Unveiling the potential of artificial intelligence in fraud detection: Trends and insights from a bibliometric perspective

Diana Witosari[1]*, Bandi[2]

[1] Faculty of Economics and Business, Universitas Sebelas Maret, Surakarta
[2] Faculty of Economics and Business, Universitas Sebelas Maret, Surakarta
*Correspondence email: dianawitosari@student.uns.ac.id

ARTICLE INFO

Article history:
Received : 3 July 2025
Accepted : 21 July 2025
Available : 31 July 2025

Keywords:
Fraud Detection, Artificial Intelligence, Machine Learning, Bibliometric Analysis, Financial Technology.

ABSTRACT

Digital transaction fraud is a growing concern that requires scalable detection solutions. Artificial Intelligence (AI) provides practical tools for uncovering complex fraud patterns through large-scale data analysis. This study conducted a bibliometric analysis of publications from 2013 to 2024, following the PRISMA protocol. Relevant literature was retrieved from major academic databases, with a focus on AI applications in fraud detection. The data were analyzed using VOSviewer to identify keyword trends, research clusters, country-level contributions, and collaboration networks. The findings reveal a significant rise in scholarly interest in recent years, with the financial and banking sectors as the primary application areas. Research is primarily dominated by developed countries, especially the United States, with universities acting as key research and funding centers. However, challenges remain, including limited access to quality datasets, the complexity of AI models, and ethical concerns related to data privacy and algorithmic fairness. AI shows strong potential in enhancing fraud detection; however, further research needs to address the technical and ethical obstacles to its broader implementation.

1. INTRODUCTION

In the current digital era, technological advancements have brought significant transformations across various sectors, including business, finance, and government. Innovations in information and communication technology have facilitated the emergence of diverse digital platforms that enable economic activities to occur faster, more efficiently, and with greater flexibility. Services such as e-commerce, mobile banking, digital payment systems, and electronic wallets (e-wallets) have revolutionized the way people conduct financial transactions. Digitalization has created substantial opportunities not only for businesses and consumers but also for governments in promoting inclusive and sustainable economic growth. However, alongside the convenience and efficiency offered, digital technology also presents vulnerabilities to increasingly complex cybercrimes, particularly fraud. Fraud in digital transactions poses a serious challenge, leading not only to substantial financial losses but also to the erosion of public trust in digital systems. According to the 2024 report by the Association of Certified Fraud Examiners (ACFE), 1,921 fraud cases were reported across 138 countries, resulting in losses totaling USD 3.1 billion (ACFE, 2024). In Indonesia, a 2019 fraud survey conducted by the ACFE Indonesia Chapter reported 239 fraud cases, resulting in financial losses of IDR 873.43 billion (ACFE, 2019). These data highlight the widespread and detrimental impact of fraud in the digital age, underscoring the urgent need for more adaptive fraud detection approaches.

According to Husnaningtyas & Dewayanto (2023), fraud detection is a critical process for identifying fraudulent activities within an organization. In the digital era, characterized by large volumes of data and high transaction speeds, fraud schemes have become increasingly diverse, sophisticated, and challenging to detect. Perpetrators exploit technological vulnerabilities and weak internal controls to conceal their illicit activities, often utilizing software tools and social engineering techniques to do so. While technological advancements offer numerous benefits, they may also inadvertently elevate the risk of fraud if not accompanied by adequate oversight and detection systems. The consequences of fraud extend beyond financial losses, potentially damaging an organization's reputation, eroding public trust, and even threatening economic stability (Choithani et al., 2024). Therefore, effective fraud detection and prevention have become crucial for both individuals and organizations.

Artificial Intelligence (AI) has emerged as a potential solution for fraud detection. AI enables large-scale data processing and analysis, uncovering hidden patterns and detecting anomalies that may indicate fraudulent activities. AI can be implemented in various forms, ranging from simple rule-based systems to complex machine learning models (Sood et al., 2023). The application of AI in fraud detection has been explored across multiple sectors, including banking and finance (Cholakov & Stoyanova-Doycheva, 2024), as well as e-commerce (Teng & Lee, 2019). AI technologies can analyze transaction data, validate user identities, monitor user behavior, and detect suspicious activities.

