Vol. 16, No. 1 (2025), pp.118–131

CHITKARA UNIVERSITY

Journal of Technology Management for Growing Economies

Artificial Intelligence and Machine Learning for Financial Fraud Detection: A Bibliometric and Thematic Review Using SPAR-4-SLR

Priyanka Chugh[1] and Devansh Gupta[1*]

[1]*University School of Business, Chandigarh University, Mohali, Punjab, India.*

[*]guptadevansh125@gmail.com (corresponding author)

RESEARCH ARTICLE **Open Access**

ARTICLE INFORMATION

Received: October 06, 2025
Accepted: November 25, 2025
Published Online: December 26, 2025

Keywords:
Artificial intelligence, Machine learning, Anomaly detection, Fraud analytics, Financial fraud

DOI: 10.15415/jtmge/2025.161010

ABSTRACT

Purpose: The study aims to map and evaluate the intellectual, conceptual, and thematic evolution of research on Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL) in financial fraud detection. It seeks to uncover dominant knowledge structures, methodological shifts, and emerging frontiers that define the progression of this rapidly expanding domain.

Methods: A systematic bibliometric and thematic analysis was conducted on a corpus of 316 Scopus-indexed publications from 2020–2025. Using the SPAR-4-SLR protocol and the Biblioshiny (R-Bibliometrix) package, the study employed co-word analysis, thematic mapping, and conceptual structure modelling through Louvain clustering and fractional counting to identify key research patterns and trends.

Results: The analysis revealed four primary thematic clusters supervised deep learning models, unsupervised anomaly detection, AI-integrated real-time monitoring, and explainable fraud analytics. The field has evolved from rule-based and static models toward scalable, interpretable, and context-aware architectures such as graph neural networks and federated learning. Emerging studies emphasise explainability, compliance, and ethical deployment.

Implications: The findings guide researchers, practitioners, and regulators toward designing transparent, adaptive, and policy-aligned AI systems for financial fraud prevention and risk management.

Originality: This paper provides the first comprehensive, SPAR-4-SLR–driven bibliometric synthesis of AI and DL applications in financial fraud detection, integrating performance analysis with thematic and conceptual evolution to highlight future research pathways.

1. Introduction

The rapid increase in the use of technology to conduct business worldwide has drastically changed the way fraud is committed, how much fraud is committed, and how quickly fraud takes place; there has been an exponential increase in cyber-enabled financial crime and artificial intelligence (AI)-based frauds (Europol, 2023; UK Finance, 2023). Recent evidence across banking and fintech ecosystems shows that fraud typologies have evolved into more adaptive, networked, and cross-border forms, challenging traditional rule-based detection systems (Zhang & Chen, 2022; Chen *et al.*, 2021). As financial systems generate vast amounts of data, the implementation of AI and ML technology is becoming more than just an operational tool to protect the integrity of transactions; it has become necessary to generate digital trust (Huang *et al.*, 2023; Li *et al.*, 2023). Most modern fraud detection studies indicate that AI and ML techniques are essential to create contextual analysis models that are scalable, generate real-time analysis, and provide more accurate, adaptive, and predictive capabilities compared to traditional fraud detection systems (Wu *et al.*, 2020; Zheng *et al.*, 2018).

Against this backdrop of rapidly advancing detection technologies, it is important to contextualize the broader economic and organizational burden of fraud. Fraud, broadly defined as intentional deceptive acts to obtain an unauthorized benefit, is a common but costly problem—the Association of Certified Fraud Examiners (ACFE, 2020) estimates fraud costs organizations about 5% of their revenues each year. In 2016, card payment fraud was approximately €1.8 billion across the European Single Euro Payments Area, indicating fraud at scale and to the financial system (European Central Bank, 2018; Van Vlasselaer *et al.*,

2017). These losses are more than financial losses; they can undermine investor confidence, institutional viability, and the integrity of global financial markets.

In this context, artificial intelligence (AI) and machine learning (ML) have become key tools for detecting and preventing financial fraud. Unlike conventional rule-based approaches that fall short of adapting to new schemes, AI can learn from historical and real-time datasets, enabling dynamic adaptation to evolving fraud patterns (Ngai *et al.*, 2011; Chen *et al.*, 2021; Zhang & Chen, 2022; Chauhan *et al.*, 2023). Applications range from classifying suspicious credit card transactions (Pumsirirat & Yan, 2018), to detecting anomalies in accounting data (Schreyer *et al.*, 2017), to using natural language analysis of financial disclosures (Purda & Skillicorn, 2015). More recently, deep learning architectures, such as autoencoders and generative adversarial networks, have shown improved accuracy in classifying fraudulent versus legitimate behaviors (Fiore *et al.*, 2019; Zheng *et al.*, 2018). As a result of these breakthroughs, the field has shifted from reactive detection to predictive and proactive fraud analytics. Recent advances demonstrate the use of transformer-based architectures for sequential fraud signal modeling (Li *et al.*, 2023) and graph neural networks for relational transaction fraud (Wu *et al.*, 2020; Zhang & Jiang, 2023), marking a shift toward context-aware anomaly detection frameworks.

These technological developments parallel an evolving regulatory environment that increasingly mandates advanced analytical capabilities. The regulatory landscape and global compliance initiatives enhance the importance of AI-enabled fraud detection. International organizations, such as the Financial Action Task Force (FATF, 2018) and the Basel Committee on Banking Supervision, have encouraged financial institutions to enhance their surveillance systems with analytics/AI methods. National regulators, such as the Reserve Bank of India, equally call for more AI-enabled systems to deal with increasing incidents of cyber fraud and money laundering (Balani, 2019). Moreover, the United Nations' Sustainable Development Goals (SDG 16) identify AI as a tool to enhance governance by reducing financial crime and corruption (Canhoto, 2021). This alignment shows that AI and ML have strategic significance not just for building resilience for corporations but also for advancing transparency for broader societal goals and, hence, sustainable development.

Despite the advancement of the knowledge base, research in AI and fraud detection remains siloed. Earlier literature reviews such as Ngai *et al.* (2011) provided foundational taxonomies of data-mining-driven fraud detection. However, contemporary analyses highlight that these taxonomies no longer capture the emergence of transformer-based fraud analytics, GNN-driven relational modeling, adversarial robustness, and multimodal detection systems (Zhang & Chen, 2022; Roy *et al.*, 2022; Li *et al.*, 2023; Zhang & Jiang, 2023). Recent domain-specific syntheses remain narrow—for instance, AML-focused AI reviews (Canhoto, 2021), credit card fraud analytics (Roy *et al.*, 2022), and transformer-based financial statement fraud detection (Huang *et al.*, 2023)—yet an integrated bibliometric mapping across AI–ML–fraud domains is largely missing. Askew and Brown (2018) note an emphasis on algorithmic methods, whereas Papageorgiou *et al.* (2020) note the absence of behavioral aspects of fraud detection, such as managerial deception or linguistic indicators contained in disclosures. Thus, this provides evidence for a bibliometric map that draws lines among the intellectual history, themes, and areas of research in an interdisciplinary space.

