Journal of Applied Research and Multidisciplinary Studies (JARMS)
Volume 7 Issue 1, Spring 2026
ISSN(P): 2707-5087, ISSN(E): 2707-5095
Homepage: https://journals.umt.edu.pk/index.php/jarms

Title: **Arcane Channels of Knowledge Generation in Artificial Intelligence for Fraud Detection in Financial Operations: A Bibliometric Overview**

Author (s): Maryam Tanveer and Farah Naz

Affiliation (s): Kinnaird College for Women, Lahore, Pakistan

DOI: https://doi.org/10.32350/jarms.71.05

History: Received: February 15, 2026, Revised: April 09, 2026, Accepted: April 27, 2026, Published: June 24, 2026

Citation: Tanveer, M., & Naz, F. (2026). Arcane channels of knowledge generation in artificial intelligence for fraud detection in financial operations: A bibliometric overview. *Journal of Applied Research and Multidisciplinary Studies*, *7*(1), 111–136. https://doi.org/10.32350/jarms.71.05

Conflict of Interest: Author(s) declared no conflict of interest

UMT

A publication of
School of Professional Advancements
University of Management and Technology, Lahore, Pakistan

Arcane Channels of Knowledge Generation in Artificial Intelligence for Fraud Detection in Financial Operations: A Bibliometric Overview

Maryam Tanveer and Farah Naz*

Accounting and Finance Department, Kinnaird College for Women, Lahore, Pakistan

Abstract

In this research, we survey and sketch the bibliometric landscape of intellectual evolution, topic distributions, and growing paths of the multidisciplinary topic of artificial intelligence (AI) used for fraud detection within the finance sector. With 243 entries indexed by Scopus between 2020-2025, this investigation provides a comprehensive overview of intellectual research in the field by exploring and illustrating its evolution across the key actors, institutions, nations, and conceptual co-occurrence, by utilizing keywords strategy in Scopus, science-mapping, and performance metrics tools in VOSviewer. The main topics discovered are machine learning, anomaly detection, and risk analytics as the maturing methodological base, emerging research areas include explainable AI, blockchain and FinTech. India emerged as the largest contributing country, though with relatively low collaboration overall. These findings also reveal how AI-based fraud classification has expanded across diverse application domains beyond finance, and how, alongside the field's traditionally technical and sophisticated methodology-driven investigations, 'softer' dimensions—fairness, ethics, and regulatory compliance—along with proactive, prevention-focused approaches, are only beginning to emerge at the margins rather than forming a central focus of the field. Instead of just reporting the data, in this study we propose a theoretical framework regarding evolution of detection field including rule-based, graph-based and explainable AI approaches, and benchmarks it against previous bibliometric researches. The finding of this paper contributes in several ways, unifying inconsistent knowledge dispersed information, indicating avenues of research in areas with research vacuum, providing ideas for academicians toward publications, and guiding practice regarding fraud-risk governance.

Keywords: artificial intelligence, bibliometric analysis, fraud detection, risk analytics

*Corresponding Author: farah.naz@kinnaird.edu.pk

Introduction

A digital-transformation-led paradigm shift in Banking, FinTech, Taxation, Trade, Insurance and Finance in general has brought along efficiency, quick transactions, and conveniences of transactions, yet has given rise to fraud of even more intricate forms, often termed virtual-collar crime (Reid, 2018). This technological transformation equipped criminals with highly sophisticated tools like, automated scripts, synthetic identities, cross-border laundering, and multi-layered transaction schemes, that make the traditional rule-based and manual auditing ineffective by design. The incurred fraud has broad consequences that extend beyond direct financial losses, including the erosion of reputation and complicated legal and regulatory exposure (Halteh & Tiwari, 2023).

Fraud, a complex phenomenon in the digital world, has evolved beyond basic larceny into a globally distributed challenge with its roots spread in integrated digital solutions (Laxman et al., 2025). Advanced digital tools readily defeat the established anti-fraud schemes. The Federal Trade Commission (2025) reports that consumers in the United States lost over $12.5B to fraud in 2024 across all categories- an increase of 25% over the last year, with the major loss categories being investment scams ($5.7B), and imposter scams ($2.95B). The increase in consumer fraud losses was largely driven by increase in reporting of these losses rather than increase in frequency (25% vs 19%). A similar trend is found in an H2 2025 Update to Top Fraud Trends Report by TransUnion. They estimate that organisations lost on average 7.7% of their annual revenue to fraud, which equates to an estimated US$534 billion loss among the 1200 participating organisations (TransUnion, 2025). Even though these numbers are based on reporting and survey data and represent only a fraction of the true value of lost assets, they reveal how an organization's lost value can stem from vulnerable internal systems and externally perceived trust when they fail to protect the entrusted data and assets (Moura et al., 2025).

The gap between the limited capacity of legacy systems for analysis of massive data-sets and fraud of higher sophistication cannot be bridged without employing sophisticated and automated tools (Dal Pozzolo et al., 2018). With widespread adoption of digital solutions for banking, FinTech, and Finance, it is inevitable for criminals to utilize the advancements for sophisticated financial crimes. Many traditional systems operate on post-facto approach and fail to proactively detect the fraud. According to the

Internet Crime Complaint Center (IC3) of the Federal Bureau of Investigation (FBI) (2024), reporting for the Internet Crimes resulted in losses of $16.6 billion for the US - an increase of 33% over 2023 - with investment fraud being the biggest contributor at $6.57 billion. Similarly, a global average of $4.88 million in data breach was recorded by the organizations in 2024, which is a 10% increase year-on-year and the steepest hike ever since the pandemic (IBM Security, 2024). The increase in losses can be attributed to criminals increasingly exploiting digital systems with high levels of sophistication using automated tools. Such a high impact incident implies a systemic weakness in enterprise security architectures (Kou et al., 2004).

To counter this threat, organizations and governments have extensively adopted Artificial Intelligence (AI) and other related technologies for financial fraud detection and prevention (Bello & Olufemi, 2024). Using machine learning, deep learning, anomaly detection, graph based techniques, data mining, and more, AI provides high accuracy, adaptability, and scalability for real time and retrospective fraud detection. Researchers are using novel AI methods like, heterogeneous graph neural networks with attention mechanisms for a much better credit-card fraud detection (Sha et al., 2025), graph neural networks on dynamically changing transaction graphs, where static analysis fails (Zakaria et al., 2025) or deep autoencoder networks to improve the detection accuracy for accounting fraud and transactions (Li et al., 2024).