Several studies have demonstrated the effectiveness of applying Artificial Intelligence (AI) in detecting fraudulent activities across various domains. For instance, Desai et al. (1996) conducted a comparative analysis between Artificial Neural Networks (ANNs) and traditional linear scoring models in the operational context of credit unions, finding that ANNs exhibited superior predictive capabilities in assessing credit risk. In another study, Putra & Kosala (2011) utilized ANNs to predict intraday trading signals in the stock market, highlighting the model's potential to capture complex non-linear relationships within high-frequency financial data. Similarly, Borovykh et al. (2018) proposed the application of Convolutional Neural Networks (CNNs) for time series forecasting, emphasizing the model's ability to extract hierarchical features from sequential data, a capability highly relevant to identifying anomalous patterns often associated with fraudulent behavior.

Although Artificial Intelligence (AI) holds the substantial potential to enhance the effectiveness and efficiency of fraud detection across various sectors, several key challenges need to be addressed to ensure optimal implementation. These challenges include the necessity for large volumes of high-quality data to accurately train AI models, the complexity of model architectures and algorithms involved in AI development, as well as a range of ethical concerns related to its use, such as data privacy, algorithmic bias, and accountability in automated decision-making processes. In light of these issues, the present study aims to conduct a bibliometric literature review to examine the research trends and patterns associated with fraud and the application of AI.

Although Artificial Intelligence (AI) holds considerable promise in enhancing the effectiveness and efficiency of fraud detection across various sectors, researchers and practitioners must still address several key challenges to ensure its optimal implementation. These include the need for high-quality, large-scale datasets to train AI models, the inherent complexity of model architectures and algorithms, and a range of ethical issues such as data privacy, algorithmic bias, and accountability in automated decision-making.

To date, many studies have focused on the technical implementation and algorithmic performance of AI in fraud detection. However, the existing body of research remains fragmented and lacks a comprehensive overview of the academic landscape in this field. In particular, there is a notable scarcity of studies that adopt a bibliometric approach to systematically examine research trends, collaborative networks, and thematic developments. Such mapping is crucial for understanding the evolution of knowledge, identifying influential contributors, and uncovering underexplored areas that warrant future investigation.

Accordingly, this study seeks to address this gap by conducting a bibliometric literature review of academic publications on the application of AI in fraud detection between 2013 and 2024. By integrating the PRISMA protocol with VOSviewer software, this research aims to analyze publication trends, keyword structures, co-authorship networks, country and institutional contributions, and the most prominent journals in the field. This study anticipates that the findings will provide both theoretical and practical insights to inform future scholarly work and policy discussions surrounding AI-based fraud prevention. The analysis encompasses key dimensions, including the distribution of academic publications, citation structures among documents, funding sponsors, university affiliations, country-level contributions, scholarly journals publishing relevant articles, author collaborations, and commonly used keywords related to this topic.

2. LITERATURE REVIEW

Fraud represents a deliberate act of deception intended to yield unlawful or unfair gain, and it occurs in various domains, including business, government, and digital finance (ACFE, 2024). The complexity of fraud schemes has intensified in the digital era, especially with the proliferation of high-speed financial transactions and increasing reliance on digital platforms. As noted by Desai et al. (1996), fraudulent behavior often involves deceptive practices, data manipulation, and the exploitation of systemic vulnerabilities, making early detection increasingly challenging.

In response to these challenges, researchers have explored the application of Artificial Intelligence (AI) as a promising tool for detecting fraudulent behavior. AI offers the capability to process large volumes of data, identify subtle patterns, and detect anomalies that would otherwise remain hidden using traditional statistical approaches (Borovykh et al., 2018; Sood et al., 2023). Various studies have demonstrated the superiority of AI techniques such as Artificial Neural Networks (ANNs), Convolutional Neural Networks (CNNs), and decision-tree-based models in identifying fraud within financial datasets and high-frequency trading environments (Borovykh et al., 2018; Putra & Kosala, 2011).

