's Law suggests that early publications on an emerging topic tend to appear in a small number of highly relevant journals, which subsequently attract increasing submissions as the field evolves.

The prominence of *IEEE Access* and *Expert Systems with Applications* in financial fraud detection research can be attributed to their broad scope, covering key topics such as artificial intelligence, machine learning, big data, and cybersecurity (Hsin et al., 2022). These fields play a pivotal role in advancing fraud detection techniques, which are essential for mitigating financial losses and maintaining institutional credibility (Almazroi & Ayub, 2023). The strong emphasis on applied and interdisciplinary research in *IEEE Access*, along with *Expert Systems with Applications*' focus on practical technological solutions, makes them ideal platforms for publishing innovative studies in this domain. Together, these two journals not only dominate the field in terms of volume but also serve as hubs for innovation and interdisciplinary integration.

Most articles published in *IEEE Access* propose hybrid fraud detection models that integrate various approaches, including deep neural networks, active learning, federated learning, and hyperparameter optimization, to enhance accuracy and efficiency (Awosika et al., 2024). Additionally, these studies commonly address challenges such as imbalanced datasets and data privacy concerns, often leveraging blockchain technology to ensure security (Dasari & Kaluri, 2024). The practical orientation of these contributions facilitates the real-world implementation of fraud detection solutions, reinforcing trust within the financial sector (Lin et al., 2018).

On the other hand, publications in *Expert Systems with Applications* distinguish themselves by prioritizing the interpretability of fraud detection models, ensuring that predictions remain transparent and explainable (Ranganatha & Syed Mustafa, 2025). These studies explore novel techniques for detecting fraud in diverse financial contexts, including digital payment systems and automotive loans. Furthermore, they emphasize collaborative

efforts among financial institutions and data integration strategies to improve fraud detection model effectiveness (Motie & Raahemi, 2024). Additional key topics addressed in these publications include data privacy protection and solution scalability (Błaszczyński et al., 2021).

3.3. Main Authors, Articles, and Affiliations

A key aspect of bibliometric analysis is evaluating authors based on their publication output and citation impact. Table 1 presents the five most prolific authors within the bibliographic database, each with a minimum of three published articles, along with their institutional affiliations. Notably, Zhao Wang emerges as a leading contributor, with four articles primarily focused on the role of artificial intelligence (AI) in financial fraud detection. While these studies underscore AI's significance in fraud prevention, they lack a comprehensive, systematic examination of its evolution and alignment with institutional requirements, leaving a critical gap in the literature.

Table 1. Authors with the highest number of publications on the subject, citations, and their affiliations.

Authors	Articles	Affiliation
Zhao Wang	4	Accounting School, Capital University of Economics and Business, China
Jingyu Li	3	School of Economics and Management, Beijing University of Technology, China
Yubin Li	3	School of Economics and Management, Harbin Institute of Technology, China
Shi Qiu	3	School of Economics and Management, Changsha University, China
Lei Wang	3	Chinese Academy of Sciences, China

Note: This table presents researchers with the most papers in the bibliometric analysis, their number of articles on the topic, and the university in which they are affiliated.

Zhang et al. (2025) apply machine learning techniques to construct enterprise portrait models for fraud prediction, while W. Liu et al. (2025) enhance detection accuracy by integrating natural language processing (NLP) with accounting indicators. D. Zhao et al. (2025) propose the Polytope Fraud Theory, introducing a multi-dimensional analytical framework for preventing accounting fraud, whereas Ileberi et al. (2022) refine credit card fraud detection through genetic algorithms. Despite the methodological diversity, current studies lack an integrated framework to assess AI's effectiveness across various fraud scenarios and its practical implementation challenges.

In line with Lotka's Law (Lotka, 1926), which posits that most authors contribute only one publication, this study finds an even higher rate: 93.5% of the 454 contributing authors published only once, while, at the other extreme, only one author published four articles. This trend underscores the emergent nature of the research topic, indicating that, while many researchers explore AI-based fraud prevention, only a few have established themselves as prolific contributors in the field. This pattern aligns with findings by Bou Reslan and Jabbour Al Maalouf (2024) and Duan et al. (2024), who highlight the evolving nature of AI research in financial fraud detection and the increasing diversification of scholarly contributions.

Beyond productivity, co-authorship networks provide valuable insights into collaborative structures within the field, as depicted in Figure 4. This visualization reveals four primary co-authorship clusters: a lilac cluster centered around authors Wang L. and Fu S.; a red cluster focused on Wang Z.; a blue cluster, with Li J. at its core; and a brown cluster primarily highlighting the collaboration between Fan G. and Song Y.

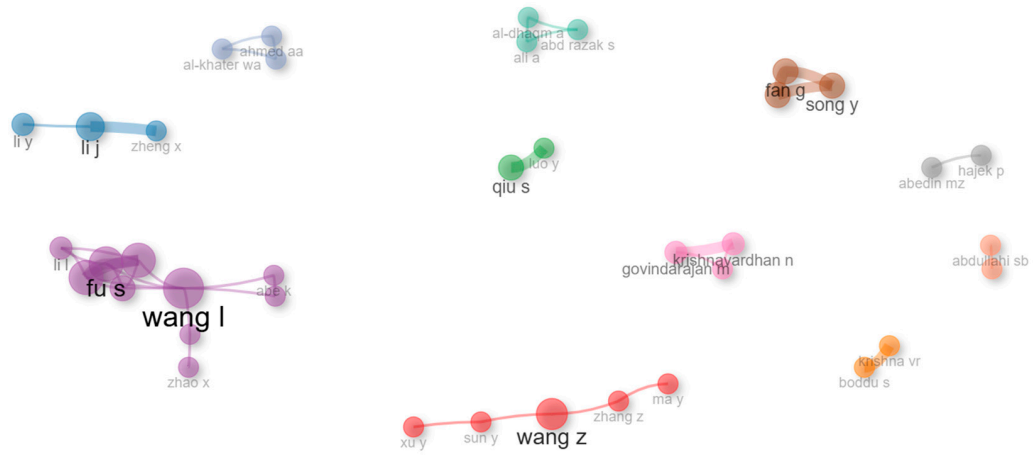

Figure 4. Co-authorship for authors.

- The lilac cluster predominantly addresses financial fraud detection through advanced big data and artificial intelligence techniques, such as deep neural networks, graph algorithms, and privacy-preserving federated learning (L. Wang et al., 2021);
- The red cluster explores cutting-edge quantum machine learning methods, including quantum graph neural networks and quantum classifiers, to improve the accuracy and efficiency of detecting fraudulent activities in financial data (Y. Wang & Zhu, 2024);
- The blue cluster investigates diverse approaches to financial fraud detection, such as the analysis of abnormal managerial tone in Chinese listed firms (X. Wang, 2024), the development of intelligent support systems based on a three-level relationship penetration model (R. Li et al., 2023), and the integration of generative AI in economic and financial research (Zhang et al., 2022);
- The brown cluster emphasizes enhancing fraud prediction models through innovative key indicator selection using hybrid machine learning approaches (L. Wang et al., 2021) and applying fusion models for more effective predictive systems (J. Li et al., 2024).

3.4. Most-Cited Articles

Analyzing bibliometric trends also involves identifying the most cited articles, as they significantly shape the field. Table 2 presents the ten most-cited articles, with the top three being West and Bhattacharya (2016), Goodell et al. (2021), and Hilal et al. (2022). These papers underscore the transformative potential of AI and ML in anomaly detection and financial decision making, while also hinting at future research directions for enhancing fraud detection systems. While these studies are highly influential, they tend to focus more on anomaly detection techniques rather than offering a longitudinal view of AI's evolution in fraud prevention.

