

Systematic Review

Artificial Intelligence Techniques for Financial Fraud Detection: A Bibliometric Analysis of Scientific Development and Future Directions

Wasim Al-Shattarat ^{1,*} , Khalaf Alhaifi ² and Yara Ibrahim ³ 

¹ College of Business Administration, Gulf University for Science and Technology, Mubarak Al-Abdullah 32093, Kuwait

² State Audit Bureau, Shuwaikh 71661, Kuwait; khalafalhaifi@sab.gov.kw

³ Investment and Finance Department, Faculty of International Business and Humanities, Egypt-Japan University of Science and Technology, Alexandria 21934, Egypt; yara.magdy@ejust.edu.eg

* Correspondence: shattarat.w@gust.edu.kw

Abstract

This study examines the development and intellectual structure of artificial intelligence (AI)-based financial fraud detection through a bibliometric analysis of 2200 Scopus- and Web of Science-indexed journal articles published between 1992 and 2026. The literature has expanded rapidly, with 89.6% of publications appearing since 2018 and an annual growth rate of 29.4%. Research is concentrated in Computer Science and Engineering, whereas Business and Economics account for 9.2% of classified publications. Credit card and payment fraud constitutes the largest research domain (32.0%), followed by banking, loan, and transaction fraud (14.3%), insurance fraud (12.2%), and accounting and financial statement fraud (9.9%). Neural networks and deep learning, ensemble and boosting methods, and classical supervised classifiers are the dominant methodological families. The field has progressively shifted from traditional data-mining and classical machine-learning approaches toward deep learning, ensemble methods, graph neural networks, and explainable AI. Science mapping shows that the intellectual structure remains strongly centered on payment fraud, while accounting and insurance fraud form more distinct research fronts. Author productivity is highly dispersed, with 88.9% of authors contributing a single publication, while international collaboration varies considerably across leading countries. By integrating performance analysis, science mapping, fraud-domain classification, bibliometric laws, and publication-growth analysis, the study provides a comprehensive assessment of the field's development, intellectual structure, and emerging research directions.

Keywords: artificial intelligence; financial fraud detection; bibliometric analysis; machine learning; deep learning; science mapping



Academic Editors: Alessio Faccia and
Pythagoras Petratos

Received: 12 September 2026

Revised: 27 September 2026

Accepted: 3 October 2026

Published: 16 October 2026

Copyright: © 2026 by the authors.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

1. Introduction

Financial fraud has become one of the most significant challenges confronting governments, financial institutions, corporations, and regulatory authorities in the digital economy. The rapid expansion of electronic payment systems, online banking, mobile commerce, cryptocurrency transactions, and digital financial services has substantially increased the volume and complexity of financial transactions, creating unprecedented opportunities for fraudulent activities. Financial fraud encompasses a broad spectrum of illegal practices, including credit card fraud, financial statement manipulation, insurance

fraud, money laundering, identity theft, tax evasion, securities fraud, and cyber-enabled financial crimes. Beyond direct financial losses, fraud undermines market integrity, reduces investor confidence, increases compliance costs, and threatens financial system stability. Consequently, developing accurate and efficient fraud detection systems has become a strategic priority for both academia and industry (Ngai et al., 2011; Bao et al., 2020).

Traditional fraud detection methods primarily relied on manual auditing, expert judgment, statistical analysis, and predefined rule-based systems. Although these approaches proved effective in relatively stable environments, they exhibit considerable limitations when applied to modern financial systems characterized by massive transaction volumes, high-dimensional data, evolving fraud patterns, and increasingly sophisticated criminal behavior. Rule-based systems require continuous manual updates and often produce excessive false-positive rates because they cannot adapt effectively to emerging fraud strategies (Fawcett & Provost, 1997). Similarly, conventional statistical techniques generally assume linear relationships and balanced datasets, assumptions that rarely hold in real-world fraud detection problems where fraudulent transactions represent only a small proportion of total observations (Bhattacharyya et al., 2011).

Artificial intelligence (AI) addresses these limitations by learning fraud patterns directly from historical data rather than from manually specified rules. Supervised classifiers, ensemble methods, and deep learning architectures have been applied to transaction, accounting, and insurance data, while anomaly detection and semi-supervised methods respond to the scarcity of labeled fraud cases (Bhattacharyya et al., 2011; Perols, 2011; Jurgovsky et al., 2018; Pourhabibi et al., 2020).

These technological advances have stimulated an extraordinary expansion of academic research. Since the early contributions of Fawcett and Provost (1997) and Chan et al. (1999), the literature has evolved from rule-based and data-mining approaches toward sophisticated machine-learning and deep-learning frameworks. During the last decade, research has diversified further through the incorporation of graph neural networks, explainable artificial intelligence, ensemble learning, federated learning, blockchain integration, and hybrid intelligent systems. This rapid methodological evolution reflects both advances in AI algorithms and the increasing complexity of fraudulent financial behavior.

The literature has also produced several narrative and systematic reviews summarizing methodological developments. Ngai et al. (2011) proposed one of the earliest comprehensive reviews by classifying data mining techniques used in financial fraud detection and identifying major application domains. Pourhabibi et al. (2020) later reviewed graph-based anomaly detection methods and highlighted the growing importance of graph learning for identifying complex fraud networks. Although these reviews offer valuable methodological insights, they focus mainly on algorithmic developments or specific fraud detection techniques. They offer limited evidence on the field's overall evolution, global collaboration patterns, influential authors and institutions, knowledge diffusion, thematic development, and emerging research frontiers.

Moreover, the literature has expanded substantially following these reviews. Numerous studies have introduced advanced deep learning architectures (Fiore et al., 2019; Esenogho et al., 2022), optimized ensemble learning models (Taha & Malebary, 2020), graph-based detection techniques (Pourhabibi et al., 2020), and machine learning approaches for accounting fraud (Bao et al., 2020). Consequently, the current state of knowledge has become increasingly fragmented across disciplines, publication outlets, institutions, and countries. Understanding how the field has evolved, identifying its intellectual foundations, and recognizing emerging research directions, therefore, requires a comprehensive bibliometric investigation rather than another traditional literature review.

Bibliometric analysis offers a quantitative approach for evaluating the development of a scientific field by combining performance analysis with science mapping (Aria & Cucurullo, 2017; Donthu et al., 2021; Zupic & Čater, 2015). Such analyses identify influential contributors, dominant research themes, and emerging directions across large publication collections. Their value, however, depends on the transparency of corpus construction, because retrieval strategies, deduplication rules, relevance screening, and preprocessing choices can materially alter rankings and network structures. The present study therefore emphasizes documenting and validating these decisions.

Accordingly, this study conducts a bibliometric analysis of research on artificial intelligence for financial fraud detection, based on journal articles indexed in the Scopus and Web of Science databases between 1992 and 2026. Specifically, the study addresses the following research questions: (1) How has research on AI-based financial fraud detection evolved over time, and how reliably can its future growth be projected? (2) Which authors, journals, institutions, and countries have made the greatest scientific contributions? (3) What are the intellectual, conceptual, and collaborative structures that characterize the field? (4) How is research distributed across financial fraud domains and methodological families? (5) Which research themes show measurable acceleration, and what do the findings imply for finance, accounting, auditing, and financial regulation?

This study contributes to the literature on AI-based financial fraud detection in several ways. First, it provides a comprehensive mapping of the field from 1992 to 2026, combining performance analysis and science mapping to document publication growth, influential authors, sources, institutions, countries, intellectual foundations, and conceptual development. Second, it extends the bibliometric assessment beyond publication and citation patterns by examining the distribution of research across distinct financial fraud domains and methodological families, revealing the extent to which the literature is concentrated in credit card and payment fraud relative to accounting fraud, insurance fraud, banking fraud, money laundering, tax fraud, and securities fraud. Third, the study combines established bibliometric laws with statistical assessment of publication growth and out-of-sample validation, allowing it to distinguish historical growth patterns from the reliability of longer-term projections. Fourth, the analysis identifies the field's thematic evolution and highlights emerging areas, particularly explainable AI and graph neural networks, alongside persistent themes such as neural networks, ensemble learning, class imbalance, and anomaly detection. Finally, the study connects these research patterns to the economic and institutional dimensions of fraud detection, highlighting issues such as false-alarm costs, model risk, information asymmetry, and the trade-off between predictive performance and explainability for financial institutions, auditors, and regulators.

The remainder of the paper is organized as follows. The next section reviews the theoretical foundations and technological evolution of artificial intelligence in financial fraud detection and outlines the study's economic perspective. The methodology section then describes the search strategy, corpus construction, harmonization procedures, and analytical settings. The results section presents the performance analysis, the distribution of research across fraud domains, the bibliometric laws, the growth models, and the science mapping result. The discussion interprets these findings for finance, auditing, and regulation, and the final section summarizes the conclusions, limitations, and directions for future research.

2. Literature Review

Financial fraud has become increasingly sophisticated as digital technologies have transformed the global financial ecosystem. The widespread adoption of electronic banking, online payment systems, e-commerce, mobile financial services, and digital assets

has substantially increased both the frequency and complexity of fraudulent activities. Financial fraud generally refers to intentional deception undertaken to obtain unlawful financial benefits through unauthorized transactions, manipulation of financial information, identity theft, insurance claims, or financial statement misrepresentation. The economic consequences extend beyond direct monetary losses, affecting organizational performance, market confidence, regulatory compliance, and financial stability. Consequently, fraud detection has become one of the most important AI applications in the financial sector (Ngai et al., 2011).

Among the diverse branches of artificial intelligence, machine learning has become the dominant methodological framework for financial fraud detection. Machine learning enables computers to construct predictive models by identifying statistical patterns within historical data rather than relying on explicit programming. The increasing availability of large-scale financial datasets, together with advances in computational power, has accelerated the adoption of machine learning algorithms across banking, insurance, accounting, taxation, and payment systems. Compared with traditional statistical models, machine learning algorithms generally perform better at modeling nonlinear relationships, complex interactions, and high-dimensional financial data (Bhattacharyya et al., 2011; Perols, 2011).

Machine learning techniques generally fall into supervised, unsupervised, semi-supervised, and reinforcement learning paradigms. Supervised learning remains the most widely used approach because historical financial datasets often contain labeled observations indicating whether transactions are legitimate or fraudulent. During model training, algorithms learn the relationship between predictor variables and known class labels before classifying previously unseen transactions. Widely adopted supervised learning algorithms include logistic regression, decision trees, support vector machines, random forests, gradient boosting, and extreme gradient boosting. Numerous empirical studies have demonstrated that these algorithms outperform traditional statistical methods across various fraud detection applications, including credit card fraud, financial statement manipulation, and accounting fraud (Bhattacharyya et al., 2011; Perols, 2011; Bao et al., 2020).

Despite their effectiveness, supervised learning approaches face important practical limitations because accurately labeled fraud data are often scarce, expensive to obtain, and highly imbalanced. In most financial datasets, fraudulent transactions constitute less than one percent of all observations, causing classification models to become biased toward the majority class. Consequently, researchers have increasingly explored alternative learning paradigms that can identify fraudulent behavior without relying exclusively on labeled observations.

Unsupervised learning addresses this limitation by discovering hidden structures and abnormal behavioral patterns directly from unlabeled datasets. Instead of predicting predefined classes, unsupervised algorithms identify observations that differ substantially from normal transaction behavior. This capability has made anomaly detection one of the most influential research directions in financial fraud detection. Goldstein and Uchida (2016) demonstrated that anomaly detection algorithms effectively identify unusual multi-variate observations without requiring prior knowledge of fraudulent activities. Similarly, Pourhabibi et al. (2020) emphasized that anomaly detection has become particularly important for identifying previously unseen fraud strategies because it focuses on behavioral deviations rather than historical fraud labels.

Anomaly detection itself represents a broader analytical framework rather than a specific algorithm. The underlying principle assumes that fraudulent transactions differ from legitimate ones and therefore appear as statistical outliers in multidimensional feature spaces. Depending on the application, anomalies may occur as individual observations, contextual deviations, or collective behavioral patterns involving groups of transactions.

Various unsupervised algorithms have therefore been developed to identify these abnormal observations, including clustering techniques, autoencoders, one-class support vector machines, isolation-based algorithms, and graph-based anomaly detection methods (Goldstein & Uchida, 2016).

Between supervised and unsupervised learning lies semi-supervised learning, which combines a relatively small number of labeled observations with a substantially larger collection of unlabeled data. This approach is particularly attractive in fraud detection because obtaining verified fraud labels requires extensive investigation by financial institutions (Dal Pozzolo et al., 2014). Semi-supervised algorithms exploit both labeled and unlabeled information to improve classification performance while reducing dependence on costly manual annotations (Pourhabibi et al., 2020). Consequently, semi-supervised methods have become increasingly important for highly imbalanced fraud datasets where labeled fraudulent transactions remain limited (Bhattacharyya et al., 2011; Pourhabibi et al., 2020).

The shift from traditional rule-based systems to machine learning and anomaly detection reflects a broader transition in fraud detection research from manually designed, knowledge-based systems to adaptive, data-driven intelligence (Fawcett & Provost, 1997; Ngai et al., 2011). However, the rapid growth of transaction data, increasing feature complexity, and continuous emergence of new fraud patterns have exposed additional limitations of conventional machine learning algorithms (Whitrow et al., 2009; Dal Pozzolo et al., 2014; Bahnsen et al., 2016). These challenges have encouraged the adoption of deep learning architectures that can automatically extract hierarchical representations from large-scale financial data (Pumsirirat & Yan, 2018; Jurgovsky et al., 2018; Fiore et al., 2019). This has enabled a new generation of intelligent fraud detection systems that increasingly dominate contemporary research (Forough & Momtazi, 2021; Alarfaj et al., 2022; Esenogho et al., 2022).

Beyond its technical dimension, fraud detection is an economic problem. Fraud arises in settings characterized by information asymmetry, where one party has private information about the legitimacy of a transaction, claim, or financial report that the counterparty cannot directly observe (Akerlof, 1970). The economic approach to crime further suggests that the incidence of fraud depends on the expected probability of detection and the magnitude of sanctions, so that improvements in detection technology alter the incentives of potential offenders rather than only the number of identified cases (Becker, 1968). From this perspective, the value of an AI-based detection system depends not on classification accuracy alone, but on the expected costs of undetected fraud, the costs of investigating false alarms, and the reputational and customer-experience costs of declining legitimate transactions (Bahnsen et al., 2016; Sahin et al., 2013).

These considerations are reinforced by the institutional environment in which financial institutions operate. Detection models used by banks and insurers are subject to model risk management expectations that require conceptual soundness, ongoing monitoring, and effective challenge (Board of Governors of the Federal Reserve System & Office of the Comptroller of the Currency, 2011), and recent regulation of AI systems in financial services emphasizes transparency, human oversight, and documentation (Regulation (EU) 2024/1689, 2024). In accounting and auditing, researchers studied the detection of material misstatements through financial ratio models before the diffusion of machine learning (Dechow et al., 2011), and recent evidence indicates that machine learning applied to raw accounting data can improve out-of-sample detection of accounting fraud (Bao et al., 2020). These economic and institutional dimensions provide the interpretive lens through which this study discusses the bibliometric findings.

Figure 1 presents a conceptual overview of the evolution and taxonomy of artificial intelligence techniques applied to financial fraud detection. The framework illustrates

the progression from traditional rule-based and statistical approaches to modern artificial intelligence paradigms, including machine learning, deep learning, and emerging intelligent technologies. It further categorizes machine learning into supervised, unsupervised, semi-supervised, and reinforcement learning, highlighting representative algorithms, data sources, fraud application domains, evaluation metrics, and current research directions. The figure provides a unified conceptual framework that summarizes the theoretical foundations and technological evolution discussed in the literature, demonstrating how advances in artificial intelligence have contributed to increasingly accurate, adaptive, and intelligent financial fraud detection systems.

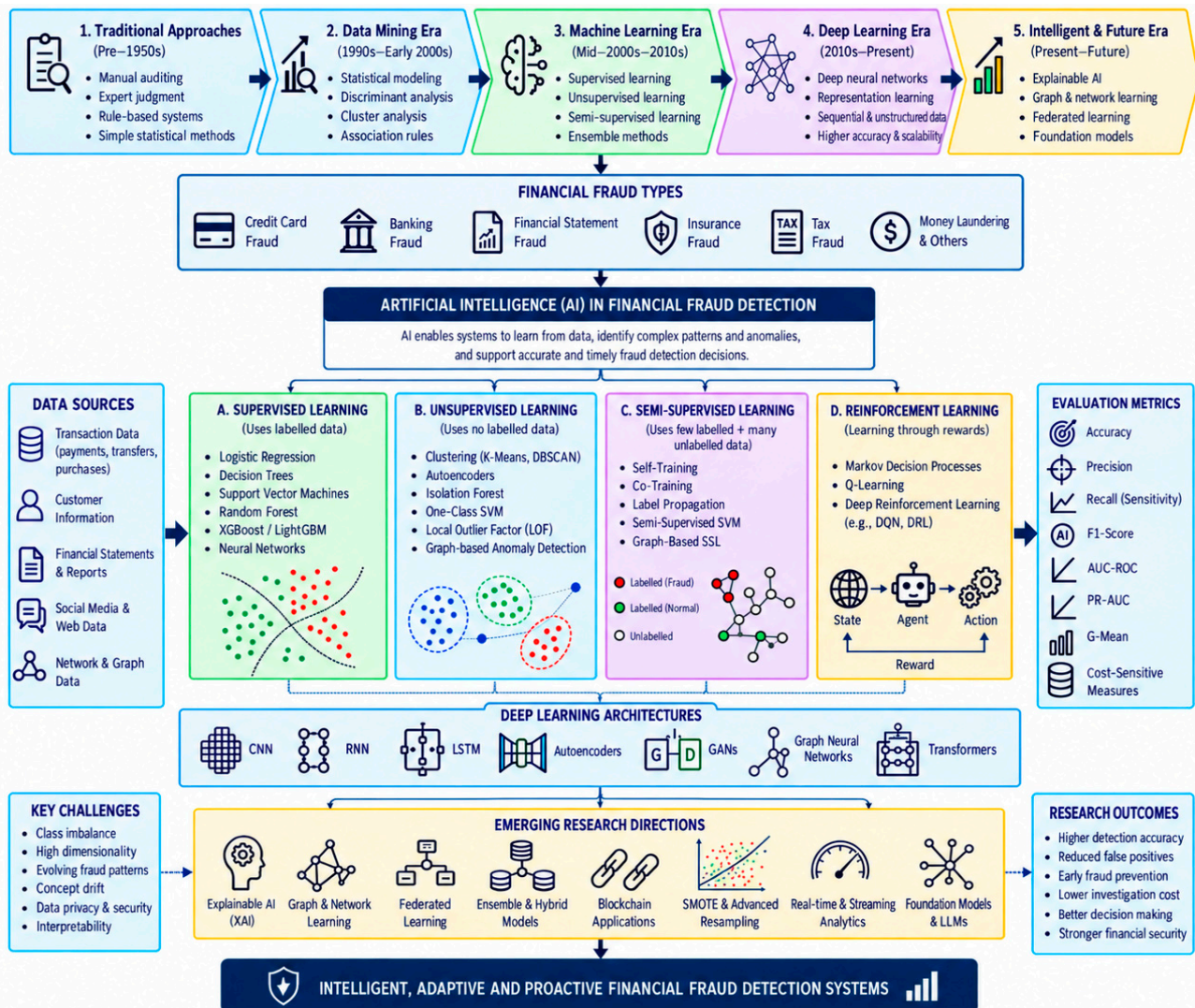


Figure 1. Evolution and Taxonomy of Artificial Intelligence Techniques in Financial Fraud Detection.

3. Methodology

3.1. Research Design

This study adopts a quantitative bibliometric research design to systematically examine the evolution, intellectual structure, conceptual development, and collaborative patterns of research on artificial intelligence (AI) in financial fraud detection. Bibliometric analysis has become one of the most widely accepted approaches for synthesizing large bodies of scientific literature because it provides an objective, transparent, and reproducible framework for evaluating scientific productivity, research impact, and knowledge development (Zupic & Čater, 2015; Donthu et al., 2021). Unlike traditional narrative reviews,

bibliometric methods use statistical indicators and network-based techniques to analyze publication patterns, citation relationships, collaboration structures, and thematic evolution across large collections of scientific documents.

This study's methodological framework combines performance analysis with science mapping techniques. Performance analysis evaluates the scientific productivity and impact of authors, journals, institutions, countries, and publications using established bibliometric indicators, whereas science mapping investigates the intellectual, conceptual, and social structures of the research field through network analyses and visualization techniques. Figure 2 illustrates the overall research procedure, summarizing the workflow from database selection and search strategy development to data screening, bibliometric analysis, and visualization following the PRISMA 2020 checklist in the Supplementary Materials.

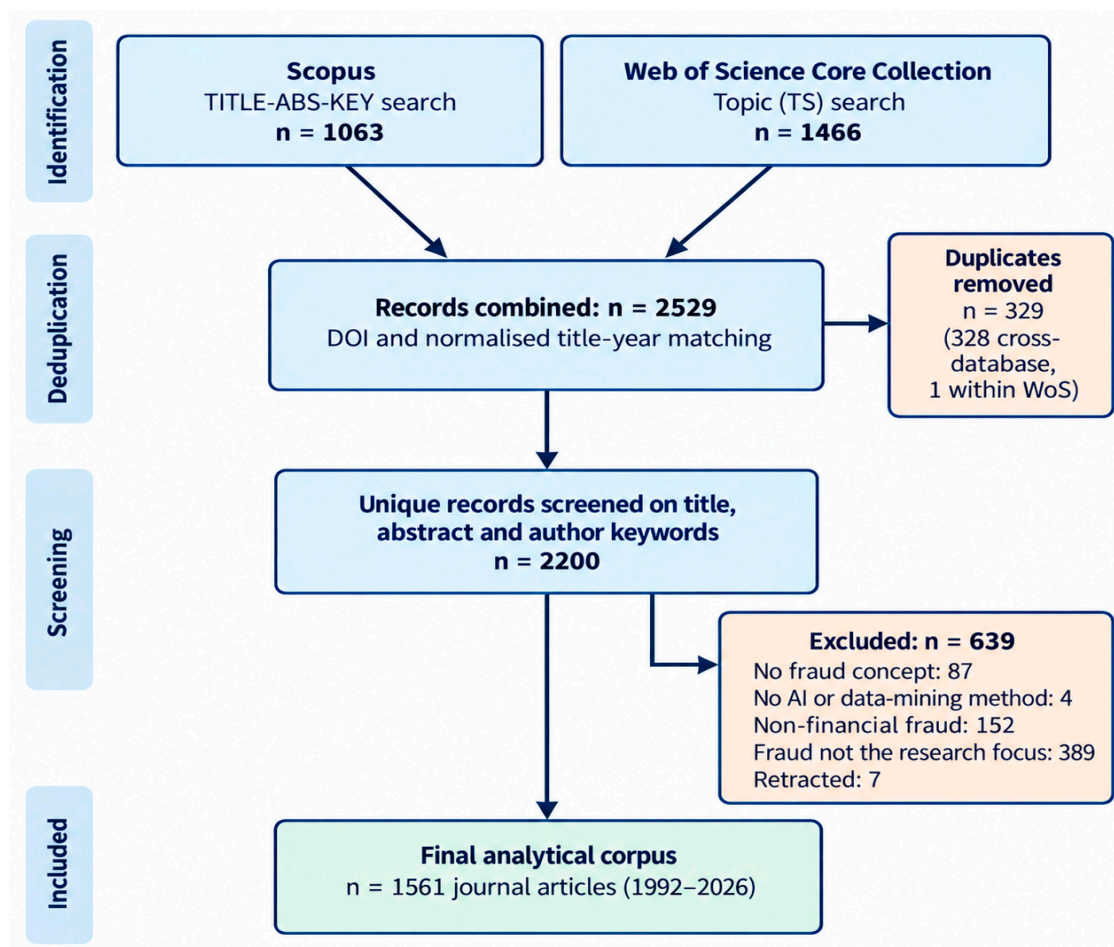


Figure 2. Bibliometric Study Flow Diagram.