Although the growing body of literature underscores the technical effectiveness of AI in fraud detection, previous studies have primarily focused on model development, algorithmic performance, or specific case applications. A lack of comprehensive analysis remains, which systematically maps the intellectual structure, thematic evolution, and collaborative dynamics within this research domain. Few studies have applied bibliometric methods to uncover research trends, dominant contributors, and underexplored areas related to AI-based fraud detection. As bibliometric analysis enables the visualization and quantification of knowledge development, applying this approach is essential for gaining a macro-level understanding of the field's progress and fragmentation (Donthu et al., 2021; Zupic & Cater, 2015).

Therefore, this study employs bibliometric techniques to systematically evaluate the scholarly landscape surrounding the application of AI in fraud detection. By focusing on publication trends, keyword co-occurrences, authorship networks, and institutional affiliations, this review aims to identify dominant themes, collaborative patterns, and gaps in the literature that warrant further investigation.

The literature review contains a systematic review on previous research that are relevant to the topic. This section contains the strengths and weaknesses of previous research which can be used as an argument that this research is carried out to improve or develop previous research. This section also contains the theoretical basis in the form of a summary of theories from the literature that support the research, as well as an explanation of the basic concepts and principles needed for problem solving. The theoretical basis is in the form of qualitative descriptions, mathematical models, or tools that are directly related to the problems studied. The sources referred to in this section must be included in the sentences/statements referred to and in the references.

3. METHODS

This study adopts a bibliometric analysis approach combined with the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) protocol. PRISMA is employed to ensure transparency and methodological rigor in conducting systematic reviews and meta-analyses. This study carefully implemented the four PRISMA phases of identification, screening, eligibility assessment, and inclusion to filter relevant documents that support its objectives (Garza-Reyes, 2015). This process ensures that the collected data remain focused on the study's aim of exploring fraud detection through the application of Artificial Intelligence.

This study selected the Scopus database as the primary data source due to its credibility, broad disciplinary coverage, and rigorous indexing standards. Several studies have confirmed Scopus as a reliable and widely used source for bibliometric analysis (Nawaz et al., 2020). During the identification phase, several key elements were considered, including source type, search engine, subject area, language, keywords, and publication years (Tautiva et al., 2024). The search was limited to English-language journal articles in the fields of

Business, Management and Accounting, Economics, and Finance (Alatawi et al., 2023), while non-peer-reviewed documents such as conference proceedings, book chapters, and editorials were excluded due to their minimal contribution to theoretical and empirical discourse (Harsanto & Firmansyah, 2023). These selection criteria were consistently applied during the PRISMA identification and screening phases to eliminate duplicate entries, irrelevant topics, and non-academic content.

Two primary bibliometric techniques, co-occurrence analysis (which examines the relationships between keywords) and co-authorship analysis (which investigates author collaborations), were employed in this study. The core premise is that the frequency with which specific terms co-occur signals a conceptual relationship between them (Zupic & Cater, 2015). These techniques have proven effective in identifying research trends, collaboration patterns, and the thematic evolution of scholarly work across disciplines (Behl et al., 2022; Sharifani & Amini, 2023). Through the application of a bibliometric network approach, this study contributes to conceptual mapping by revealing key term linkages within the academic literature (Callon et al., 1983). To perform the analysis, the researchers used VOSviewer software, which effectively generates visual network maps that illustrate structural and conceptual relationships. The following search query was applied on December 15, 2024, to retrieve the relevant data: (TITLE-ABS-KEY ("fraud detection") AND TITLE-ABS-KEY ("artificial intelligence") AND TITLE-ABS-KEY ("machine learning") OR TITLE-ABS-KEY ("artificial intelligence in fraud detection") OR TITLE-ABS-KEY ("machine learning in fraud detection") OR TITLE-ABS-KEY (fraud)) AND PUBYEAR > 2013 AND PUBYEAR < 2025 AND (LIMIT-TO (SUBJAREA , "BUSI") OR LIMIT-TO (SUBJAREA , "ECON")) AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (SRCTYPE , "j")) AND (LIMIT-TO (DOCTYPE , "ar")).