These most-cited articles have in common the fact that they portray financial fraud prevention scenarios using or testing various types of algorithms. It is important to highlight concern with aspects of system vulnerabilities and data security that must be available and complete at the same time (Khetani et al., 2023). Finally, it can be highlighted that these articles converge with their discussions to propose to overcome the main problems and limitations imposed by the continuous modification of the systems developed to defraud financial data or carry out illicit transactions (Goodell et al., 2021).

A notable gap in the literature pertains to the integration of other technologies with AI and ML for fraud detection, as well as the continuous evolution of these technologies to counter increasingly sophisticated fraudulent tactics. Future research must address these limitations, focusing on adaptive AI mechanisms capable of identifying emerging fraud patterns and ensuring robust financial security.

Table 2. Articles with the highest number of citations.

Reference	Citations	Major Contributions and Objectives	Top Criticisms or Issues Reviewed	Main Methodological Aspects
West and Bhattacharya (2016)	714	Addresses the association between fraud types, CI-based detection algorithms, and their performance	The growing reliance on new technologies can exacerbate the problem of financial fraud	Uses data mining to review the literature
Goodell et al. (2021)	687	It highlights aspects of fraud prevention with concern for 3 main aspects: portfolio construction, valuation, and investor behavior; financial fraud and distress; and sentiment inference, forecasting, and planning	Problems and vulnerabilities in fraud detection systems	It uses analyses of co-citation, co-occurrence, confluence, and bibliometric coupling
Hilal et al. (2022)	534	Focuses on highlighting recent advances in the areas of semi-supervised and unsupervised learning in financial fraud prevention	Increasing vulnerabilities in financial data security systems	Review and multi-methods
Masood et al. (2023)	511	Detailed analysis of existing tools and machine learning (ML)-based approaches to deepfake generation	Improve the domains of deepfake generation and detection	Review and multi-methods
Hajek and Henriques (2017)	397	Combines financial information and management commentary in corporate annual reports in structuring fraud prevention methods	Document-based fraud detection	Use of wide range of machine learning methods
Ileberi et al. (2022)	303	Proposes a credit card fraud detection mechanism based on machine learning (ML) using the genetic algorithm (AG) for trait selection	Specific assessment of credit card fraud	Use of multiple algorithms for testing
Itoo et al. (2021)	298	Uses a logistic-regression-based model for fraud prediction that has been found to be better compared to other prediction models developed from naïve Bayes and K-nearest neighbors for credit card fraud prevention	Credit card data is highly skewed, which leads to inefficient prediction of fraudulent transactions	Resampling (oversampling or subsampling) for best results

Table 2. *Cont.*

Reference	Citations	Major Contributions and Objectives	Top Criticisms or Issues Reviewed	Main Methodological Aspects
X. Zhao et al. (2019)	226	A visual analytical system is proposed with the objective of interpreting models and predictions of random forests	Low interpretability of the decision tree model	Two use scenarios and a qualitative user study were conducted
Choi and Lee (2018)	186	Fraud detection by resource selection, sampling, and application of supervised and unsupervised algorithms	Accurate detection based on multiple technologies	Use of multiple algorithms for testing
Khetani et al. (2023)	121	It covers the effects of DL and ML algorithms in different industries, such as healthcare, NLP, financial services, and network security	Lack of a study that holistically encompasses different sectors	Multi-domain analysis of DL and ML algorithms in various domains

Note: This table presents the top 10 papers with highest number of citations on the topic.

3.5. Institutional Contributions

Table 3 highlights the most relevant institutions (universities or research centers) with at least five published articles, showcasing the top 13 institutions and their respective publication counts. Hunan University of Finance and Economics (China) ranks first with 13 publications, followed by Shandong University (China) with 7. Figure 5 further illustrates this trend by mapping the countries with the highest publication counts, considering both multiple-country publications (MCPs) and single-country publications (SCPs). The overwhelming presence of Chinese institutions among the top contributors underscores the country's strategic focus on integrating AI into financial systems.

Table 3. Main authors' affiliations.

Affiliation	Articles
Hunan University of Finance and Economics (China)	13
Shandong University (China)	7
Luoyang Normal University (China)	6
Beijing University of Technology (China)	5
Chongqing University (China)	5
Guizhou Normal University (China)	5
Shandong University of Finance and Economics (China)	5
Sun Yat-sen University (China)	5
Tongji University (China)	5
Universidad Cooperativa de Colombia (Colombia)	5
Universiti Teknologi Malaysia (Malaysia)	5
University of Chinese Academy of Sciences (China)	5
Yantai University (China)	5

Note: This table presents the main universities with which researchers in the topic are affiliated.

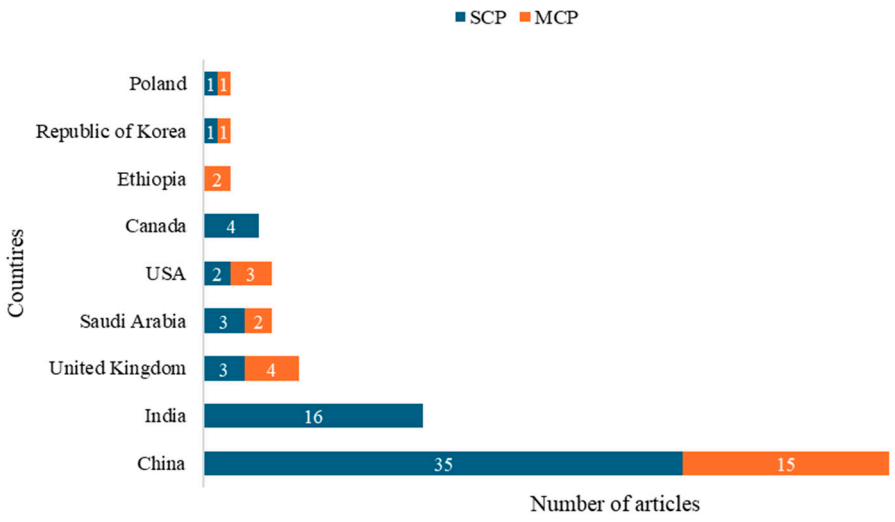

Figure 5. Number of articles per country.

This finding aligns with Jeong et al. (2024), who emphasize China's substantial investments in research and development, particularly in AI and ML, as part of its broader strategy for economic cohesion and financial fraud prevention. Additionally, Zheng et al. (2024) highlight China's educational focus on science, mathematics, and engineering, which has significantly bolstered its research capabilities. This underscores the need for other nations to invest in similar technological advancements to expand scientific knowledge in these critical areas.

Furthermore, China has a significant presence in research and studies on financial fraud, with several ongoing initiatives and research projects (Figure 5). The focus of

Chinese research is on areas such as online fraud detection and prevention, financial platform security, and data analysis to identify fraudulent patterns (Shi & Zhao, 2023). It is also worth noting that Chinese research on financial fraud also involves partnerships with financial institutions, technology companies, and law enforcement agencies to share information and experiences (Huang et al., 2022).

A particularly noteworthy aspect of Hunan University of Finance and Economics' research is its emphasis on AI and ML applications for fraud prevention in supply chain financing. Several studies from this institution explore AI-driven solutions to enhance financial transaction security, helping businesses finance receivables more efficiently and at lower interest rates. These approaches foster financial integration across supply chains while mitigating risks (Zhou et al., 2020).

Taken together, the bibliometric findings highlight the rapid expansion and geographical concentration of research in AI-driven financial fraud prevention. Despite growing interest, the field still lacks cohesive frameworks and practical integration models, opening pathways for future research. Another notable gap is the limited international collaboration observed in this domain. The co-authorship analysis (Figure 4) revealed that research teams tend to be nationally or regionally siloed, with relatively few cross-country collaborations. For example, China's dominance in publication output—while reflecting strong domestic research initiatives—has not been matched by proportionate multi-country studies. This prevalence of single-country publications suggests that knowledge exchange across borders is scarce. Possible causes of the dearth of international collaboration include data privacy and regulatory barriers (banks are often reluctant or legally unable to share fraud data across jurisdictions), language barriers and regional networks (researchers may collaborate more within their language group or local region), and differences in fraud typologies and financial systems (which lead teams to focus on country-specific fraud issues).