This research focuses on an in-depth bibliometric analysis of AI-based financial fraud detection research conducted between 2020-2025 and published in Scopus-indexed sources. It defines AI-driven financial fraud detection as the process of using any form of artificial intelligence - including machine learning, deep learning, anomaly detection, data mining - in any of the financial sector domains – (a) banking, (b) auditing, (c) accounting, (d) finance & FinTech, insurance & trade – to identify, prevent, and deter fraudulent activity at any point of the lifecycle of a financial transaction, at real time or post transaction to mitigate financial, reputational, and regulatory risk. Consistent with extant literature, AI systems utilized in fraud detection often have a capacity to “learn” from historical data patterns to discriminate legitimate activity from suspicious behaviour (Kamuangu, 2024; Moura et al., 2025).

Extant literature on AI for fraud detection is spread across various fields such as finance, auditing, cybersecurity, risk management, corporate governance, compliance, supply chain, accounting etc. Researchers study various types of fraud, dataset, analytical techniques, and also emphasize on interpretability and data privacy in their works, thereby fostering multidisciplinary approach linking computer science, finance, auditing, and regulation (Bello et al., 2023; Yuhertiana & Amin, 2024). However, the literature in the area is fragmented, and not widely surveyed beyond a single sector, fraud type, or analytical approach (Abdallah et al., 2016). Without a comprehensive view on what research has been carried out in this domain, it becomes difficult to conceptualize and strategize towards effective research or practical implementations (Ngai et al., 2011). In this context, with increasing fraud sophistication and changing digital transformation, there has been an ever growing need for an extensive bibliometric review that provides a methodical overview and unambiguous guidelines for further research (West & Bhattacharya, 2016).

This bibliometric study maps and analyzes research works published in the last six years (2020 to 2025) for AI-based financial fraud detection on a selected list of 243 publications from Scopus database. The analysis provides insights on: (1) The integrated usage of AI across the financial sectors for fraud detection; (2) Interdisciplinary collaborations and contributions to the field; (3) Emerging research trends and their evolution over time; (4) Key actors (authors, countries and institutions) in the field and their network structures; and (5) Research gaps and future directions. The study makes three major contributions: Firstly, it presents a recent and holistic bibliometric analysis of the highly interdisciplinary field of AI in fraud detection which will aid researchers, professionals, and policy makers to get acquainted with emerging research and devise more robust systems. Secondly, by presenting a conceptual framework of the field's development (Section 2), the paper offers theoretical understanding beyond description for the growth of research in finance, auditing, risk management, and cybersecurity. Lastly, by contextualizing the results of the current study with previous bibliometric literature, this research highlights the unique contributions of the paper, thus, fostering more cross-disciplinary research collaboration and enabling effective research–practice alignment of academic work and fraud management strategy.

The rest of this paper is organized as follows. Section 2 presents the methodology, including data sources, collection, and analysis tools. Section

3 illustrates the co-authorship analysis at the author, organization, and country levels; keywords co-occurrence based on author, index, and all keywords; and abstracts, semantically analyzed, to deliver emerging thematic patterns. Finally, Sections 4 and 5 present key findings, discussion, and conclusion while underscoring implications for practice, limitations, and research opportunities.

Conceptual Framework: The Evolution of Fraud-Detection Research

As bibliometric analysis represents the structure of a literature rather than hypothesis testing, an explicit conceptual lens, which accounts for the presence of clusters and themes, is particularly desirable. Developing this lens, this section examines the progression of the literature in fraud-detection along four overlapping stages. The synthesis draws insights from key disciplines, including finance, auditing, cyber-security, and risk-management, and supplies the interpretive scaffold against which the results of bibliometrics in Section 4 are thereafter interpreted. Instead of viewing detection techniques as a homogeneous catalogue, the proposed framework views them as evolving solutions to two underlining problems: the dilemma between detection decision model accuracy and its understandability, and between detection as a reactive mechanism and pre-emptive prevention.

Stage One: Rule-Based and Expert Systems

On a practical level, earlier fraud detection was based on simple dependable rules and expert systems where signatures of known fraud were directly encoded into thresholds and decision logic (Bolton & Hand, 2002). Expert systems were explainable and auditable, but brittle: they detected only previously specified patterns, often returned high false-positive rates, and required manual intervention as attackers evolved their tactics. This is the problem that has driven the field ever since, to find ways to locate adaptive fraud without explicitly listing them all out in advance.

Stage Two: Statistical and Data-Mining Approaches

The second stage saw the formulation of fraud detection as statistical classification and outlier identification. Bolton and Hand (2002) produced a seminal overview of this class of statistical fraud detection methods. Phua et al. (2010) and Ngai et al. (2011) amalgamated the exploding fields of data-mining research, with Ngai et al. (2011) also proposing a classification system that associated detection techniques with specific types of financial fraud. Moreover, Abdallah et al. (2016) surveyed fraud detection systems across specific application domains. This phase introduced the concepts of supervised and unsupervised learning, association rules and clustering, and fundamentally shifted the perception of fraud detection from rule-based to data-based activity. It also identified the methodological challenges of class imbalance, concept drift, and the limited availability of labelled fraud examples, which continue to be prominent today.

Stage Three: Machine Learning and Deep Learning

The final phase is characterized by the exponential growth in the use of machine learning, and ultimately deep learning. In the transition from standard classifiers to ensemble methods and neural network models, Kou et al. (2004) and West and Bhattacharya (2016) measured the trend, and Dal Pozzolo et al. (2018) refined the emerging approaches with realistic techniques to account for verification latency and concept drift in card-payment fraud. The adoption of neural architectures- convolutional, recurrent, long short-term memory, autoencoders, ensembles led to superior prediction on complex, high-dimensional transactional data (Ali et al., 2022; Li et al., 2024). Increasing the accuracy, however, exacerbated the conflict of output understandability. The more powerful models displayed decision opacity, presenting issues for auditing, contractual provisions, and liability purposes.

Stage Four: Graph-Based, Explainable, and Governance-Aware Architectures

The most recent stage directly addresses the tension between explainability and adaptability that has defined the field's evolution. Methodologically, graph-based models -particularly graph neural networks used on dynamic transaction graphs - estimate relational and temporal dependence that traditional, less-structured models cannot, dramatically increasing accuracy for real-time detection (Sha et al., 2025; Zakaria et al., 2025). Governing structures have reformed as well, shifting from reactive, regulator-driven oversight towards models of explainable AI (XAI) (Ali et al., 2022; Hafez et al., 2025). These changes in methodology and governance represent a conceptualization of fraud detection as a socio-technical problem where technical capabilities, social performance, ethical governance, and regulatory compliance are undergirded by the other and emerge together, and it anticipates the proactive, prevention-focused orientation that is the research area's current final frontier.