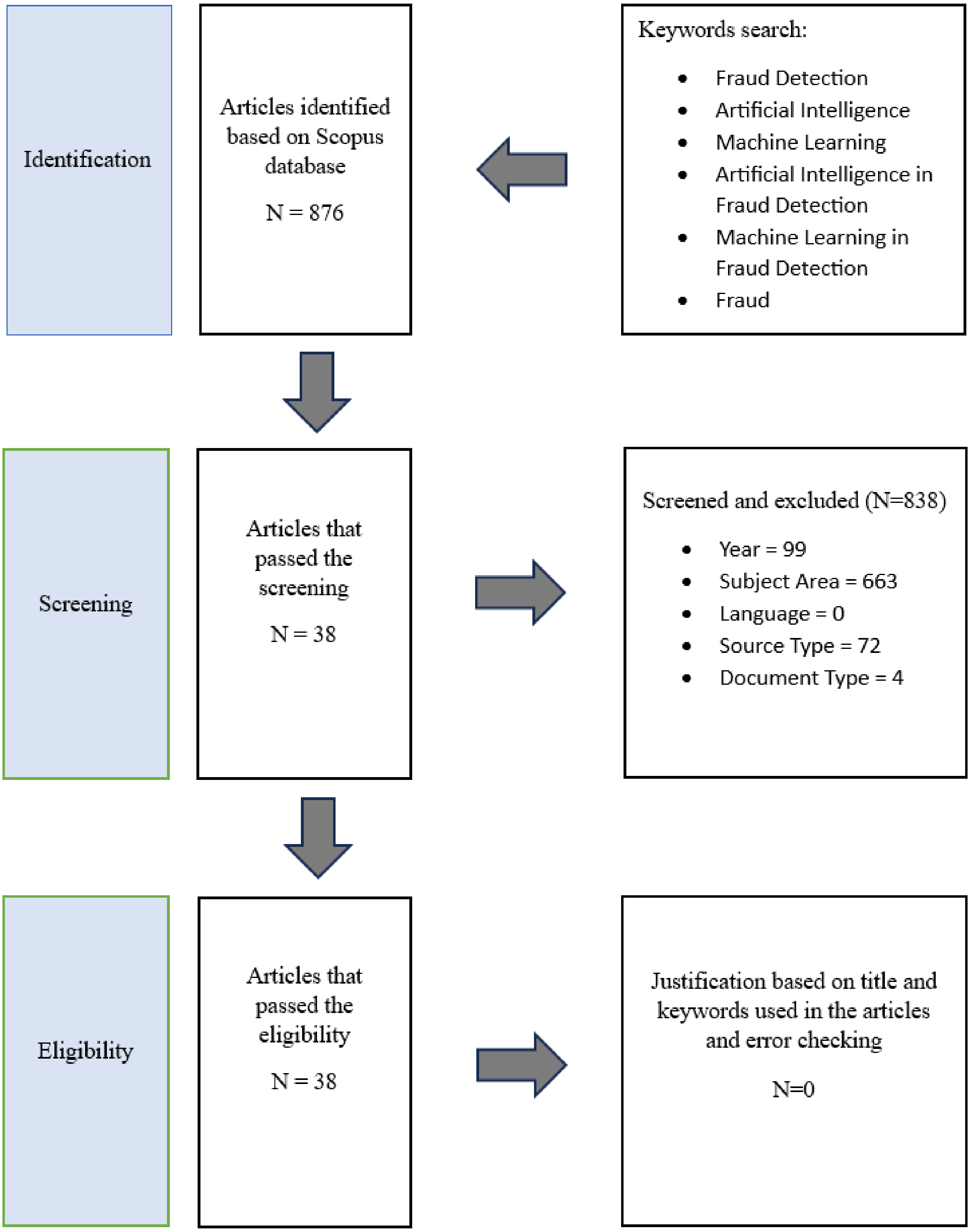
Identification
Articles identified based on Scopus database
N = 876
Keywords search:
Fraud Detection
Artificial Intelligence
Machine Learning
Artificial Intelligence in Fraud Detection
Machine Learning in Fraud Detection
Fraud
Screening
Articles that passed the screening
N = 38
Screened and excluded (N=838)
Year = 99
Subject Area = 663
Language = 0
Source Type = 72
Document Type = 4
Eligibility
Articles that passed the eligibility
N = 38
Justification based on title and keywords used in the articles and error checking
N=0