Beyond co-authorship patterns, thematic and citation-based isolation can also be observed. Certain regions predominantly focus on specific themes, such as blockchain integration in Asian institutions, particularly China, while ethical and regulatory dimensions receive more attention from European and North American researchers. These thematic silos highlight areas that could substantially benefit from enhanced international engagement. For example, broader collaboration combining Asian technical expertise with European regulatory and ethical frameworks could lead to more holistic fraud prevention solutions. Addressing these gaps could strengthen global understanding and applicability of AI-driven financial fraud detection systems.

Overcoming these hurdles is important because fraud is a global problem that often exploits cross-border loopholes. To foster global collaboration, the community could establish secure data-sharing frameworks (for instance, using privacy-preserving techniques like federated learning to enable interbank data exchange without violating privacy), create international consortia or working groups focused on AI in fraud prevention, and encourage joint conferences or special issues that bring together experts from different countries. Such efforts would facilitate the pooling of diverse expertise and datasets, ultimately leading to more robust and universally applicable fraud detection models.

3.6. Research Clusters, Trends, and Gaps

Building upon the bibliographic foundation of this study, the research themes are categorized into four distinct clusters (Figure 6). The largest cluster, depicted in red, revolves around the terms "machine learning", "financial fraud", and "fraud detection", which form the core discussion of this article. Machine learning plays a crucial role in detecting financial fraud by analyzing vast datasets to identify patterns indicative of fraudulent activities, particularly in financial markets (Krishna & Boddu, 2023). Fraud

can take various forms, including fraudulent transactions, money laundering, and market manipulation, all of which pose significant threats to the global financial system's stability and integrity (Innan et al., 2024). However, recent technological advancements, particularly in machine learning, present promising new avenues for tackling these challenges more effectively (Usman et al., 2024).

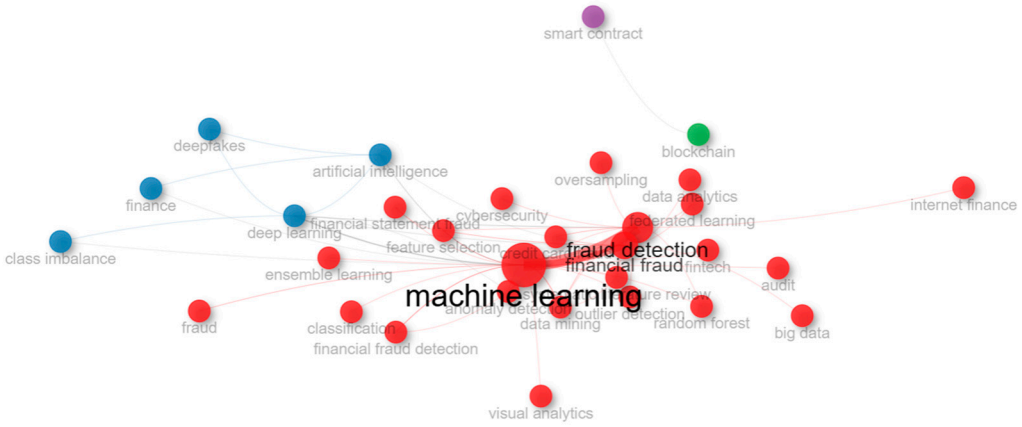

Figure 6. Keyword co-occurrence. The size of the nodes indicates the frequency of occurrence, while the curves between the nodes represent their co-occurrence. The shorter the distance between the two nodes, the larger the number of co-occurrences of the two keywords. This figure can help identify the content clusters.

A crucial distinction must be made between machine learning and artificial intelligence (AI) in the context of financial fraud prevention. The term "artificial intelligence" appears in the second-largest cluster (blue) and represents a broader field that encompasses machine learning as one of its key components (Chhatwani, 2022). AI includes capabilities such as natural language processing, complex problem solving, and decision making (Huang et al., 2022), whereas machine learning focuses primarily on learning from and adapting to previous experiences (Baabdullah et al., 2024).

To safeguard financial institutions, customers, and the broader financial ecosystem from the escalating threat of fraud, a comprehensive fraud detection and management system is necessary within the banking sector (Ismail & Haq, 2024). This can be achieved through a combination of machine learning, real-time fraud analysis based on business rules, and proactive detection approaches (Shi & Zhao, 2023). AI further strengthens this process by identifying suspicious patterns and fraudulent behavior through real-time data analysis (Sengupta & Das, 2023). Additionally, blockchain technology, represented in a smaller cluster (green), along with smart contracts in another (lilac), holds promise in this context. Due to its immutable and transparent nature, blockchain significantly reduces the ability of fraudsters to manipulate data or conduct illicit activities undetected (Baabdullah et al., 2024). Blockchain also facilitates the creation of real-time alert systems capable of identifying suspicious patterns and preventing fraudulent transactions before they are completed (Pranto et al., 2022).

Smart contracts offer another promising application for blockchain in financial services. These self-executing contracts automate agreements between parties, eliminating the need for intermediaries (L. Liu et al., 2022). For example, a smart contract can be programmed to automatically distribute dividends to a company's shareholders once predefined conditions are met (L. Wang et al., 2021). This innovation reduces bureaucracy, costs, and processing time while ensuring contractual compliance with accuracy and transparency (Ranganatha & Syed Mustafa, 2025).

Although blockchain and smart contracts are closely related, they remain insufficiently integrated into broader financial fraud research. Baabdullah et al. (2024) identified this

gap, suggesting that future studies could explore the synergy between blockchain, smart contracts, AI, and machine learning for fraud prevention. This research opportunity is also evident in Figure 7, which presents a thematic map generated from an analysis of 120 author keywords using the Leiden clustering algorithm. The map highlights seven primary themes, each varying in density (development level) and centrality (relevance in the research field).

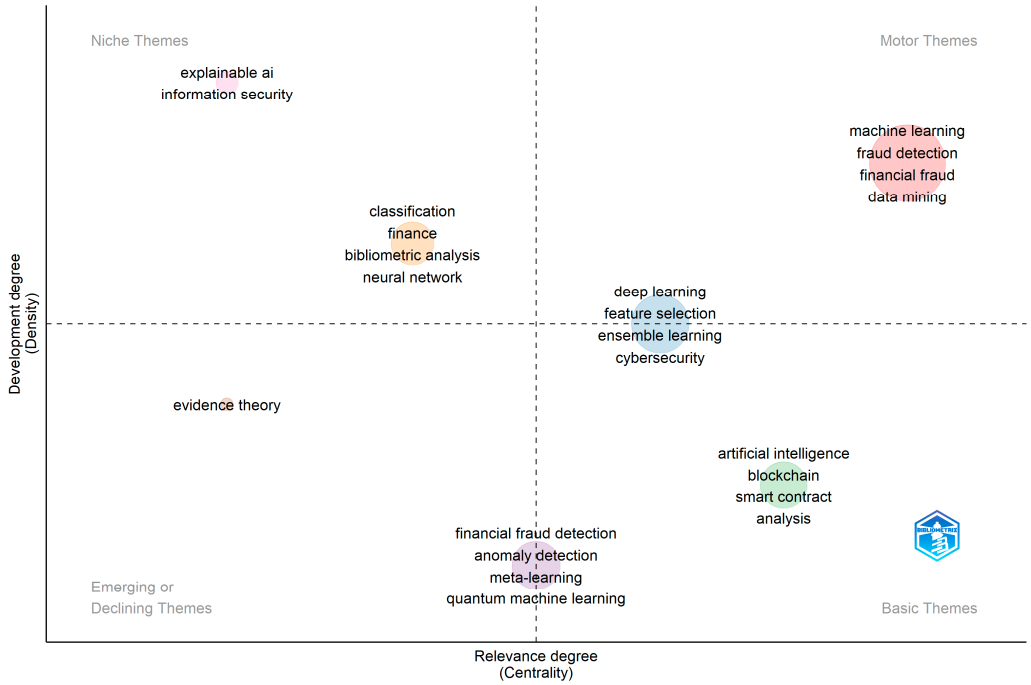

Figure 7. Thematic Map.