Taken together, these four stages form the interpretive rubric on which the bibliometric results are based. The system offers two hypotheses about the overall core/periphery configuration: that machine-learning and detection language should predominate the core of the literature (Stages Two and Three), that an emergent periphery should be centered on explainability, blockchain, and FinTech (Stage Four), and that proactive prevention should be comparatively lagging in development. Sections 4 and 5 attempt to verify these hypotheses with the instantiated networks so that the bibliometric structures may be analyzed rather than catalogued.

Methodology

Data Sources and Collection

Figure 1 overviews the data collection method, documented as a PRISMA style flow so that transparency and reproducibility is maintained. A Scopus database search was conducted to provide the basis for the bibliometric analysis; this bibliographic database was used since it has wide multidisciplinary coverage and curated indexing facilities (Baas et al., 2020).

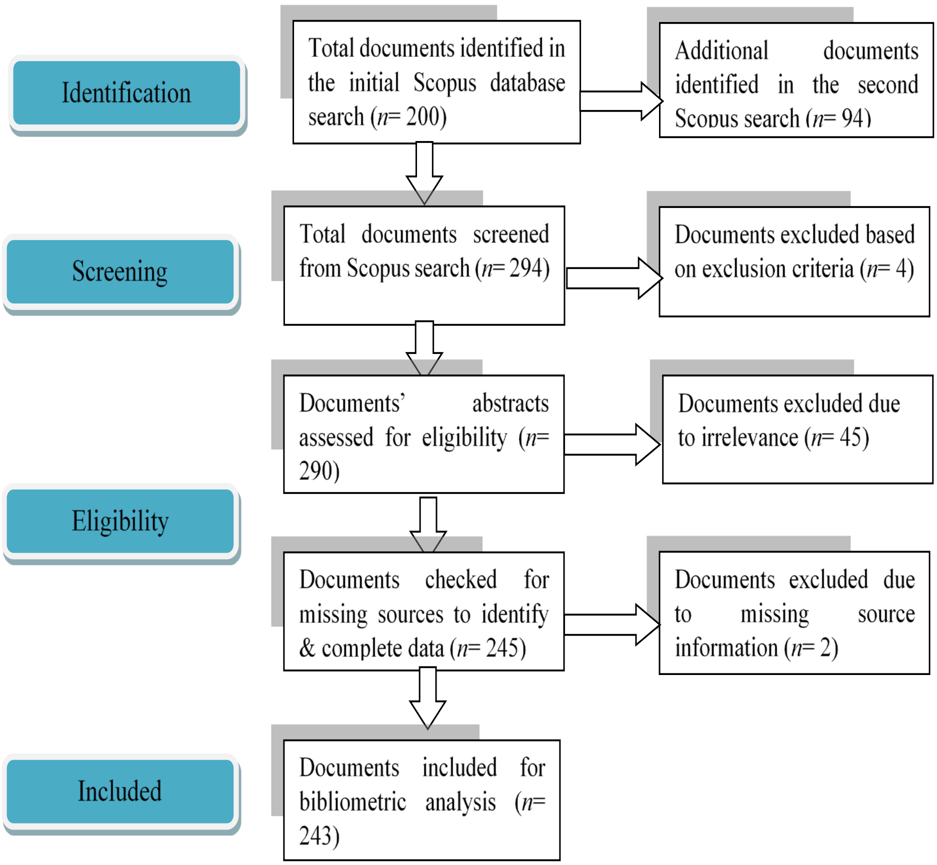
The first data search identified the most recent publications; then the date of the original search was broadened retrospectively to ensure complete 2020-2025 coverage (which subsequently returned more records, mostly already captured in the first search). The search query targeted AI-based fraud detection using the terms "artificial intelligence" and "fraud detection" in the title, abstract, and keyword fields, restricted to publications from 2020 to 2025 in English, and including journal articles, conference papers, book chapters, and lecture notes across finance, accounting, auditing, risk management, FinTech, and related transactional fields. The full Boolean query, applied to the title-abstract-keyword index, was:

TITLE-ABS-KEY("artificial intelligence" AND "fraud detection") AND PUBYEAR > 2019 AND PUBYEAR < 2026 AND (LIMIT-TO(LANGUAGE, "English"))

As illustrated in Figure 1, the initial search on Scopus retrieved 200 documents and a hand search retrieved an additional 94 records, totaling 294 before reading. After de-duplication and application of the exclusion criteria (*n* = 4), 290 documents were screened by their abstract and title. Publications were retained only if they described applications of AI to financial fraud detection and risk mitigation; publications describing applications in other domains, - such as AI-based marketing fraud detection, AI-based product quality or substance checkers, deepfakes for fake reviews, etc. were excluded (n = 45). The remaining 245 publications were checked against missing source details. Two publications were discarded for lack of metadata, leaving 243 for bibliometric analysis. The search was completed in 2025; the counts given refer to the date of search on the database.

Figure 1

PRISMA Framework



Note. The two-stage search reflects an initial query for recent literature followed by a supplementary query extending coverage across the full 2020–2025 window; overlapping records were removed during de-duplication.

Data Analysis

The bibliographic data was exported from the database in comma separated value (.csv) format and then cleaned in Microsoft Excel to confirm that the data was correct, and to eliminate any duplication prior to analysis. Bibliometric analysis was conducted using VOSviewer. Its visualisation capabilities, user-friendly interface, and support for co-authorship, co-occurrence, and text-mining analyses make it an optimal tool for this study (van Eck &Waltman, 2010).

Three complementary bibliometric analyses were conducted: (1) co-authorship analysis, to assess author, organisation, and country collaboration; (2) author keyword and index keyword occurrence and co-occurrence analysis, to determine the most prominent authors and keywords, and to identify common themes and conceptual structures within the field; and (3) bibliometric mapping of latent themes, through text mining abstracts, and term co-occurrence analysis. Default VOSviewer's threshold and normalisation parameter were used respectively for each analysis. These analyses together reveal the prevalent AI fraud-detection authors, organsations and countries as well as the themes or research trajectory within the field. Consistent with good bibliometric practice, both the network density and total link strength for each network are presented so as to elucidate the structural significance of each network in light of the document and citation count.