Figure 1. Research Protocol

Source: Figure created by authors, 2025

4. RESULTS AND DISCUSSION

Publication Trends

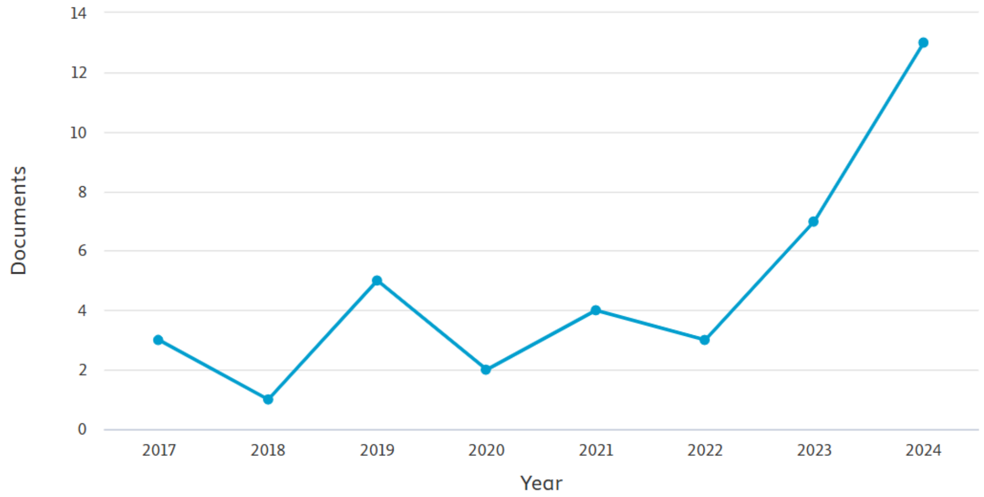

Figure 2. Number of Article Production

Source: Analyze results by scopus, 2025

The graph presented in Figure 2 illustrates the trend of scholarly publications from 2017 to 2024 related to the application of Artificial Intelligence (AI) in fraud detection. The data show a steady increase over the years, with a particularly sharp rise in 2023, where the number of publications increased by 133.3% (n = 4) compared to 2022. This upward trend continued into 2024, which saw an additional 85.7% increase (n = 6). Together, the years 2023 and 2024 contributed approximately 75% of the total publications indexed in the Scopus database on this topic.

This substantial growth in publication volume suggests a heightened academic interest in AI-driven fraud detection, likely fueled by the increasing sophistication of digital fraud schemes and the rapid evolution of AI technologies. The notable spike in 2024 may also reflect a broader global shift toward digital transformation and a growing awareness of the need for intelligent, data-driven solutions in financial and cybersecurity contexts. As such, AI-based fraud detection appears to be an emerging and timely research focus within the interdisciplinary landscape of technology, finance, and security. This accelerating trend highlights the urgent need for robust and adaptable fraud detection mechanisms in an increasingly digital world. The significant increase in recent years indicates that researchers are actively responding to the growing challenges posed by complex digital fraud, leveraging advancements in AI to develop more effective countermeasures.

This momentum suggests that AI in fraud detection is not merely a passing trend but a rapidly maturing field with sustained research interest and practical relevance.

Leading Countries in Research

Table 1. 10 Most Contributing Countries

Country	Documents
United States	6
China	5
India	5
United Kingdom	5
Australia	2
Belgium	2
Brazil	2
France	2
Germany	2
Jordan	2

Source: Table created by authors, 2025

The analysis of country contributions, as presented in Table 1, indicates that the United States ranks as the leading contributor to research on the application of Artificial Intelligence in fraud detection, with a total of six published articles. China, India, and the United Kingdom follow closely behind, each with five publications. Other countries, including Australia, Belgium, Brazil, France, Germany, and Jordan, each contributed two publications. The data suggest that research in this field is concentrated primarily in technologically advanced nations with strong research infrastructures and established academic networks.