Bibliometric analysis provides a systematic way to evaluate the knowledge base of a research domain. It supports performance evaluation—identifying high-performing authors, journals, and institutions—and science mapping, which identifies collaboration networks, co-citation relationships, and thematic clustering (Aria & Cuccurullo, 2017). Bibliometric analysis in general management and social sciences has become more prominent in synthesizing large bodies of literature (Donthu *et al.*, 2021). The SPAR-4-SLR protocol (Paul *et al.*, 2021) builds on this approach, providing a structured protocol to help researchers scope, plan, analyze, and report research in a transparent, replicable, and methodologically rigorous way. Finally, the SPAR-4-SLR protocol, supplemented with bibliographic tools like Biblioshiny, will support this paper in systematically synthesizing AI- or ML-based fraud detection literature.

In line with these gaps, the present study has two aims. First, it examines the impact and intellectual influence of worldwide scholarship on AI and ML as applied to financial fraud detection from 2000 to 2025. Second, it discusses conceptual structures and thematic maps, using keyword co-appearance, to examine both established areas (e.g., supervised learning, anomaly detection) and emerging domains (e.g., federated learning, graph neural networks, and large language models for forensic text analysis). By integrating scholarship from banking, insurance, and fintech ecosystems, this study not only records the historical trajectory but also maps future directions for scholarship about explainable, ethical, and hybrid frameworks for mechanisms that split algorithmic precision and human judgment.

The remainder of this article is organized as follows. Section 2 describes the SPAR-4-SLR-based methodology. Section 3 contains descriptive and science mapping results. Section 4 considers thematic structures and emerging research frontiers. Section 5 describes implications for academic, industry, and policy. Section 6 describes

limitations and future research directions, followed by concluding comments in Section 7. Through this synthesis, the study aims to provide a transparent and replicable evidence base for understanding the trajectory of AI- and ML-enabled financial fraud detection.

2. Methodology

2.1. SPAR-4-SLR Protocol

The research used the SPAR-4-SLR framework (Paul *et al.*, 2021) for systematic review. This framework gives a clear, systematic, and repeatable approach to conducting systematic reviews by dividing the overall process into three overarching processes: Assembling, Arranging, and Assessing. An overview of the workflow used in this research is summarised in the diagram in Figure 1.

2.1.1. Assembling

Assembling established the subject area of AI/ML applications in detecting financial fraud, and comprised defining three guiding research questions that focused on 1) the evolution of intellectual thought; 2) the structure of performance; and 3) emerging methodological frontiers. The search strategy included restricting the quality of the source type to Scopus-indexed journals and book chapters to ensure the highest quality and credibility of research material available.

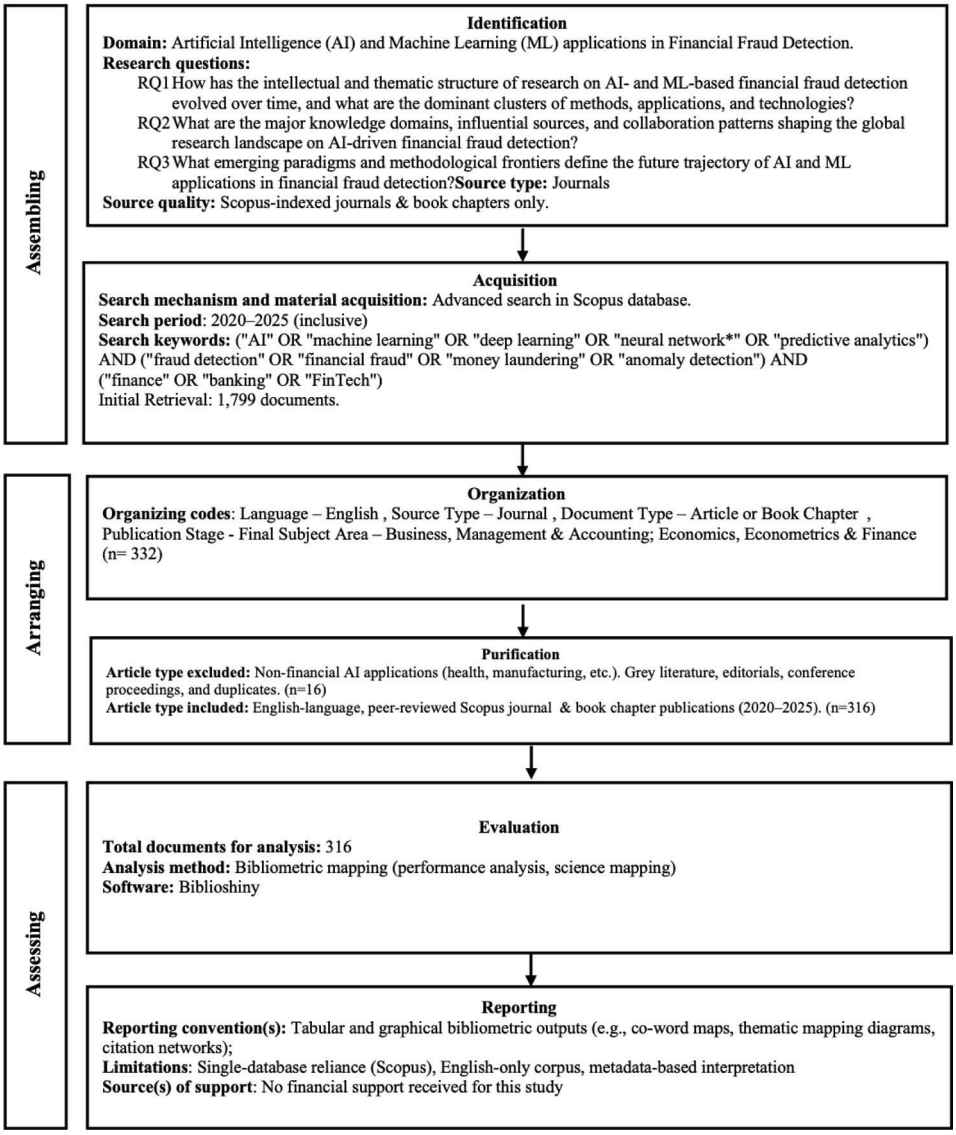

Figure 1: Data Collection Flow (Adapted from SPAR-4 SLR Protocol)

The search process was through an advanced Boolean search strategy executed in Scopus for the period from 2020–2025 using the following search terms:

> *"("AI" OR "machine learning" OR "deep learning" OR "neural network" OR "predictive analytics") AND ("fraud detection" OR "financial fraud" OR "money laundering" OR "anomaly detection") AND ("finance" OR "banking" OR "FinTech")"**

2.1.2. Arranging

Based on SPAR-4-SLR guidelines, the Arranging phase was organized and purified. The articles were organized according to the inclusion coding of English peer-reviewed journals or book chapters as well as final publications located within Business, Management and Accounting or Economics, Econometrics, and Finance. The purification process encompassed the removal of any AI-related item that did not relate to finance, such as healthcare and manufacturing, as well as editorials, conference papers, grey literature, and any duplicates. Through this screening process, 316 documents were determined to be eligible for analysis.