Research that holistically incorporates "artificial intelligence", "blockchain", "smart contracts", and "analysis" is positioned as a high-centrality topic with significant growth potential, given its current low density in literature. Consequently, this represents a promising research avenue to explore synergies between these technologies. The increasingly sophisticated nature of fraudulent activities, coupled with continuous technological advancements, underscores the demand for innovative approaches to safeguarding financial assets and ensuring transactional integrity (Tudisco et al., 2024).

Conversely, topics associated with "explainable AI", "information security", and "neural networks" exhibit high density but low centrality, indicating that, while these areas are well-developed, they may not be highly influential in future research. Similarly, "evidence theory" demonstrates minimal relevance, as it shows both low centrality and below-median density, suggesting that research focused solely on these terms may have limited impact. Y. Wang and Zhu (2024) argue that these topics need to be associated with others, especially those related to the new technologies used to combat financial fraud, as fraud mechanisms increasingly become more dangerous and more sophisticated.

However, several emerging research opportunities remain, particularly in areas related to "financial fraud detection", "anomaly detection", "meta-learning", and "quantum machine learning". These topics currently exhibit low density but medium centrality, indicating that, while they are underdeveloped, they hold moderate relevance. Gupta and Mehta (2024) emphasize the challenge of enhancing research relevance through breakthrough discoveries and the development of innovative tools. Notably, "quantum machine learning" presents substantial potential for prevention of financial fraud, though its accessibility remains a challenge.

Key terms such as "machine learning", "data mining", "financial fraud", and "fraud detection" occupy central positions in research themes, demonstrating above-average levels of both centrality and density. This suggests that these themes are well-established and fundamental to understanding the field. Other well-developed topics include "ensemble learning", "deep learning", "cybersecurity", and "feature selection", which remain relevant but are primarily associated with machine-learning-based fraud prevention in financial transactions, particularly credit card fraud (Krishna & Boddu, 2023).

It is also worth showing how some of these terms unfold or merge over time in a brief longitudinal analysis. Figure 8 presents the thematic evolution diagram (author's keywords, number of words = 100; minimum word frequency = 5; Clustering Algorithm Edge Betweenness). The presented grouping of author's keywords used in each period is compared with the following period, showing their thematic connections and substitutions. It should be briefly explained that the Clustering Algorithm Edge Betweenness is an algorithm for grouping elements into networks (Aria & Cuccurullo, 2017). Such an algorithm, in summary, is suitable for small networks due to its slow performance (Newman & Girvan, 2004) and, therefore, was used to obtain the "thematic evolution" graph that does not require large clustering networks.

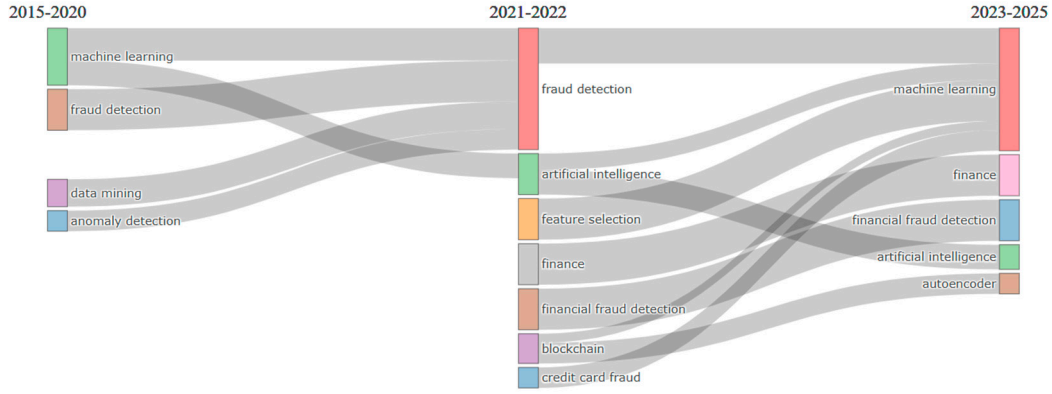

Figure 8. Thematic Evolution.

So, in the thematic evolution diagram (Figure 8), each of the nodes represents a group and is indicated by the main words of the topics, as well as by the time intervals. The number of words included in each topic is represented by the size of the corresponding node. Topics in adjacent time intervals are related when they contain the same words. The amplitude of the links is proportional to the number of words shared by connected topics and indicates relevance between them.

It is important to note some aspects, starting with the fact that research on "machine learning", "fraud detection", "data mining", and "anomaly detection" covered in the period from 2015 to 2020 converged, in the period from 2021 to 2022, in studies on "fraud detection" in a significant amount. This may indicate that the research carried out in this first period considered agreed that data mining can use machine learning to support the prevention of financial fraud. X. Zhao et al. (2019) and Zhou et al. (2020) had this same perception when they argued that data mining and machine learning can together reveal important insights and patterns in an organization's financial data to more clearly perceive patterns of fraudulent behavior.

Another relevant aspect to be noted is that, between 2021 and 2022, topics around artificial intelligence and blockchain technologies in financial fraud prevention mechanisms gained tenor. These two technologies are coupled and joined by "machine learning", as pointed out in the years 2023–2025, to aggregate these prevention mechanisms. This finding was discussed by Ileberi et al. (2022) and Masood et al. (2023) showing that such

technologies together can be more effective, bringing greater efficiency, reliability, and accessibility to financial institutions, as these technologies together allow analyzing large volumes of data in real time, identifying suspicious patterns and behaviors that indicate fraud attempts. For Tudisco et al. (2024), while AI and machine learning improve data analysis, automate processes, and improve decision making, blockchain networks ensure security, transparency, and decentralization in financial transactions.

It is also relevant to note the prominence of the term "autoencoder" in the 2023–2025 interval unfolding from studies on blockchain. This prominence demonstrates the novelty of the topic in the research field, as planned by Tayeb and El Kafhali (2025) when explaining that the autoencoder can be used in the prevention of financial fraud because it is an artificial neural network trained to learn a compact representation of the input data (encoding) and then reconstruct the original input from this compact representation (decoding).

For identifying future research directions, multiple correspondence analysis (MCA) provides valuable insights. As illustrated in Figure 9 (which includes 20 terms and 137 articles), the proximity of keywords in this analysis indicates their frequent co-occurrence in research articles. The closer the dots representing each keyword, the more often they appear together, while greater distances reflect less frequent associations. This analysis effectively maps the conceptual and contextual relationships between key terms, using Dim 1 and Dim 2 values to establish a structured representation (Payer et al., 2024).

Figure 9. Multiple Correspondence Analysis (MCA).

The resulting keyword map reveals three distinct clusters: red, green, and blue. Each cluster comprises closely related keywords, with proximity signifying frequent co-occurrence in articles. The red cluster highlights the core concepts in financial fraud detection, focusing on machine learning and artificial intelligence, with "financial fraud detection" and "artificial intelligence" occupying central positions. The predominance of the red cluster is notorious, as it brings together topics that are widely addressed in research on financial fraud prevention and that are, at the same time, very interconnected. In this sense, Krishna and Boddu (2023) point out that the role of artificial intelligence is increasingly consolidated when it comes to the need to prevent financial fraud, and this consolidation is mainly due to the interest in improving these techniques, as well as the constant search for joining with other technologies for more security.