This pattern reflects the global disparity in research capacities, where countries with more developed technological ecosystems and access to funding are better positioned to lead innovation in AI applications. The prominence of the United States and China aligns with their strategic focus on AI research, supported by substantial investments in higher education, cybersecurity, and digital finance infrastructure. For instance, both countries have launched national AI strategies that prioritize research and development in critical sectors, including finance and security, thereby fostering a conducive environment for academic contributions. These findings suggest that institutional and national priorities play a significant role in shaping the direction of academic discourse in fraud detection. Moreover, the relatively low participation from developing countries highlights an opportunity and a need for more inclusive global collaboration in advancing AI-driven solutions to financial fraud. This disparity may stem from limited access to advanced computing resources, insufficient funding for AI research, and a potential lack of specialized expertise in these regions. Addressing this gap requires targeted international collaborations, capacity-building initiatives, and increased investment in research infrastructure within developing nations to ensure a more equitable global contribution to AI-based fraud detection.

Table 2. Top Institutions Funding Research on Artificial Intelligence in Fraud Detection

Organizations	Region	Number of Publications
The University of Edinburgh	United Kingdom	2
Wenzhou-Kean University	China	2
Corn Exchange Chambers	United Kingdom	1
SWIFT	Belgium	1
GAECO	Brazil	1
Technical Consultant	United States	1
RS	United States	1
Troy University	United States	1
University of Johannesburg	South Africa	1
Universidade Federal Fluminense	Brazil	1

Source: Table created by authors, 2025

Table 2 shows that the majority of contributing institutions in this study are universities, underscoring the dominant role of higher education in producing research on artificial intelligence for fraud detection. The University of Edinburgh (United Kingdom) and Wenzhou-Kean University (China) each contributed two publications, reflecting a strong and sustained research focus on this topic. These universities are located in different global regions, indicating that geography does not limit institutional engagement with AI-based fraud detection. The consistent output from these institutions suggests dedicated research centers or strong faculty groups specializing in AI and cybersecurity, attracting significant research grants and talent. In addition to universities, contributions from non-academic organizations such as Corn Exchange Chambers (United Kingdom) and SWIFT (Belgium) demonstrate the growing relevance of this topic in real-world financial and regulatory contexts. These institutions, representing industry stakeholders and global financial infrastructure providers, reflect the growing cross-sectoral interest in applying AI to prevent fraud. This distribution highlights the strategic role of academic environments in driving innovation while also emphasizing the value of collaboration between academia and industry in tackling complex challenges in fraud detection. The participation of institutions from both Western Europe and East Asia further suggests that research interest in this topic is expanding globally and transcending institutional boundaries.

Table 3. 10 Companies (Funding Sponsors) Involved in Artificial Intelligence in Fraud Detection Research

Organizations	Region	Numbers
National Natural Science Foundation of China	China	2
Agriculture and Agri-Food Canada	Canada	1
Argonne National Laboratory	United States	1
City, University of London	United Kingdom	1
Conselho Nacional de Desenvolvimento Científico e Tecnológico	Brazil	1
Coordenação de Aperfeiçoamento de Pessoal de Nível Superior	Brazil	1
Deanship of Scientific Research, Prince Sattam bin Abdulaziz University	Saudi Arabia	1
Dell Technologies	United States	1
Department of Chemical Engineering, Universiti Teknologi Petronas	Malaysia	1
Deutscher Akademischer Austauschdienst	Germany	1

Source: Table created by authors, 2025

Table 3 shows that the majority of funding sponsors involved in AI-based fraud detection research are governmental agencies and academic institutions. The National Natural Science Foundation of China is identified as the most active funding body, supporting two publications on this topic. Other institutions, including Agriculture and Agri-Food Canada, Argonne National Laboratory (United States), City, University of London, and several others, each contributed to one or more publications. This distribution illustrates a relatively broad range of contributors from multiple regions and sectors.

These findings underscore the pivotal role of public sector funding in advancing technological innovation for fraud detection. The leadership of national science foundations, particularly from countries such as China and Canada, reflects a growing governmental interest in applying artificial intelligence to address systemic risks in the digital finance sector. This strong governmental involvement suggests that AI-based fraud detection is increasingly recognized as a matter of national security and economic stability rather than solely a private sector concern. Public funding often supports fundamental research and long-term projects that may not yield immediate commercial returns, which is crucial for developing robust AI models and addressing complex ethical considerations. Moreover, the involvement of both research-oriented universities and government agencies indicates a convergence of policy and academia in promoting secure digital infrastructures. While the number of sponsors per publication remains limited, the diversity of contributing institutions signals emerging cross-sector support for research on AI-driven fraud mitigation. The relatively limited direct funding from private companies, as observed in this bibliometric analysis, might indicate that much of the industry-driven AI development in fraud detection occurs internally or through proprietary research, which academic publication databases typically do not capture. Highlights a potential gap in understanding the full scope of AI innovation in this domain, suggesting a need for more transparent reporting or collaborative models between academia and industry.