2.1.3. Assessing

During the Assessing phase, there were evaluations and reports produced. Bibliometric evaluations used Biblioshiny to do performance analyses (journals, authors, countries) and science mapping (co-word networks, thematic evolution, conceptual and intellectual structures) of a comprehensive literature pool. In conjunction with how the data was prepared for the Assessing phase, all documentation produced for collection and analysis adhered to the SPAR-4-SLR protocols of transparent methods and methodologies along with graphical representations of each paper in a scientometric context, recognising limitations associated with the data (e.g., single database, English-only).

2.2. Bibliometric Procedure

The bibliometric aspect of this research adheres to the innovative method set out by Zupic and Čater (2015), which proposes a structured approach to progress systematically through the process of designing a study, conducting data collection, employing bibliometric methods for analysis, followed by the visualization and interpretation phase. This four-stage trajectory—design, data collection, bibliometric analysis, and visualization of the areas of knowledge—has become the methodological approach to bibliometric literature and analysis, particularly in management, finance, and information systems. Other researchers also built on this process to include approaches such as Bibliometrix (Aria & Cuccurullo, 2017) and to facilitate systematic review processes across disciplines (Donthu *et al.*, 2021). The sequence is presented in Figure 2.

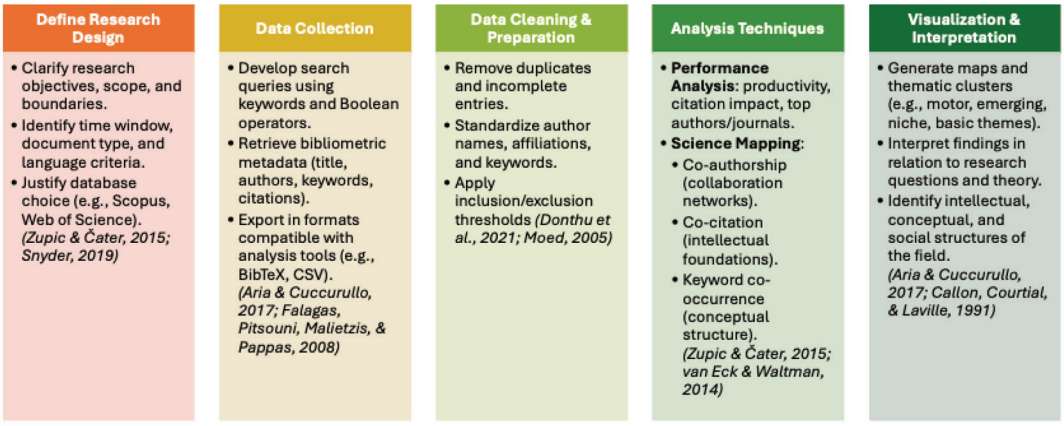

Figure 2: Procedure for Bibliometric Analysis

3. Results & Findings

3.1. Descriptive Performance Analysis

3.1.1. Annual Publication Growth

Figure 3 depicts the yearly publication output on AI- and ML-assisted financial fraud detection from 2020–2025. The area revealed strong growth—from just 16 releases in 2020 to a peak of 107 in 2024—before falling back to 55 in 2025. This growth pattern is indicative of Price's (1963) exponential growth phase of scientific disciplines, characterized by rapid consolidation in nascent areas of research. The decline in 2025 is possibly due to indexing delays that are common in bibliometric datasets (Donthu *et al.*, 2021).

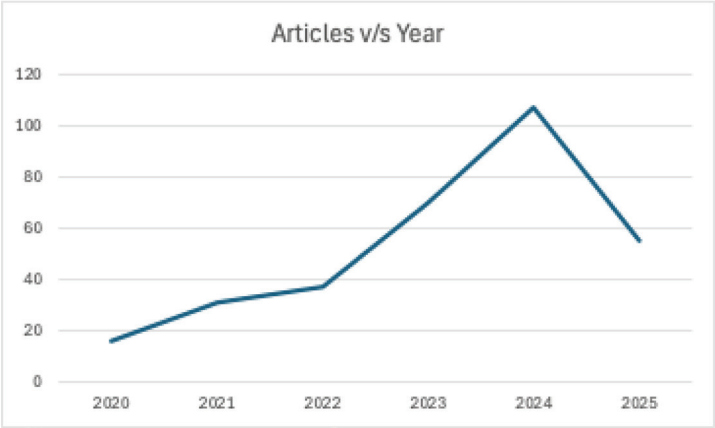

Figure 3: Annual Scientific Production

The shape of the curve coincides with the widespread expansion of digital transactions after the pandemic that increased fraud risk (Europol, 2021), and the growing influx of AI into the finance and accounting academic dialogue (Abbasi *et al.*, 2012). The trajectory also suggests an overall leap from an isolated area of specialty practice towards the more common area of interdisciplinary study in AI-based fraud detection that is within the framework of bibliometric scattering norms (Egghe, 2005).

3.1.2. Most Relevant Sources

Figure 4 indicates the distribution of the most active sources of publications on AI and ML in financial fraud detection. The Journal of Money Laundering Control topped the list (14 articles), followed by Knowledge-Based Systems (12), and Finance Research Letters (7). The Journal of Financial Crime (7) and the Journal of Risk and Financial Management (7) are also specialized publications that augment this interdisciplinary field at the crossroads of criminology, finance, and information systems, as opposed to other less relevant outlets.

This distribution is consistent with Bradford's Law of Scattering (Bradford, 1934), where a smaller number of "core journals" publish a higher share of the articles, whilst distribution at the remaining periphery decreases. The strong representation of *Decision Support Systems* (6) and *Knowledge-Based Systems* (12) demonstrates the significance of AI paradigms, while the appearance of applied books such as *The AI Book* and *Generative Artificial Intelligence in Finance* indicates the growing dialogue between academics and practitioners (Chauhan, Kaur, & Gupta, 2023).

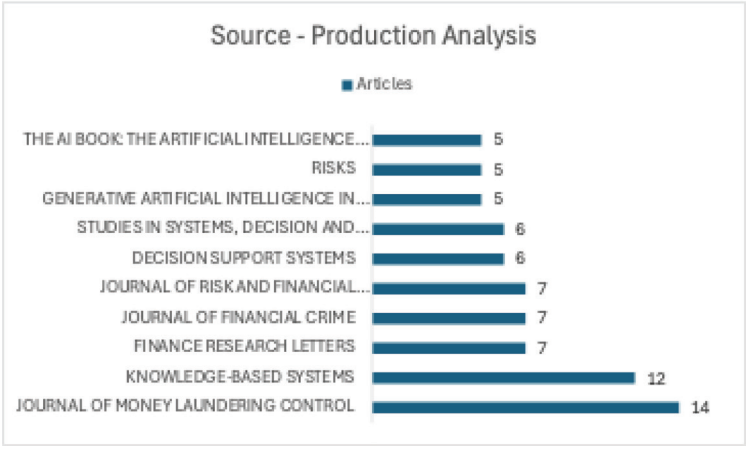

Figure 4: Source Production Analysis

Bibliometric developments suggest that the fraud detection study has transformed into a hybrid knowledge domain: legal and compliance journals focus on anti-money laundering (e.g., JMLC) while computer science outlets explore algorithmic architectures (e.g., KBS, DSS). Such disciplinary cross-pollination resonates with previous bibliometric examinations in fraud analytics (Ngai *et al.*, 2011) and indicates the shift of fraud detection from a small criminological niche to the more interdisciplinary mainstream (Donthu *et al.*, 2021).