Results and Interpretation

Co-authorship Analysis

Authors

The top co-authors in the AI fraud detection network, Geetha Manoharan and Sanjeev Kumar form the visible hub of the network (Figure 2). They jointly authored several articles exploring how the financial sector, particularly customer relationship management, is being influenced by AI and machine learning (Bayero et al., 2025; Manoharan et al., 2025). Bhupinder Singh's position in the periphery signifies a comparatively peripheral influence, as he researched generative AI in cybersecurity policy, machine learning for fraudulent e-commerce transactions, and AI applications for ad-click and credit-card fraud (Singh et al., 2024; Singh, Dutta, & Kaunert, 2025; Singh, Raghav, et al., 2025). Both temporal overlay and density map demonstrate a sustained co-authorship by Manoharan and

Kumar. However, these conclusions must be qualified: the total link strength of publications in the network is not high (maximum of 2; Table 1), and there are few authors and limited documents cited; as such, the relative prominence of these individuals stems from their field's early development and limited interconnectivity. The relative density of the network implies a limited but meaningful concentration of attention and research among this small group of authors rather than the development of an independent research school of thought.

Figure 2

Major Authors

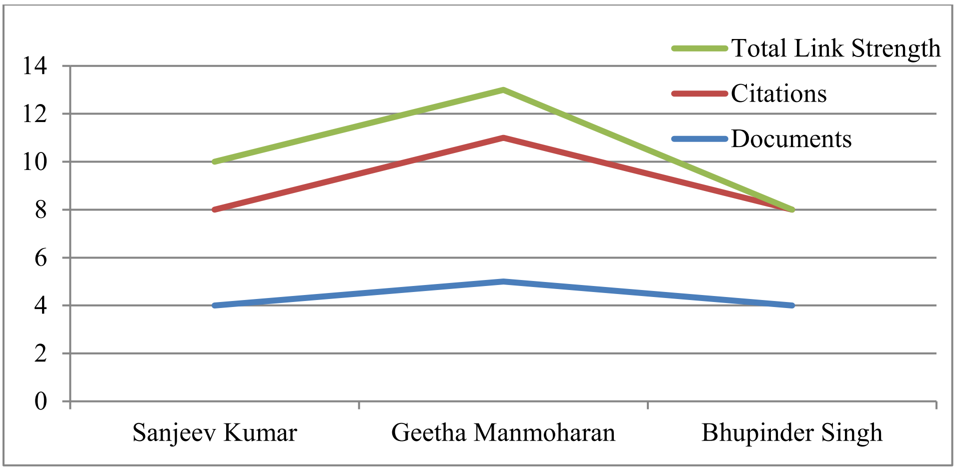


Table 1

Major Contributors and Their Thematic Directions in AI-Driven Fraud Detection Research

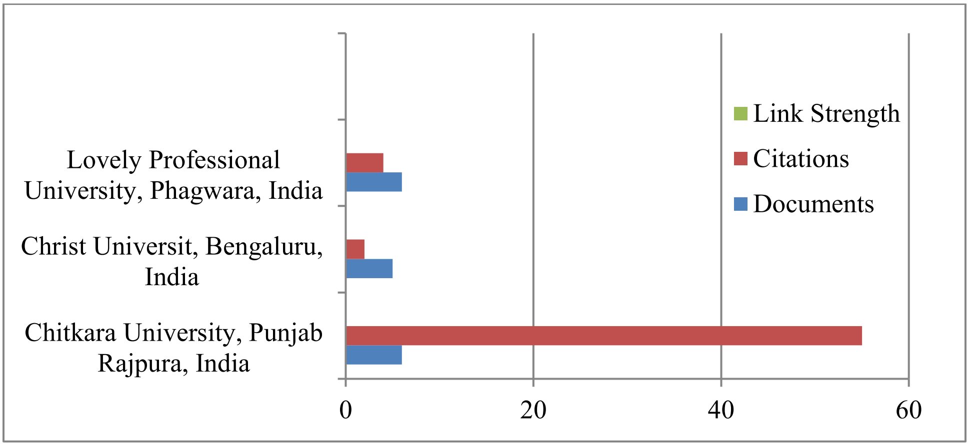
Authors	Documents	Citations	Link Strength	Thematic Focus
Sanjeev Kumar	4	4	2	AI's role in enhancing CRM in financial sectors, ML and AI fusion in finance and their role enhancing financial fraud detection, and financial analysis.

Authors	Documents	Citations	Link Strength	Thematic Focus
Geetha Manmoharan	5	6	2	AI and ML role in revolutionizing financial services and in enhancing CRM in financial sector.
Bhupinder Singh	4	4	0	AI and ML in financial fraud associated to credit cards, Ad-clicks, e-commerce transactions and generative AI in cybersecurty.

Organizations

Figure 3

Institutional Contributions



At the organizational level, Chitkara University, Lovely Professional University, and Christ University are the top performing institutions in terms of output volume and citation count. Proximity between these universities in the network suggests a strong thematic overlap but the lack of connecting ties signifies an absence of co-authorship between institutions in the domain of AI fraud-detection (Figure 3). Even though Chitkara University is cited quite highly (55) per output, all of the institutions show no collaboration, and work in isolation. This is reflected even in the density overlay which shows each university to be separate from the other, a singular dot rather than being connected to an integrated group of studies.

Table 2

Major Organizational Contributors and their thematic directions in AI-Driven Fraud Detection

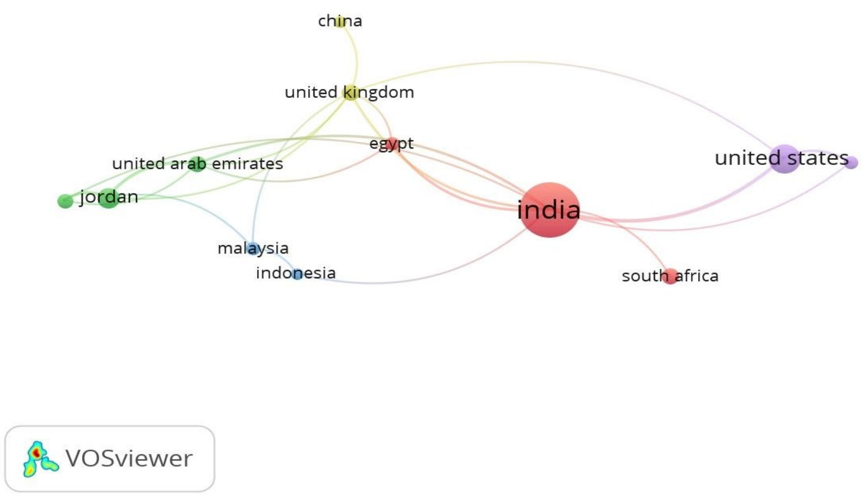
Organizations	Documents	Citations	Link Strength	Thematic Focus
Chitkara University, Punjab Rajpura, India	6	55	0	ML for fraud detection in decision support systems in Insurance Sector; Prevention of financial fraud using NLP; and role of AI in mitigating financial crimes (Rohilla & Jindal, 2025; Sood et al., 2023; Verma, 2022)
Christ University, Bengaluru, India	5	2	0	AI for predictive financial risk management in emerging markets (Parth, 2025).
Lovely Professional University, Phagwara, India	6	4	0	Resilience development against deepfakes in financial sector; and financial risk management using AI- potentials, ethical challenges and threats (Kaur & Dhiman, 2025; Khanday et al., 2025).