3.2. Data Collection

We compiled the bibliometric dataset from the Scopus and Web of Science Core Collection (WoS) databases, recognized as the most comprehensive multidisciplinary citation databases and widely used in bibliometric research because of their extensive journal coverage and high-quality indexing (Mongeon & Paul-Hus, 2016). Combining these databases reduces database-specific bias while increasing the comprehensiveness and reliability of the retrieved literature.

We conducted searches in both databases on 29 June 2026. We imposed no lower publication-year limit; the earliest retrieved record dates to 1992, so the observation window extends from 1992 to 29 June 2026, and we treat 2026 as an incomplete publication year. We restricted the document type to articles and applied no language restriction. The Scopus

search used the TITLE-ABS-KEY field (titles, abstracts, author keywords, and indexed keywords), and the Web of Science search used the Topic (TS) field (titles, abstracts, author keywords, and Keywords Plus).

3.3. Search Strategy

A comprehensive Boolean search strategy was developed by combining fraud-related terminology with keywords from artificial intelligence and machine learning. The search query consisted of two principal keyword groups linked with the Boolean operator AND, with keywords within each group connected with the operator OR. Mathematically, the search strategy can be expressed as

$$Q = \left(\bigvee_{i=1}^m F_i \right) \wedge \left(\bigvee_{j=1}^n AI_j \right),$$

where Q denotes the complete search query, F_i represents the set of fraud-related keywords, and AI_j denotes the set of artificial intelligence and machine learning terms.

The fraud-related search terms included “fraud detection,” “financial fraud,” “credit card fraud,” “insurance fraud,” “bank fraud,” “accounting fraud,” “financial statement fraud,” “cyber fraud,” and “transaction fraud.” These were combined with artificial intelligence terms such as “artificial intelligence,” “machine learning,” “deep learning,” “neural network,” “convolutional neural network,” “recurrent neural network,” “graph neural network,” “transformer,” “support vector machine,” “decision tree,” “random forest,” “XGBoost,” “LightGBM,” “gradient boosting,” “logistic regression,” “anomaly detection,” “data mining,” “predictive analytics,” “natural language processing,” and “explainable AI.” Database-specific syntax was employed to ensure consistency between Scopus and Web of Science searches. The exact database-specific search strings and filters are reported in Appendix A, Table A1.

3.4. Data Screening and Preparation

The literature selection process followed the workflow presented in Figure 2. The database exports contained 1063 Scopus records and 1466 Web of Science records, of which 2500 records (1059 from Scopus and 1441 from the Web of Science Core Collection) were retained when the files were imported into BiblioSpy®. After merging the two datasets, duplicate detection identified 300 cross-database duplicates, while no duplicates were detected within the individual databases. Consequently, 2200 unique publications remained for subsequent analysis. The final analytical dataset therefore comprised 2200 publications.

We then applied two verification procedures to the analytical dataset. First, duplicates were re-examined by matching records on normalized DOIs and on normalized titles with publication years differing by no more than one year. This check identified 27 residual cross-database pairs (1.2% of the records) that had not been merged by the software because one version lacked a DOI or used a different title capitalization, including the Scopus and Web of Science versions of Ngai et al. (2011) and Chan et al. (1999). We merged these pairs in the tables of highly cited publications and historiograph nodes and assessed their effect on the aggregate indicators. Second, because keyword retrieval alone does not ensure that every record address AI-based financial fraud detection, we screened the titles, abstracts, and author keywords of the deduplicated records against explicit relevance criteria, using rule-based flagging followed by manual review of flagged titles and the most highly cited records.

Before conducting the bibliometric analyses, the merged dataset underwent several preprocessing procedures to improve data consistency. These procedures included dupli-

cate verification, author name disambiguation, journal title standardization, affiliation harmonization, country normalization, and keyword cleaning. Synonymous author keywords and spelling variants were merged to ensure consistency in the subsequent co-occurrence and thematic analyses (Aria & Cuccurullo, 2017). Only author-provided keywords were used for the co-occurrence, trend, and clustering analyses; Scopus-indexed keywords and Web of Science Keywords Plus were not used because databases assign them rather than authors, and they are not consistently available across both sources (J. Zhang et al., 2016).

3.5. Bibliometric Analysis

The bibliometric analysis was conducted using BiblioSpy® (Ahmi, 2026), an integrated platform that combines descriptive performance indicators, science mapping techniques, bibliometric laws, and predictive modeling in a single analytical environment. The software supports comprehensive quantitative assessments of scientific literature and offers advanced visualization tools for exploring the evolution and structure of research domains. Following the framework proposed by Donthu et al. (2021), the analysis consisted of two complementary components: performance analysis and science mapping. Performance analysis evaluates scientific productivity and research impact using descriptive bibliometric indicators, whereas science mapping investigates the relationships among publications, authors, journals, institutions, countries, and research themes through network-based techniques. Integrating these complementary approaches provides a comprehensive understanding of both the quantitative development and the knowledge structure of AI research in financial fraud detection.

3.6. Performance Analysis

Performance analysis evaluated the literature's productivity and scientific impact across multiple bibliometric units, including publications, journals, authors, institutions, and countries. Publication productivity was assessed using annual publication counts and cumulative publication growth, whereas scientific influence was evaluated through total citations, average citations per publication, average citations per cited publication, and citation trends over time.

We further evaluated author and journal performance using the h-index, g-index, m-index, and e-index. The h-index measures the number of publications receiving at least h citations, thereby combining productivity and citation impact (Hirsch, 2005). The g-index extends the h-index by weighting highly cited publications more heavily (Egghe, 2006), while the m-index normalizes the h-index by academic age to facilitate comparisons across researchers with different career lengths. The e-index complements the h-index by capturing excess citations beyond the h-core (C. T. Zhang, 2009). Additional analyses examined annual citation dynamics, journal quality by quartile rankings, publication life-cycle characteristics, subject-area distribution, leading journals, influential authors, highly cited publications, and emerging publication sources.

3.7. Science Mapping Analysis

Science mapping techniques were employed to reveal the conceptual, intellectual, and social structures of the AI-based financial fraud detection literature. The social structure of the field was examined using co-authorship networks at the author and country levels to identify collaboration patterns and research communities.

The intellectual structure was investigated using citation analysis, Reference Publication Year Spectroscopy (RPYS), and a historiograph. RPYS identifies historically influential publication years by comparing the number of cited references in each year with the median of neighboring years (Marx et al., 2014), and the historiograph traces direct citation links among the publications with the highest local citation counts, that is, citations received

from other publications in the dataset (Garfield, 2004). Local citations were verified by matching cited references to dataset records through the first-author surname, publication year, volume and first page, the DOI, or the normalized title combined with the first-author surname and year.

The conceptual structure of the literature was explored through author keyword co-occurrence analysis, trend topic analysis, the classification of emerging topics, and hierarchical clustering of keywords. Keyword co-occurrence networks identify relationships among frequently occurring concepts, trend topic analysis locates each keyword over time using quartiles of publication years, and keyword clustering groups concepts that tend to occur in the same publications.

3.8. Bibliometric Laws and Growth Modeling

To examine the literature's structural characteristics, three classical bibliometric laws were employed. Bradford's Law was applied to identify the core journals contributing to AI-based financial fraud detection research (Bradford, 1934). The cumulative distribution of articles across ranked journals is represented as

$$C(r) = a + b \ln(r),$$

where $C(r)$ denotes the cumulative number of publications, r represents journal rank, and a and b are estimated model parameters. The Bradford multiplier was subsequently estimated to determine the expansion of journal zones and the concentration of publications among core journals (Bradford, 1934). Because the log-linear form is only an approximation of Bradford's formulation, the observed zone sizes were also compared with the theoretical ratio $1:k:k^2$, where the multiplier was estimated as $k = (e^\gamma \times Y_m)^{(1/p)}$, with γ denoting Euler's constant, Y_m the number of articles in the most productive source, and $p = 3$, the number of zones (Egghe, 1986). The Kolmogorov–Smirnov distance is interpreted descriptively, because the parameters are estimated from the same ranked and non-independent observations.

Author productivity was evaluated using Lotka's inverse power law, expressed as

$$y = \frac{C}{x^n},$$

where y represents the proportion of authors publishing x documents, c is a normalization constant, and n denotes the productivity exponent (Lotka, 1926). The exponent was estimated by least squares following Pao (1985) and, because least squares on log-log data are biased for power-law distributions, also by maximum likelihood for a discrete power law (Clauset et al., 2009). We evaluated conformity with the Kolmogorov–Smirnov test using Pao's critical values and, for the maximum likelihood estimate, with a parametric bootstrap of 500 samples that accounts for parameter estimation.

The distribution of author keywords was examined according to Zipf's Law,

$$f(r) = \frac{k}{r^\alpha},$$

where $f(r)$ represents the frequency of the keyword ranked r , k is a scaling constant, and α is the distribution exponent (Zipf, 1949). This analysis helps identify dominant concepts and the degree of concentration within the field's conceptual structure.

To evaluate the maturity of the research field and estimate its future development, publication growth was modeled using the logistic growth function,

$$P(t) = \frac{K}{1 + e^{-r(t-t_0)}},$$

where $P(t)$ denotes the cumulative number of publications at time t , K is the estimated saturation level, r represents the intrinsic growth rate, and t_0 is the inflection point corresponding to the year of maximum publication growth. Because we identify the saturation level only when the observed series approaches its inflection point, we compared the logistic model with Gompertz and exponential models. All models were fitted by nonlinear least squares to cumulative publications for the complete years 1992 to 2025; the incomplete year 2026 was excluded from estimation and used only in a sensitivity analysis. We evaluated model adequacy using the coefficient of determination, root mean square error (RMSE), Akaike Information Criterion (AIC), and Bayesian Information Criterion (BIC). Forecast accuracy was evaluated out of sample with rolling-origin validation, in which each model was re-estimated with data ending in each year from 2015 to 2020 and used to forecast annual publications one to five years ahead, and the mean absolute percentage error (MAPE) was compared with a naive benchmark (Tashman, 2000; Hyndman & Athanasopoulos, 2021).

3.9. Data Visualization

The bibliometric findings were visualized through a comprehensive set of statistical tables, temporal trend analyses, citation maps, collaboration networks, Sankey diagrams, three-field plots, Bradford distributions, Lotka distributions, subject-area maps, and publication growth forecasts generated using BiblioSpy® (Ahmi, 2026). These visualizations help interpret publication dynamics, collaboration structures, topic trends, intellectual foundations, and emerging research frontiers. Together, performance indicators and science mapping techniques provide a comprehensive representation of the evolution and current state of AI research in financial fraud detection, while also identifying promising directions for future investigation.

4. Results and Discussion

4.1. Bibliometric Overview of the Research Field

Table 1 presents the overall bibliometric profile of AI research in financial fraud detection. The dataset comprises 2200 publications from 1992 to 2026, with an annual growth rate of 24.59%, indicating rapid field expansion. The literature has accumulated 52,679 citations, averaging 23.95 citations per publication, demonstrating substantial scientific impact. The field is highly collaborative, with 7707 contributing authors from 2536 institutions across 106 countries, an average of 3.5 authors per paper, and a 65.59% international co-authorship rate. Furthermore, the h-index (101) and g-index (163) indicate numerous highly influential publications.

4.2. Scientific Growth and Evolution of the Literature

4.2.1. Annual Publication and Citation Trends

Table 2 and Figures 3 and 4 illustrate the annual evolution of AI research in financial fraud detection. The field remained relatively small until 2017, followed by a rapid increase in publications from 2018 onward. Annual output reached 445 publications in 2025, highlighting the field's accelerated growth. Citation performance peaked for earlier publications, particularly those from 2018 to 2022, reflecting their greater citation maturity. The three-field plot (Figure 3) further demonstrates the strong relationships among leading countries, influential authors, and dominant research topics.

Table 1. Bibliometric Summary.

Indicator	Value
Timespan	1992:2026
Total Publications (TP)	2200
Citable Year Span	35 years
Annual Growth Rate	24.59%
Document Average Age	4.53 years
Total Citations (TC)	52,679
Average Citations per Document	23.95
Number of Cited Papers (NCP)	1819
Average Citations per Cited Paper	28.96
Average Citations per Year	1505.11
Total Contributing Authors	7707
Total Unique Authors	6612
Total Institutions	2536
Total Countries	106
Single-Authored Documents	172
Average Authors per Paper	3.5
International Co-authorship Rate	65.59%
Unique Author Keywords	3910
Total References	183,663
h-index	101
g-index	163
m-index	2.886
Citation Sum within h-Core	21,322

Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

Table 2. Yearly Bibliometric Statistics.

Year	TP	NCA	NCP	TC	C/P	C/CP	h	g	m	e
2026	199	652	47	126	0.63	2.68	5	7	0.143	4.36
2025	445	1570	317	2392	5.38	7.55	24	33	0.706	19
2024	312	1066	283	4498	14.42	15.89	35	51	1.061	30.46
2023	291	978	272	5867	20.16	21.57	42	61	1.312	37.2
2022	216	749	203	6752	31.26	33.26	43	74	1.387	51.55
2021	170	611	166	4983	29.31	30.02	38	63	1.267	42.7
2020	131	382	122	4740	36.18	38.85	35	65	1.207	48.95
2019	91	289	85	2554	28.07	30.05	29	48	1.036	33.41
2018	63	228	60	3295	52.3	54.92	30	57	1.111	44.79
2017	33	96	30	1563	47.36	52.1	16	33	0.615	35.1
2016	21	60	20	1518	72.29	75.9	13	21	0.52	36.04
2015	22	63	21	1015	46.14	48.33	12	22	0.5	28.93
2014	19	74	17	828	43.58	48.71	10	19	0.435	26.46
2013	15	46	14	932	62.13	66.57	9	15	0.409	28.6
2012	25	86	24	1014	40.56	42.25	17	25	0.81	26.12
2011	23	68	23	4128	179.48	179.48	16	23	0.8	61.68
2010	16	48	15	390	24.38	26	8	16	0.421	17.12
2009	20	63	19	898	44.9	47.26	15	20	0.833	25.65
2008	17	43	16	494	29.06	30.88	9	17	0.529	19.36
2007	7	22	5	588	84	117.6	5	7	0.312	23.73
2006	20	63	18	839	41.95	46.61	11	20	0.733	26.15
2005	6	16	6	270	45	45	5	6	0.357	15.59
2004	13	36	12	527	40.54	43.92	9	13	0.692	20.81
2003	3	8	2	196	65.33	98	2	3	0.167	13.86
2002	3	8	3	172	57.33	57.33	3	3	0.273	12.77

Note: TP = Total Publications; NCA = Number of Contributing Authors; NCP = Number of Cited Publications; TC = Total Citations; C/P = Citations per Publication; C/CP = Citations per Cited Publication; h = h-index; g = g-index; m = m-Quotient; e = e-index. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

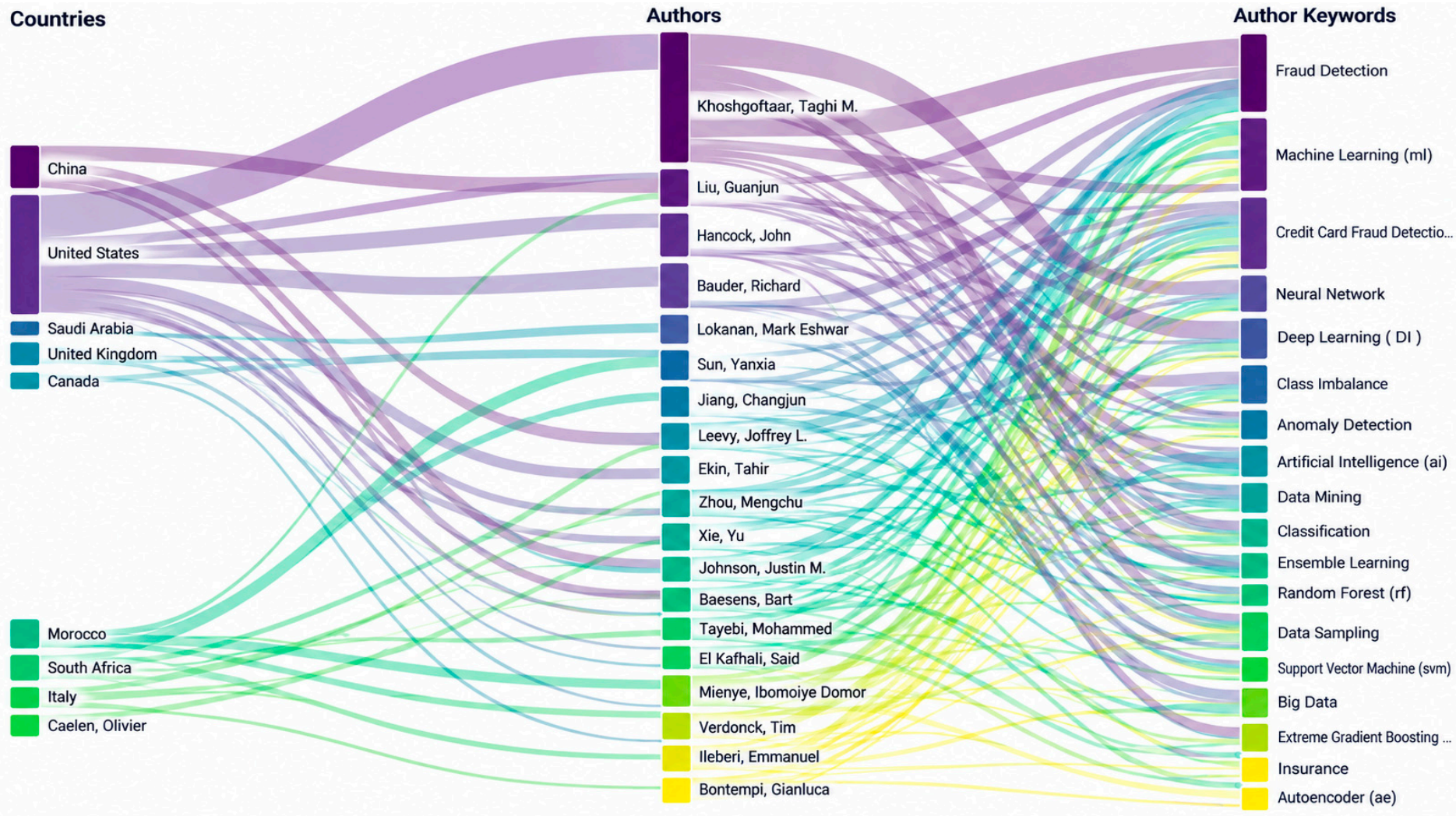


Figure 3. Three-Field Plot. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

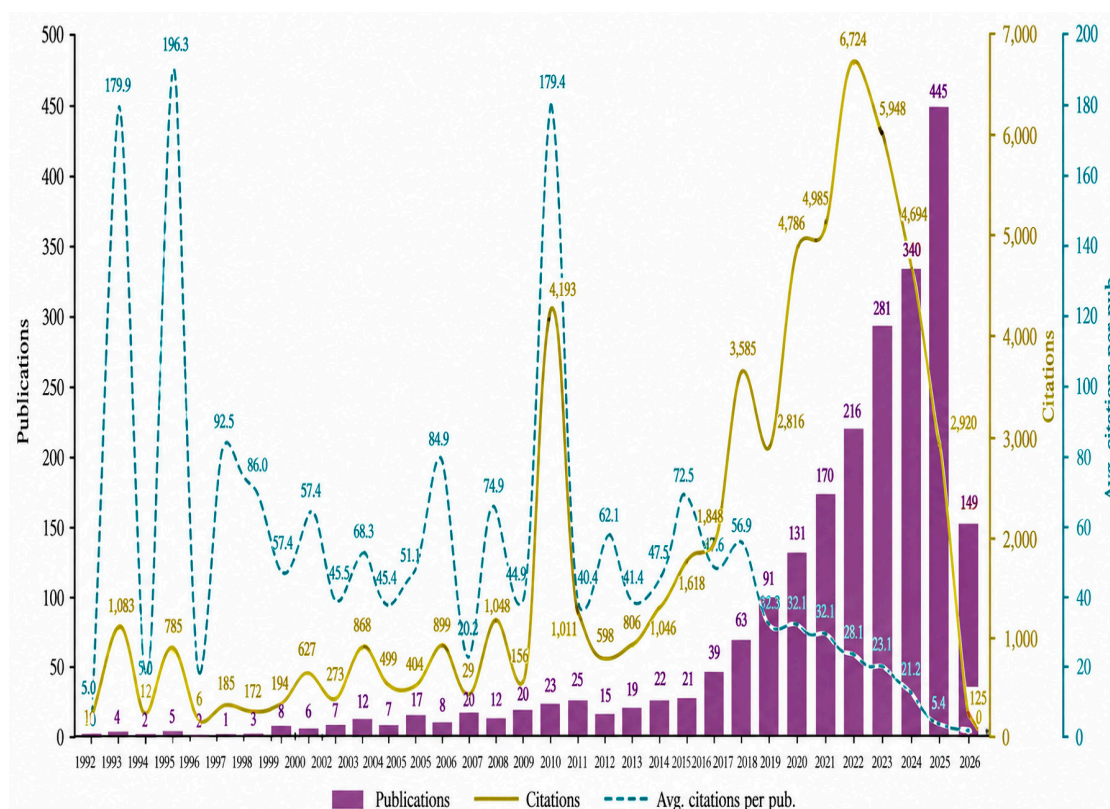


Figure 4. Annual Publications & Citations. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

4.2.2. Relative Citation Impact

Figure 5 presents the Relative Citation Impact (RCI) across publication years. Earlier publications generally show higher citation impact because they have had longer exposure within the scientific community, whereas recent publications show lower citation averages because they have had less time to accumulate citations. Nevertheless, the increasing publication volume indicates sustained scholarly interest and continued expansion of the research field.

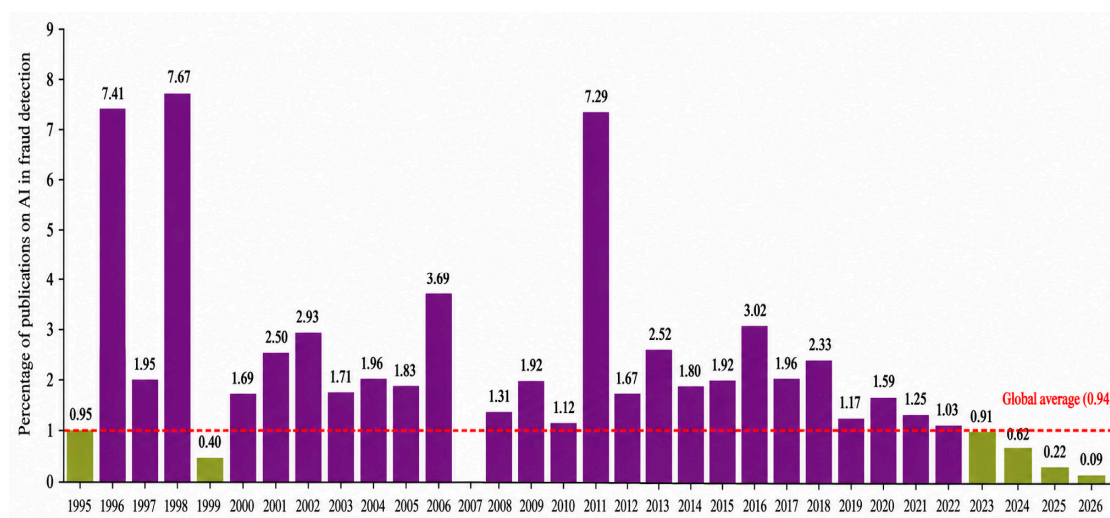


Figure 5. Relative Citation Impact (RCI). Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

4.2.3. Journal Quality Evolution

Table 3 and Figure 6 show the distribution of publications across journal quartiles over time. The majority of recent studies have been published in Q1 and Q2 journals. In 2025 alone, 313 publications appeared in Q1 and Q2 journals, indicating that research on AI-based financial fraud detection is increasingly being disseminated through high-impact publication outlets.