3.1.3. Source Impact Indicators

Table 1 provides an overview of the bibliometric impact of the top journals. The *Journal of Money Laundering Control* (h = 8, TC = 247) is designated as the premier outlet in this field due to its affiliation with the compliance and regulatory aspect of AI capability in fraud detection. *Knowledge-Based Systems* (h = 6, TC = 443) has the greatest citation impact, correlating with its established reputation in the domain of intelligent systems (Aria & Cuccurullo, 2017).

Table 1: Source Impact Indicators of Top 10 Sources in Corpus (Source – Biblioshiny)

Source	h-index	g-index	m-index	TC	NP	PY_start
Journal of Money Laundering Control	8	14	1.333	247	14	2020
Knowledge-Based Systems	6	12	1	443	12	2020
Decision Support Systems	5	6	0.833	296	6	2020
Finance Research Letters	5	7	1.25	75	7	2022
Journal of Financial Crime	5	7	1.667	113	7	2023
Artificial Intelligence and Machine Learning in Business Management: Concepts, Challenges, and Case Studies	3	3	0.6	12	3	2021
Computational Economics	3	4	0.6	19	4	2021
Latin American Journal of Central Banking	3	4	0.5	26	4	2020
Research in International Business and Finance	3	4	0.75	277	4	2022
Risks	3	5	0.6	48	5	2021

3.1.4. Journal Impact Discussion

The h-index and g-index of the research article above *Decision Support Systems* (h = 5, g = 6; TC = 296) also support its essential nature on decision-analytic and anomaly-detection techniques. With the *Journal of Financial Crime* boasting a current m-index of 1.667, which further demonstrates its quick accumulation of citations from its initial 2023 AI–ML fraud publications, this indicates a greater interest and growth of scholarly research efforts in this area despite its new publication position.

Smaller but emergent contributions are also apparent in *Research in International Business and Finance* (h = 3, TC = 277) and *Risks* (h = 3, TC = 48), indicating there is some diffusion across disciplines into finance and risk management. This distribution appears consistent with evidence from bibliometric charts that indicate for core journals, balance productivity with impact, whereas peripheral journals tend to play a breadth function (Bradford, 1934; Zupic & Čater, 2015).

Overall, the results show the journal structure has two components: journals focused on regulatory and compliance components (e.g., JMLC, JFC), and journals focused on computer science and decision-making support (e.g., KBS, DSS), which forms the core methodological journals.

3.1.5. Country-Level Production Over Time

Figure 5 conveys the distribution over time of country-level contributions to research on AI–ML detection of financial fraud—from 2020 to 2025. The largest rise is in India, which increased from 4 to 243 in 2025, outpacing the other countries in terms of outputs. India's rise relates to government-backed programs promoting digital finance (e.g., the UPI and Aadhaar ecosystem) and academic attention to fintech inclusion (Balani, 2018; Canhoto, 2021).

China is close behind, rising from 1 to 175 articles in 2025, also indicative of significant investments The US and UK appear to show steady increases at a more modest pace, with 56 and 43 articles, respectively, consistent with a mature but regulated financial system (FATF, 2018). Even though Ukraine produces fewer articles overall, its consistency in output could be assumed to relate to the emphasis on cyber-resilience and fraud prevention since the beginning of the Russian invasion in 2022, identified as a gap in the literature (IMF, 2023).

This distribution aligns with longitudinal bibliometric evidence showing that emerging economies dominate high-growth periods in applied AI, while established countries contribute at more tempered and consistent levels of increasing contributions (Donthu *et al.*, 2021). In addition, geographic diffusion of outputs supports emergent patterns of use in digital finance and regulatory innovation and places India and China as crucial nexus points for understanding trajectories in AI–ML research outputs.

3.2. Scientific Mapping of Literature

3.2.1. Keyword Cloud

The word cloud (Figure 6) shows the most common terms identified in fraud detection research utilizing AI–ML

techniques. The prominence of *anomaly detection* (n = 27) reinforces its positioning as the methodological pillar of identifying anomalous patterns in financial data; this is consistent with previous reviews which placed anomaly-based methods at the heart of fraud analytics. The next most common item, *crime* (n = 22), reflects the criminological framing of financial wrongdoing, while *deep learning* (n = 16) usage reinforces the implementation of neural architectures for the purpose of extracting features and classifying (Zheng *et al.*, 2018).

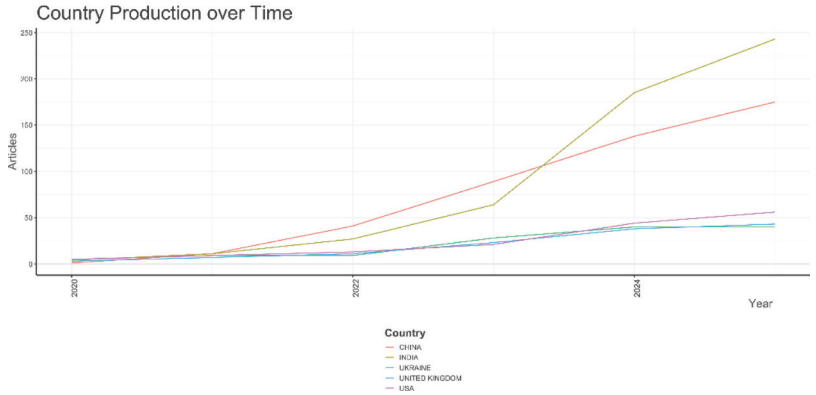

Figure 5: Country-Level Production Over Time (Source – Biblioshiny)

Terms such as *machine learning* and *machine learning* (combined, n = 25), *fraud detection* (n = 9), *risk assessment* (n = 9), and *learning systems* (n = 9) reflect the method–application nexus where predictive analytic methods are being conceived and implemented for more specific fraud contexts within financial resources. The prevalence of *graph neural networks* (n = 6), *adversarial machine learning* (n = 7), and *long short-term memory* (n = 5) mark a frontier of advanced architectures being developed to confer greater robustness towards adaptability in the combat of fraud strategies (Goodfellow, Shlens, & Szegedy, 2015; Fiore, Santis, Perla, Zanetti, & Palmieri, 2019).

To summarise, the word cloud depicts a corpus of a field of inquiry that is firmly rooted in supervised anomaly detection but is expeditiously developing in directions of deep learning, adversarial robustness, and fintech orientations such as blockchain and decentralized finance (Xu *et al.*, 2019).