The blue cluster includes terms such as "data mining", "outlier detection", and "systematic literature review", reflecting their significance in academic discourse. Although it appears with a smaller intensity and size than the red cluster, these terms are gathered since outlier detection has particular relevance in the context of financial fraud prevention as it represents a process of identifying data points that deviate significantly from the

typical pattern or distribution of a data set, which can be increased with the use of data mining (Baabdullah et al., 2024). These deviations are often referred to as outliers and detecting them is crucial to ensure reliable data analysis (Zhou et al., 2020). The challenge is to undertake research that shows how these technologies can be associated with artificial intelligence (the central term of the red cluster) for the prevention of financial fraud, such as credit card fraud, for example.

Finally, the green cluster emphasizes emerging research on "blockchain" and "smart contracts", indicating growing interest in these technologies for financial fraud prevention. According to Dasari and Kaluri (2024), the interest in this relationship between blockchain and smart contracts can be explained by the fact that smart contracts are executed on a blockchain, and all the clauses contained in them are recorded on this network. Once the rules, obligations, and penalties are entered, contracts are automatically executed as agreed and in a secure and verifiable manner. On the other hand, there is the challenge of adding this knowledge to research involving AI (red cluster) for fraud prevention or even associated with data mining mechanisms aimed at outlier detection (blue cluster).

3.7. Further Analysis

Factor analysis highlights a notable gap in the literature regarding the interplay between the key themes identified in the three main clusters. This presents a valuable opportunity for future research to explore the integration of blockchain technologies and smart contracts with machine learning and artificial intelligence in financial fraud prevention. As indicated in the cluster map (Figure 6) and thematic map (Figure 7), the convergence of these technologies has the potential to enable faster and more precise behavioral analysis, strengthening the security of financial transactions. Additionally, this integration could facilitate the secure, transparent, and efficient exchange and monetization of data.

Smart contracts, which are self-executing agreements triggered when predefined conditions are met, operate on blockchain platforms. These contracts automate processes based on encoded rules, obligations, and penalties, eliminating the need for intermediaries (L. Liu et al., 2022). Blockchain plays a fundamental role in ensuring the secure execution of these agreements, preventing tampering or manipulation for personal gain (L. Wang et al., 2021). Stored and digitally recorded within blockchain networks, smart contracts follow predefined logical instructions, automatically initiating actions once specified conditions are satisfied (Ranganatha & Syed Mustafa, 2025).

A detailed examination of Figures 7–9 underscores the potential for further investigation into the synergy between blockchain, smart contracts, machine learning, and artificial intelligence in combating financial fraud. Integrating these technologies could lead to more sophisticated fraud detection mechanisms, enabling financial institutions to respond more effectively to emerging threats. Moreover, advancements in data mining techniques hold promise for enhancing fraud prediction and prevention capabilities, adapting dynamically to evolving fraudulent schemes.

However, it should be noted that many of these cutting-edge technologies remain at an early stage of practical implementation. Blockchain-based solutions and smart contracts, for instance, are largely confined to pilot projects or niche applications (such as cryptocurrency exchanges) and are not yet part of standard anti-fraud toolkits in mainstream banking. This aligns with our observation that blockchain and smart contracts, while promising, are insufficiently integrated into current fraud prevention practice. Likewise, quantum machine learning approaches exist mostly as theoretical models or laboratory experiments (e.g., the QFNN-FFD framework proposed by Innan et al. (2024) is a proof-of-concept), given the nascent state of quantum computing infrastructure. In contrast, more established AI techniques (e.g., machine learning classifiers and anomaly detection algorithms) have

already seen considerable adoption in industry settings. It is crucial for future research not only to innovate in these emerging areas but also to bridge the gap between concept and reality—through field trials, prototype deployments, and collaboration with industry—so that technologies like blockchain and quantum ML can move from theory to practice in fraud prevention.

4. Conclusions

Based on the bibliometric and content analysis, several key trends emerge in the field of AI-driven financial fraud detection. The analysis confirms a sharp increase in publications on AI-driven financial fraud detection over the past decade. The field grew at an average annual rate of 23%, with a pronounced surge after 2021. This trend underscores growing academic and industry attention to combating fraud with advanced technologies. Notably, the dataset of 137 articles involved 454 distinct authors (a collaboration index of ~3.57 authors per paper), indicating that research teams are often interdisciplinary—a reflection of the complex, multifaceted nature of fraud detection.

A few scholarly journals account for a large portion of relevant publications. *IEEE Access* and *Expert Systems with Applications* lead with 15 and 7 papers, respectively, reflecting their broad scope encompassing AI, machine learning, big data, and cybersecurity—all critical areas for fraud prevention. The prominence of these outlets aligns with their focus on applied technological solutions, suggesting that much of the fraud detection research is application-oriented. According to Hsin et al. (2022), such broad-scope venues attract innovative fraud detection studies due to their interdisciplinary appeal. This also echoes Bradford's Law (Figure 3), which shows a core set of journals drawing the most influential work in this emerging subject area.

Another trend is the pursuit of explainable and scalable AI solutions. Researchers recognize that fraud models must not only be accurate but also interpretable to gain trust in operational settings. Several papers in *Expert Systems with Applications* specifically aim to improve the interpretability of fraud detection models so that human analysts can understand and act on AI predictions. Alongside interpretability, studies are considering the scalability of AI methods to massive transaction volumes and fast-changing fraud patterns. For example, recent research highlights collaboration between institutions and integration of diverse data sources to enhance model effectiveness. This indicates a practical orientation in the literature: beyond algorithms, issues of deployment, data integration, and real-time processing are being tackled (Motie & Raahemi, 2024; Błaszczyński et al., 2021).

The findings of this study highlight how AI-driven methodologies have transformed financial fraud detection. Over time, research has shifted from exploratory work to highly practical and scalable solutions. The evolution of academic work on AI for financial fraud prevention, as revealed by this study, demonstrates a clear trajectory toward more effective and practical fraud detection solutions. Over time, the focus has shifted from isolated experiments to a more cohesive and application-driven body of research. Key themes identified—such as the integration of advanced machine learning, emphasis on explainability, and attention to data challenges—illustrate how the academic debate has matured. In particular, the convergence of research on machine learning techniques (from decision trees to deep learning) with domain-specific knowledge of fraud patterns has significantly improved detection capabilities. As our findings show, many recent studies report higher accuracy and lower false positives by leveraging AI models that can capture complex patterns of fraudulent behavior (Baghdadi et al., 2025). For example, innovative hybrid models (combining techniques like restricted Boltzmann machines and LSTM networks) have achieved superior performance, balancing speed and accuracy better than earlier approaches (Baghdadi et al., 2025). Such improvements are crucial, as even marginal

gains in fraud detection accuracy can translate to millions in savings given the scale of financial transactions.

A core advantage evident in AI methodologies is their contribution to efficiency in fraud detection. Traditional rule-based or manual fraud detection systems often struggle with the volume and velocity of modern transactions. In contrast, AI systems excel at processing vast amounts of data in real time, flagging anomalies within milliseconds. This real-time analytical capability means fraudulent transactions can be intercepted before losses occur. For instance, integrating AI with blockchain technology enables the creation of live alert systems that automatically block suspicious activities as they unfold. The literature reflects this shift toward proactive fraud prevention: financial institutions are now employing machine learning models to continuously monitor streams of transactions and user behavior. These models adapt and respond faster than human-driven processes, thereby reducing the window of opportunity for fraud. Moreover, AI algorithms have proven adept at detecting subtle, non-intuitive patterns (such as cross-account linkages or unusual spending sequences) that human auditors might miss. By uncovering hidden relationships in data, AI enhances the accuracy of fraud detection—catching more fraudulent events while minimizing false alarms (which otherwise burden analysts and customers). In summary, the collective evidence confirms that AI methodologies markedly boost both the efficiency and accuracy of fraud detection systems, enabling more timely responses to threats and more precise identification of illicit activities. These improvements strengthen the security of financial platforms and build greater trust with customers, as institutions can mitigate fraud risks more effectively.