Table 3. Quartile Summary by Year.

Year	Q1	Q2	Q3	Q4	No Q	Total
2026	84	52	45	16	2	199
2025	151	162	64	50	18	445
2024	94	107	54	27	30	312
2023	78	85	64	30	34	291
2022	61	67	41	16	31	216
2021	44	61	36	11	18	170
2020	32	41	22	11	25	131
2019	22	26	13	8	22	91
2018	19	16	10	5	13	63
2017	12	4	5	4	8	33
2016	8	2	3	1	7	21
2015	6	6	5	3	2	22
2014	7	1	4	1	6	19
2013	6	5	2	0	2	15
2012	13	3	4	1	4	25
2011	10	4	4	3	2	23
2010	5	5	1	2	3	16
2009	9	6	2	0	3	20
2008	7	2	5	2	1	17
2007	2	1	1	2	1	7
2006	5	5	2	1	7	20
2005	1	1	1	0	3	6
2004	2	5	0	1	5	13
2003	1	1	0	0	1	3
2002	0	2	1	0	0	3

Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

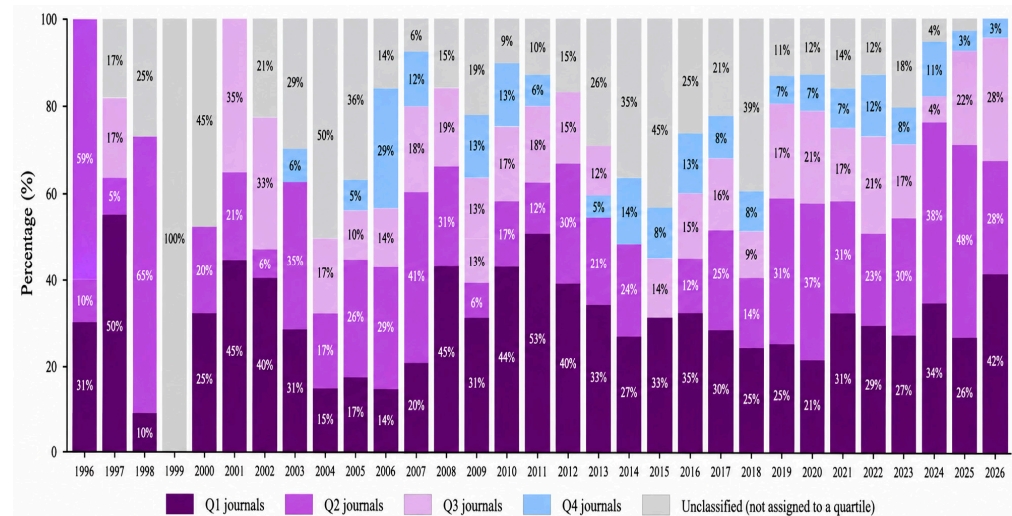


Figure 6. Publication by Quartile per Year. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

4.2.4. Research Life Cycle and Growth Forecast

Table 4 and Figures 7 and 8 report the growth models, estimated for the full period 1992 to 2025. The exponential and logistic models fit the historical series almost identically ($R^2 = 0.994$), and the exponential model is preferred by both information criteria ($AIC = 248.76$ versus 250.77). The logistic Model, however, is saturated: its estimate moves to the upper bound of the parameter space with an unbounded standard error, and fixing the saturation level anywhere between 10,000 and 1,000,000 publications changes R^2 only in the third decimal place while moving the shifted midpoint from 2030 to 2052. Rolling-origin validation further shows that none of the models forecast reliably beyond the short term: averaged over forecast origins from 2015 to 2020 and horizons of one to five years, the MAPE is 50.0% for the exponential model, 59.3% for the naive benchmark, 68.5% for the Gompertz model and 74.7% for the logistic model. The literature therefore remains in a strong growth phase, with an estimated growth rate of 0.232 per year (bootstrap 95% interval 0.221 to 0.246), equivalent to 26.1% annual growth and a doubling time of about three years. Long-term figures are not reported as forecasts; if the historical rate persisted, annual output would reach approximately 817 publications in 2028 (bootstrap interval 740 to 908), but this projection is highly assumption dependent.

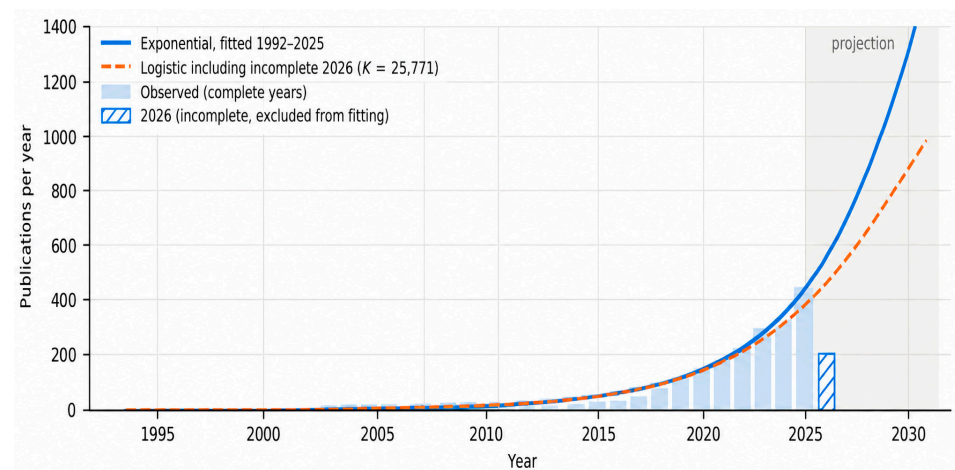


Figure 7. Observed annual publications and fitted growth curves (2026 incomplete and excluded from fitting).

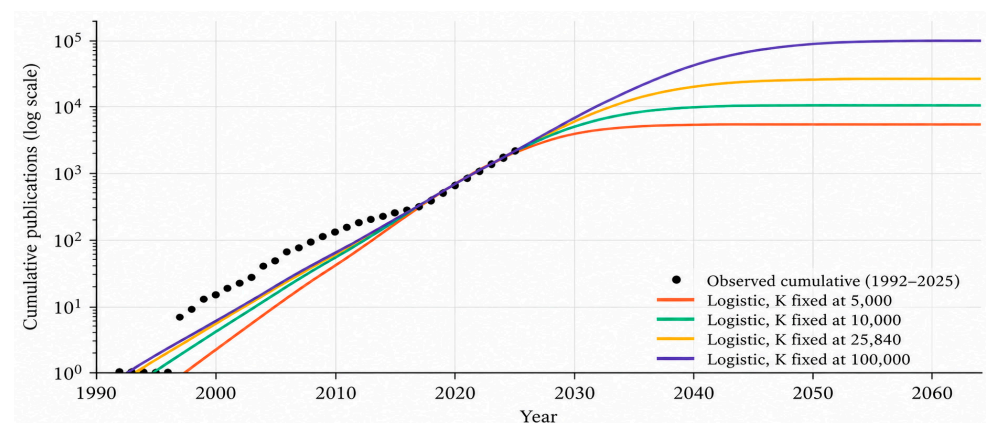


Figure 8. Cumulative publications and logistic curves with alternative saturation levels fitted to 1992–2025.

Table 4. Growth model estimates, sensitivity to the incomplete year 2026 and out-of-sample accuracy.

Component	Specification	Result
Model estimation (1992–2025)	Exponential	$r = 0.232$ (SE 0.005); $R^2 = 0.994$; RMSE = 36.58; AIC = 248.76; BIC = 251.82
	Logistic	K not identified (estimate at upper bound); $r = 0.232$ (SE 0.017); $R^2 = 0.994$; RMSE = 36.58; AIC = 250.77; BIC = 255.35
	Gompertz	K not identified (estimate at upper bound); $R^2 = 0.989$; RMSE = 48.21; AIC = 269.54; BIC = 274.12
Profile of logistic saturation level	K fixed at 5000	$R^2 = 0.9873$; implied midpoint 2026.7; projected annual output in 2030 = 309
Profile of logistic saturation level	K fixed at 10,000	$R^2 = 0.9914$; implied midpoint 2030.5; projected annual output in 2030 = 633
Profile of logistic saturation level	K fixed at 25,840	$R^2 = 0.9931$; implied midpoint 2035.4; projected annual output in 2030 = 980
Profile of logistic saturation level	K fixed at 100,000	$R^2 = 0.9937$; implied midpoint 2041.7; projected annual output in 2030 = 1208
Profile of logistic saturation level	K fixed at 1,000,000	$R^2 = 0.9939$; implied midpoint 2051.8; projected annual output in 2030 = 1290
Sensitivity to 2026	Logistic including observed 2026	K = 25,771; midpoint 2036.2 (spurious saturation driven by the incomplete year)
	Logistic including annualized 2026	K not identified (estimate at upper bound)
Out-of-sample accuracy (MAPE, horizons 1–5 years)	Exponential	50.1%/45.3%/45.1%/51.9%/57.6% (average 50.0%)
	Naive (last value)	28.8%/50.2%/65.4%/73.0%/79.2% (average 59.3%)
	Gompertz	47.0%/61.7%/73.1%/78.2%/82.5% (average 68.5%)
	Logistic	55.1%/70.1%/79.2%/82.9%/86.3% (average 74.7%)
Current status	Cumulative publications	2001 by 2025 (2200 including 199 records indexed for 2026 up to 29 June 2026)
Illustrative projection	Exponential model	Approximately 817 publications in 2028 (bootstrap 95% interval 740–908); longer horizons not reported

Note: Models were fitted by nonlinear least squares to cumulative publications for 1992 to 2025 (34 annual observations).

4.3. Source Journal Analysis

4.3.1. Leading Publication Sources

Table 5 identifies the most influential publication sources in AI-based financial fraud detection. IEEE Access is the most productive journal with 138 publications, followed by Expert Systems with Applications (70 publications) and the International Journal of Advanced Computer Science and Applications (44 publications). Although IEEE Access publishes the most articles, Decision Support Systems exhibits the highest citation impact, averaging 239.95 citations per publication, underscoring its role as a leading high-impact outlet. Most of the top journals are classified as Q1 in Scopus and Web of Science, indicating that research in this field is primarily disseminated through high-quality journals.

Table 5. Source Statistics.

Source Title	Publisher	TP	TC	NCA	NCP	C/P	C/CP	h	g	m	e	CiteScore	SJR	SNIP	Q (Scopus)	JIF	Q (WoS)	ABDC	AJG
IEEE Access	IEEE-Inst Electrical Electronics Engineers INC	138	5326	517	120	38.594	44.383	36	70	4	53.58	9	0.849	1.504	Q1	3.6	Q2	nan	nan
Expert Systems with Applications	Pergamon-Elsevier Science LTD	70	4300	242	69	61.429	62.319	33	65	1.1	51.54	15	1.854	2.548	Q1	7.5	Q1	C	1
International Journal of Advanced Computer Science and Applications	Science & Information Sai Organization LTD	44	714	142	34	16.227	21	12	26	1.2	22.23	2.7	0.285	0.516	Q3	nan	nan	nan	nan
Applied Sciences-Basel	MDPI	41	684	135	37	16.683	18.486	13	25	1.625	19.72					2.5	Q2	nan	nan
Mathematics	MDPI	32	618	122	28	19.312	22.071	13	24	2.167	19.36	4.6	0.498	0.908	Q1	2.2	Q1	nan	nan
Journal of Big Data	Springer Nature	30	1337	59	28	44.567	47.75	17	30	1.889	31.08	22.3	1.979	4.17	Q1	6.4	Q1	nan	nan
Scientific Reports	Nature Portfolio	27	149	113	21	5.519	7.095	7	11	1.4	7.14	6.7	0.874	1.213	Q1	3.9	Q1	nan	nan
Journal of Theoretical and Applied Information Technology	Little Lion Scientific	25	82	98	15	3.28	5.467	5	8	0.833	5.83	1.4	0.168	0.258	Q3	nan	nan	nan	nan
Sensors	MDPI	24	693	107	21	28.875	33	13	24	1.083	21.93	8.2	0.764	1.312	Q1	3.5	Q2	nan	nan
Decision Support Systems	Elsevier	19	4559	61	19	239.947	239.947	18	19	1.059	65.02	13.5	2.366	2.592	Q1	6.8	Q1	A *	3
Knowledge-Based Systems	Elsevier	19	1089	64	16	57.316	68.062	10	19	0.526	30.92	15	1.934	2.344	Q1	7.6	Q1	A	nan
ELECTRONICS	MDPI	18	369	56	15	20.5	24.6	7	18	1	17.29	1.6	0.499	0.221	Q3	2.6	Q2	nan	nan
PeerJ Computer Science	PEERJ INC	18	183	66	14	10.167	13.071	7	13	0.875	10.49	7.1	0.719	1.386	Q1	2.5	Q2	nan	nan
Engineering Applications of Artificial Intelligence	Pergamon-elsevier science LTD	17	425	78	15	25	28.333	9	17	0.562	17.8	9.5	1.652	1.888	Q1	8.0	Q1	nan	nan

Table 5. Cont.

Source Title	Publisher	TP	TC	NCA	NCP	C/P	C/CP	h	g	m	e	CiteScore	SJR	SNIP	Q (Scopus)	JIF	Q (WoS)	ABDC	AJG
Computational Economics	Springer	16	123	40	11	7.688	11.182	4	11	0.444	9.59	4.9	0.535	1.195	Q1	2.2	Q2	B	1
Applied Soft Computing	Elsevier	16	777	61	14	48.562	55.5	11	16	0.688	25.26	14.5	1.511	1.971	Q1	6.6	Q1	C	nan
Knowledge and Information Systems	Springer London LTD	15	219	50	14	14.6	15.643	8	14	0.381	10.95	5.7	0.827	1.37	Q2	3.1	Q2	C	nan
Information Sciences	Elsevier Science INC	14	1154	49	14	82.429	82.429	10	14	0.526	32.2	14.4	1.803	1.978	Q1	6.8	Q1	nan	nan
Data Mining and Knowledge Discovery	Springer	14	1461	49	14	104.357	104.357	12	14	0.4	36.08	8.2	1.019	1.876	Q1	4.3	Q2	nan	nan
CMC-Computers Materials & Continua	Tech Science Press	14	226	62	13	16.143	17.385	8	14	1	12					1.7	Q3	nan	nan
IEEE Transactions on Computational Social Systems	IEEE-Inst Electrical Electronics Engineers INC	14	510	48	13	36.429	39.231	10	14	1.667	19.8	9.2	1.257	1.942	Q1	4.9	Q1	nan	nan
Artificial Neural Networks—ICANN 2006, PT 2	Springer-Verlag Berlin	12	169	41	12	14.083	14.083	7	12	1	10					nan	nan	nan	nan
Neural Computing & Applications	Springer London LTD	12	251	44	12	20.917	20.917	8	12	1	12.96					nan	nan	nan	nan
Journal Of Intelligent & Fuzzy Systems	IOS Press	12	177	40	11	14.75	16.091	6	12	1	11.49					1.0	Q4	nan	nan
Multimedia Tools and Applications	Springer	12	190	33	12	15.833	15.833	6	12	1.2	11.62	7.7	0.777	1.435	Q1	nan	nan	nan	nan

Note: TP = Total Publications; TC = Total Citations; NCA = Number of Contributing Authors; NCP = Number of Cited Publications; C/P = Citations per Publication; C/CP = Citations per Cited Publication; h = h-index; g = g-index; m = m-Quotient; e = e-index; SJR = SCImago Journal Rank; SNIP = Source-Normalised Impact per Paper; JIF = Journal Impact Factor; ABDC = Australian Business Deans Council Rating; AJG = Academic Journal Guide. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

4.3.2. Emerging and High-Momentum Journals

Table 6 highlights journals experiencing the strongest recent growth. IEEE Access remains the leading hot journal with the highest momentum score (152.2), reflecting its rapid increase in publications. Scientific Reports, Computational Economics, and the Journal of Risk and Financial Management are emerging journals with substantial recent growth, while established journals such as Expert Systems with Applications and Applied Sciences maintain stable publication performance. The results indicate that AI-based financial fraud detection research is expanding across both established and emerging publication outlets.

Table 6. Rising Sources Ranking.

#	Source	Category	Total	Recent	ADY	RAI %	GR %	Momentum
1	IEEE Access	Hot	138	71	23.67	51.4	73.2	152.2
2	Expert Systems with Applications	Stable	70	19	6.33	27.1	5.6	35.2
3	Scientific Reports	Emerging	27	24	8.00	88.9	700.0	34.7
4	Applied Sciences-Basel	Stable	41	20	6.67	48.8	17.6	32.5
5	International Journal of Advanced Computer Science and Applications	Stable	44	15	5.00	34.1	−16.7	24.8
6	Mathematics	Stable	32	15	5.00	46.9	−11.8	22.8
7	Journal of Theoretical and Applied Information Technology	Hot	25	16	5.33	64.0	77.8	22.6
8	Journal of Big Data	Stable	30	13	4.33	43.3	18.2	19.4
9	PeerJ Computer Science	Hot	18	12	4.00	66.7	140.0	15.3
10	Computational Economics	Emerging	16	12	4.00	75.0	500.0	14.8
11	Electronics	Hot	18	11	3.67	61.1	83.3	14.1
12	Engineering Applications of Artificial Intelligence	Hot	17	10	3.33	58.8	233.3	12.6
13	Sensors	Stable	24	8	2.67	33.3	−33.3	11.2
14	IEEE Transactions on Computational Social Systems	Hot	14	8	2.67	57.1	100.0	9.4
15	Knowledge-Based Systems	Hot	19	7	2.33	36.8	133.3	9.1
16	Journal of Risk and Financial Management	Emerging	9	9	3.00	100.0	NEW	9.0
17	Engineering, Technology and Applied Science Research	Emerging	10	7	2.33	70.0	133.3	7.3
18	Knowledge and Information Systems	Hot	15	6	2.00	40.0	500.0	7.2
19	Neural Computing & Applications	Hot	12	6	2.00	50.0	100.0	6.7
20	Information	Hot	11	6	2.00	54.5	100.0	6.5
21	PLOS ONE	Hot	10	6	2.00	60.0	200.0	6.2
22	Applied Soft Computing	Stable	16	5	1.67	31.3	−16.7	6.2
23	Intelligent Decision Technologies-Netherlands	Emerging	8	6	2.00	75.0	500.0	5.7
24	Multimedia Tools and Applications	Stable	12	5	1.67	41.7	−28.6	5.6
25	Journal of Computational Methods in Sciences and Engineering	Emerging	6	6	2.00	100.0	NEW	5.1

Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

4.4. Bradford's Law

Figure 9 and Table 7 show that the distribution of publications across journals is concentrated and is closely approximated by the log-linear Bradford model ($R^2 = 0.9741$). Formal conformity to Bradford's Law, however, is not supported. The Kolmogorov–Smirnov distance between the observed and fitted distributions is substantial ($D = 0.1477$), the observed zone multipliers decline from 5.48 between the first and second zones to 3.66 between the second and third zones instead of remaining constant; and the core contains 31 journals, compared with approximately 18 implied by Egghe's multiplier ($k = 6.26$). Because the parameters are estimated from the same ranked data, the Kolmogorov–Smirnov result is interpreted descriptively rather than as a formal test. The departure from Bradford's pattern is substantively meaningful: the core is larger, and the dispersion across peripheral journals is greater than the classical law implies, which reflects the interdisciplinary nature of the field, in which articles are distributed across computing, engineering, decision sciences, accounting, and finance outlets rather than accumulating in a small set of specialized journals.

Table 7. Bradford's Law Model and Goodness-of-Fit Results.

Category	Indicator	Value
Bradford's Law Model	Model Equation	$C(r) = -684.212 + 414.1259 \times \log(r)$
	Intercept (a)	−684.212
	Slope (b)	414.1259
	R^2	0.9741
	Bradford Multiplier (k)	4.57
Kolmogorov–Smirnov Goodness-of-Fit	KS Statistic (D)	0.1477
	<i>p</i> -value	3.63×10^{-16}
	Decision	The empirical distribution differs significantly from Bradford's Law ($p < 0.001$).
	Interpretation	The empirical distribution follows the theoretical Bradford distribution with a statistically significant deviation.
Dataset Summary	Total Number of Sources (Journals)	824
	Total Publications	2200

Table 8 further shows that only 31 journals (3.8%) constitute the core zone, yet they account for 738 publications (33.5%), while the remaining publications are distributed across many more journals. This concentration confirms that a relatively small group of highly productive publication outlets dominates the literature.

Table 8. Bradford Zone Summary.

Zone	N. Sources	% Sources	N. Articles	% Articles
Zone 1	31	3.8%	738	33.5%
Zone 2	170	20.6%	729	33.1%
Zone 3	623	75.6%	733	33.3%
Total	824	100.0%	2200	100.0%

Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

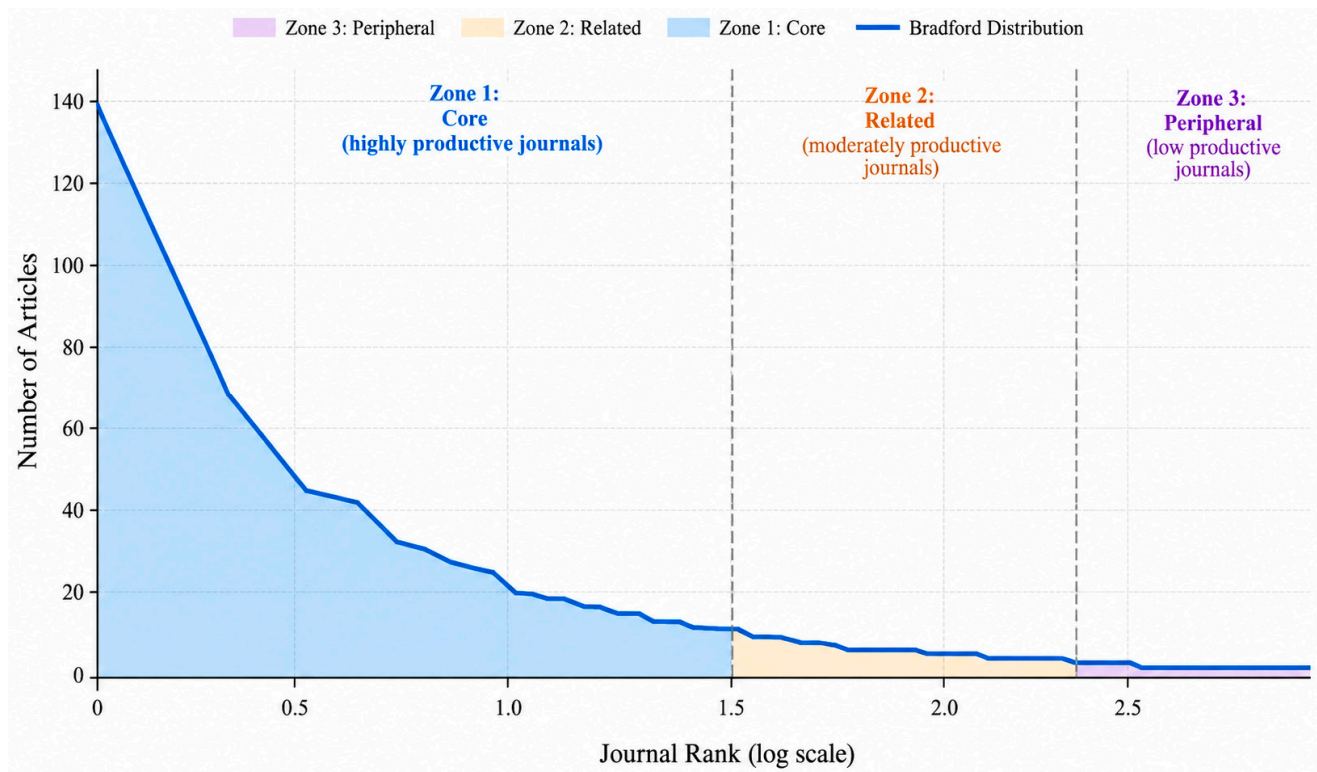


Figure 9. Bradford's Law. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

Table 9 identifies these core journals, with IEEE Access, Expert Systems with Applications, International Journal of Advanced Computer Science and Applications, Applied Sciences, and Mathematics ranking among the most productive sources. Overall, the Bradford analysis indicates that AI research in financial fraud detection is concentrated within a limited number of influential journals, while the remaining publications are dispersed across a broad range of specialized outlets.