Figure 6: Keyword Cloud (Source – Biblioshiny)

3.2.2. Trend Topic Analysis

Figure 7 illustrates how topical emphases vary in AI–ML empirics of fraud detection research over the period of 2022 to 2025. The initial period of the analysis shows clustering of topics around learning algorithms (median year = 2022) and domain-level terms, including *crime* (median year = 2023) and *finance* (median year = 2023), which reflect the early-stage attempts to apply machine learning broadly to emergent financial misconduct (Ngai *et al.*, 2011; Phua *et al.*, 2010).

In the years 2023 and beyond, modal specificity increases around methodology. Terms of *machine learning* (median year = 2023) and *anomaly detection* (Q1 year = 2023; median year = 2024) are evident and consistent with the bibliometric analysis of the use of anomaly detection as the foundation of fraud analytics (Abbasi *et al.*, 2012). The use of *deep learning* (median year = 2024) and machine learning variants is now visible, indicating that neural architectures are beginning to be integrated into mainstream fraud detection pipelines (Zheng *et al.*, 2018).

Emerging topics are also visible in 2024 and 2025, marked by the emergence of *graph neural networks* (Q1 year = 2024; median year = 2025), where the move towards graph-based fraud detection is now on the leading edge, especially in transaction networks (Wu *et al.*, 2020). This evolution highlights a field that has migrated from general algorithmic discourse to higher-order domain-specific architectures, which is reflected in consideration of the "emerging theme" quadrants in thematic evolution mapping (Aria & Cuccurullo, 2017).

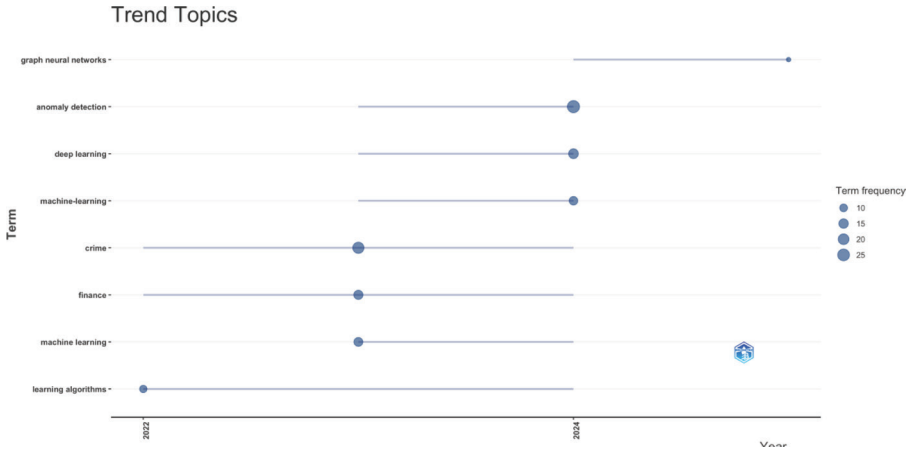

Figure 7: Trend Topic Analysis (Source – Biblioshiny)

3.2.3 Thematic Mapping

The Thematic Map as displayed in Figure 8 can be interpreted as follows:

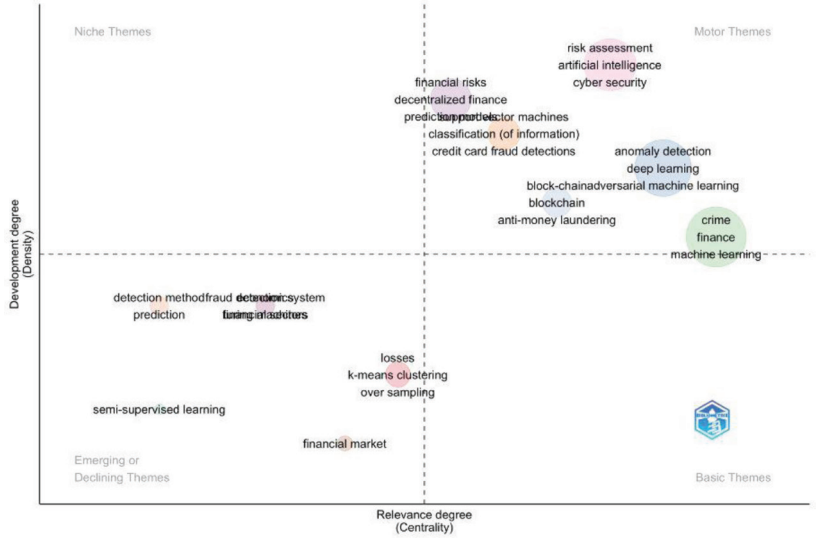

Figure 8: Thematic Map (Source – Biblioshiny)

Table 2: Thematic Map Interpretation

Cluster	Thematic Position (Callon Centrality × Density)	Interpretation & Meaning	Representative Keywords	Key References
Crime	High centrality & high density (motor theme)	Anchors the field by connecting criminological constructs with machine learning. Strong integration across finance, fraud detection, and predictive analytics.	Crime, finance, machine learning, learning algorithms, fraud detection, financial fraud	Ngai *et al.* (2011); Phua *et al.* (2010)
Anomaly Detection	High centrality & strong density (motor theme)	Core methodological theme; anomaly detection serves as backbone for fraud analytics, now enriched by deep learning, GNNs, adversarial ML.	Anomaly detection, deep learning, adversarial ML, graph neural networks, LSTMs, intrusion detection	Abbasi *et al.* (2012); Zheng *et al.* (2018); Fiore *et al.* (2019)
Risk Assessment	High density, high centrality (motor theme)	Applied focus on fraud risk, financial statement frauds, investments, and cybersecurity; bridges AI methods with financial governance.	Risk assessment, risk management, fraud prevention, NLP systems, investments, systematic reviews	Perols (2011); Canhoto (2021)
Support Vector Machines	Moderate centrality, high density (niche theme)	Specialized algorithmic approaches for classification and credit card fraud; impactful in early literature but gradually displaced by deep learning.	SVMs, decision trees, SMOTE, classification	Phua *et al.* (2010); Ngai *et al.* (2011)
Financial Risks	Moderate density, low centrality (niche theme)	Focused sub-stream linking AI/ML to risk prediction and decentralized finance. Frontier methods such as federated learning and CNNs emerging.	Financial risks, risk predictions, federated learning, DeFi	Xu *et al.* (2019); Wu *et al.* (2020)
Blockchain	Moderate centrality & density (emerging theme)	Highlights distributed ledger integration for AML and fraud detection; still peripheral but gaining traction.	Blockchain, anti-money laundering, laundering, fraud detection system	Chen *et al.* (2021); Xu *et al.* (2019)
Losses	Low centrality & moderate density (basic theme)	Examines cost quantification and financial impacts of fraud; often linked to oversampling/class imbalance and clustering methods.	Losses, k-means clustering, over-sampling	ACFE (2020); Bolton & Hand (2002)
Financial Market / Economics	Low centrality & density (peripheral/ declining themes)	Economic and market-wide studies on fraud remain marginal compared to technical AI-focused clusters.	Economics, financial sectors, financial market	Sengupta (1992); Moed (2005)
Semi-Supervised Learning / Detection Methods	Very low centrality & density (emerging/isolated themes)	Indicative of nascent experimentation with semi-supervised ML and hybrid detection models; potential frontier.	Semi-supervised learning, prediction, detection methods	Van Vlasselaer *et al.* (2017); Wu *et al.* (2020)

3.2.4. Factorial Mapping

The factorial map (Figure 9) indicates that co-occurring keywords are projected into a two-dimensional space, which can provide an understanding of the intellectual structure of AI–ML fraud detection research. With respect to Dim1 (horizontal axis), the keywords on the left side, for example, *anomaly detection*, *deep learning*, *graph neural networks*, *adversarial machine learning*, and *contrastive learning*, can be associated with advanced technical methods, which represent algorithm-driven innovations related to unsupervised and representation learning for fraud and deception analytics (Zheng *et al.*, 2018; Wu *et al.*, 2020).