Another important implication of our review is the clear alignment between academic research and real-world fraud prevention needs. The dominant research trends—such as handling imbalanced datasets, emphasizing interpretability, and preserving privacy—directly address pain points faced by financial institutions. For example, banks and payment companies require models that not only perform well but can also explain their decisions under regulatory scrutiny. The rise of explainable AI in fraud detection research is thus a response to practical demands for transparency in automated decisions (e.g., why a transaction was flagged). Similarly, concerns around customer data privacy have spurred research into privacy-preserving techniques like federated learning and blockchain-based data sharing. These approaches allow multiple institutions to collaboratively improve fraud detection models without exposing sensitive data, a crucial feature for industry adoption. The literature's emphasis on such solutions suggests that academic innovations are being designed with deployment in mind. Indeed, many studies included in our analysis explicitly discuss how their proposed models could be implemented in operational settings or evaluated on real transaction data, bridging the gap between lab research and field application.

In fact, the prevalence of these themes is quantifiable. A significant subset of the reviewed papers addresses class imbalance in fraud datasets—a practical challenge since fraudulent cases are rare. For example, Itoo et al. (2021) demonstrate that highly skewed credit card data impairs detection and show that applying resampling techniques can markedly improve predictive performance, underlining the importance of handling imbalanced data in practice. Likewise, numerous studies (especially in Błaszczyński et al., 2021) emphasize model interpretability and explainability as key objectives, ensuring that AI-driven predictions can be understood and trusted by human analysts and regulators. The fact that many researchers are incorporating interpretability and even testing their models on real-world transactions indicates a conscious effort to align academic outputs with the needs of industry practitioners. These observations suggest that future research could further explore how domain-specific knowledge from financial institutions can be system-

atically integrated into model design—for example, through human-in-the-loop systems or hybrid decision pipelines. Nevertheless, it is also evident that some gaps remain—notably, relatively few publications delve into the organizational and regulatory dimensions of deploying AI (e.g., change management, compliance with specific laws), suggesting areas where academia has yet to fully engage with all aspects of practical implementation.

This synergy between scholarly work and practical implementation means the advances documented in academic publications are likely to rapidly translate into more robust fraud prevention tools in the finance sector. Despite the considerable technological progress captured in the literature, deploying AI solutions in financial institutions brings real-world challenges that extend beyond algorithmic performance—challenges that our review found are only partially reflected in current research. Regulatory compliance is one such challenge: banks must ensure that AI-driven fraud detection systems adhere to financial regulations and privacy laws (for instance, avoiding decisions that could inadvertently violate anti-discrimination laws or customer data protections). Ethical considerations are equally important, as AI models can inherit biases from training data or operate opaquely, leading to fairness issues in how fraud risk is assessed across different customer groups. Yet, only a small fraction of the surveyed studies explicitly discusses ethics or fairness in fraud AI, indicating a gap between technical research and the socio-ethical context of implementation. Explainability is another critical deployment factor—financial institutions and their regulators increasingly demand that AI models provide transparent justifications for flags or decisions. While our findings show an emerging emphasis on explainable AI (XAI) in fraud detection research, this is still a developing area. Overall, out of the 137 articles reviewed, very few (under 10%) substantially engage with regulatory or broader governance issues, and only a subset present in-depth discussions on ethical implications. There are, however, encouraging signs: a number of recent works do tackle model transparency and privacy-preserving techniques (e.g., Awosika et al., 2024 focus on XAI and federated learning for fraud detection), which directly respond to regulatory demands for accountability and customer expectations of privacy. These efforts need to be expanded. Future studies might benefit from interdisciplinary approaches that combine technical development with insights from legal studies, organizational behavior, and public policy. This would allow researchers to anticipate implementation barriers and build frameworks for accountable, auditable AI systems. To truly bridge the gap between research and practice, future studies should integrate considerations of compliance, ethics, and explainability into the development of AI models. Collaboration with legal and policy experts, as well as incorporating frameworks for accountable AI, will ensure that the next generation of fraud prevention tools is not only technologically robust but also trustworthy and aligned with real-world constraints.

Overall, the findings of this study affirm that AI-driven methodologies have become indispensable in the fight against financial fraud. They offer scalable, precise, and intelligent means to detect and prevent fraud in ways traditional methods could not achieve. The academic community has played a pivotal role in this progress, tackling various challenges (from algorithmic performance to data issues) and in turn equipping practitioners with better techniques. In practical terms, modern fraud prevention systems—powered by machine learning models, anomaly detection algorithms, and even early-stage AI like deep learning—are now core components of risk management in banks, credit card companies, and fintech services. As fraud tactics evolve, these AI systems also continue to learn and adapt, highlighting a key advantage of AI: the ability to improve over time as they process more data. The academic debate has thus evolved to not only explore novel algorithms but also to ensure those algorithms can be effectively deployed to safeguard financial transactions in the real world. This comprehensive understanding of AI's role, as mapped

out in this paper, provides valuable insights for developing next-generation fraud detection strategies that are both effective and practical.

Limitations

Like any study, ours has limitations that must be acknowledged. First, our literature search was conducted using three major databases (Scopus, Web of Science, and ScienceDirect); while these are comprehensive, relevant studies indexed elsewhere (e.g., IEEE Xplore or conference proceedings) might have been missed. This choice of databases, along with our inclusion criteria, could introduce a selection bias. Second, our review focused on publications in English—potentially overlooking significant research reported in other languages. This language bias means findings from non-English speaking regions (which might have substantial fraud and AI research, especially in local contexts) are underrepresented. Third, the timeframe of 2015–2025 captures the recent decade of research but may exclude important earlier foundational work on fraud detection. Fourth, bibliometric analysis inherently emphasizes publication metadata and citation trends, which may favor quantity and citation counts over deeper qualitative insights. As a result, some nuanced developments or industry efforts (including proprietary or unpublished innovations in financial institutions) are beyond the scope of our analysis. Finally, while we identified broad trends and gaps, we did not perform a full qualitative meta-analysis of implementation case studies—thus our conclusions about practical impact are drawn mainly from author discussions in the literature. These limitations suggest caution in generalizing the results. Future research could address these issues by expanding database scope, incorporating multi-language sources, and blending bibliometric analysis with case studies or expert interviews to enrich the understanding of how AI is deployed against fraud in practice.

Author Contributions: Conceptualization, L.M.; methodology, R.P.; software, R.P.; validation, L.M. and A.B.; formal analysis, L.M. and R.P.; investigation, R.P.; writing—original draft preparation, L.M.; writing—review and editing, A.B. and R.P.; visualization, L.M., A.B. and R.P.; supervision, L.M.; project administration, L.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Acknowledgments: The authors would like to express their appreciation to Beatriz Galino Soares. The original idea behind this article stems from her undergraduate thesis, which laid the foundation for the present study.

Conflicts of Interest: The authors declare no conflicts of interest.

References

Ahmed, S., Alshater, M. M., El Ammari, A., & Hammami, H. (2022). Artificial intelligence and machine learning in finance: A bibliometric review. *Research in International Business and Finance*, *61*, 101646. [CrossRef]

Almazroi, A. A., & Ayub, N. (2023). Online payment fraud detection model using machine learning techniques. *IEEE Access*, *11*, 137188–137203. [CrossRef]

Araújo, C. A. (2006). Bibliometria: Evolução histórica e questões atuais. *Em Questão*, *12*(1), 11–32.