Table 9. Bradford Source Ranking.

Source	Rank	Freq	cumFreq	Zone
IEEE Access	1	138	138	Zone 1
Expert Systems with Applications	2	70	208	Zone 1
International Journal of Advanced Computer Science and Applications	3	44	252	Zone 1
Applied Sciences-Basel	4	41	293	Zone 1
Mathematics	5	32	325	Zone 1
Journal of Big Data	6	30	355	Zone 1
Scientific Reports	7	27	382	Zone 1
Journal of Theoretical and Applied Information Technology	8	25	407	Zone 1
Sensors	9	24	431	Zone 1
Decision Support Systems	10	19	450	Zone 1
Knowledge-Based Systems	11	19	469	Zone 1
Electronics	12	18	487	Zone 1
PeerJ Computer Science	13	18	505	Zone 1
Engineering Applications of Artificial Intelligence	14	17	522	Zone 1
Computational Economics	15	16	538	Zone 1
Applied Soft Computing	16	16	554	Zone 1
Knowledge and Information Systems	17	15	569	Zone 1

Table 9. Cont.

Source	Rank	Freq	cumFreq	Zone
Data Mining and Knowledge Discovery	18	14	583	Zone 1
CMC-Computers Materials & Continua	19	14	597	Zone 1
Information Sciences	20	14	611	Zone 1
IEEE Transactions on Computational Social Systems	21	14	625	Zone 1
Journal Of Intelligent & Fuzzy Systems	22	12	637	Zone 1
Artificial Neural Networks—ICANN 2006, Pt 2	23	12	649	Zone 1
Neural Computing & Applications	24	12	661	Zone 1
Multimedia Tools and Applications	25	12	673	Zone 1

Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

4.5. Subject Area Analysis

Table 10 illustrates the distribution of subject areas in AI research on financial fraud detection. Computer Science is the dominant discipline, assigned to 1527 publications, followed by Engineering with 770 publications and Mathematics with 437 publications. Because one publication may belong to several subject categories, Table 10 reports two percentages: the share of all 4229 subject-category assignments, which sums to 100% (for example, 36.1% for Computer Science), and the share of the 2200 publications assigned to each category, which sums to more than 100% (69.4% for Computer Science). The predominance of Computer Science and Engineering reflects the field's technical nature, where advances in machine learning, deep learning, data mining, and computational algorithms drive research and practical applications in fraud detection.

Table 10. Subject Area Distribution.

Color	Abbreviation	Full Discipline Name	Number of Publications	Percentage (%)	% of Publications (n = 2200)
	CS	Computer Science	1527	36.1%	69.4%
	ENGIN	Engineering	770	18.2%	35.0%
	MATHE	Mathematics	437	10.3%	19.9%
	BMAA	Business, Management and Accounting	272	6.4%	12.4%
	DS	Decision Sciences	233	5.5%	10.6%
	MS	Materials Science	190	4.5%	8.6%
	EEAF	Economics, Econometrics and Finance	174	4.1%	7.9%
	SS	Social Sciences	148	3.5%	6.7%
	GENER	General	76	1.8%	3.5%
	PAA	Physics and Astronomy	63	1.5%	2.9%
	CHEMI	Chemistry	43	1.0%	2.0%
	MEDIC	Medicine	42	1.0%	1.9%
	BGAMS	Biochemistry, Genetics and Molecular Biology	40	0.9%	1.8%
	AAM	Arts and Humanities	33	0.8%	1.5%
	PSYCH	Psychology	32	0.8%	1.5%
	ES	Environmental Science	29	0.7%	1.3%
	ENERG	Energy	26	0.6%	1.2%
	AABS	Agricultural and Biological Sciences	25	0.6%	1.1%
	NEURO	Neuroscience	24	0.6%	1.1%
	CE	Chemical Engineering	18	0.4%	0.8%
	OTHER	Others	27	0.6%	1.2%

Business-oriented disciplines also contribute significantly, including Business, Management, and Accounting (6.4%), Decision Sciences (5.5%), and Economics, Econometrics, and Finance (4.1%), highlighting the integration of AI techniques with financial decision-making and risk management. Publications in Social Sciences, Medicine, Psychology, and other disciplines further demonstrate the broad applicability of AI-based fraud detection

across multiple research domains. Appendix A, Table A4 complements this analysis by classifying the publications by financial fraud domain. Credit card and payment fraud accounts for 526 publications (23.9%), whereas anti-money laundering (0.9%), tax and public-sector fraud (1.6%), and securities and cryptocurrency fraud (4.0%) remain marginal, and 559 publications (25.4%) were identified by the relevance verification as addressing non-financial fraud or mentioning fraud only incidentally.

4.6. Citation Analysis

Table 11 presents the most influential publications in AI-based financial fraud detection, while Figure 10 illustrates the distribution of citations across publication years. The most highly cited study is Ngai et al. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature, with 1041 citations, highlighting its foundational contribution to the field. Other highly influential publications include Bhattacharyya et al. (2011), which reports 832 citations, and Goldstein and Uchida (2016), with 649 citations. The highly cited literature reflects the field's major methodological and application domains, particularly data mining, machine learning, anomaly detection, deep learning, and credit card fraud detection. More recent contributions, including Alarfaj et al. (2022) and Ileberi et al. (2022), show particularly high citation rates and normalized citation impact relative to their publication age, suggesting these studies have achieved substantial scholarly visibility in a relatively short period. Overall, the citation profile indicates that the field has developed from foundational data-mining and statistical approaches toward increasingly sophisticated machine-learning and deep-learning applications in financial fraud detection.

Table 11. Highly Cited Papers.

#	Authors	Title	Source	TC	C/Y	NTC
1	Ngai et al. (2011)	The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature	Decision Support Systems	1041	65.06	5.8
2	Bhattacharyya et al. (2011)	Data mining for credit card fraud: A comparative study	Decision Support Systems	832	52	4.64
3	Goldstein and Uchida (2016)	A Comparative Evaluation of Unsupervised Anomaly Detection Algorithms for Multivariate Data	PLOS ONE	649	59	8.98
4	Kirkos et al. (2007)	Data Mining techniques for the detection of fraudulent financial statements	Expert Systems with Applications	520	26	6.19
5	Fawcett and Provost (1997)	Adaptive fraud detection	Data Mining and Knowledge Discovery	489	16.3	2.79
6	Ravisankar et al. (2011)	Detection of financial statement fraud and feature selection using data mining techniques	Decision Support Systems	450	28.12	2.51
7	Chan et al. (1999)	Distributed Data Mining in Credit Card Fraud Detection	IEEE Intelligent Systems and Their Applications	388	13.86	2.11

Table 11. Cont.

#	Authors	Title	Source	TC	C/Y	NTC
8	Pourhabibi et al. (2020)	Fraud detection: A systematic literature review of graph-based anomaly detection approaches	Decision Support Systems	382	54.57	10.56
9	Alarfaj et al. (2022)	Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms	IEEE ACCESS	374	74.8	11.96
10	Taha and Malebary (2020)	An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine	IEEE ACCESS	368	52.57	10.17
11	Sahin et al. (2013)	A cost-sensitive decision tree approach for fraud detection	Expert Systems with Applications	344	24.57	5.54
12	Ileberi et al. (2022)	A machine learning-based credit card fraud detection using the GA algorithm for feature selection	Journal Of Big Data	340	68	10.88
13	Bao et al. (2020)	Detecting Accounting Fraud in Publicly Traded U.S. Firms Using a Machine Learning Approach	Journal of Accounting Research	338	48.29	9.34
14	Fiore et al. (2019)	Using generative adversarial networks for improving classification effectiveness in credit card fraud detection	Information Sciences	327	40.88	11.65
15	Esenogho et al. (2022)	A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection	IEEE ACCESS	311	62.2	9.95
16	Hajek and Henriques (2017)	Mining corporate annual reports for intelligent detection of financial statement fraud—A comparative study of machine learning methods	Knowledge-Based Systems	291	29.1	6.14
17	Wang and Xu (2018)	Leveraging deep learning with LDA-based text analytics to detect automobile insurance fraud	Decision Support Systems	290	32.22	5.54
18	Pumsirirat and Yan (2018)	Credit Card Fraud Detection using Deep Learning based on Autoencoder and Restricted Boltzmann Machine	International Journal of Advanced Computer Science and Applications	289	32.11	5.53
19	Perols (2011)	Financial statement fraud detection: An analysis of statistical and machine learning algorithms	Auditing	272	17	1.52
20	Dal Pozzolo et al. (2014)	Learned lessons in credit card fraud detection from a practitioner perspective	Expert Systems with Applications	265	20.38	6.08
21	Yamanishi et al. (2004)	On-line unsupervised outlier detection using finite mixtures with discounting learning algorithms	Data Mining and Knowledge Discovery	240	10.43	5.92
22	Jurgovsky et al. (2018)	Sequence classification for credit-card fraud detection	Expert Systems with Applications	238	26.44	4.55

Note: TC = Total Citations; C/Y = Citations per Year; NTC = Normalised Total Citations. Source: Generated by the author(s) using BiblioSpy® ([Ahmi, 2026](#)).

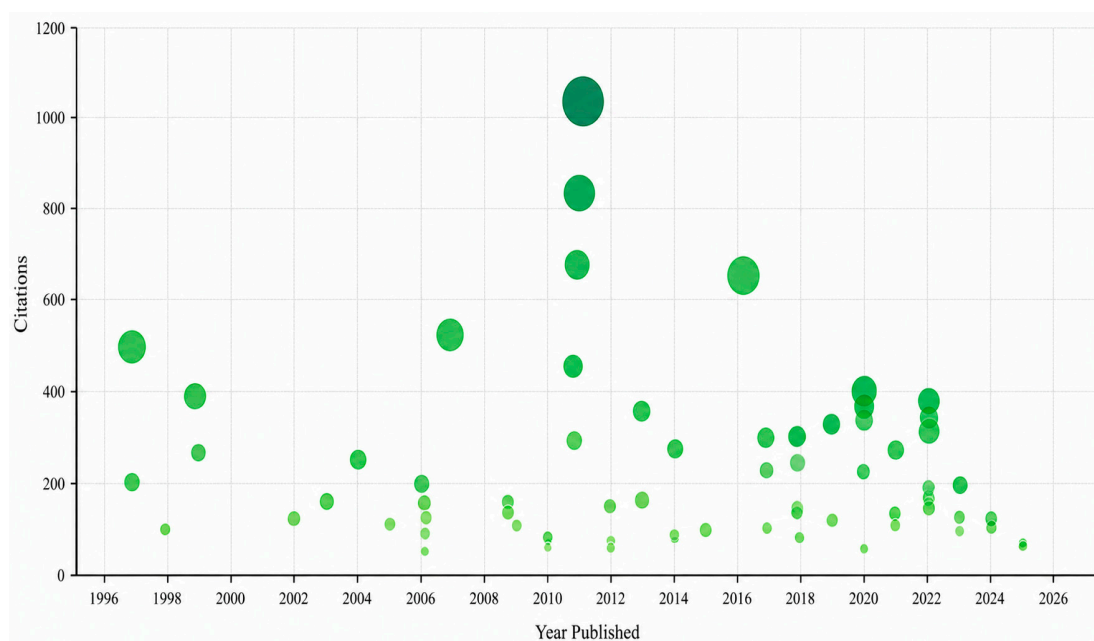


Figure 10. Citations Over Time. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

4.7. Author Analysis

Table 12 and Figures 11 and 12 present the productivity and citation performance of the leading authors in AI-based financial fraud detection. Khoshgoftaar, Taghi M., is the most prolific author with 34 publications, followed by Liu, Guanjun (12 publications) and Bauder, Richard (11 publications). In terms of citation impact, Khoshgoftaar also leads with 1011 citations, while authors such as Sun, Yanxia, and Mienye, Ibomoye Domor exhibit exceptionally high average citations per publication, reflecting the strong influence of their contributions.

Table 12. Author Statistics.

Author	Affiliation	Country	TP	NCP	TC	C/P	C/CP	h	g	m	e
Khoshgoftaar, Taghi M.	Florida Atlantic University	United States	34	31	1011	29.74	32.61	16	31	1.78	25.48
Liu, Guanjun	Monmouth University	United States	12	12	682	56.83	56.83	11	12	1.38	23.45
Bauder, Richard	Florida Atlantic University	United States	11	11	553	50.27	50.27	9	11	1.00	21.52
Hancock, John	Florida Atlantic University	United States	11	10	242	22.00	24.20	8	11	1.60	13.27
Lokanan, Mark Eshwar	Royal Roads University	Canada	9	8	162	18.00	20.25	6	9	1.20	11.00
Leevy, Joffrey L.	Florida Atlantic University	United States	8	7	294	36.75	42.00	7	8	1.00	15.65
Ekin, Tahir	Texas State Univ	United States	8	7	135	16.88	19.29	6	8	0.60	9.70
Jiang, Changjun	Tongji University	China	8	7	538	67.25	76.86	7	8	0.88	22.11
Sun, Yanxia	University of Johannesburg	South Africa	8	7	842	105.25	120.29	6	8	1.20	28.34
Zhou, Mengchu	Tongji University	China	7	7	334	47.71	47.71	7	7	1.17	16.88
El Kafhali, Said	Hassan First University of Settat	Morocco	6	6	112	18.67	18.67	6	6	1.50	8.72

Table 12. Cont.

Author	Affiliation	Country	TP	NCP	TC	C/P	C/CP	h	g	m	e
Mienye, Ibomoiye Domor	Walter Sisulu University	South Africa	6	6	760	126.67	126.67	5	6	1.25	27.06
Tayebi, Mohammed	Hassan First University of Settat	Morocco	6	6	112	18.67	18.67	6	6	1.50	8.72
Caelen, Olivier		France	6	6	725	120.83	120.83	5	6	0.46	26.40
Xie, Yu	Tongji University	China	6	6	245	40.83	40.83	6	6	1.20	14.46
Baesens, Bart	KU Leuven (Katholieke Universiteit Leuven)	Belgium	6	6	352	58.67	58.67	6	6	0.26	17.78
Verdonck, Tim	University of Antwerp	Belgium	6	6	199	33.17	33.17	5	6	1.25	13.08
Johnson, Justin M.	Florida Atlantic University	United States	6	6	218	36.33	36.33	5	6	1.00	13.78
Yuan, Zhong	Sichuan University	China	5	4	228	45.60	57.00	4	5	0.44	14.56
Jain, Anurag	Guru Gobind Singh Indraprastha Univ	India	5	5	97	19.40	19.40	5	5	1.25	8.49
Chen, Hongchang	Information Engineering University	China	5	5	124	24.80	24.80	5	5	1.67	9.95
Panigrahi, Suvasini	Veer Surendra Sai University of Technology	India	5	5	113	22.60	22.60	4	5	0.22	9.75
Liu, Shuxin	Pla Strategic Support Force Information Engineering University	China	5	5	124	24.80	24.80	5	5	1.67	9.95
Kolli, Chandra Sekhar	Shri Vishnu Engineering College for Women	India	5	4	60	12.00	15.00	3	5	0.50	7.00
Sisodia, Deepti	National Institute of Technology Raipur	India	5	5	58	11.60	11.60	4	5	1.33	6.24

Note: TP = Total Publications; NCP = Number of Cited Publications; TC = Total Citations; C/P = Citations per Publication; C/CP = Citations per Cited Publication; h = h-index; g = g-index; m = m-Quotient; e = e-index. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

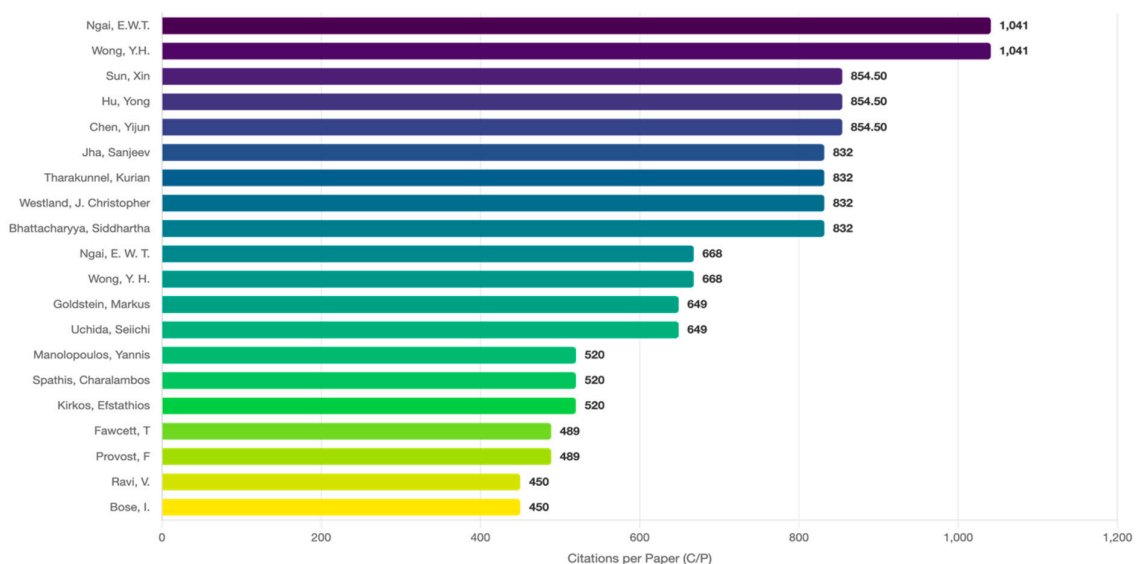


Figure 11. Top Authors. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

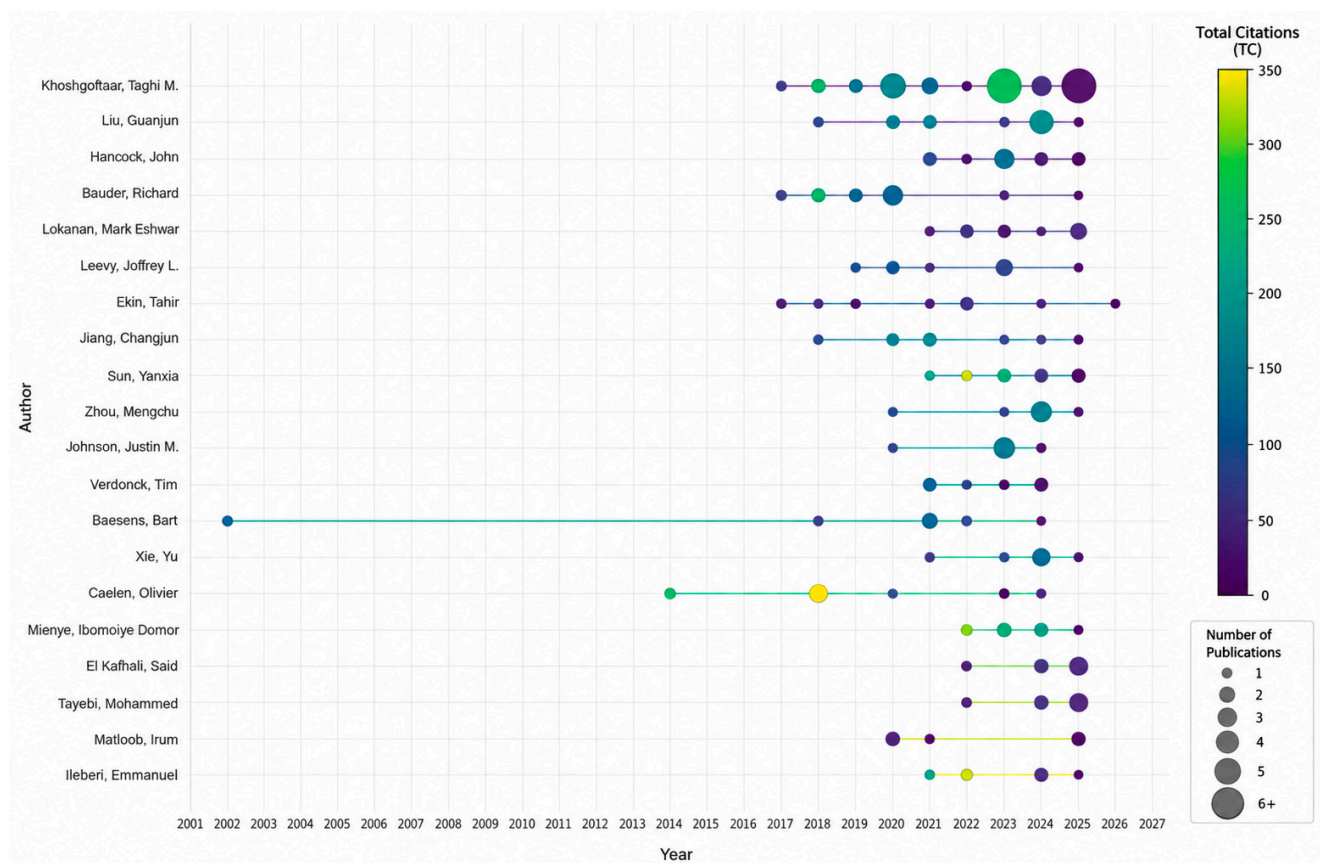


Figure 12. Author Production Over Time. Source: Generated by the author(s) using BiblioSpy[®] (Ahmi, 2026).

Table 13 and Figure 13 identify emerging and rapidly growing researchers. Liu, GuanJun is classified as a hot author, whereas Zhou, Mengchu, El Kafhali, Said, and Tayebi, Mohammed are identified as emerging authors with high recent publication activity and growth momentum. These findings suggest that new contributors are increasingly shaping the field's development.

Table 13. Rising Authors Ranking.