In contrast, the keywords on the right represent more application-centric terms, for example, *fraud detection*, *financial system*, *financial statement frauds*, which are more directly associated with use cases in the financial sector (Ngai *et al.*, 2011; Perols, 2011).

On Dim2 (vertical axis), the upper half of the space roughly corresponds with language associated with the general discourse of machine learning (machine learning, neural networks, random forests, support vector machines), representing classification approaches that are traditional and widely used for classification tasks (Phua *et al.*, 2010).

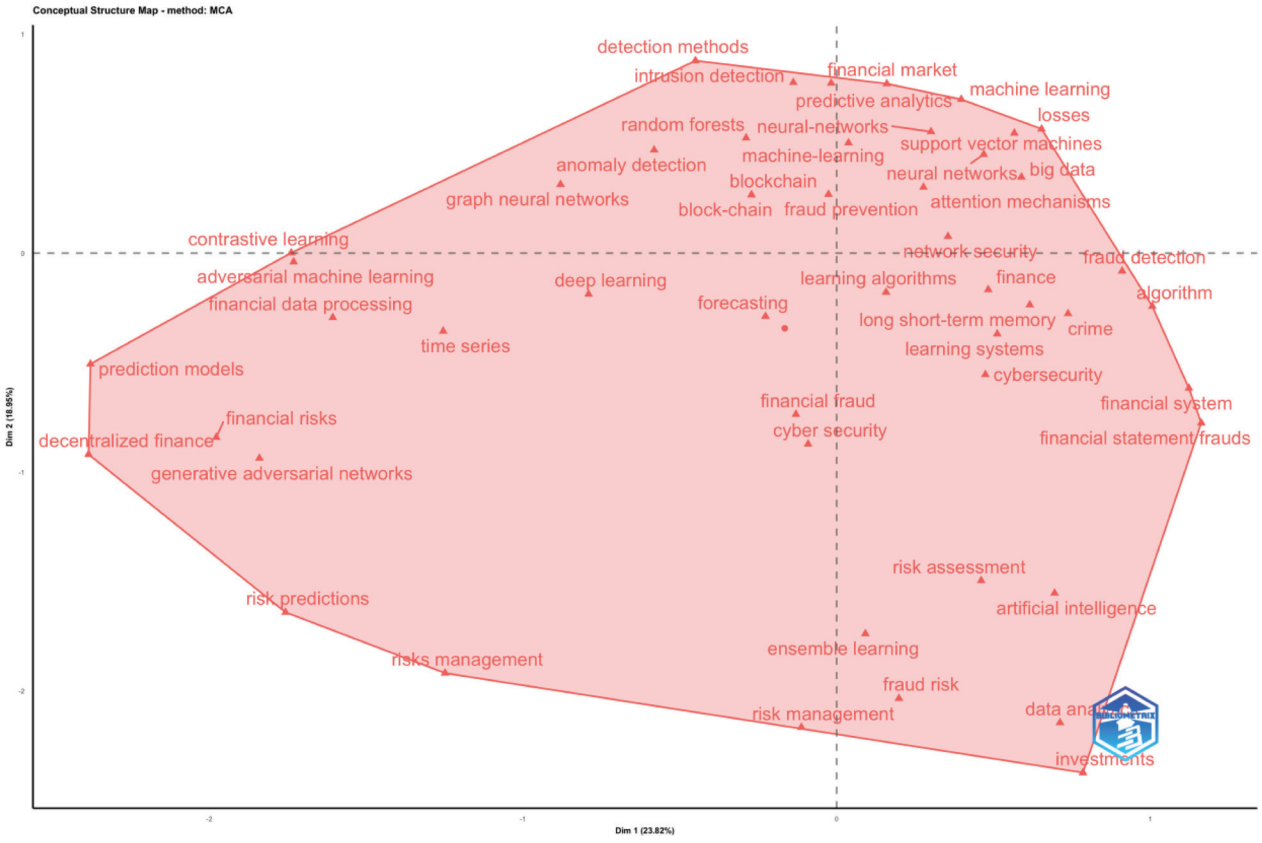

Figure 9: Factorial Map (Source – Biblioshiny)

The lower half contains terms associated with risk and governance (risk assessment, fraud risk, risk management, and investments), signaling broadening into financial risk and governance decision-making frameworks (Abbasi *et al.*, 2012; Canhoto, 2021). Peripheral terms such as *blockchain*, *decentralized finance*, and *generative adversarial networks* occupy the periphery, pointing to emerging but not yet well-integrated research.

Data analytics and risk predictions appear in the lower-left quadrant, highlighting hybrid approaches that combine traditional statistical risk predictions with ML-enhanced anomaly detection. Overall, the factorial map provides a conceptual spectrum: method-oriented innovation (left) → financial innovation (right), and general ML algorithms (top) → risk and governance integration (bottom). This pattern mirrors the thematic mapping: anomaly detection and crime are motor themes, whereas blockchain and DeFi occupy emerging peripheral positions.

4. Discussion

According to this bibliometric review, the field has reached an advanced stage of development due primarily to technological advancements, regulatory needs, and increased risk associated with digitally enabled fraud. The spike in publication volume after 2020 mirrors global trends towards digitalization, coupled with rising financial crimes conducted online (Europol, 2023; UK Finance, 2023).

The increase also suggests that AI-based fraud detection systems have progressed beyond experimental applications and are increasingly implemented in financial services operations (Chen *et al.*, 2021; Zhang & Chen, 2022).

Country-level trends reveal China and India as major contributors to global output, consistent with larger scientometric analyses showing leadership in AI development. The US and UK maintain strong contributions, reflecting global reach and influence on public policy in fraud analytics. Source impact metrics identify Knowledge-Based Systems, Decision Support Systems, and the Journal of Money Laundering Control as central journals bridging computer science, finance, and risk management.

Core research focuses on anomaly detection, supervised machine learning, and deep neural networks. With the emergence of graph neural networks, adversarial learning, attention mechanisms, and transformer models, there is a clear shift from feature engineering to representation

learning. Thematic evolution moves beyond traditional fraud types (credit card fraud, AML detection, financial statement inconsistencies) towards decentralized finance risks, cyber intrusions, and multimodal fraud behavior.