Aria, M., & Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Infometrics*, *11*(4), 959–975. [CrossRef]

Awosika, T., Shukla, R. M., & Pranggono, B. (2024). Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection. *IEEE Access*, *12*, 64551–64560. [CrossRef]

Baabdullah, T., Alzahrani, A., Rawat, D. B., & 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*, 196. [CrossRef]

Baghdadi, P., Korukoglu, S., Bilici, M. A., & Onan, A. (2025). The potential of energy-based RBM and xLSTM for real-time predictive analytics in credit card fraud detection. *Journal of Data Analysis and Information Processing*, *13*(1), 79–100. [CrossRef]

Belanche, D., Belk, R. W., Casaló, L. V., & Flavián, C. (2024). The dark side of artificial intelligence in services. *The Service Industries Journal*, *44*(3–4), 149–172. [CrossRef]

Biswas, B., Mukhopadhyay, A., Kumar, A., & Delen, D. (2024). A hybrid framework using explainable AI (XAI) in cyber-risk management for defence and recovery against phishing attacks. *Decision Support Systems*, *177*, 114102. [CrossRef]

Błaszczyński, J., De Almeida Filho, A. T., Matuszyk, A., Szeląg, M., & Słowiński, R. (2021). Auto loan fraud detection using dominance-based rough set approach versus machine learning methods. *Expert Systems with Applications*, *163*, 113740. [CrossRef]

Bou Reslan, F., & Jabbour Al Maalouf, N. (2024). Assessing the transformative impact of AI adoption on efficiency, fraud detection, and skill dynamics in accounting practices. *Journal of Risk and Financial Management*, *17*(12), 577. [CrossRef]

Bradford, S. (1985). Specific subjects. *Journal of Information Science*, *10*(4), 173–180.

Chadegani, A. A., Salehi, H., Yunus, M. M., Farhadi, H., Fooladi, M., Farhadi, M., & Ebrahim, N. A. (2013). A comparison between two main academic literature collections: Web of Science and Scopus databases. *Asian Social Science*, *9*(5), 18–26. [CrossRef]

Chen, Y., Zhao, C., Xu, Y., & Nie, C. (2025). Year-over-year developments in financial fraud detection via deep learning: A systematic literature review. *arXiv*, arXiv:2502.00201.

Chhatwani, M. (2022). Does robo-advisory increase retirement worry? A causal explanation. *Managerial Finance*, *48*, 611–628. [CrossRef]

Choi, D., & Lee, K. (2018). An artificial intelligence approach to financial fraud detection under IoT environment: A survey and implementation. *Security and Communication Networks*, *2018*(1), 5483472. [CrossRef]

Chueke, G. V., & Amatucci, M. (2015). O que é bibliometria? Uma introdução ao fórum. *Internext*, *10*(2), 1–5. [CrossRef]

Cummings, M. (2021). Rethinking the maturity of artificial intelligence in safety-critical settings. *AI Magazine*, *42*(1), 6–15. [CrossRef]

Dasari, S., & Kaluri, R. (2024). An effective classification of DDoS attacks in a distributed network by adopting hierarchical machine learning and hyperparameters optimization techniques. *IEEE Access*, *12*, 10834–10845. [CrossRef]

Deng, T., Bi, S., & Xiao, J. (2025). Transformer-based financial fraud detection with cloud-optimized real-time streaming. *arXiv*, arXiv:2501.19267.

Duan, W., Hu, N., & Xue, F. (2024). The information content of financial statement fraud risk: An ensemble learning approach. *Decision Support Systems*, *182*, 114231. [CrossRef]

Gerhardt, T. E., & Silveira, D. T. (2009). *Métodos de pesquisa*. Plageder.

Goodell, J. W., Kumar, S., Lim, W. M., & Pattnaik, D. (2021). Artificial intelligence and machine learning in finance: Identifying foundations, themes, and research clusters from bibliometric analysis. *Journal of Behavioral and Experimental Finance*, *32*, 100577. [CrossRef]

Gupta, S., & Mehta, S. K. (2024). Feature selection for dimension reduction of financial data for detection of financial statement frauds in context to indian companies. *Global Business Review*, *25*, 323–348. [CrossRef]

Hajek, P., & Henriques, R. (2017). Mining corporate annual reports for intelligent detection of financial statement fraud—A comparative study of machine learning methods. *Knowledge-Based Systems*, *128*, 139–152. [CrossRef]

Hamadou, I., Yumna, A., Hamadou, H., & Jallow, M. S. (2024). Unleashing the power of artificial intelligence in Islamic banking: A case study of Bank Syariah Indonesia (BSI). *Modern Finance*, *2*(1), 131–144. [CrossRef]

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: A review of anomaly detection techniques and recent advances. *Expert Systems with Applications*, *193*, 116429. [CrossRef]

Hsin, Y. Y., Dai, T. S., Ti, Y. W., Huang, M. C., Chiang, T. H., & Liu, L. C. (2022). Feature engineering and resampling strategies for fund transfer fraud with limited transaction data and a time-inhomogeneous modi operandi. *IEEE Access*, *10*, 86101–86116. [CrossRef]

Huang, L., Abrahams, A., & Ractham, P. (2022). Enhanced financial fraud detection using cost-sensitive cascade forest with missing value imputation. *Intelligent Systems in Accounting, Finance and Management*, *29*(3), 133–155. [CrossRef]

Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, *9*(1), 24. [CrossRef]

Innan, N., Marchisio, A., Bennai, M., & Shafique, M. (2024). QFNN-FFD: Quantum federated neural network for financial fraud detection. *arXiv*, arXiv:2404.02595.

Ismail, M. M., & Haq, M. A. (2024). Enhancing enterprise financial fraud detection using machine learning. *Engineering, Technology & Applied Science Research*, *14*(4), 14854–14861. [CrossRef]

Itoo, F., Mittal, M., & Singh, S. (2021). Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. *International Journal of Information Technology*, *13*(4), 1503–1511. [CrossRef]

Jagtiani, J., & John, K. (2018). Fintech: The impact on consumers and regulatory responses. *Journal of Economics and Business*, *100*, 1–6. [CrossRef]

Jeong, D. H., Jeong, B. K., & Ji, S. Y. (2024). Leveraging machine learning to analyze semantic user interactions in visual analytics. *Information*, *15*, 351. [CrossRef]

Jullum, M., Løland, A., Huseby, R. B., Ånonsen, G., & Lorentzen, J. (2020). Detecting money laundering transactions with machine learning. *Journal of Money Laundering Control*, *23*(1), 173–186. [CrossRef]

Khetani, V., Gandhi, Y., Bhattacharya, S., Ajani, S. N., & Limkar, S. (2023). Cross-domain analysis of ML and DL: Evaluating their impact in diverse domains. *International Journal of Intelligent Systems and Applications in Engineering*, *11*(7s), 253–262.

Kirkos, E., Spathis, C., & Manolopoulos, Y. (2007). Data mining techniques for the detection of fraudulent financial statements. *Expert Systems with Applications*, *32*(4), 995–1003. [CrossRef]

Krishna, V. R., & Boddu, S. (2023). Financial Fraud detection using improved artificial humming bird algorithm with modified extreme learning machine. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*, 5–14. [CrossRef]

Kumar, B. S., & Ravi, V. (2016). A survey of the applications of text mining in financial domain. *Knowledge-Based Systems*, *114*, 128–147. [CrossRef]

Kumar, N., Srivastava, J. D., & Bisht, H. (2019). Artificial intelligence in insurance sector. *Journal of the Gujarat Research Society*, *21*(7), 79–91.