#	Author	Category	Total	Recent	ADY	RAI %	GR %	Momentum
1	Khoshgoftaar, Taghi M.	Stable	34	12	4.00	35.3	0.0	18.5
2	Liu, GuanJun	Hot	12	6	2.00	50.0	100.0	6.7
3	Zhou, Mengchu	Emerging	7	5	1.67	71.4	400.0	4.5
4	Hancock, John	Stable	11	4	1.33	36.4	−42.9	4.3
5	El Kafhali, Said	Emerging	6	5	1.67	83.3	400.0	4.2
6	Tayebi, Mohammed	Emerging	6	5	1.67	83.3	400.0	4.2
7	Lokanan, Mark Eshwar	Stable	9	4	1.33	44.4	−20.0	4.0
8	Sun, Yanxia	Stable	8	4	1.33	50.0	0.0	3.8
9	Xie, Yu	Hot	6	4	1.33	66.7	100.0	3.4
10	Chen, Wen	Emerging	5	4	1.33	80.0	300.0	3.1
11	Kim, Song-Kyoo	Emerging	4	4	1.33	100.0	NEW	2.8
12	Li, Wenjuan	Emerging	4	4	1.33	100.0	NEW	2.8
13	Mienye, Ibomoiye Domor	Stable	6	3	1.00	50.0	0.0	2.5
14	Banirostan, Hamid	Stable	5	3	1.00	60.0	50.0	2.3
15	Panigrahi, Suvasini	Stable	5	3	1.00	60.0	NEW	2.3

Table 13. Cont.

#	Author	Category	Total	Recent	ADY	RAI %	GR %	Momentum
16	Kolli, Chandra Sekhar	Stable	5	3	1.00	60.0	50.0	2.3
17	Ileberi, Emmanuel	Stable	5	3	1.00	60.0	50.0	2.3
18	Zhou, Xujuan	Emerging	4	3	1.00	75.0	200.0	2.1
19	Btoush, Eyad Abdel Latif Marazqah	Emerging	4	3	1.00	75.0	200.0	2.1
20	Yang, Yue	Emerging	4	3	1.00	75.0	200.0	2.1
21	Ekin, Tahir	Stable	8	2	0.67	25.0	−33.3	1.9
22	Jiang, Changjun	Stable	8	2	0.67	25.0	−33.3	1.9
23	Darwish, Saad M.	Emerging	3	3	1.00	100.0	NEW	1.8
24	Ykhlef, Mourad	Emerging	3	3	1.00	100.0	NEW	1.8
25	Mridha, M.F.	Emerging	3	3	1.00	100.0	NEW	1.8

Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

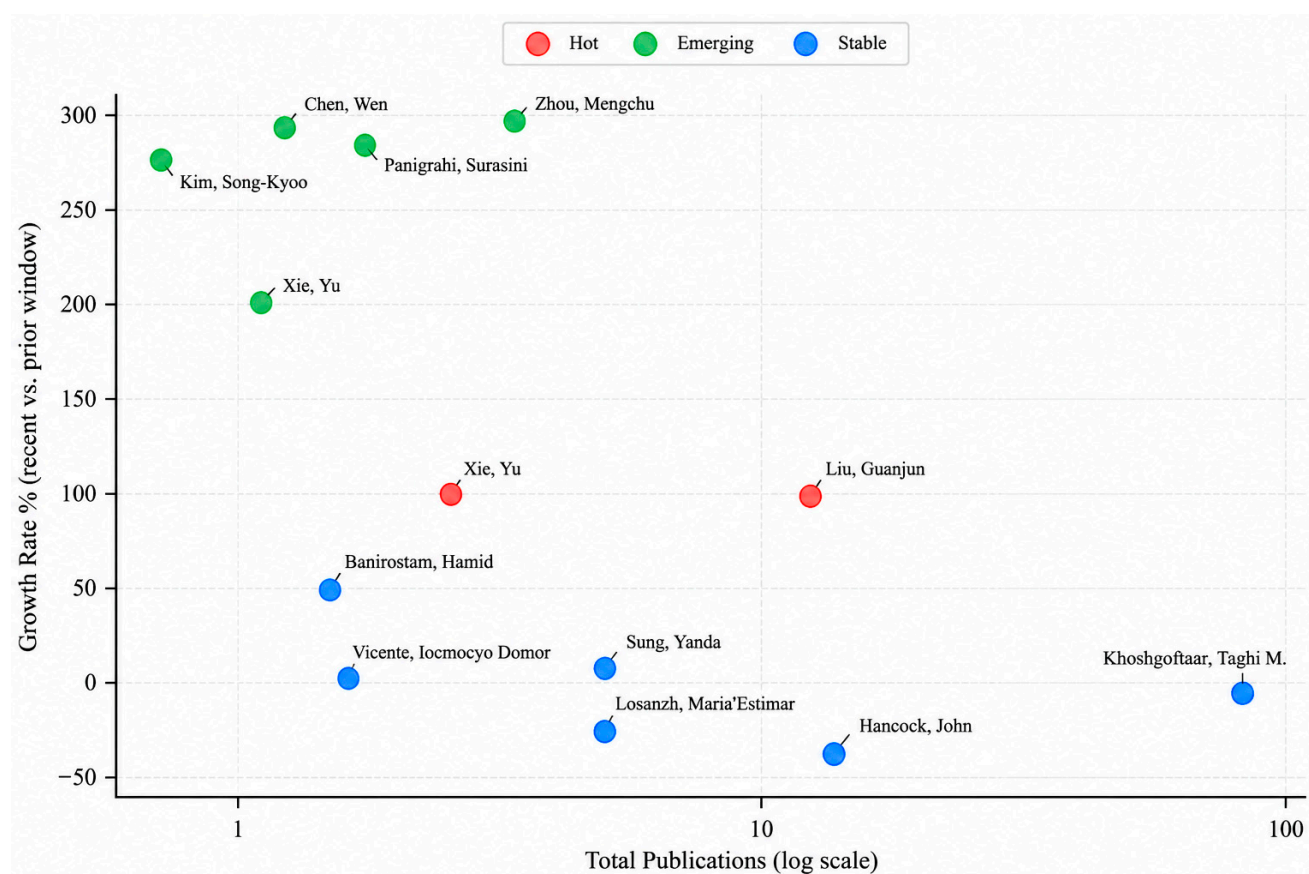


Figure 13. Rising Authors Map. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

Figure 14 and Table 14 illustrate the co-authorship network, revealing several well-defined collaboration clusters led by highly productive researchers such as Khoshgoftaar, Liu, and Sun. The network indicates that collaboration is concentrated within several established research groups, with strong links among authors from leading institutions in the United States, China, and South Africa, reflecting the collaborative nature of AI research on financial fraud detection.

Table 14. Authors.

#	Author	Cluster	Documents	Links	Total Link Strength	Relevance	Avg. Pub. Year	Avg. Citations	Avg. Norm. Citations	X	Y
1	Khoshgoftaar, Taghi M.	1	34	4	26.00	34.000	2022.2	29.74	1.09	−0.771	−0.328
2	Liu, Guanjun	2	12	3	11.00	12.000	2022.3	56.83	2.54	−0.825	−0.114
3	Bauder, Richard	1	11	3	11.00	11.000	2019.9	50.27	1.34	−0.833	−0.019
4	Hancock, John	1	11	4	11.00	11.000	2023.1	22.00	1.02	0.899	−0.032
5	Lokanan, Mark Eshwar	12	9	0	0.00	9.000	2023.3	18.00	1.42	0.040	−0.003
6	Sun, Yanxia	3	8	2	7.00	8.000	2023.4	105.25	4.22	−0.711	0.441
7	Jiang, Changjun	2	8	3	7.00	8.000	2021.5	67.25	2.41	−0.521	0.661
8	Leevy, Joffrey L.	1	8	4	8.00	8.000	2021.8	36.75	1.34	0.437	0.767
9	Ekin, Tahir	10	8	0	0.00	8.000	2021.1	16.88	0.55	0.040	−0.001
10	Zhou, Mengchu	2	7	3	7.00	7.000	2023.4	47.71	2.80	0.095	−0.862
11	Caelen, Olivier	9	6	1	3.00	6.000	2019.5	120.83	2.81	0.828	−0.365
12	Verdonck, Tim	8	6	1	4.00	6.000	2022.5	33.17	1.19	0.882	0.065
13	Tayebi, Mohammed	4	6	1	6.00	6.000	2024.2	18.67	2.01	−0.125	0.633
14	El Kafhali, Said	4	6	1	6.00	6.000	2024.2	18.67	2.01	0.602	−0.523
15	Baesens, Bart	8	6	1	4.00	6.000	2018.0	58.67	1.57	0.539	−0.683
16	Johnson, Justin M.	1	6	3	6.00	6.000	2022.7	36.33	1.60	−0.395	−0.758
17	Mienye, Ibomoiye Domor	3	6	1	2.00	6.000	2023.5	126.67	6.14	−0.744	0.376
18	Xie, Yu	2	6	3	6.00	6.000	2023.5	40.83	2.61	0.757	0.464
19	Ileberi, Emmanuel	3	5	1	5.00	5.000	2023.2	121.20	4.33	−0.783	0.275
20	Bontempi, Gianluca	9	5	1	3.00	5.000	2020.0	82.60	1.95	0.868	−0.257
21	Panigrahi, Suvasini	13	5	0	0.00	5.000	2020.8	22.60	1.49	0.040	−0.004
22	Chen, Hongchang	5	5	1	5.00	5.000	2023.0	24.80	1.19	0.155	0.859
23	Liu, Shuxin	5	5	1	5.00	5.000	2023.0	24.80	1.19	0.081	0.865
24	Singh, Ajeet	6	5	1	5.00	5.000	2020.8	19.40	0.62	0.001	−0.657
25	Jain, Anurag	6	5	1	5.00	5.000	2020.8	19.40	0.62	0.530	0.437

Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

4.8. Author Productivity Distribution (Lotka's Law)

Tables 15–17 and Figure 15 examine author productivity using Lotka's Law. As shown in Table 15, the literature shows a highly skewed productivity distribution, with 5874 authors (88.83%) contributing only one publication, while only a very small proportion of authors produced multiple publications. This finding indicates that occasional contributors dominate the field, while a small number of highly productive researchers account for a substantial share of the literature.

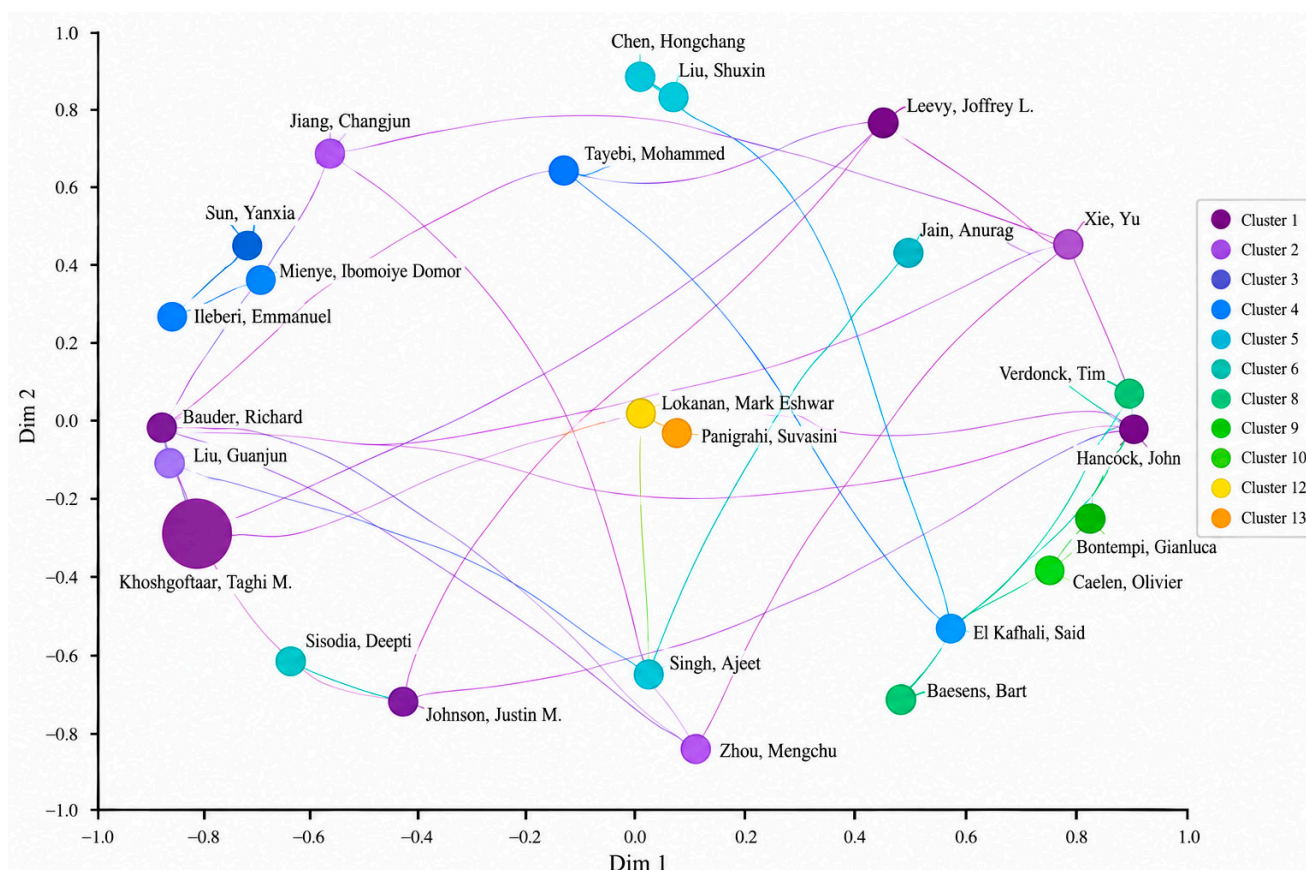


Figure 14. Network visualisation of authors. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026). Note: Node size is proportional to the number of citations received by each author. Larger circles represent authors with higher citation counts.

Table 15. Author Productivity Distribution.

Documents (x)	No. of Authors (y)	Proportion (%)	Fitted Lotka C/xn (%)	Classic Lotka $60/x^2$ (%)
1	5874	88.83%	80.86%	60.00%
2	558	8.44%	11.30%	15.00%
3	113	1.71%	3.58%	6.67%
4	36	0.54%	1.58%	3.75%
5	14	0.21%	0.84%	2.40%
6	8	0.12%	0.50%	1.67%
7	1	0.02%	0.32%	1.22%
8	4	0.06%	0.22%	0.94%
9	1	0.02%	0.16%	0.74%
11	2	0.03%	0.09%	0.50%
12	1	0.02%	0.07%	0.42%
34	1	0.02%	0.00%	0.05%

Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

The least-squares estimate of the Lotka exponent reported in Table 17 is 2.8386, and the Kolmogorov–Smirnov test rejects the corresponding distribution ($D = 0.0796$; critical value 0.0200 at the 1% level). This rejection partly reflects the bias of the least-squares estimator on log-log data. The maximum likelihood estimate of the exponent is 3.57 (standard error 0.04), and the maximum distance between the observed and fitted cumulative distributions falls to 0.0054, below Pao’s critical values at the 5% and 1% levels. A parametric bootstrap that accounts for parameter estimation, however, still detects a statistically significant deviation ($p = 0.002$), as expected given the test’s power with 6613 authors. The productivity

distribution therefore closely approximates a power law, but with an exponent substantially steeper than the classical value of two, indicating that the field is populated mainly by occasional contributors who apply AI methods to fraud data once rather than by a stable community of specialized researchers.

Table 16. Least Squares for Exponent n .

x (Pubs)	y (Authors)	X ($\log_{10}x$)	Y ($\log_{10}y$)	XY	X ²
1	5874	0.0000	3.7689	0.0000	0.0000
2	558	0.3010	2.7466	0.8267	0.0906
3	113	0.4771	2.0531	0.9795	0.2276
4	36	0.6021	1.5563	0.9370	0.3625
5	14	0.6990	1.1461	0.8011	0.4886
6	8	0.7782	0.9031	0.7028	0.6056
7	1	0.8451	0.0000	0.0000	0.7142
8	4	0.9031	0.6021	0.5438	0.8156
9	1	0.9542	0.0000	0.0000	0.9105
11	2	1.0414	0.3010	0.3135	1.0845

Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

Table 17. Lotka's Law Overview and Goodness-of-Fit Validation.

Category	Indicator	Value
Lotka's Law Overview	Total Authors	6613
	Single-Publication Authors	88.83%
	Classic Lotka Prediction ($60/x^2$)	60.00%
Exponent Determination	Exponent (n)	2.8386
	Constant (C)	0.8086
	Lotka's Law Formula	$y = 0.8086/x^{2.8386}$
	Interpretation	$n > 2.0$ indicates higher concentration among core authors with rapid decline in productivity.
Kolmogorov–Smirnov (K–S) Test	D _{max}	0.0796
	Critical Value ($\alpha = 0.01$)	0.0200
	Decision	Reject H ₀
	Interpretation	The observed author productivity distribution differs significantly from the fitted Lotka's Law model because D _{max} > CV.

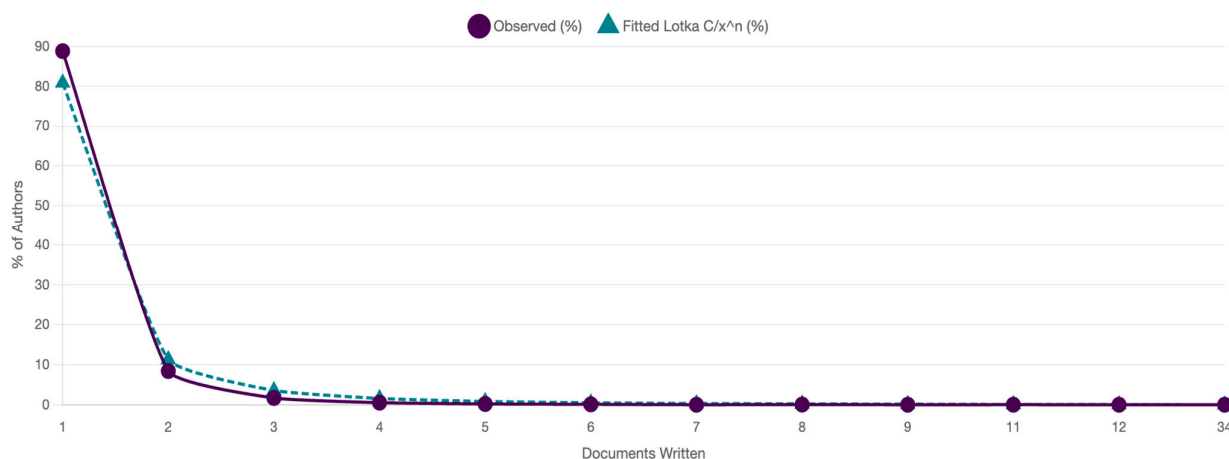


Figure 15. Lotka's Law. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

4.9. Institution Analysis

Table 18 and Figure 16 present the most productive and influential institutions in AI-based financial fraud detection research. Florida Atlantic University ranks first with 36 publications, followed by Koneru Lakshmaiah Education Foundation (31 publications) and Tongji University (27 publications). In terms of scientific impact, the University of Johannesburg recorded the highest average citations per publication (96.07), while Tongji University accumulated 1330 total citations, demonstrating its strong research influence.

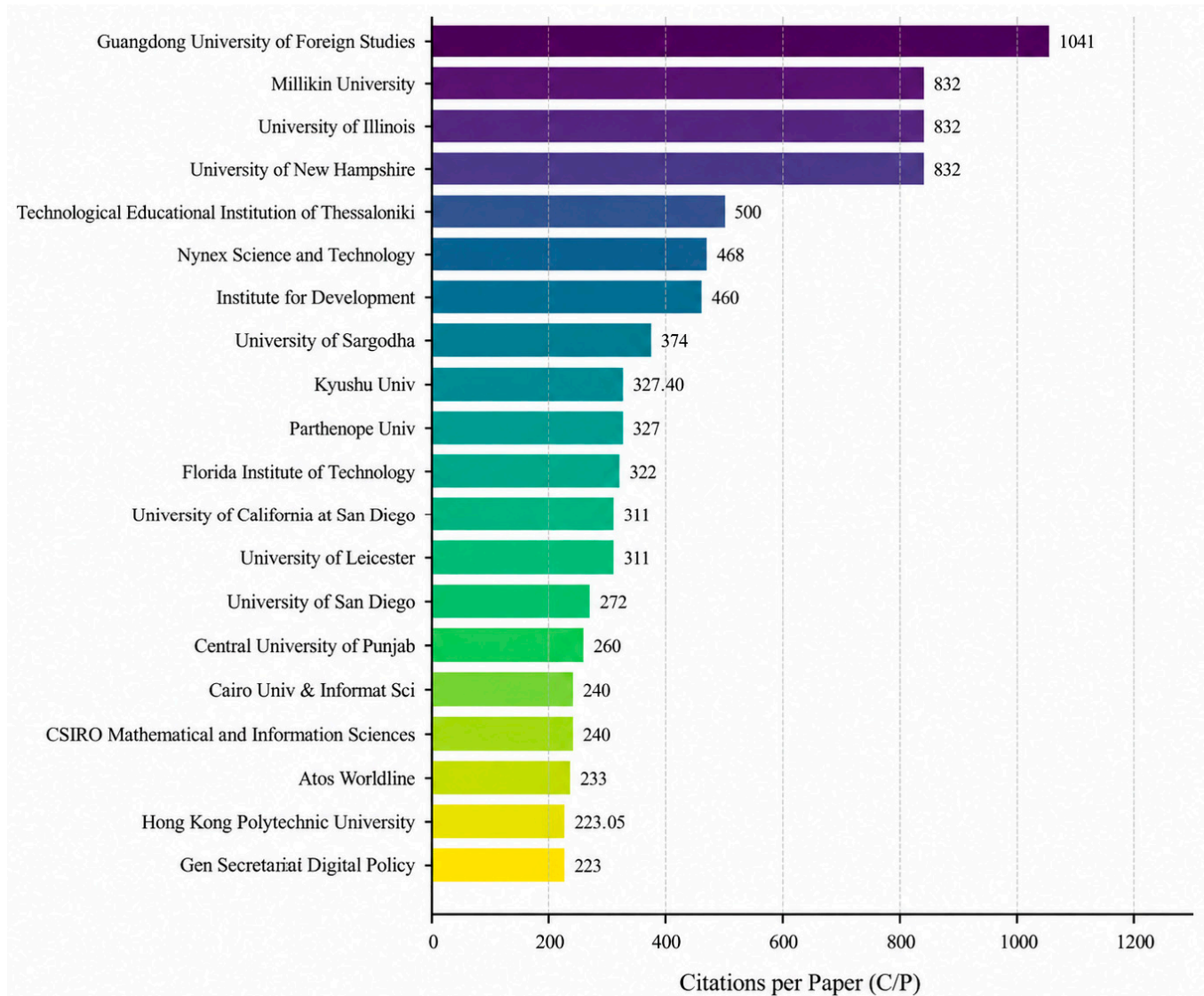


Figure 16. Top Institutions. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

The leading institutions are predominantly located in the United States, China, India, and Saudi Arabia, highlighting the global distribution of research activity in this field. Figure 16 further shows that institutional productivity is concentrated among a relatively small group of universities, reflecting the important role of leading research institutions in advancing AI applications for financial fraud detection.

Table 18. Institutional Statistics.