The pattern indicates development of hybrid, context-aware, and explainable AI systems to tackle complex fraud types. These findings reinforce prior work on intellectual clustering and frontier research in AI-enabled fraud alerts and analyses, offering a comprehensive framework for technological and legislative development in AI-enabled fraud analysis.

4.1. Implications

The bibliometric study presents implications across academic, managerial, policy, and methodological contexts, showing a shift from isolated algorithm development to integrated, data-intelligent systems fostering financial integrity.

4.1.1. Academic Implications

Intellectual and conceptual mapping highlights the emphasis on algorithmic perspectives—anomaly detection, deep learning, and neural network frameworks—while behavioral and organizational dimensions of fraud are relatively underexplored. Future research should integrate behavioral finance and criminology insights into AI-driven models to better understand the drivers of fraudulent activity (Ngai *et al.*, 2011; Morales *et al.*, 2019).

Emerging themes such as adversarial machine learning and graph neural networks signal the need for cross-disciplinary integration of computer science, finance, and regulatory studies (Wu *et al.*, 2020), providing a more holistic understanding of fraud ecosystems and preventing over-reliance on purely technical approaches (Abbasi *et al.*, 2012).

4.1.2. Managerial Implications

For banking, insurance, and fintech professionals, deep learning and ensemble models improve detection accuracy but lack interpretability (Goodfellow *et al.*, 2015), creating tensions between efficiency and explainability. Managers should adopt hybrid approaches integrating interpretable ML models (decision trees, rules-based systems) with high-performing black-box models to improve detection and stakeholder trust (Doshi-Velez & Kim, 2017).

The emergence of risk assessment and fraud detection clusters underscores the need for proactive monitoring systems embedded in core business processes rather than after-the-fact anomaly checks (Perols, 2011). Graph-based fraud detection can also provide fintech innovators with competitive advantages and richer transaction network insights.

4.1.3. Policy Implications

Emerging clusters around blockchain and decentralized finance indicate regulatory gaps. As digital assets proliferate, agencies such as FATF and the Basel Committee face increased pressure to enforce AML and KYC compliance (Xu *et al.*, 2019). Policy frameworks should mandate AI-based monitoring while ensuring model interpretability, accountability, and ethical customer data usage (Brkan & Bonnet, 2020).

Cross-border collaboration is essential, as digital fraud schemes are global. Findings provide evidence for regulators to benchmark research-driven tools and recognize emerging fraud typologies.

4.1.4. Methodological Implications

This study demonstrates the value of systematic transparency and replicability using the SPAR-4-SLR protocol (Paul *et al.*, 2021). Performance analysis, science mapping, and thematic mapping reveal structural and evolutionary patterns, moving beyond descriptive statistics to show "how" the field develops.

Future research can expand methodological rigor via full-text text mining, application of antecedents-decisions-outcomes (ADO) frameworks, or cross-sector comparative mapping to enhance methodological pluralism in fraud analytics research.

5. Limitations and Future Research Directions

Although this study offers the initial SPAR-4-SLR–based bibliometric synthesis of AI and ML applications in the detection of financial fraud, certain limitations must be recognized. First, although comprehensive, the analysis is restricted to publications listed in Scopus, which may result in relevant studies assessed in Web of Science, IEEE Xplore, or specific repositories not being included. The potential bias of using a single database in bibliometric analysis is prevalent and could impact the generalizability of results (Donthu *et al.*, 2021). Second, while most of our search strings related at least somewhat to fraud in connection with AI/ML technologies, some adjacent research areas (like cyber forensics, forensic accounting, or fraud analytics based on behavioral psychology) may be omitted due to the nature of the search strings. Third, bibliometric mapping only includes metadata on the report (title, abstract, keywords, citation, etc.), and the methodology, performance of models, and complete description of applications of AI systems in context are beyond the bibliometric mapping process. As

Moed (2005) states, while bibliometrics reveal structural trends, they cannot replace comprehensive qualitative approaches or algorithm-based benchmarking.

The following three directions should extend this work in future research. First, the integration of multiple databases (Scopus, WoS, IEEE) would mitigate database bias and could create a broader evidence base for existing knowledge (Aria & Cuccurullo, 2017). Second, text-mining and natural language processing (NLP) of the full text has the potential to enrich understanding by extracting hidden themes that were never identified by the author in keywords. Third, researchers could draw upon hybrid frameworks like ADO (antecedents–decisions–outcomes) to agglomerate conceptual relationships to collectively design integrative theory in terms of fraud detection (Paul & Rosado-Serrano, 2019). Comparative bibliometric studies between banking, insurance, and fintech could also pinpoint differences, contextualized by sector, with engagement to AI tools developed/adopted. Lastly, integrating ethics (i.e., explainability, fairness, and accountability) into bibliometric mapping can help show how academia is responding to ethical risks of questions that appear opaque to society as a consequence of the adoption of AI methodology for fraud detection (Brkan & Bonnet, 2020).

Addressing these angles could enhance future scholarship towards a richer understanding related to the theoretical, technical, and policy implications of AI and fraud detection.

6. Conclusion

This research offered a systematic bibliometric and thematic review of the literature on the use of artificial intelligence and machine learning in financial fraud detection with the SPAR-4-SLR protocol. The analysis shows a notable increase in publications since 2020, with China, India, and the USA serving as leading contributors. The intellectual landscape is dominated by motor themes related to anomaly detection, crime, and risk assessment, while emerging themes related to graph neural networks, adversarial learning, blockchain, and decentralized finance provide suggestions for future research pathways. The review offers a strong methodological emphasis on anomaly-based and deep learning-based techniques yet examines emerging themes from behavioral and governance perspectives that have been less fully theorized and researched. Overall, by mapping the intellectual, conceptual, and thematic structures, this review integrates existing scholarship and provides a research agenda for academics, practitioners, and policymakers to build on the evolving frontier of fraud detection, particularly related to the application of AI technology.

Acknowledgement

The authors declare that there are no acknowledgements for this research paper.

Authorship Contribution

All authors made equal contributions to the conception, analysis, and writing of this manuscript.

Funding

The author received no external funding to conduct this study.

Declaration

The author hereby declares that this research paper is an original work conducted by the author. All sources and references have been properly acknowledged, and the work has not been submitted or published elsewhere.

Conflict of Interest

The author declares that they have no conflict of interest regarding the publication of this paper.

References

Abbasi, A., Albrecht, C., Vance, A., & Hansen, J. (2012). Metafraud: A meta-learning framework for detecting financial fraud. *MIS Quarterly, 36*(4), 1293–1327.

ACFE. (2020). *Report to the Nations: Global Study on Occupational Fraud and Abuse.* Association of Certified Fraud Examiners.

Aria, M., & Cuccurullo, C. (2017). Bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics, 11*(4), 959–975. https://doi.org/10.1016/j.joi.2017.08.007

Balani, H. (2019). Assessing the introduction of Anti-Money Laundering regulations on bank stock valuation: An empirical analysis. *Journal of Money Laundering Control, 22*(1), 76–88. https://doi.org/10.1108/JMLC-03-2018-0021

Brkan, M., & Bonnet, G. (2020). Artificial intelligence and the GDPR: Towards trustworthy AI. *European Journal of Law and Technology, 11*(1), 1–35.