Countries

The country map depicts the overwhelming dominance of India, both in terms of volume of output (107 documents) and in its extensive collaboration linkages (total link strength 14) with the US, the UK, and China. Secondary major collaborative linkages with other nations are seen for Jordan, United Arab Emirates, and South Africa. The temporal overlay indicates continued, clear dominance of India, which is seen to lead from 2020 up to 2024, whilst contributions from other nations increase gradually. Four to five clusters of nations have been depicted, suggesting research is rather dispersed on a national and even regional basis, rather than being evenly spread on a global scale.

Figure 4

Network Map: Countries



Notwithstanding India’s statistical lead, caution should be employed when drawing too direct conclusions for two main reasons: Firstly, neither productivity nor team size correlates strongly with impact on knowledge in general (as measured by citations): Indian output (107 documents) generated only 285 citations, compared with South Africa's 9 documents generating 365 citations, the UK's 10 documents generating 184 citations, and Malaysia's 6 documents generating 155 citations — far higher citation-to-output ratios despite substantially lower total output. Secondly, whilst there is a compelling set of motivations for this output such as India’s massive, rapidly digitizing financial economy, concerted national efforts in FinTech and AI investment, an extensive workforce well versed in Englishspeaking research and profound exposure to digital payment fraud, these are drivers for output production not research impact or innovation within a network-based paradigm, especially as the strength of collaboration links for India are so low indicating much of the work being produced is within India itself and the impact is being made in a national rather than international research domain. Accordingly, India's current status is best described as high volume national production rather than leadership in the global AI-based financial fraud detection, implying that further expansion in the global reach and impact of this field is dependent upon expanding inter-border collaboration efforts rather than strengthening the current output within this nation alone.

Table 3

Contributions by Countries in Interdisciplinary Research on AI and Fraud Detection

Countries	Documents	Citations	Total Link Strength
India	107	285	14
Jordan	16	23	8
United Arab Emirates	10	11	8
United Kingdom	10	184	8
United States	31	74	7
Saudi Arabia	8	6	5
Egypt	6	10	4
Canada	7	22	3
Malaysia	6	155	3
Indonesia	5	6	2
China	5	35	1
South Africa	9	365	1

Keyword Co-occurrence Analysis: All, Author and Index Keywords

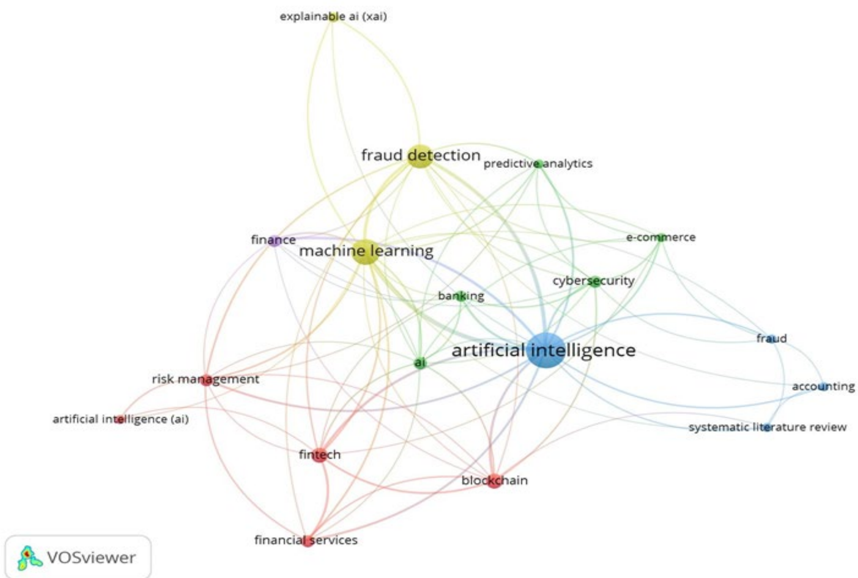
With all-keyword analysis, artificial intelligence and fraud detection is shown to be the centre of attention, surrounded by machine learning, deep learning, risk assessment, cybersecurity, and fintech. Explainable Artificial Intelligence (XAI) and transparency were observed to be emerging trends reflecting concerns in AI ethics and accountability, whereas, e-commerce and adversarial machine learning highlight diversity in application, and explainability concerns are highlighted as emerging, with increasing growth at the expense of earlier established concepts.

All-keywords in the author-keywords analysis show AI and fraud detection at the centre with machine learning, XAI and blockchain playing a key role in defining the current trends. The presence of blockchain can be explained by the use of blockchain for fraud mitigation while XAI reflects emerging concerns of the transparency, trustworthiness, and explainability of AI fraud detection algorithms and the use of predictive analytics for financial institutions. These findings correspond with the four-stage conceptual frame proposed in Section 2 where ML maturity is evident in stages 2 and 3 whereas blockchain and XAI represent stage 4 concerns (explainability and graph-based, governance-focused modelling). Lighter coloured regions within density grid signify uncharted areas of research, including proactive and preventative measures.

The keyword index analysis shows that fraud detection is the central theme, closely linked with machine learning, risk management, predictive analytics, and crime. In contrast, financial markets, investment, cyber threats, and network security represent key application areas. Decentralised finance and blockchain emerge as growing research trends, reflecting the evolving financial landscape and increasing technological adaptation.