Institution	Country	TP	NCA	NCP	TC	C/P	C/CP	h	g	m	e
Florida Atlantic University	United States	36	21	32	995	27.64	31.09	16	31	1.78	25.48
Koneru Lakshmaiah Education Foundation	India	31	100	20	181	5.84	9.05	7	12	1.00	9.64
Tongji University	China	27	20	26	1330	49.26	51.15	20	27	2.50	29.58
King Saud University	Saudi Arabia	22	39	21	517	23.50	24.62	12	22	2.00	18.00
SRM Institute of Science and Technology	India	21	43	17	236	11.24	13.88	8	15	1.00	12.12
Islamic Azad University	Iran	17	21	14	137	8.06	9.79	6	11	0.50	8.66
KU Leuven (Katholieke Universiteit Leuven)	Belgium	17	16	17	453	26.65	26.65	10	17	0.48	17.80
King Abdulaziz University	Saudi Arabia	15	27	15	556	37.07	37.07	8	15	1.33	21.73
Chongqing University	China	14	25	12	572	40.86	47.67	10	14	0.50	21.47
Shanghai Jiao Tong University	China	14	34	11	700	50.00	63.64	8	14	0.89	24.94
University of Johannesburg	South Africa	14	20	12	1345	96.07	112.08	11	14	1.83	34.94
Zhejiang Gongshang University	China	14	44	13	417	29.79	32.08	10	14	0.67	17.35
University of Chinese Academy of Sciences	China	13	20	12	199	15.31	16.58	8	13	1.14	10.95
University of Electronic Science and Technology of China	China	13	17	13	350	26.92	26.92	8	13	0.44	16.25
Bina Nusantara University (BINUS)	Indonesia	12	29	9	99	8.25	11.00	3	9	0.27	8.94
Department of Information Technology	India	12	12	6	64	5.33	10.67	4	8	0.36	6.56
Seoul National University	South Korea	12	15	10	231	19.25	23.10	5	12	0.33	14.18
Vellore Institute of Technology	India	12	26	8	183	15.25	22.88	4	12	0.80	12.61
University of Tehran	Iran	11	36	8	146	13.27	18.25	4	11	0.36	10.95
Hefei University of Technology	China	10	7	9	273	27.30	30.33	6	10	0.40	15.13
Imam Mohammad Ibn Saud Islamic University (Imsiu)	Saudi Arabia	10	30	7	531	53.10	75.86	5	10	0.56	22.34
University of Jeddah	Saudi Arabia	10	16	10	423	42.30	42.30	8	10	2.00	18.89
Chinese Acad Sci	China	9	3	7	338	37.56	48.29	6	9	0.33	17.29
Sichuan University	China	9	11	7	197	21.89	28.14	5	9	0.63	12.96
University of Antwerp	Belgium	9	4	9	284	31.56	31.56	7	9	0.54	15.10

Note: TP = Total Publications; NCA = Number of Contributing Authors; NCP = Number of Cited Publications; TC = Total Citations; C/P = Citations per Publication; C/CP = Citations per Cited Publication; h = h-index; g = g-index; m = m-Quotient; e = e-index. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

4.10. Country Analysis

Table 19 and Figures 17–19 present the geographical distribution and collaboration patterns of AI research in financial fraud detection. China is the most productive country with 469 publications, followed by India (377) and the United States (287). In terms of

scientific impact, the United States accumulated 10,090 citations, while China recorded the highest total citations (12,446) owing to its larger publication volume. Countries such as the United Kingdom, Belgium, South Africa, and Greece achieved relatively high average citations per publication, indicating strong research quality.

Table 19. Country Statistics.

Country	TP	NCA	NCP	TC	C/P	C/CP	h	g	m	e
China	469	1561	404	12,446	26.54	30.81	52	96	2.08	68.92
India	377	1245	298	5763	15.29	19.34	37	64	1.762	44.9
United States	287	942	250	10,090	35.16	40.36	53	93	1.514	66.56
Saudi Arabia	114	400	101	3322	29.14	32.89	28	55	2.8	41.62
United Kingdom	95	376	90	3935	41.42	43.72	38	61	1.462	43.51
Australia	69	275	64	2745	39.78	42.89	27	52	0.9	40.6
South Korea	69	222	55	1194	17.3	21.71	18	33	0.6	25.77
Iran	65	173	54	1594	24.52	29.52	21	39	1.105	30.92
Taiwan	64	182	60	1767	27.61	29.45	24	41	1.043	29.36
Türkiye	62	145	46	1182	19.06	25.7	17	34	0.944	27.48
Spain	61	208	51	1267	20.77	24.84	17	34	0.739	27.75
Malaysia	55	237	45	1084	19.71	24.09	19	32	1.357	23.71
Canada	51	158	45	979	19.2	21.76	20	30	0.87	20.25
Pakistan	50	232	46	1505	30.1	32.72	17	38	1.133	32.2
Morocco	47	144	38	1068	22.72	28.11	15	32	1.667	26.83
Indonesia	47	165	34	317	6.74	9.32	10	16	0.909	11.58
Egypt	37	123	30	392	10.59	13.07	11	19	1.833	14.04
South Africa	34	82	31	1950	57.35	62.9	18	34	1	38.99
Italy	34	119	27	984	28.94	36.44	13	31	1.444	26.81
Brazil	32	121	26	508	15.88	19.54	9	22	0.391	18.81
Belgium	31	95	31	1353	43.65	43.65	15	31	0.625	31.86
France	31	120	22	585	18.87	26.59	12	24	0.8	19.36
United Arab Emirates	30	138	24	562	18.73	23.42	12	23	0.923	19.03
Germany	26	94	22	431	16.58	19.59	12	20	0.667	15.43
Greece	26	90	21	1297	49.88	61.76	13	26	0.542	32.66

Note: TP = Total Publications; NCA = Number of Contributing Authors; NCP = Number of Cited Publications; TC = Total Citations; C/P = Citations per Publication; C/CP = Citations per Cited Publication; h = h-index; g = g-index; m = m-Quotient; e = e-index. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

Figures 17 and 18 show that research activity is concentrated in Asia, North America, and Europe, with China, India, and the United States serving as the primary contributors. Figure 19 further reveals extensive international collaboration among these leading countries, highlighting the global and collaborative nature of AI research in financial fraud detection.

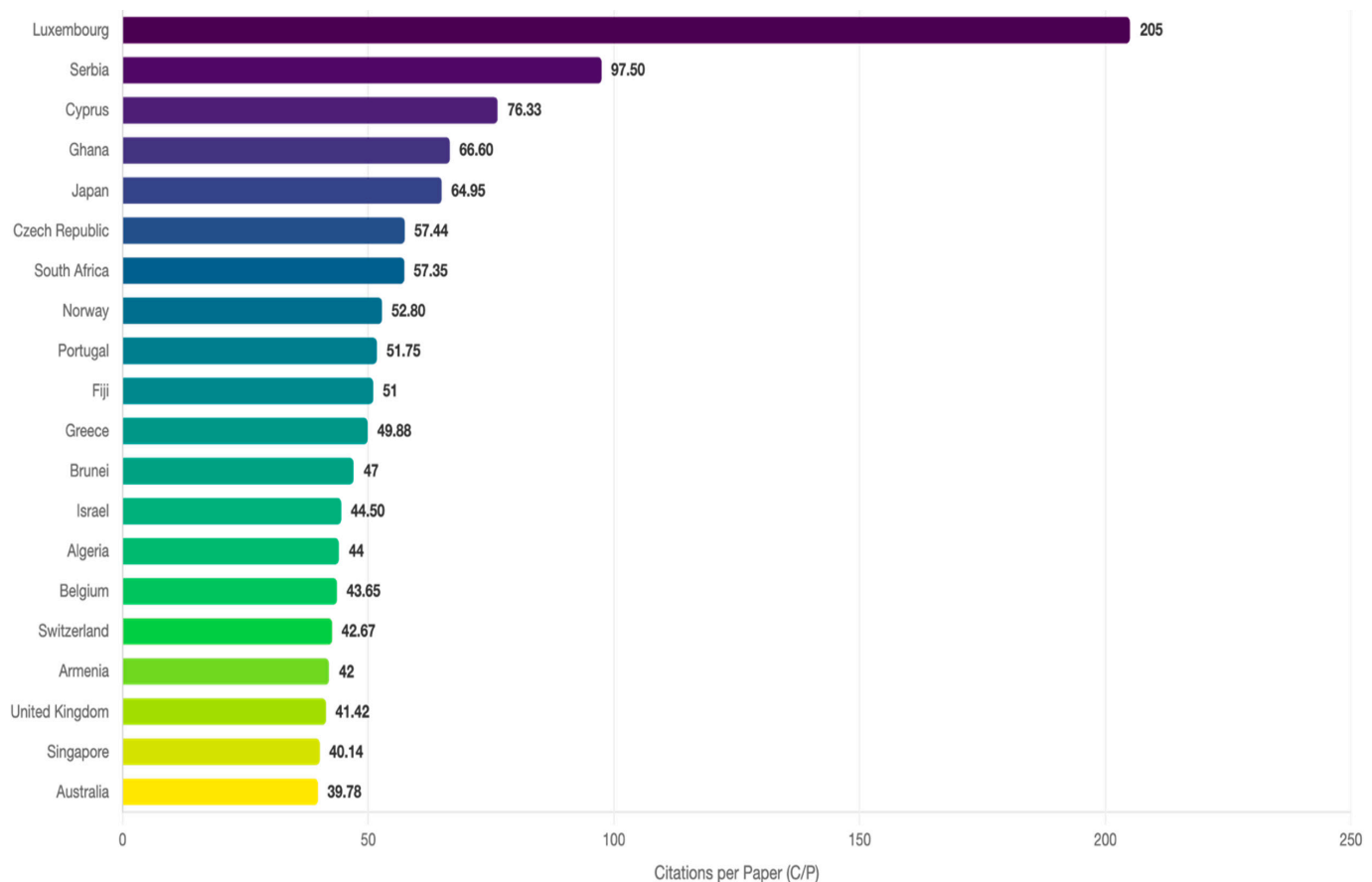


Figure 17. Top Countries. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

4.11. Intellectual Structure of the Research Field

Table 20 and Figure 20 present the Reference Publication Year Spectroscopy (RPYS) analysis, which identifies the historical foundations of AI research in financial fraud detection. Several citation peaks are observed, particularly in the 1950s, 1960s, and early 1970s, indicating the influence of seminal methodological and computational studies that have shaped subsequent research. These peaks represent foundational works that continue to serve as the intellectual basis for modern AI and fraud detection research.

Table 21 illustrate the intellectual evolution of the field through the historiograph. We determined local citations by matching cited references to dataset records using the first-author surname, publication year, volume and first page, DOI, or a normalized title combined with the first-author surname and year. After validation, local citations are lower than global citations for all historiograph nodes. Bhattacharyya et al. (2011) and Ngai et al. (2011) occupy central positions, with citation pathways extending from Whitrow et al. (2009), Bhattacharyya et al. (2011), and Dal Pozzolo et al. (2014) through Jurgovsky et al. (2018) and Fiore et al. (2019) to more recent ensemble and deep-learning studies, including Taha and Malebary (2020), Forough and Momtazi (2021), Esenogho et al. (2022), and Alarfaj et al. (2022). Seventeen of the twenty nodes focus on credit card fraud, highlighting its central role in the field's intellectual development. The accounting fraud studies of Kirkos et al. (2007) and Ravisankar et al. (2011) form a separate methodological strand that is subsequently connected to payment-fraud research, indicating a predominantly payment-centered intellectual lineage.

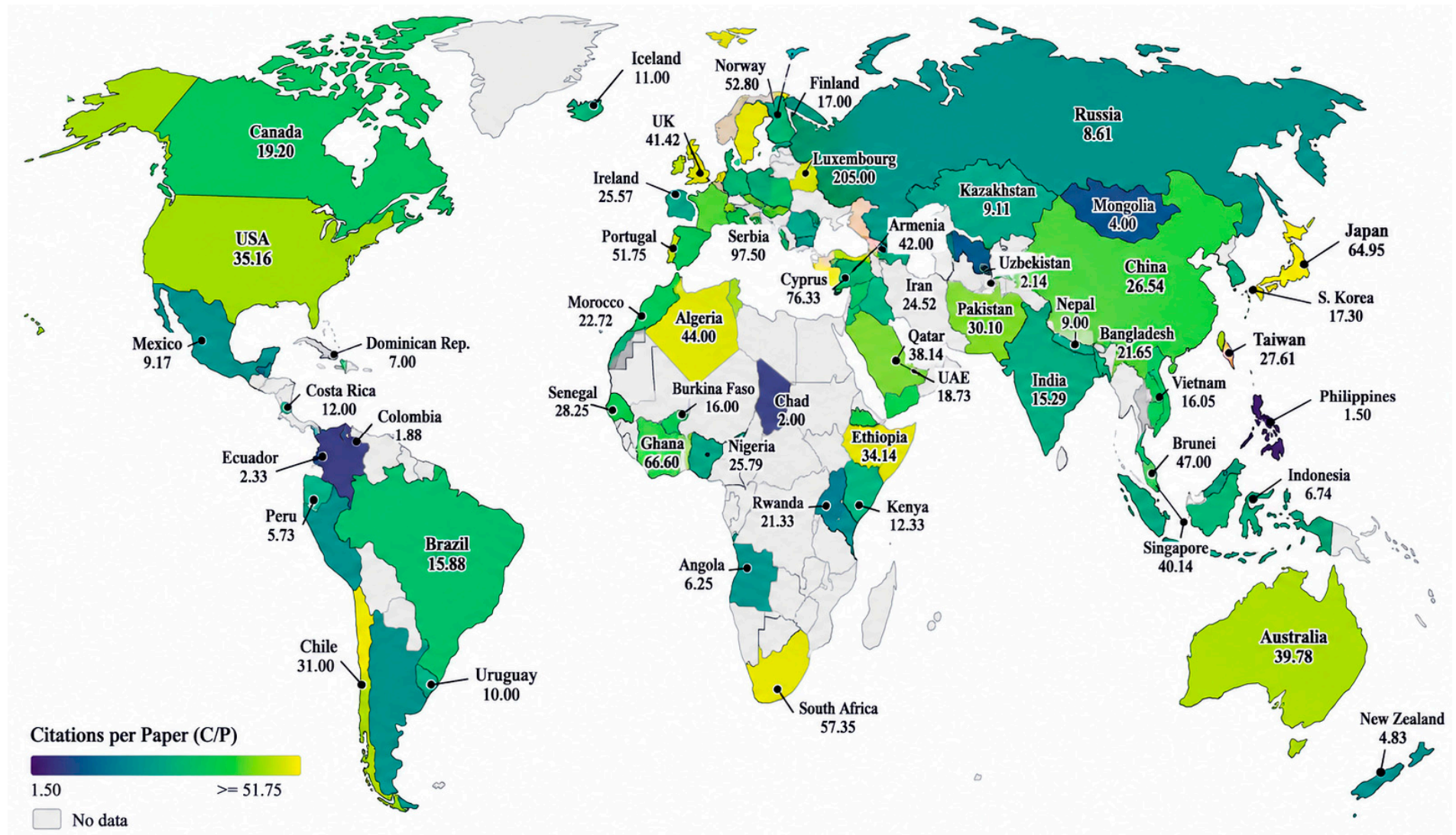


Figure 18. World Map. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

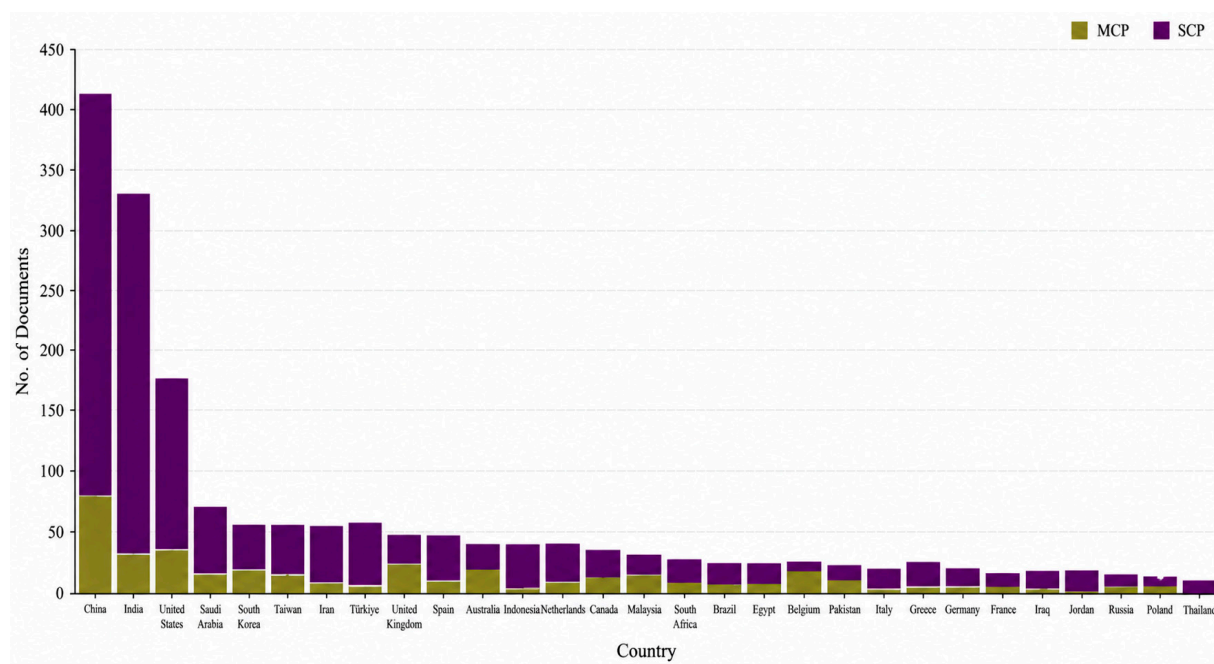


Figure 19. Country Collaboration. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

Table 20. RPYS Table.

Year	Citations	diffMedian5	diffMedian2	diffMedian
1950	15	3	1.5	3
1951	12	−1.5	0	−1.5
1952	8	−4	−4	−4
1953	38	30	30	30
1954	6	0	0	0
1955	5	−1	−1	−1
1956	6	0	0	0
1957	9	0	0	0
1958	26	16	16	16
1959	10	−1	−1	−1
1960	11	−5	0	−5
1961	16	0	0	0
1962	19	3	0	3
1963	20	1	1	1
1964	10	−10	−10	−10
1965	32	0	0	0
1966	42	0	0	0
1967	43	1	0	1
1968	57	15	14	15
1969	24	−7	−7	−7
1970	31	0	7	0
1971	21	−10	−10	−10
1972	54	16	16	16
1973	38	−7	−7	−7
1974	45	−9	0	−9

Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

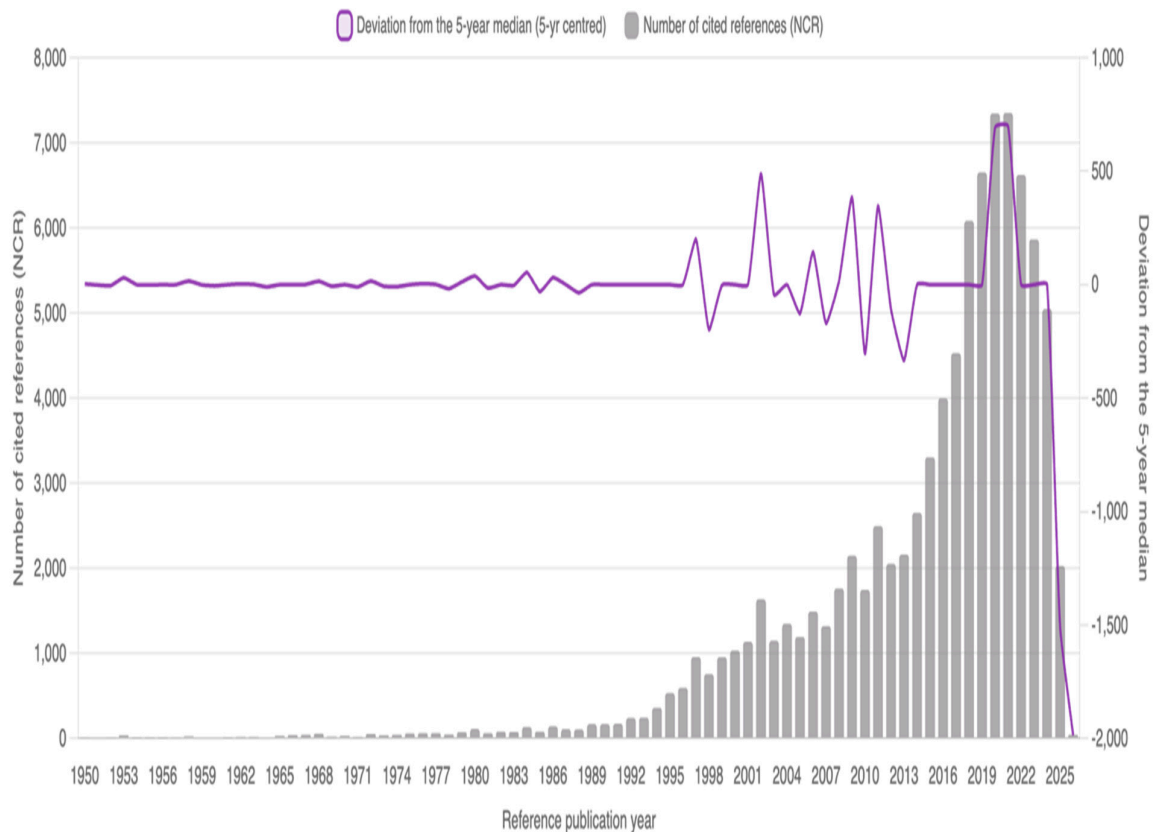


Figure 20. Reference Spectroscopy (RPYS). Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

Table 21. Historiograph Nodes.

Publication	Title	Year	Source	Global Cit.	Local Cit.
Bhattacharyya et al.	Data mining for credit card fraud: A comparative study	2011	Decision Support Systems	832	151
Ngai et al.	The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature	2011	Decision Support Systems	1041	138
Randhawa et al.	Credit Card Fraud Detection Using AdaBoost and Majority Voting	2018	IEEE Access	192	112
Esenogho et al.	A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection	2022	IEEE Access	311	101
Dal Pozzolo et al.	Learned lessons in credit card fraud detection from a practitioner perspective	2014	Expert Systems with Applications	265	101
Jurgovsky et al.	Sequence classification for credit-card fraud detection	2018	Expert Systems with Applications	238	100
Fiore et al.	Using generative adversarial networks for improving classification effectiveness in credit card fraud detection	2019	Information Sciences	327	94

Table 21. Cont.

Publication	Title	Year	Source	Global Cit.	Local Cit.
Taha and Malebary	An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine	2020	IEEE Access	368	91
Alarfaj et al.	Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms	2022	IEEE Access	374	85
Ravisankar et al.	Detection of financial statement fraud and feature selection using data mining techniques	2011	Decision Support Systems	450	81
Bahnsen et al.	Feature engineering strategies for credit card fraud detection	2016	Expert Systems with Applications	205	79
Makki et al.	An Experimental Study with Imbalanced Classification Approaches for Credit Card Fraud Detection	2019	IEEE Access	142	76
Ileberi et al.	A machine learning-based credit card fraud detection using the GA algorithm for feature selection	2022	Journal Of Big Data	340	75
Forough and Momtazi	Ensemble of deep sequential models for credit card fraud detection	2021	Applied Soft Computing	126	74
Sahin et al.	A cost-sensitive decision tree approach for fraud detection	2013	Expert Systems with Applications	344	70
Alfaiz and Fati	Enhanced Credit Card Fraud Detection Model Using Machine Learning	2022	Electronics	201	70
Kirkos et al.	Data Mining techniques for the detection of fraudulent financial statements	2007	Expert Systems with Applications	520	68
Whitrow et al.	Transaction aggregation as a strategy for credit card fraud detection	2009	Data Mining and Knowledge Discovery	164	65
Zhang et al.	HOBA: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture	2021	Information Sciences	220	61
Pumsirirat and Yan	Credit Card Fraud Detection using Deep Learning based on Autoencoder and Restricted Boltzmann Machine	2018	International Journal of Advanced Computer Science and Applications	289	60

4.12. Conceptual Structure of the Research Field

Figure 21 and Table 22 illustrate how research topics have evolved over time. Fraud detection, machine learning, and credit card fraud detection remain the dominant themes throughout the study period, while more recent years show increasing attention to artificial intelligence, deep learning, and anomaly detection. These trends indicate a gradual shift from traditional data mining approaches toward more advanced AI-driven techniques.