Li, J., Guo, C., Lv, S., Xie, Q., & Zheng, X. (2024). Financial fraud detection for Chinese listed firms: Does managers' abnormal tone matter? *Emerging Markets Review*, *62*, 101170. [CrossRef]

Li, R., Liu, Z., Ma, Y., Yang, D., & Sun, S. (2023). Internet financial fraud detection based on graph learning. *IEEE Transactions on Computational Social Systems*, *10*(3), 1394–1401. [CrossRef]

Lin, H., Gao, S., Gotz, D., Du, F., He, J., & Cao, N. (2018). RCLens: Interactive rare category exploration and identification. *IEEE Transactions on Visualization and Computer Graphics*, *24*, 2223–2237. [CrossRef]

Liu, L., Tsai, W. T., Bhuiyan, M. Z. A., Peng, H., & Liu, M. (2022). Blockchain-enabled fraud discovery through abnormal smart contract detection on Ethereum. *Future Generation Computer Systems*, *128*, 158–166. [CrossRef]

Liu, W., Wang, Z., & Zhang, X. (2025). Research on financial fraud detection by integrating latent semantic features of annual report text with accounting indicators. *Journal of Accounting & Organizational Change*. [CrossRef]

Lotka, A. J. (1926). The frequency distribution of scientific productivity. *Journal of the Washington Academy of Sciences*, *16*(12), 317–323.

Lu, X., Wijayaratna, K., Huang, Y., & Qiu, A. (2022). AI-enabled opportunities and transformation challenges for SMEs in the post-pandemic era: A review and research agenda. *Frontiers in Public Health*, *10*, 885067. [CrossRef] [PubMed]

Masood, M., Nawaz, M., Malik, K. M., Javed, A., Irtaza, A., & Malik, H. (2023). Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward. *Applied Intelligence*, *53*(4), 3974–4026. [CrossRef]

Merigó, J. M., Pedrycz, W., Weber, R., & de la Sotta, C. (2018). Fifty years of Information Sciences: A bibliometric overview. *Information Sciences*, *432*, 245–268. [CrossRef]

Moher, D., Shamseer, L., Clarke, M., Ghersi, D., Liberati, A., Petticrew, M., Shekelle, P., & Stewart, L. A. (2015). Preferred reporting items for Systematic Review and Meta-Analysis Protocols (PRISMA-P) 2015: Elaboration and explanation. *Research Methods & Reporting*, *349*, g7647.

Mongeon, P., & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: A comparative analysis. *Scientometrics*, *106*, 213–228. [CrossRef]

Motie, S., & Raahemi, B. (2024). Financial fraud detection using graph neural networks: A systematic review. *Expert Systems with Applications*, *240*, 122156. [CrossRef]

Navarrete, C. B., Malverde, M. G. M., Lagos, P. S., & Mujica, A. D. B. (2018). A web-based systematic literature review management software. *SoftwareX*, *7*, 360–372. [CrossRef]

Newman, M. E., & Girvan, M. (2004). Finding and evaluating community structure in networks. *Physical Review E*, *69*(2), 026113. [CrossRef] [PubMed]

Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*(3), 559–569. [CrossRef]

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., Mcdonald, S., . . . Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *The British Medical Journal*, *372*(71), n71. [CrossRef] [PubMed]

Payer, R. C., Quelhas, O. L. G., & Bergiante, N. C. R. (2024). Framework to supporting monitoring the circular economy in the context of industry 5.0: A proposal considering circularity indicators, digital transformation, and Sustainability. *Journal of Cleaner Production*, *466*, 142850. [CrossRef]

Pranto, T. H., Hasib, K. T. A. M., Rahman, T., Haque, A. B., Islam, A. K. M. N., & Rahman, R. M. (2022). Blockchain and machine learning for fraud detection: A privacy-preserving and adaptive incentive based approach. *IEEE Access*, *10*, 87115–87134. [CrossRef]

Quevedo-Silva, F., Santos, E. B. A., Brandão, M. M., & Vils, L. (2016). Estudo bibliométrico: Orientações sobre sua aplicação. *Revista Brasileira de Marketing*, *15*(2), 246–262. [CrossRef]

Ranganatha, H. R., & Syed Mustafa, A. (2025). Enhancing fraud detection efficiency in mobile transactions through the integration of bidirectional 3d quasi-recurrent neural network and blockchain technologies. *Expert Systems with Applications*, *260*, 125179. [CrossRef]

Secinaro, S., Brescia, V., Calandra, D., & Biancone, P. (2020). Employing bibliometric analysis to identify suitable business models for electric cars. *Journal of Cleaner Production*, *264*, 121503. [CrossRef]

Sengupta, K., & Das, P. K. (2023). Detection of financial fraud: Comparisons of some tree-based machine learning approaches. *Journal of Data, Information and Management*, *5*(1), 23–37. [CrossRef]

Shi, F., & Zhao, C. (2023). Enhancing financial fraud detection with hierarchical graph attention networks: A study on integrating local and extensive structural information. *Finance Research Letters*, *58*, 104458. [CrossRef]

Tayeb, M., & El Kafhali, S. (2025). Combining autoencoders and deep learning for effective fraud detection in credit card transactions. *Operations Research Forum*, *6*, 8. [CrossRef]

Tudisco, A., Volpe, D., Ranieri, G., Curato, G., Ricossa, D., Graziano, M., & Corbelletto, D. (2024). Evaluating the computational advantages of the variational quantum circuit model in financial fraud detection. *IEEE Access*, *12*, 102918–102940. [CrossRef]

Usman, A. U., Abdullahi, S. B., Liping, Y., Alghofaily, B., Almasoud, A. S., & Rehman, A. (2024). Financial fraud detection using value-at-risk with machine learning in skewed data. *IEEE Access*, *12*, 64285–64299. [CrossRef]

Wang, L., Cheng, H., Zheng, Z., Yang, A., & Zhu, X. (2021). Ponzi scheme detection via oversampling-based long short-term memory for smart contracts. *Knowledge-Based Systems*, *228*, 107312. [CrossRef]

Wang, X. (2024). A study on financial early warning for technology companies incorporating big data and random forest algorithms. *International Journal of Grid and Utility Computing*, *15*(3–4), 343–351. [CrossRef]

Wang, Y., & Zhu, G. (2024). Construction of accounting fraud and its audit countermeasure model based on computer technology. *Journal of Information & Knowledge Management*, *23*(4), 2450042. [CrossRef]

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, *57*, 47–66. [CrossRef]

Xia, P., Zhu, X., Charles, V., Zhao, X., & Peng, M. (2024). A novel heuristic-based selective ensemble prediction method for digital financial fraud risk. *IEEE Transactions on Engineering Management*, *71*, 8002–8018. [CrossRef]

Zhang, Z., Ma, Y., & Hua, Y. (2022). Financial fraud identification based on stacking ensemble learning algorithm: Introducing MD&A text information. *Computational Intelligence and Neuroscience*, *2022*, 1–14. [CrossRef]

Zhang, Z., Wang, Z., & Cai, L. (2025). Predicting financial fraud in Chinese listed companies: An enterprise portrait and machine learning approach. *Pacific-Basin Finance Journal*, *90*, 102665. [CrossRef]

Zhao, D., Wang, Z., Schweizer-Gamborino, F., & Sornette, D. (2025). Polytope fraud theory. *International Review of Financial Analysis*, *97*, 103734. [CrossRef]

Zhao, X., Wu, Y., Lee, D. L., & Cui, W. (2019). iForest: Interpreting random forests via visual analytics. *IEEE Transactions on Visualization and Computer Graphics*, *25*, 407–416. [CrossRef]

Zheng, X., Li, J., Lu, M., & Wang, F.-Y. (2024). New paradigm for economic and financial research with generative AI: Impact and perspective. *IEEE Transactions on Computational Social System*, *11*, 3457–3467. [CrossRef]

Zhou, H., Sun, G., Fu, S., Fan, X., Jiang, W., Hu, S., & Li, L. (2020). A Distributed approach of big data mining for financial fraud detection in a supply chain. *Computers, Materials & Continua*, *64*, 1091–1105. [CrossRef]

Zhu, S., Wu, H., Ngai, E. W. T., Ren, J., He, D., Ma, T., & Li, Y. (2024). A financial fraud prediction framework based on stacking ensemble learning. *Systems*, *12*, 588. [CrossRef]