Figure 5

Network Map: Author Keywords



Term Co-occurrence Analysis

All the words from the abstracts are compiled together and tested. Using text mining, the output from 'detection' comes in the center surrounded by 'fraud', 'risk management', 'methodological techniques' and 'pattern recognition'. The text mining also shows 'transparency', 'explainable artificial intelligence', 'regulatory compliance' as words surrounding the centre reflecting concerns over AI ethics. Moreover, FinTech, customer service, and digital financial services are shown representing applications in sectors other than traditional banking. For temporal overlay, the centre terms of 'detection' and 'fraud' are seen to dominate while at the frontier, 'explainable', 'accountable', and 'hybrid AI models' have shown growth, again reflecting the four-stage evolution previously demonstrated (Table 4). In the case of the 'density grid', largest density can be observed in the center, where risk management and governance are located in the middle density region and 'promising but not widely developed' regions represent the research in promising but under developed areas (Figure 5 and Figure 6).

Table 4

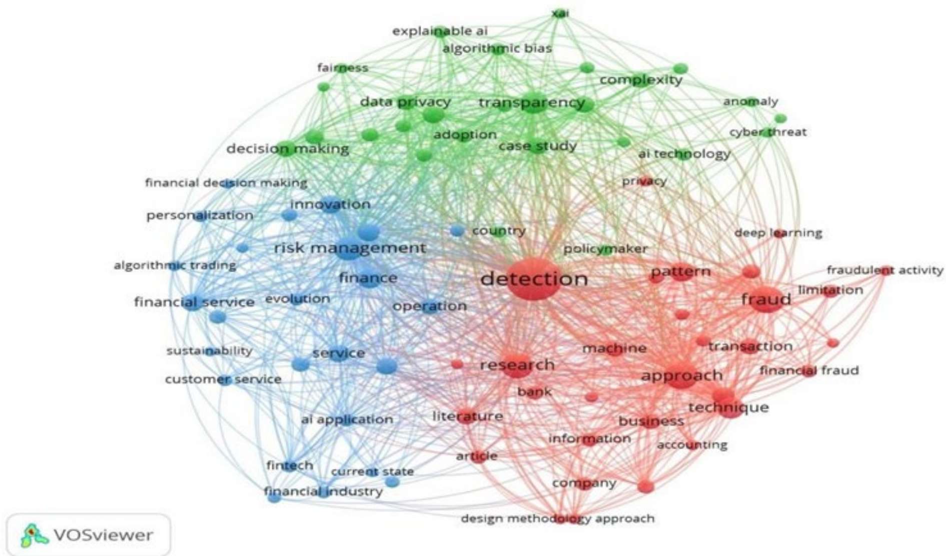
Term Co-occurrence: Text Mining of Abstracts

Term	Occurrence	Relevance
Fraudulent Activity	14	2.57
Originality Value	14	2.11
Design Methodology Approach	14	2.11
Algorithm Trading	13	1.93
Financial Fraud	18	1.89
Ethical Considerations	17	1.86
Detection	208	0.08
Fraud	81	1.05
Approach	73	0.89
Research	68	0.33
Risk Management	62	0.56
Transparency	57	0.68
Technique	50	1.01
Pattern	43	0.59
Finance	40	0.54
Innovation	37	0.76

Term	Occurrence	Relevance
Automation	33	0.77
Prevention	33	0.93
Service	33	0.48
Case Study	32	0.36

Figure 6

Network Map: Term Co-occurrence



Discussion

The synthesis of bibliometric evidence (2020-2025) provided here establishes the relationship between theory and practice in AI-based financial fraud detection and identifies the changing nature of the field. The analysis, interpreted through the four-stage model developed in Section 2, demonstrates how a well-established methodological foundation has been complemented by the development of governance and prevention components.

Comparative to recent systematic reviews, our bibliometric findings suggest that both machine learning and deep learning techniques (including CNNs, LSTMs, and ensemble methods) are central to credit-card and related fraud detection due to increasing challenges for rule-based systems, and conform to the field's Stage Three maturity level (Hafez et al., 2025).

Increased centrality for graph-based modelling and anomaly detection in the networks reflect their relevance for relational and temporal analysis, with recent studies indicating the effectiveness of GNNs on dynamic transaction graphs over static ones due to the enhanced capturing of interactions (Zakaria et al., 2025). One of the most striking trends in the literature is the growing emphasis on explainability, transparency, and trust in models; while initial publications were driven by predictive accuracy, more recent contributions employ XAI methods such as SHAP and LIME for more transparent output intended for audit and compliance purposes (Ali et al., 2022; Hafez et al., 2025). This shows an alignment with the Stage Four shift we posited and that is confirmed by cluster interpretations: the 'explainability' keyword is among the most recent publications.

Another shift in the application domain is the inclusion of tax, insurance, and general audit fraud from only credit-card fraud in a regulated environment. For instance, research on cryptocurrency compliance presents a variety of AI methods including language processing, deep learning, and generative models to avoid and uncover fraud in de-centralised finance (Valencia et al., 2025). These new domains are evident in the increased thematic links in the bibliometric network vizualisation to FinTech, blockchain and other digital finance services.

The real-world implementation has other outstanding issues such as class imbalance, concept drift, data privacy and data protection, and lack of effective system integration. Balancing high accuracy with imbalanced data, interpretability, and privacy compliance is a major concern (Albalawi & Dardouri, 2025), leading to concrete barriers for financial institutions such as continuous model updating due to changing fraud patterns, the reconciliation of transparency needs for auditors/regulators with model opacity, and the data-sharing restrictions imposed by privacy regulations for effective cross-institutional detection (the near-zero institutional links illustrate the extent of this last problem).

Ethical and regulatory concerns — including fairness, accountability, compliance, and transparency — appear only as recent, peripheral nodes in the co-occurrence map (indicated by their light coloring, denoting emergence rather than centrality), suggesting that bibliometric analysis may not fully capture these 'softer' but critical dimensions of the field relative to their significance in systematic reviews. Their emergence at the periphery, however, likely signals where the field's research focus is shifting next, positioning ethical and regulatory considerations as a key direction for future work.

Our findings are consistent with and build upon existing bibliometric analyses of financial fraud prevention. Moura et al. (2025) examined the AI and financial fraud prevention field over the period between 2015-2025 across more than a hundred articles from multiple databases. Laxman et al. (2025) reviewed digital-payment fraud and broader financial crimes. The analysis of AI in financial activities is narrowed here: by using recent 2020–2025 data and pointing out the growing prevalence of explainability and graph-based methods; and by using a clear conceptual framework to establish relations between structural patterns and evolution of the discipline. Our understanding reveals a situation which is missing from previous catalogs of collaboration – i.e. low institutional collaboration and strong national focus of research. Our findings reflect a twofold evolution toward maturity in the field: enhancement of the methodological sophistication in detection techniques and a greater concern for transparency, ethics, explainability, and good governance. Indeed, a mixed-methods approach can further help elaborate these insights, capturing the structural and thematic dimensions of the field with greater depth and breadth.