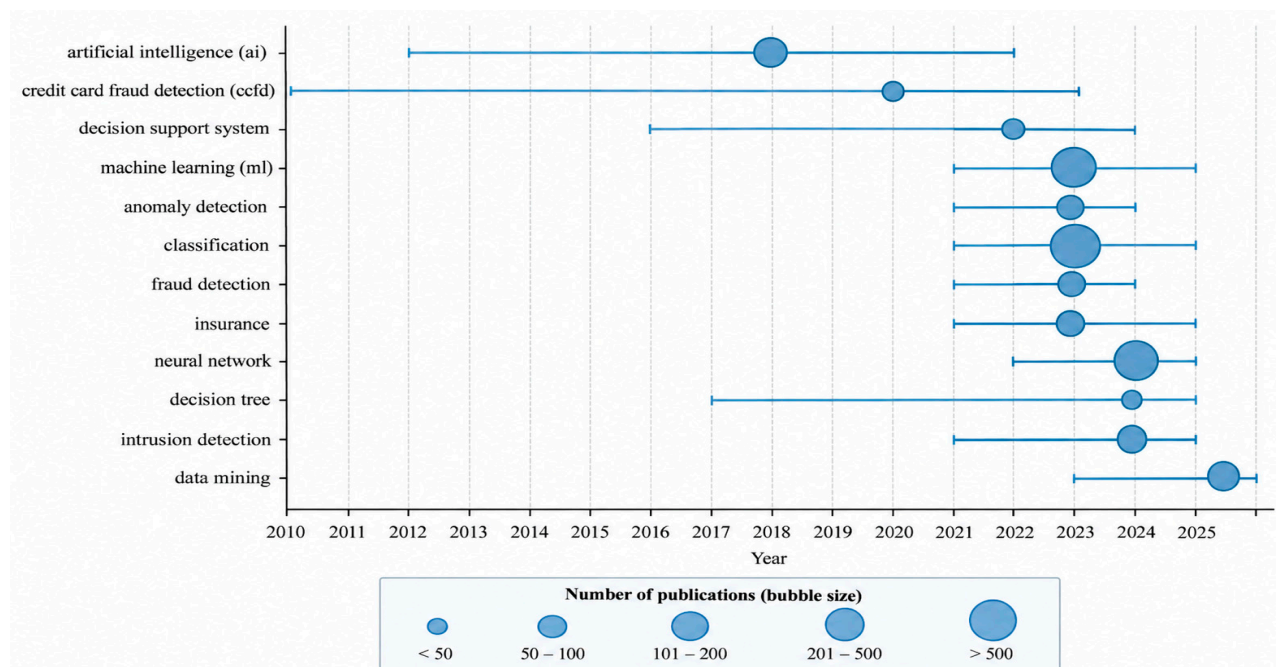


Figure 21. Keyword Trend Topics. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

Table 22. Trend Topics.

Term	Frequency	Year (Q1)	Year (Median)	Year (Q3)
artificial intelligence (ai)	199	2023	2025	2025
credit card fraud detection (ccfd)	375	2021	2024	2025
decision support system	14	2017	2024	2025
machine learning (ml)	620	2022	2024	2025
anomaly detection	208	2021	2023	2025
classification	172	2021	2023	2024
fraud detection	1073	2021	2023	2025
insurance	79	2021	2023	2024
neural network	336	2021	2023	2025
decision tree	56	2016	2022	2024
intrusion detection	21	2010	2020	2023
data mining	183	2012	2018	2022

Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

Table 23 identifies the most rapidly developing research topics. In this table, recent activity refers to 2024 to 2026 (including the incomplete year 2026), ADY is the average number of documents per year in that window, and RAI is the share of a topic's documents published in it. Because raw counts in a rapidly growing field increase for almost every topic, we complemented the classification with a comparison of each topic's share of all publications in the complete windows 2020 to 2022 and 2023 to 2025 (Appendix A, Table A5). On this basis, artificial intelligence (from 4.4% to 12.7% of publications), explainable AI (from 1.2% to 4.8%), cybersecurity (from 2.7% to 4.7%), and blockchain (from 1.7% to 3.0%)

show measurable acceleration, whereas the shares of anomaly detection and support vector machines declined. Graph learning, federated learning, and large language models also grew, but they appear in fewer than 20 recent publications each, so their trajectories are indicative only, and they are treated as proposed rather than established research directions.

Table 23. Emerging Topics Ranking.

#	Term	Category	Total	Recent	ADY	RAI %	GR %	Momentum
1	fraud detection	Hot	1073	519	173.00	48.4	63.7	1573.1
2	machine learning (ml)	Hot	620	322	107.33	51.9	57.8	899.4
3	credit card fraud detection (ccfd)	Hot	375	190	63.33	50.7	68.1	489.3
4	neural network	Hot	336	159	53.00	47.3	50.0	401.9
5	artificial intelligence (ai)	Emerging	199	143	47.67	71.9	248.8	329.0
6	deep learning (dl)	Hot	245	132	44.00	53.9	57.1	315.6
7	class imbalance	Stable	234	113	37.67	48.3	34.5	267.9
8	anomaly detection	Hot	208	99	33.00	47.6	65.0	229.7
9	classification	Stable	172	66	22.00	38.4	4.8	147.7
10	ensemble learning	Hot	132	69	23.00	52.3	64.3	146.5
11	random forest (rf)	Stable	124	60	20.00	48.4	30.4	125.8
12	extreme gradient boosting (xgboost)	Hot	85	46	15.33	54.1	53.3	89.0
13	data sampling	Stable	101	39	13.00	38.6	−7.1	78.3
14	big data	Stable	99	39	13.00	39.4	39.3	78.0
15	cybersecurity	Hot	73	41	13.67	56.2	51.9	76.6
16	smote	Hot	66	40	13.33	60.6	135.3	73.0
17	security	Hot	66	38	12.67	57.6	153.3	69.4
18	feature extraction	Hot	56	39	13.00	69.6	160.0	68.5
19	blockchain	Emerging	51	38	12.67	74.5	245.5	65.2
20	support vector machine (svm)	Stable	101	32	10.67	31.7	−5.9	64.3
21	feature selection	Hot	65	34	11.33	52.3	61.9	61.9
22	data models	Emerging	49	35	11.67	71.4	191.7	59.5
23	insurance	Stable	79	30	10.00	38.0	3.4	57.1
24	autoencoder (ae)	Stable	68	31	10.33	45.6	14.8	57.0
25	unsupervised learning	Stable	66	29	9.67	43.9	38.1	53.0

Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

Table 24 and Figure 22 present the keyword co-occurrence network, showing that fraud detection, machine learning, credit card fraud detection, neural networks, and deep learning occupy central positions in the field's conceptual structure of the field. These highly connected keywords form the core knowl demonstrate the close integration of AI techniques with fraud detection applications.

Table 25 and Figure 23 further reveal the conceptual clustering of research themes. The largest cluster is centered on machine learning, deep learning, neural networks, and related AI algorithms, while another major cluster focuses on credit card fraud detection, class imbalance, and data mining. These clusters indicate that current research is organized around two complementary streams: developing advanced AI methodologies and applying them to financial fraud detection problems.

Table 24. Terms.

#	Term	Cluster	Occurrences	Links	Total Link Strength	Relevance	Avg. Pub. Year	Avg. Citations	Avg. Norm. Citations	X	Y
1	fraud detection	2	1073	39	988.00	1073.000	2022.0	25.98	1.14	−0.030	0.167
2	machine learning (ml)	3	620	38	573.00	620.000	2023.0	21.81	1.18	0.370	0.554
3	credit card fraud detection (ccfd)	1	375	39	356.00	375.000	2022.4	31.49	1.37	0.217	−0.120
4	neural network	4	336	38	309.00	336.000	2021.9	23.46	1.17	−0.073	−0.472
5	deep learning (dl)	4	245	39	234.00	245.000	2023.3	27.71	1.41	−0.274	0.079
6	class imbalance	1	234	36	221.00	234.000	2022.8	20.79	1.28	0.488	−0.054
7	anomaly detection	2	208	39	175.00	208.000	2021.8	20.27	1.10	−0.830	0.225
8	artificial intelligence (ai)	3	199	37	177.00	199.000	2024.0	12.86	1.17	0.054	0.973
9	data mining	2	183	31	158.00	183.000	2016.6	45.57	0.86	0.304	−0.674
10	classification	1	172	37	160.00	172.000	2021.3	26.98	0.93	0.183	−0.443
11	ensemble learning	1	132	37	128.00	132.000	2022.7	21.91	1.32	0.244	0.241
12	random forest (rf)	1	124	38	120.00	124.000	2023.0	24.10	1.18	0.909	−0.084
13	data sampling	1	101	35	98.00	101.000	2022.3	28.03	1.24	0.418	−0.326
14	support vector machine (svm)	1	101	34	90.00	101.000	2020.5	29.50	0.87	0.630	−0.590
15	big data	3	99	30	86.00	99.000	2022.0	26.58	1.06	−0.116	0.469
16	extreme gradient boosting (xgboost)	1	85	35	84.00	85.000	2023.4	18.27	1.12	0.833	0.241
17	insurance	2	79	30	76.00	79.000	2021.5	22.10	0.89	−0.105	−0.173
18	cybersecurity	3	73	30	71.00	73.000	2023.6	21.81	1.28	−0.253	0.932
19	autoencoder (ae)	4	68	31	67.00	68.000	2023.0	24.56	1.25	−0.392	−0.362
20	security	3	66	30	61.00	66.000	2021.9	24.98	1.29	−0.315	0.742
21	smote	1	66	31	65.00	66.000	2023.5	21.67	1.29	0.658	−0.278
22	unsupervised learning	2	66	29	64.00	66.000	2021.9	22.36	0.93	−0.824	−0.037
23	feature selection	1	65	31	63.00	65.000	2022.5	25.75	0.82	0.702	0.453
24	logistic regression	1	56	26	53.00	56.000	2022.0	38.63	1.31	1.127	−0.304
25	decision tree	1	56	30	55.00	56.000	2019.5	18.75	0.73	0.923	−0.563

Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

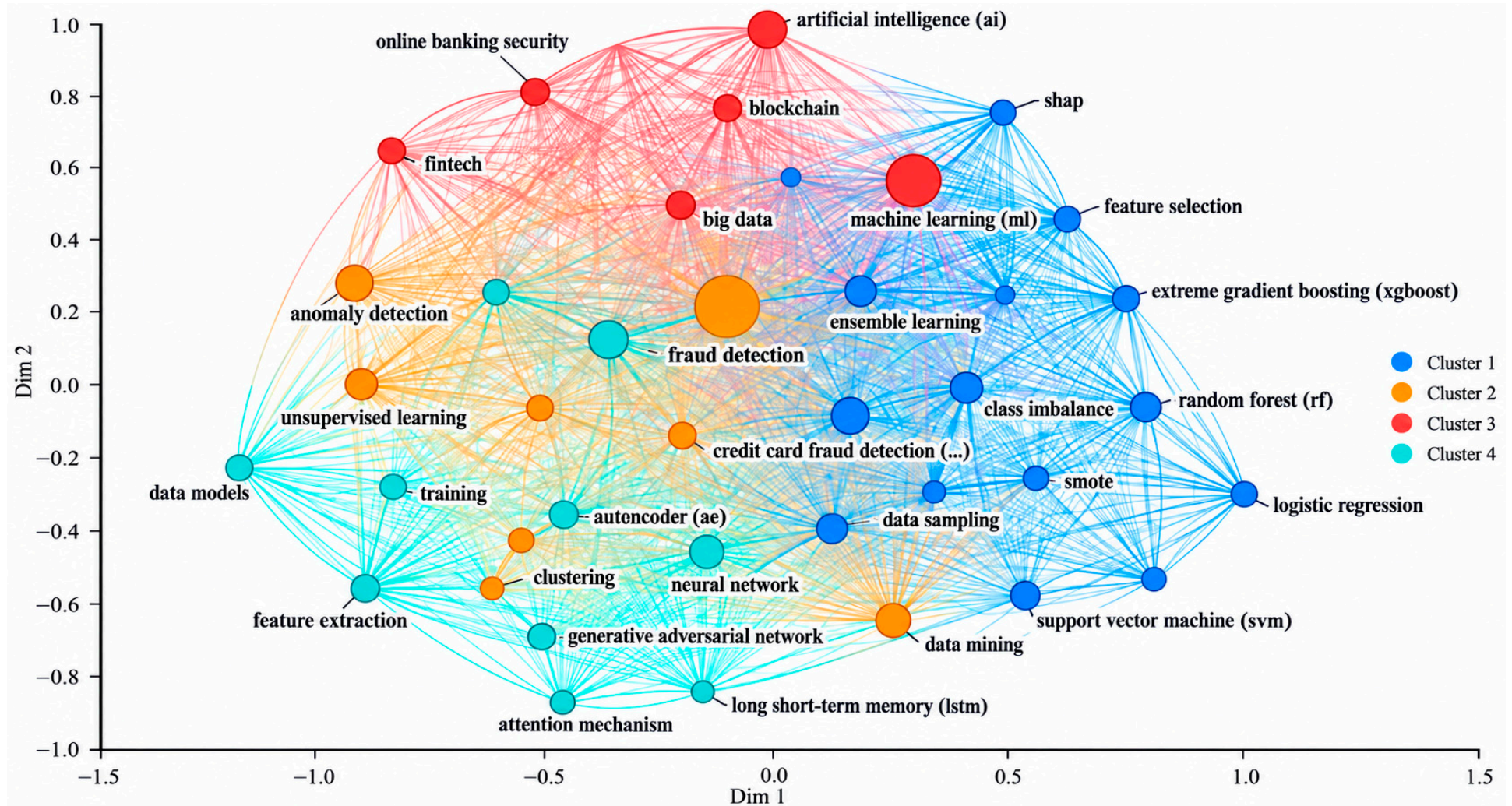


Figure 22. Network visualization of author keywords. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

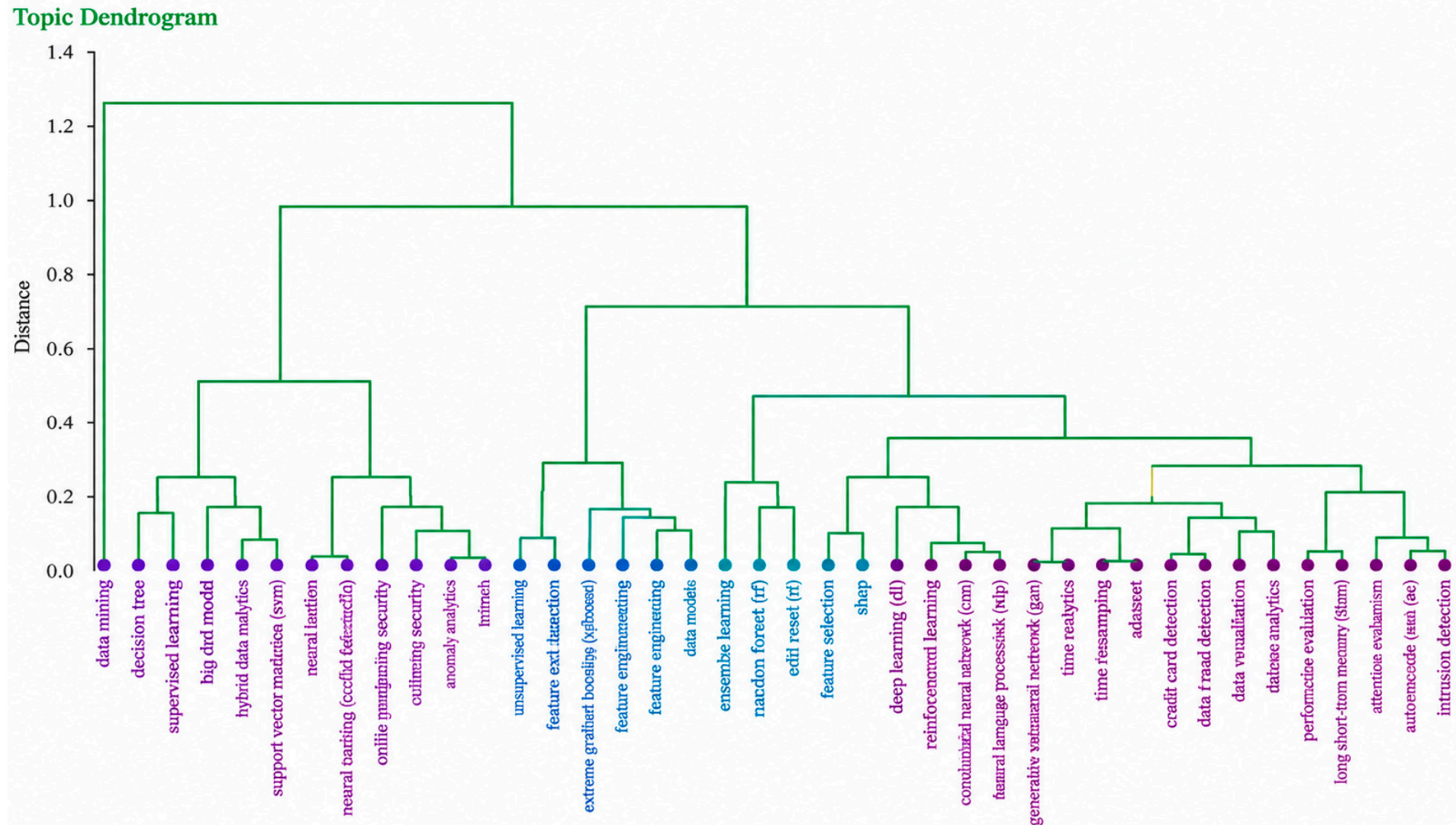


Figure 23. Topic Dendrogram. Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

Table 25. Words by Cluster.

Word	Dim1	Dim2	Cluster
machine learning (ml)	−0.0757	−0.0339	Cluster 1
neural network	0.2144	0.1006	Cluster 1
deep learning (dl)	0.4408	0.2584	Cluster 1
ensemble learning	−0.1285	0.1125	Cluster 1
big data	0.1773	0.0050	Cluster 1
autoencoder (ae)	0.3361	0.1901	Cluster 1
feature selection	−0.1614	0.0797	Cluster 1
feature extraction	0.1303	0.2025	Cluster 1
data models	0.1434	0.2036	Cluster 1
predictive modeling	0.0649	0.0874	Cluster 1
supervised learning	0.0290	−0.0762	Cluster 1
long short-term memory (lstm)	0.2729	0.2256	Cluster 1
generative adversarial network	0.0134	0.1999	Cluster 1
training	0.0277	0.1906	Cluster 1
feature engineering	0.0737	0.0476	Cluster 1
e-commerce	−0.0200	−0.0703	Cluster 1
attention mechanism	0.2645	0.1817	Cluster 1
credit card fraud detection (ccfd)	−0.3684	0.2198	Cluster 2
class imbalance	−0.5612	0.3234	Cluster 2
data mining	−0.5031	−1.0000	Cluster 2

Source: Generated by the author(s) using BiblioSpy® (Ahmi, 2026).

5. Discussion

5.1. Evolution of the Research Field

The bibliometric findings show that artificial intelligence (AI) has become one of the most dynamic research domains in financial fraud detection. The substantial increase in publications, citations, and international collaboration indicates that the field has progressed from an emerging topic to a mature and rapidly expanding area of research. This growth has been driven by the increasing digitalization of financial services, the complexity of modern fraud schemes, and advances in computational intelligence.

The field's evolution reflects a clear methodological transition. Early studies primarily relied on statistical analysis, expert systems, and data mining techniques to identify fraudulent transactions. As computational capabilities improved, research shifted toward machine learning algorithms capable of modeling nonlinear relationships and learning directly from historical financial data. More recently, deep learning architectures and intelligent anomaly detection methods have become increasingly dominant, reflecting the need to analyze high-dimensional and continuously evolving financial datasets.

The results further demonstrate that scientific production is concentrated within a relatively small number of influential journals, authors, institutions, and countries. This concentration approximates Bradford's and Lotka's laws, but departures from both are informative: the journal core is larger than Bradford's pattern implies, reflecting the field's dispersion across disciplines, and the steep Lotka exponent indicates that most contributors publish only once. The divergence between quantity and impact is also evident, since high-volume outlets such as IEEE Access absorb a large share of applied comparative studies, whereas a few selective journals, above all Decision Support Systems, publish the frameworks and reviews on which the field builds and accumulate the highest citations per publication. At the same time, the high level of international collaboration indicates that financial fraud detection has become a global research challenge requiring interdisciplinary expertise across artificial intelligence, computer science, finance, and cybersecurity.

5.2. Emerging Research Themes

The conceptual and intellectual analyses reveal four major research themes that currently define the field.

First, machine learning remains the dominant research paradigm. The high occurrence of keywords such as machine learning, fraud detection, and credit card fraud detection indicates that predictive classification continues to underpin most intelligent fraud detection systems. Traditional supervised algorithms remain widely adopted because they can achieve high predictive accuracy using historical labeled datasets.

Second, deep learning has become one of the fastest-growing research areas. Neural networks, autoencoders, and other deep architectures increasingly replace conventional machine learning algorithms because they automatically extract complex features from large-scale financial data. This transition reflects the increasing availability of big data and computational resources.

Third, anomaly detection has emerged as a core research direction. Because fraudulent transactions are rare and continuously evolving, researchers increasingly use unsupervised and semi-supervised approaches that can identify abnormal behavioral patterns without relying exclusively on labeled fraud data.

Finally, the literature shows growing interest in next-generation technologies, but the strength of the evidence differs across them. Explainable AI, cybersecurity, and blockchain show measurable increases in their share of publications, whereas graph learning, federated learning, and large language models appear in too few publications for their growth to be established and are better regarded as proposed directions. The pattern indicates that the research focus is gradually shifting from predictive accuracy toward transparent, secure, and scalable fraud detection systems suitable for real-world financial environments.

5.3. Implications for Finance, Accounting, Auditing and Regulation

The bibliometric structure of the field has direct implications for the economics of fraud detection. The first concerns the costs of classification errors. Fraud detection systems generate two types of costs: undetected fraud produces direct losses, whereas false alarms generate investigation costs, declined legitimate transactions, and customer attrition. Because these costs are asymmetric, the economically relevant objective is minimizing expected costs rather than maximizing accuracy (Bahnsen et al., 2016; Sahin et al., 2013). The prominence of class imbalance, SMOTE, and accuracy-oriented model comparisons in the keyword and trend analyses suggests that much of the literature optimizes statistical performance on benchmark data, which may overstate the economic value of the proposed models; cost-based and alert-budget metrics that reflect the investigation capacity of financial institutions would provide a more relevant basis for evaluation.