Callon, M., Courtial, J. P., & Laville, F. (1991). Co-word analysis as a tool for describing the network of interactions between basic and technological research: The case of polymer chemistry. *Scientometrics, 22*(1), 155–205. https://doi.org/10.1007/BF02019280

Canhoto, A. (2021). The persistent challenges of AML: A review of AI-based solutions. *Journal of Money Laundering Control, 24*(4), 765–781.

Canhoto, A. I. (2021). Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective. *Journal of Business Research, 131*, 441–452. https://doi.org/10.1016/j.jbusres.2020.10.054

Chauhan, A., Kaur, P., & Gupta, M. (2023). AI-driven financial fraud detection: Advances and challenges. *Decision Support Systems, 170*, 113882.

Chauhan, V., Kaur, P., & Gupta, A. (2023). Artificial intelligence in financial services: Opportunities, challenges, and future research directions. *Journal of Financial Services Marketing, 28*(2), 131–144.

Chen, H., Zhang, Y., & Xiang, Y. (2021). Machine learning-based financial fraud detection: A survey. *Expert Systems with Applications, 169*, 114418.

Chen, X., Zhang, Z., & Xu, J. (2021). Artificial intelligence in finance: Applications, challenges, and future directions. *Technological Forecasting and Social Change, 170*, 120899.

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research, 133*, 285–296. https://doi.org/10.1016/j.jbusres.2021.04.070

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable machine learning. *arXiv preprint arXiv:1702.08608.*

Egghe, L. (2005). *Power laws in the information production process: Lotkaian informetrics.* Elsevier.

European Central Bank. (2018). *Fifth report on card fraud.* Retrieved from https://www.ecb.europa.eu

Europol. (2021). *Internet organised crime threat assessment (IOCTA).* European Union Agency for Law Enforcement Cooperation.

Europol. (2023). *Internet organised crime threat assessment (IOCTA) 2023.* European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu/cms/sites/default/files/documents/europol_internet_organised_crime_threat_assessment_iocta_2023.pdf

Falagas, M. E., Pitsouni, E. I., Malietzis, G. A., & Pappas, G. (2008). Comparison of PubMed, Scopus, Web of Science, and Google Scholar: Strengths and weaknesses. *FASEB Journal, 22*(2), 338–342. https://doi.org/10.1096/fj.07-9492LSF

FATF. (2018). *Guidance for a risk-based approach to virtual assets and virtual asset service providers.* Financial Action Task Force.

Fiore, U., Santis, A. D., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. *Information Sciences, 479*, 448–455. https://doi.org/10.1016/j.ins.2018.12.044

Goel, S., & Uzuner, O. (2016). Do sentiments matter in fraud detection? Estimating semantic orientation of annual reports. *Intelligent Systems in Accounting, Finance and Management, 23*(3), 215–239. https://doi.org/10.1002/isaf.1384

Goodfellow, I., Shlens, J., & Szegedy, C. (2015). Explaining and harnessing adversarial examples. *International Conference on Learning Representations (ICLR).*

Huang, R., Li, P., & Yang, J. (2023). Detecting financial statement fraud using transformer-based language models. *Decision Support Systems, 167*, 113905.

IMF. (2023). *Ukraine: Financial sector stability report.* International Monetary Fund.

Li, Y., Chen, H., & Zhang, Y. (2023). Transformer-based sequential modeling for financial fraud detection. *Expert Systems with Applications, 219*, 119619.

Moed, H. F. (2005). *Citation analysis in research evaluation.* Springer.

Morales, J., Gendron, Y., & Guénin-Paracini, H. (2019). The construction of the risky individual and vigilant organization: A genealogy of fraud detection. *Accounting, Organizations and Society, 81*, 101080.

Ngai, E. W. T., 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. https://doi.org/10.1016/j.dss.2010.08.006

Paul, J., Lim, W. M., & O'Cass, A. (2021). Scientific procedures and rationales for systematic literature reviews (SPAR-4-SLR). *International Journal of Consumer Studies, 45*(4), O1–O16. https://doi.org/10.1111/ijcs.12695

Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. *Auditing: A Journal of Practice & Theory, 30*(2), 19–50. https://doi.org/10.2308/ajpt-50009

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *arXiv preprint arXiv:1009.6119.*

Price, D. J. de Solla. (1963). *Little science, big science.* Columbia University Press.

Pumsirirat, A., & Yan, L. (2018). Credit card fraud detection using deep learning based on auto-encoder and restricted Boltzmann machine. *International Journal of Advanced Computer Science and Applications, 9*(1), 18–25. https://doi.org/10.14569/IJACSA.2018.090103

Purda, L., & Skillicorn, D. (2015). Accounting variables, deception, and a bag of words: Assessing the tools of fraud detection. *Contemporary Accounting Research, 32*(3), 1193–1223. https://doi.org/10.1111/1911-3846.12117

Roy, S., Dutta, A., & Kar, A. (2022). Emerging machine learning techniques for credit card fraud detection: A review. *Financial Innovation, 8*(1), 1–20.

Schreyer, M., Sattarov, T., Borth, D., Dengel, A., & Reimer, B. (2017). Detection of anomalies in large-scale accounting data using deep autoencoder networks. *CoRR, abs/1709.05254.* https://arxiv.org/abs/1709.05254

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

UK Finance. (2023). *Annual fraud report 2023.* UK Finance.

van Eck, N. J., & Waltman, L. (2014). Visualizing bibliometric networks. In Y. Ding, R. Rousseau, & D. Wolfram (Eds.), *Measuring scholarly impact: Methods and practice* (pp. 285–320). Springer.

Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C., & Yu, P. S. (2020). A comprehensive survey on graph neural networks. *IEEE Transactions on Neural Networks and Learning Systems, 32*(1), 4–24. https://doi.org/10.1109/TNNLS.2020.2978386

Xu, J., Chen, Y., & Kou, G. (2019). Analyzing the diffusion of blockchain technology in the financial industry. *Technological Forecasting and Social Change, 141*, 1–9.

Zhang, L., & Chen, X. (2022). Deep learning for financial anomaly detection: A comprehensive review. *Information Sciences, 600*, 1–25.

Zhang, W., & Jiang, T. (2023). Graph neural networks for fraud detection in financial transaction networks. *Engineering Applications of Artificial Intelligence, 124*, 106572.

Zheng, Y. J., Zhou, X. H., Sheng, W. G., Xue, Y., & Chen, S. Y. (2018). Generative adversarial network based telecom fraud detection at the receiving bank. *Neural Networks, 102*, 78–86. https://doi.org/10.1016/j.neunet.2018.02.010

Zupic, I., & Čater, T. (2015). Bibliometric methods in management and organization. *Organizational Research Methods, 18*(3), 429–472. https://doi.org/10.1177/1094428114562629