Conclusion

From 2020 to 2025, AI application in financial fraud detection has matured, evolving from standalone models to cross-domain applied framework systems based on methodological development and focusing on transparency and governance. Our bibliometric analysis reveals that graph-based methods, combined with machine learning-based anomaly detection methods, form the core area of interest, supported by systematic reviews which increasingly highlight the importance of explainability and compliance-aware systems. AI's applications span beyond credit-card fraud to cover insurance and blockchain but challenges to full adoption, such as data imbalance, concept drift, and ethical implications, persist. The research has provided a baseline map of the trend and the theoretical development of this field.

Theoretical, Practical, and Policy Implications

Theoretically, the study contributes to understanding the maturation of digital detection architecture methods and suggests that with its four-stage evolution, the field is ripe for innovation in the synthesis of behavioural, relational, and temporal inputs. The strong and clear trend towards explainability and transparency underscores the necessity for embedding social and ethical dimensions into the design phase, rather than an afterthought, and a management of the trade-offs between predictive accuracy, fairness, and compliance as a primary design challenge. From a practical and policy perspective, financial institutions need to deploy sophisticated machine and deep learning models that enable real-time and multi-layered detections integrated with behavioral and relational dimensions to address escalating money laundering and identity schemes, as crucial for building trust and meeting regulatory compliance in a fraud-prevalent environment. The integrated approach should be strengthened through interdisciplinary collaboration between cyber-security experts, data scientists, auditors, and compliance officers, as well as through common governance standards agreed upon by stakeholders and regulators regarding monitoring, data privacy, and transparency. Policy initiatives to reduce regulatory and competitive barriers to secure data sharing could be beneficial, given the limited collaboration identified in this review, in facilitating shared information for sustainable and responsible deployment.

Limitations

The present study has several limitations: relying on the Scopus database only provides access to a portion of published academic literature and excludes other languages and other indexing sources; the use of VOSviewer alone is restrictive and does not reflect all existing bibliometric analyses and mapping visualization tools; the keyword-based query search strategy could miss some studies under different terms. Drawing upon only published academic literature, excluding official documents, reports, or data; the time-lag in citation-based metric might underestimate newer publications. Finally, network structure visualization is affected by the normalisation and clustering settings of VOSviewer.

Future Research Directions

These limitations naturally define potential avenues for future research. The development of new themes requires applying other databases (e.g., Web of Science, Dimensions) and other quantitative analysis techniques to ensure triangulation and comparative analyses (Moura et al., 2025). A greater emphasis on proactive and preventive fraud control measures, rather than only on reactive detection methods, is also suggested. Integration of real datasets, case studies, and public reports will contribute to closing the gap between theoretical findings and real-world practice. Stronger inter-sector collaboration will enable better insights and the generation of novel methodological approaches, along with common standards that will cover ethical, regulatory, and governance aspects to support more transparent and responsible AI deployment.

Author Contribution

Maryam Tanveer: formal analysis, investigation, methodology, visualization, writing – original draft. **Farah Naz:** conceptualization, data curation, project administration, resources, supervision, validation, writing – review & editing

Conflict of Interest

The authors of the manuscript have no financial or non-financial conflict of interest in the subject matter or materials discussed in this manuscript.

Data Availability Statement

The data associated with this study will be provided by the corresponding author upon request.

Funding Details

No funding has been received for this research.

Generative AI Disclosure Statement

The authors did not use any type of generative artificial intelligence software for this research.

References

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, *68*, 90–113. https://doi.org/10.1016/j.jnca.2016.04.007

Albalawi, T., & Dardouri, S. (2025). Enhancing credit card fraud detection using traditional and deep learning models with class imbalance mitigation. *Frontiers in Artificial Intelligence*, *8*, Article e1643292. https://doi.org/10.3389/frai.2025.1643292

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences*, *12*(19), Article e9637. https://doi.org/10.3390/app12199637

Baas, J., Schotten, M., Plume, A., Côté, G., & Karimi, R. (2020). Scopus as a curated, high-quality bibliometric data source for academic research in quantitative science studies. *Quantitative Science Studies*, *1*(1), 377–

386. https://doi.org/10.1162/qss_a_00019

Bayero, S. A., Manoharan, G., & Kumar, S. (2025). Machine learning in finance: The revolutionized fusion. In F. Ghosn, G. Awad, & K. Darwich (Eds.), *AI's transformative impact on finance, auditing, and investment* (pp. 43–72). IGI Global Scientific Publishing.

Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications, challenges, and opportunities. *Computer Science & IT Research Journal*, *5*(6), 1505–1520. https://doi.org/10.51594/csitrj.v5i6.1252

Bello, O. A., Ogundipe, A., Mohammed, D., Folorunso, A., & Alonge, O. A. (2023). AI-driven approaches for real-time fraud detection in US financial transactions: Challenges and opportunities. *European Journal of Computer Science and Information Technology*, *11*(6), 84–102. https://doi.org/10.37745/ejcsit.2013/vol11n684102

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, *17*(3), 235–255. https://doi.org/10.1214/ss/1042727940

Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018). Credit card fraud detection: A realistic modeling and a novel learning strategy. *IEEE Transactions on Neural Networks and Learning Systems*, *29*(8), 3784–3797. https://doi.org/10.1109/TNNLS.2017.2736643

Federal Bureau of Investigation. (2025). *Internet crime report 2024*. FBI Internet Crime Complaint Center. https://www.ic3.gov/Media/PDF/AnnualReport/2024_IC3Report.pdf

Federal Trade Commission. (2025, March 10). *New FTC data show a big jump in reported losses to fraud to $12.5 billion in 2024*. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

Hafez, I. Y., Hafez, A. Y., Saleh, A., Abd El-Mageed, A. A., & Abohany, A. A. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data*, *12*(1), Article e6. https://doi.org/10.1186/s40537-024-01048-8

Halteh, K., & Tiwari, M. (2023). Preempting fraud: A financial distress prediction perspective on combating financial crime. *Journal of Money Laundering Control*, *26*(6), 1194–1202. https://doi.org/10.1108/JMLC-01-2023-0013

IBM Security. (2024). *Cost of a data breach report 2024*. IBM. https://www.ibm.com/reports/data-breach

Kamuangu, P. (2024). A review on financial fraud detection using AI and machine learning. *Journal of Economics, Finance and Accounting Studies*, *6*(1), 67–77. https://doi.org/10.32996/jefas.6.1.7

Kaur, M., & Dhiman, B. (2025). A multidisciplinary approach to building resilience against deepfakes in the financial sector. In S. Taneja, S. Gupta, M. Kukreti, & A. S. Chauhan (Eds.), *Mastering deepfake technology: Strategies for ethical management and security* (pp. 111–121). River Publishers.