The second implication concerns information asymmetry and fraudsters' strategic behavior. Fraud exploits private information about the legitimacy of transactions, claims, or financial reports, and detection systems reduce this asymmetry only as far as they remain effective when offenders adapt (Akerlof, 1970; Becker, 1968). Evaluation designs that ignore temporal change therefore risk overstating the durable value of detection models, and out-of-time validation and evidence from operational deployments are required to assess their economic effect.

The third implication concerns regulatory constraints, model risk, and the trade-off between effectiveness and explainability. Detection models used by banks and insurers fall within model risk management frameworks that require documentation, validation, and ongoing monitoring (Board of Governors of the Federal Reserve System & Office of the Comptroller of the Currency, 2011), and the regulation of AI in the European Union imposes transparency and human oversight requirements (Regulation (EU) 2024/1689,

2024). The measurable growth of explainable AI can be in may reflect to these constraints. Complex ensemble and deep learning models may improve detection rates, but when investigators, customers, auditors, or supervisors cannot understand their decisions, part of their performance advantage is offset by higher model risk and compliance costs, and interpretable models may be preferable for high-stakes decisions (Rudin, 2019).

The fourth implication concerns the domains that receive limited attention. Anti-money laundering, tax fraud, and securities fraud together account for less than 7% of the publications, although they are central to the work of regulators and supervisory authorities, while accounting and financial statement fraud, which directly concerns auditors, represents about 7% of the publications but achieves high citation impact. For auditing, the evidence indicates that machine learning can complement traditional analytical procedures, particularly when it exploits raw accounting data and textual disclosures (Bao et al., 2020; Hajek & Henriques, 2017), but the implications for audit evidence, professional skepticism, and auditor liability remain largely unexplored. The predominance of Computer Science and Engineering outlets further suggests that closer collaboration between computer scientists, finance and accounting researchers, financial institutions and supervisory authorities is needed to generate evidence on the economic consequences of implementing AI in financial institutions.

5.4. Research Gaps and Future Research Directions

Despite the field's remarkable development, several important opportunities remain for future research. Table 26 summarizes the principal research gaps, the evidence supporting each gap and the type of that evidence, together with corresponding future research directions. Gaps supported by bibliometric indicators are distinguished from directions proposed on conceptual grounds, which should be regarded as hypotheses requiring verification through systematic content analysis of individual studies.

Table 26. Research Gaps and Future Research Directions Summary.

Research Gap	Evidence from Bibliometric Findings	Type of Evidence	Future Research Direction
Heavy concentration on credit card fraud detection	Credit card and payment fraud is the largest domain (23.9% of publications) and accounts for 17 of the 20 historiograph nodes; anti-money laundering, tax fraud and securities fraud together account for less than 7%.	Bibliometric (domain classification, historiograph)	Extend AI applications to insurance fraud, accounting fraud, securities fraud, anti-money laundering, tax fraud, cryptocurrency fraud and decentralized finance.
Limited interdisciplinary integration	Publications are concentrated in Computer Science and Engineering, with relatively few in Business, Economics and Finance categories.	Bibliometric (subject areas, sources)	Promote collaboration integrating AI with finance, accounting, auditing, regulation, law and behavioral sciences.
Limited model interpretability	Explainable AI shows the clearest measured growth in the share of publications but remains a small part of the literature.	Bibliometric (normalized keyword growth)	Develop transparent and explainable models that satisfy regulatory, model risk and managerial requirements.

Table 26. Cont.

Research Gap	Evidence from Bibliometric Findings	Type of Evidence	Future Research Direction
Dependence on supervised learning and benchmark data	Class imbalance, SMOTE and supervised classifiers dominate the keyword network and trend topics.	Bibliometric (keyword co-occurrence); prevalence of benchmark-only evaluation requires verification	Investigate semi-supervised, self-supervised and continual learning, and evaluate models on institutional data with out-of-time validation.
Limited real-world implementation studies	Few keywords refer to deployment or operational settings.	Proposed direction; requires content analysis of individual studies	Conduct industry-based validation and report deployment case studies in partnership with financial institutions.
Evaluation misaligned with economic costs	Accuracy-oriented comparisons are prominent, whereas cost-sensitive learning appears rarely among keywords.	Bibliometric (keyword frequencies); requires content analysis	Adopt cost-sensitive and alert-budget metrics and standardized, reproducible evaluation protocols.
Privacy, fairness and governance	Fairness, bias and governance terms are rare among author keywords.	Proposed direction; requires content analysis	Investigate bias in fraud alerts, privacy-preserving collaboration and governance frameworks.
Emerging AI technologies	Graph learning, federated learning and large language models grew but appear in fewer than 20 recent publications each; blockchain shows moderate measured growth.	Indicative bibliometric evidence (low frequencies)	Assess graph learning in network-based fraud and treat generative AI and large language models as hypotheses to be tested.

The identified gaps suggest that future research should move beyond improving predictive performance alone. As artificial intelligence systems become increasingly integrated into financial decision-making, future research should place greater emphasis on explainability, robustness, privacy, fairness, and regulatory compliance. Moreover, expanding AI applications beyond traditional credit card fraud and evaluating emerging technologies such as graph neural networks, federated learning, and generative AI, whose bibliometric footprint remains small, may contribute to more trustworthy and scalable fraud detection systems. Addressing these challenges will not only advance the scientific understanding of AI-enabled fraud detection but also facilitate its practical adoption across diverse financial sectors.

6. Conclusions

This study presents a comprehensive bibliometric analysis of artificial intelligence (AI) research on financial fraud detection, based on 2200 publications indexed in the Scopus and Web of Science databases between 1992 and 29 June 2026, with duplicate and relevance checks confirming the robustness of the main findings. Using performance analysis, science mapping, bibliometric laws, and research life-cycle modeling, the study provides a systematic overview of the field's scientific development, intellectual foundations, collaboration patterns, and conceptual evolution. The findings confirm that AI has become a core technology for financial fraud detection, with machine learning, deep learning, and anomaly detection as the principal research directions; explainable AI shows the clearest measurable

acceleration, while graph learning, federated learning, and generative AI remain promising but emerging areas. The growth analysis indicates continued expansion but does not support precise long-term forecasts of the field's size.

This study extends the existing literature by providing a holistic bibliometric assessment of AI research in financial fraud detection. Unlike previous review studies that primarily synthesize algorithms or specific fraud applications, this research integrates performance indicators, science mapping, bibliometric laws, and knowledge structure analyses to provide a comprehensive understanding of the field. The findings establish a reference framework for future bibliometric studies and improve understanding of the evolution, intellectual structure, and emerging research directions of AI-enabled financial fraud detection.

The findings offer practical value for multiple stakeholders. Researchers can use the identified influential journals, authors, institutions, and emerging topics to guide future investigations and collaborations. Financial institutions may benefit from the identified technological trends when developing more effective AI-driven fraud detection systems, while policymakers and regulators can use the findings to support governance frameworks that promote transparent, reliable, and responsible AI adoption within financial services.

This study is limited to publications indexed in the Scopus and Web of Science databases and focuses on bibliometric relationships rather than the comparative technical performance of AI algorithms. Because the dataset was retrieved through keyword searches that include database-assigned keywords, part of the dataset addresses non-financial fraud or mentions fraud only incidentally; the robustness check shows that the main rankings are unchanged when these records are removed, but indicators for smaller units should be interpreted with caution. In addition, 2026 is an incomplete publication year, and the relevance verification and domain classification rely on titles, abstracts, and keywords rather than full texts. Future research should investigate underexplored fraud domains, including insurance fraud, anti-money laundering, cryptocurrency fraud, and decentralized finance, and examine emerging technologies such as explainable AI, graph neural networks, federated learning, generative AI, and large language models. Greater interdisciplinary collaboration and the use of real-world financial datasets will further enhance the practical relevance and applicability of AI-based fraud detection research.

Supplementary Materials: The following supporting information can be downloaded at: <https://www.mdpi.com/article/10.3390/jrfm19100819/s1>, PRISMA 2020 Checklist (Page et al., 2021).

Author Contributions: Conceptualization, W.A.-S., K.A. and Y.I.; methodology, W.A.-S., K.A. and Y.I.; software, W.A.-S. and Y.I.; validation, W.A.-S. and Y.I.; formal analysis, W.A.-S., K.A. and Y.I.; investigation, W.A.-S. and K.A. resources, W.A.-S. and K.A. data curation, W.A.-S., K.A. and Y.I. writing—original draft preparation, W.A.-S., K.A. and Y.I.; writing—review and editing, W.A.-S., K.A. and Y.I.; visualization, W.A.-S., K.A. and Y.I.; supervision, W.A.-S. and Y.I.; project administration, W.A.-S. and K.A.; funding acquisition, W.A.-S. and K.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Kuwait Foundation for the Advancement of Sciences (KFAS) under project code PY24-9OB-2554.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data is available upon request.

Acknowledgments: The authors would like to thank the Gulf University for Science and Technology (GUST), Kuwait, for its support of this research project. During preparation of this manuscript, ChatGPT 5.5 (OpenAI) and Grammarly assisted with language editing, grammar, spelling, punctuation, readability, clarity, and overall writing quality. ChatGPT 5.5 was also used to develop the initial concept and design of Figures 1 and 2. The authors carefully reviewed, verified, and revised all outputs and take full responsibility for the accuracy, originality, interpretation, and content of this manuscript.

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

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
ML	Machine Learning
DL	Deep Learning
CNN	Convolutional Neural Network
RNN	Recurrent Neural Network
LSTM	Long Short-Term Memory
GNN	Graph Neural Network
GAN	Generative Adversarial Network
SVM	Support Vector Machine
XGBoost	Extreme Gradient Boosting
LightGBM	Light Gradient Boosting Machine
NLP	Natural Language Processing
XAI	Explainable Artificial Intelligence
WoS	Web of Science Core Collection
RMSE	Root Mean Square Error
AIC	Akaike Information Criterion
BIC	Bayesian Information Criterion
RCI	Relative Citation Impact
RPYS	Reference Publication Year Spectroscopy
KS	Kolmogorov–Smirnov Test
h-index	Hirsch Index
g-index	Egghe Index
m-index	m-index (normalized h-index)
e-index	Excess Citation Index
SJR	SCImago Journal Rank
SNIP	Source Normalized Impact per Paper
JIF	Journal Impact Factor
ABDC	Australian Business Deans Council Journal Ranking
AJG	Academic Journal Guide
MDPI	Multidisciplinary Digital Publishing Institute
IEEE	Institute of Electrical and Electronics Engineers

Appendix A

Table A1. Database-specific search strings.

Database	Field and Query	Filters	Records Exported
Scopus	TITLE-ABS-KEY (fraud*) AND TITLE-ABS-KEY ("artificial intelligence" OR "machine learning" OR "deep learning" OR "neural network*" OR "convolutional neural network*" OR "recurrent neural network*" OR "graph neural network*" OR transformer* OR "support vector machine*" OR "decision tree*" OR "random forest*" OR xgboost OR lightgbm OR "gradient boosting" OR "logistic regression" OR "anomaly detection" OR "data mining" OR "predictive analytics" OR "natural language processing" OR "explainable AI")	DOCTYPE (ar); no language or year restriction; search date 29 June 2026	1063
Web of Science Core Collection	TS = (fraud*) AND TS = ("artificial intelligence" OR "machine learning" OR "deep learning" OR "neural network*" OR "convolutional neural network*" OR "recurrent neural network*" OR "graph neural network*" OR transformer* OR "support vector machine*" OR "decision tree*" OR "random forest*" OR xgboost OR lightgbm OR "gradient boosting" OR "logistic regression" OR "anomaly detection" OR "data mining" OR "predictive analytics" OR "natural language processing" OR "explainable AI")	Document type: Article; all Core Collection indexes; no language or year restriction; search date 29 June 2026	1466

Note: TITLE-ABS-KEY includes Scopus-indexed keywords, and TS includes Web of Science Keywords Plus.

Table A2. Relevance verification of the deduplicated records.

Criterion	Operational Rule	Records
Deduplicated records	Normalized DOI or normalized title and year (± 1) matching	2173
No fraud concept	No fraud-related term in title, abstract or author keywords (retrieved through indexed keywords or Keywords Plus)	77
No AI or data-mining method	No AI, machine learning or data mining term in title, abstract or author keywords	3
Non-financial fraud	Fraud context outside financial services, reporting, payments, insurance, taxation or markets (for example food, energy, advertising, education)	144
Fraud not the research focus	No fraud term in title or author keywords and fewer than two mentions of fraud in the abstract	328
Retracted	Record flagged as retracted	7
Verified core	Publications directly addressing AI-based financial fraud detection	1614

Table A3. Robustness of the main indicators to duplicates and out-of-scope records.

Indicator	Analytical Dataset (<i>n</i> = 2200)	Deduplicated (<i>n</i> = 2173)	Verified Core (<i>n</i> = 1614)
Total citations	52,679	51,271	40,061
Citations per publication	23.95	23.59	24.82
h-index/g-index	101/163	101/160	92/151
Five most productive sources (rank order)	IEEE Access; Expert Systems with Applications; IJACSA; Applied Sciences; Mathematics	Unchanged	Unchanged (Mathematics tied with the Journal of Theoretical and Applied Information Technology)
Three most productive countries	China; India; United States	Unchanged	Unchanged
Most productive author	Khoshgoftaar, T. M.	Unchanged	Unchanged
Five most frequent author keywords	Fraud detection; machine learning; credit card fraud detection; neural network; deep learning	Unchanged	Unchanged

Note: IJACSA = International Journal of Advanced Computer Science and Applications. Rankings in the deduplicated and verified datasets were computed with the same definitions as in the main analysis.

Table A4. Distribution of publications by financial fraud domain and period.

Domain	1992–2012	2013–2017	2018–2022	2023–2026	Total	Share (%)	C/P
Credit card and payment fraud	25	13	165	323	526	23.9	32.0
Banking, loan and transaction fraud	8	9	72	146	235	10.7	17.8
Insurance fraud	21	4	70	93	188	8.5	25.8
Accounting and financial statement fraud	22	14	37	83	156	7.1	32.3
Securities, cryptocurrency and market fraud	8	3	20	56	87	4.0	22.1
Anti-money laundering	4	0	7	9	20	0.9	17.1
Tax, customs and public-sector fraud	2	1	13	19	35	1.6	11.0
E-commerce, telecom and other consumer fraud	18	6	22	58	104	4.7	14.0
General or multi-domain financial fraud	14	12	69	195	290	13.2	22.2
Non-financial fraud or fraud not the research focus	50	48	196	265	559	25.4	20.1
Total	172	110	671	1247	2200	100.0	23.9

Note: Each publication is assigned to one domain on the basis of its title and author keywords, or its abstract when these are not informative; general reviews and multi-domain studies form a separate category. The last category contains the records identified by the relevance verification. C/P = citations per publication.

Table A5. Change in the share of publications using selected keyword families between 2020–2022 and 2023–2025.

Keyword Family	Total	2020–2022	2023–2025	Share 2020–2022 (%)	Share 2023–2025 (%)	Change in Share (%)
Artificial intelligence	199	23	133	4.4	12.7	185.3
Explainable AI (including SHAP and LIME)	67	6	50	1.2	4.8	311.1
Graph neural networks and graph learning	23	1	16	0.2	1.5	689.3
Blockchain	54	9	31	1.7	3.0	69.9
Federated learning	18	1	16	0.2	1.5	689.3
Large language models and generative AI	15	0	11	0.0	1.0	n.a.
Deep learning	245	64	144	12.4	13.7	11.0
Ensemble learning	165	38	92	7.4	8.8	19.4
Anomaly detection	226	59	97	11.4	9.3	−18.9
Support vector machine	116	37	45	7.2	4.3	−40.0
Cybersecurity	75	14	49	2.7	4.7	72.7

References

- Ahmi, A. (2026). *BiblioSpy*. Available online: <https://bibliospy.me> (accessed on 25 June 2026).
- Akerlof, G. A. (1970). The market for “lemons”: Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, 84(3), 488–500. [\[CrossRef\]](#)
- Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. *IEEE Access*, 10, 39700–39715. [\[CrossRef\]](#)
- Aria, M., & Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, 11(4), 959–975. [\[CrossRef\]](#)
- Bahnsen, A. C., Aouada, D., Stojanovic, A., & Ottersten, B. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications*, 51, 134–142. [\[CrossRef\]](#)
- Bao, Y., Ke, B., Li, B., Yu, Y. J., & Zhang, J. (2020). Detecting accounting fraud in publicly traded U.S. firms using a machine learning approach. *Journal of Accounting Research*, 58(1), 199–235. [\[CrossRef\]](#)
- Becker, G. S. (1968). Crime and punishment: An economic approach. *Journal of Political Economy*, 76(2), 169–217. [\[CrossRef\]](#)
- Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, 50(3), 602–613. [\[CrossRef\]](#)
- Board of Governors of the Federal Reserve System & Office of the Comptroller of the Currency. (2011). *Supervisory guidance on model risk management* (SR letter 11-7). Board of Governors of the Federal Reserve System.
- Bradford, S. C. (1934). Sources of information on specific subjects. *Engineering*, 137, 85–86.
- Chan, P. K., Fan, W., Prodromidis, A. L., & Stolfo, S. J. (1999). Distributed data mining in credit card fraud detection. *IEEE Intelligent Systems and Their Applications*, 14(6), 67–74. [\[CrossRef\]](#)
- Clauset, A., Shalizi, C. R., & Newman, M. E. J. (2009). Power-law distributions in empirical data. *SIAM Review*, 51(4), 661–703. [\[CrossRef\]](#)
- Dal Pozzolo, A., Caelen, O., Le Borgne, Y., Waterschoot, S., & Bontempi, G. (2014). Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications*, 41(10), 4915–4928. [\[CrossRef\]](#)
- Dechow, P. M., Ge, W., Larson, C. R., & Sloan, R. G. (2011). Predicting material accounting misstatements. *Contemporary Accounting Research*, 28(1), 17–82. [\[CrossRef\]](#)
- 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. [\[CrossRef\]](#)
- Egghe, L. (1986). The dual of Bradford’s law. *Journal of the American Society for Information Science*, 37(4), 246–255. [\[CrossRef\]](#)
- Egghe, L. (2006). Theory and practice of the g-index. *Scientometrics*, 69(1), 131–152. [\[CrossRef\]](#)
- Esenogho, E., Mienye, I. D., Swart, T. G., Aruleba, K., & Obaido, G. (2022). A neural network ensemble with feature engineering for improved credit card fraud detection. *IEEE Access*, 10, 16400–16407. [\[CrossRef\]](#)
- Fawcett, T., & Provost, F. (1997). Adaptive fraud detection. *Data Mining and Knowledge Discovery*, 1(3), 291–316. [\[CrossRef\]](#)
- Fiore, U., De Santis, A., 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. [\[CrossRef\]](#)
- Forough, J., & Momtazi, S. (2021). Ensemble of deep sequential models for credit card fraud detection. *Applied Soft Computing*, 99, 106883. [\[CrossRef\]](#)
- Garfield, E. (2004). Historiographic mapping of knowledge domains literature. *Journal of Information Science*, 30(2), 119–145. [\[CrossRef\]](#)
- Goldstein, M., & Uchida, S. (2016). A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. *PLoS ONE*, 11(4), e0152173. [\[CrossRef\]](#)
- Hajek, P., & Henriques, R. (2017). Mining corporate annual reports for intelligent detection of financial statement fraud—A comparative study of machine learning methods. *Knowledge-Based Systems*, 128, 139–152. [\[CrossRef\]](#)
- Hirsch, J. E. (2005). An index to quantify an individual’s scientific research output. *Proceedings of the National Academy of Sciences*, 102(46), 16569–16572. [\[CrossRef\]](#)
- Hyndman, R. J., & Athanasopoulos, G. (2021). *Forecasting: Principles and practice* (3rd ed.). OTexts.
- Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning-based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, 9(1), 24. [\[CrossRef\]](#)
- Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. *Expert Systems with Applications*, 100, 234–245. [\[CrossRef\]](#)
- Kirkos, E., Spathis, C., & Manolopoulos, Y. (2007). Data mining techniques for the detection of fraudulent financial statements. *Expert Systems with Applications*, 32(4), 995–1003. [\[CrossRef\]](#)
- Lotka, A. J. (1926). The frequency distribution of scientific productivity. *Journal of the Washington Academy of Sciences*, 16(12), 317–323.
- Marx, W., Bornmann, L., Barth, A., & Leydesdorff, L. (2014). Detecting the historical roots of research fields by reference publication year spectroscopy (RPYS). *Journal of the Association for Information Science and Technology*, 65(4), 751–764. [\[CrossRef\]](#)
- Mongeon, P., & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus. *Scientometrics*, 106, 213–228. [\[CrossRef\]](#)

- 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. [CrossRef]
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., . . . Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, 372, n71. [CrossRef]
- Pao, M. L. (1985). Lotka's law: A testing procedure. *Information Processing & Management*, 21(4), 305–320. [CrossRef]
- Perols, J. (2011). Financial statement fraud detection: An analysis of statistical and machine learning algorithms. *Auditing*, 30(2), 19–50. [CrossRef]
- Pourhabibi, T., Ong, K., Kam, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems*, 133, 113303. [CrossRef]
- 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. [CrossRef]
- Ravisankar, P., Ravi, V., Raghava Rao, G., & Bose, I. (2011). Detection of financial statement fraud and feature selection using data mining techniques. *Decision Support Systems*, 50(2), 491–500. [CrossRef]
- Regulation (EU) 2024/1689 of the European parliament and of the council of 13 June 2024 laying down harmonised rules on artificial intelligence (artificial intelligence act). *Official Journal of the European Union, L Series*. (2024). Available online: <https://eur-lex.europa.eu/TodayOJ/index.html> (accessed on 25 June 2026).
- Rudin, C. (2019). Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead. *Nature Machine Intelligence*, 1(5), 206–215. [CrossRef]
- Sahin, Y., Bulkan, S., & Duman, E. (2013). A cost-sensitive decision tree approach for fraud detection. *Expert Systems with Applications*, 40(15), 5916–5923. [CrossRef]
- Taha, A. A., & Malebary, S. J. (2020). An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. *IEEE Access*, 8, 25579–25587. [CrossRef]
- Tashman, L. J. (2000). Out-of-sample tests of forecasting accuracy: An analysis and review. *International Journal of Forecasting*, 16(4), 437–450. [CrossRef]
- Wang, Y., & Xu, W. (2018). Leveraging deep learning with LDA-based text analytics to detect automobile insurance fraud. *Decision Support Systems*, 105, 87–95. [CrossRef]
- Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). Transaction aggregation as a strategy for credit card fraud detection. *Data Mining and Knowledge Discovery*, 18(1), 30–55. [CrossRef]
- Yamanishi, K., Takeuchi, J., Williams, G., & Milne, P. (2004). On-line unsupervised outlier detection using finite mixtures with discounting learning algorithms. *Data Mining and Knowledge Discovery*, 8(3), 275–300. [CrossRef]
- Zhang, C. T. (2009). The e-index, complementing the h-index. *PLoS ONE*, 4(5), e5429. [CrossRef]
- Zhang, J., Yu, Q., Zheng, F., Long, C., Lu, Z., & Duan, Z. (2016). Comparing keywords plus of WOS and author keywords: A case study of patient adherence research. *Journal of the Association for Information Science and Technology*, 67(4), 967–972. [CrossRef]
- Zipf, G. K. (1949). *Human behavior and the principle of least effort*. Addison-Wesley.
- Zupic, I., & Čater, T. (2015). Bibliometric methods in management and organization. *Organizational Research Methods*, 18(3), 429–472. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.