Khanday, M. A., Negi, N., & Hirani, T. (2025). AI in financial risk management: Transformative potential, ethical challenges, and emerging threats. In A. M. S. Derbali (Ed.), *Artificial intelligence for financial risk management and analysis* (pp. 335–354). IGI Global Scientific Publishing.

Kou, Y., Lu, C.-T., Sirwongwattana, S., & Huang, Y.-P. (2004, March 21–23). S*urvey of fraud detection techniques*. Proceedings of 2004 IEEE International Conference on Networking, Sensing and Control, Taipei, Taiwan.

Laxman, V., Ramesh, N., Jaya Prakash, S. K., & Aluvala, R. (2025). Emerging threats in digital payment and financial crime: A bibliometric review. *Journal of Digital Economy, 3*, 205–222. https://doi.org/10.1016/j.jdec.2025.04.002

Li, W., Liu, X., & Zhou, S. (2024). Deep learning model based research on anomaly detection and financial fraud identification in corporate financial reporting statements. *Journal of Combinatorial Mathematics and Combinatorial Computing*, *123*, 343–355. https://doi.org/10.61091/jcmcc123-24

Manoharan, G., Kumar, S., & Talukder, M. B. (2024). Artificial intelligence enhancing customer relations in financial sectors. In D. Darwish & S. Kumar (Eds.), *Utilizing AI and machine learning in financial analysis* (pp. 283–300). IGI Global Scientific Publishing.

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), Article e323. https://doi.org/10.3390/jrfm18060323

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

Parth, P. (2025). Leveraging artificial intelligence for predictive financial risk management in emerging markets. In A. M. S. Derbali (Ed.), *Artificial intelligence for financial risk management and analysis* (pp. 249–270). IGI Global Scientific Publishing.

Phua, C., Lee, V., Smith-Miles, K., & Gayler, R. (2010). *A comprehensive survey of data mining-based fraud detection research*. ArXiv. https://doi.org/10.48550/arXiv.1009.6119

Reid, A. S. (2018). Financial crime in the twenty-first century: The rise of the virtual collar criminal. In N. Ryder (Ed.), *White collar crime and risk: Financial crime, corruption and the financial crisis* (pp. 231–251). Palgrave Macmillan.

Rohilla, A., Jindal, A., & Jindal, P. (2025). Revolutionizing the indigenous financial system with the utilization of artificial intelligence. In I. Ghosal, S. Gupta, S. Rana, & D. Saha (Eds.), *Indigenous empowerment through human–machine interactions: The challenges and strategies from business lenses* (pp. 153–165). Emerald Publishing.

Sha, Q., Tang, T., Du, X., Liu, J., Wang, Y., & Sheng, Y. (2025). *Detecting credit card fraud via heterogeneous graph neural networks with graph attention*. ArXiv. https://doi.org/10.48550/arXiv.2504.08183

Singh, B., Dutta, P. K., & Kaunert, C. (2025). Deep diving into financial frauds via ad click, credit card management, and document dispensation in e-commerce transactions. In P. R. Chelliah, P. K. Dutta, A. Kumar, E. D. R. S. Gonzalez, M. Mittal, & S. Gupta (Eds.), *Generative artificial intelligence in finance: Large language models, interfaces, and industry use cases to transform accounting and finance processes* (pp. 99–123). Wiley.

Singh, B., Kaunert, C., & Kaushik, T. K. (2024). Unscrambling financial fraud with AI and machine learning in e-commerce transactions: Airing into ad clicks, credit card management. In B. A. Pandow (Ed.), *Navigating the future of finance in the age of AI* (pp. 253–271). IGI Global Scientific Publishing.

Singh, B., Raghav, A., Ahmed, S., Arora, M. K., & Lal, S. (2025). Smearing machine learning and deep learning in e-commerce transactions for monetary justice: Crushing financial frauds and fostering strong financial institutions. In C. Kaunert, A. Raghav, K. Ravesangar, B. Singh, & B. A. Riswandi (Eds.), *Artificial intelligence in peace, justice, and strong institutions* (pp. 303–320). IGI Global Scientific Publishing.

Sood, P., Sharma, C., Nijjer, S., & Sakhuja, S. (2023). Review the role of artificial intelligence in detecting and preventing financial fraud using natural language processing. *International Journal of System Assurance Engineering and Management*, *14*(6), 2120–2135. https://doi.org/10.1007/s13198-023-02043-7

TransUnion. (2025). *H2 2025 update: Top fraud trends*. https://www.transunion.com/fraud-trends

Valencia, L. R., Ochoa Arellano, M. J., Gutiérrez Figueroa, S. A., Mur Nuño, C., Monsalve Piqueras, B., Corrales Paredes, A. D. V., Bemposta Rosende, S., López López, J. M., Puertas Sanz, E., & Levi Alfaroviz, A. (2025). A systematic review of artificial intelligence applied to compliance: Fraud detection in cryptocurrency transactions. *Journal of Risk and Financial Management*, *18*(11), Article e612. https://doi.org/10.3390/jrfm18110612

van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, *84*(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

Verma, J. (2022). Application of machine learning for fraud detection—A decision support system in the insurance sector. In K. Sood, B. Balusamy, S. Grima, & P. Marano (Eds.), *Big data analytics in the insurance market* (pp. 251–262). Emerald Publishing. https://doi.org/10.1108/978-1-80262-637-720221014

West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security*, *57*, 47–66. https://doi.org/10.1016/j.cose.2015.09.005

Yuhertiana, I., & Amin, A. H. (2024). Artificial intelligence driven approaches for financial fraud detection: A systematic literature review. *KnE Social Sciences*, *9*(20), 448–468. https://doi.org/10.18502/kss.v9i20.16551

Zakaria, R. M., Rahman, M. M., Choudhury, M. T. H., Rahman, H., & Rafi, M. A. (2025). Detecting financial fraud in real-time transactions using graph neural networks and anomaly detection techniques. *Journal of Economics, Finance and Accounting Studies*, *7*(6), 1–13.