Journal Analysis

Table 4. Top 5 Journals by Annual Production

Journal	Document
Decision Support Systems	2
Finance Research Letters	2
Journal of Payments Strategy and Systems	2
Journal of Risk Management in Financial Institutions	2
Accounting And Finance	1

Source: Table created by authors, 2025

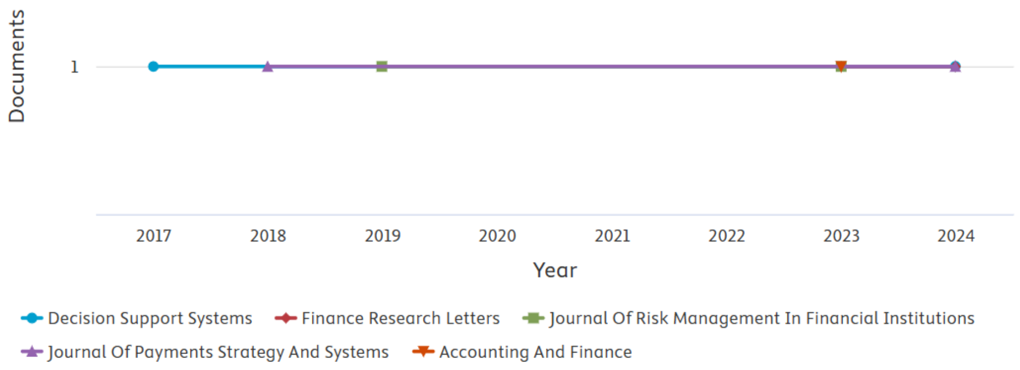

Figure 3. Journals by Annual Production
Source: Analyze results by scopus, 2025

Researchers published the 38 articles identified in this study across 34 academic journals, with five journals emerging as the most prominent venues for research on artificial intelligence in fraud detection, as shown in Table 4. These five journals, Decision Support Systems, Finance Research Letters, Journal of Payments Strategy and Systems, Journal of Risk Management in Financial Institutions, and Accounting and Finance, account for approximately 13% of total publications. Four of them published two articles each, while one journal contributed a single publication. Figure 3 illustrates the annual distribution of publications across these journals, which remained relatively stable from 2017 to 2024, with an average of one article per year per journal.

This pattern indicates a moderate degree of concentration in a small group of scholarly journals, suggesting that the field is beginning to establish dedicated publication outlets for AI-based research on fraud detection. The consistent output across these journals over several years reflects sustained academic interest in this interdisciplinary topic. The presence of journals focused on decision science (Decision Support Systems), finance (Finance Research Letters, Accounting and Finance), payments systems (Journal of Payments Strategy and Systems), and risk management (Journal of Risk Management in Financial Institutions) also underscores the cross-cutting nature of fraud detection as a research area that intersects multiple fields. This interdisciplinary spread highlights that AI in fraud detection is not confined to a single academic discipline but instead draws insights and methodologies from various domains. The moderate concentration suggests that while the field is gaining traction, it has not yet fully converged into a few highly specialized journals. This could imply opportunities for new specialized journals to emerge or for existing journals to create special issues dedicated to this rapidly evolving area, thereby further consolidating the research landscape. These findings highlight the potential for further thematic consolidation and specialization in journal coverage as the field continues to mature.

Keyword Co-Occurance

Researchers analyzed keyword occurrences and thematic trends to identify future research directions regarding the application of artificial intelligence in fraud detection. Keywords serve as essential components in academic publications, functioning as indicators for research focus and emerging trends within a specific field. In this context, the researchers employed keyword co-occurrence analysis to construct thematic networks and explore conceptual relationships across the literature (Castro-Espin & Agudo, 2022). The graphical representation of these relationships, generated using the VOSviewer software, is presented in Figure 4. In this bibliometric network, nodes represent keywords, while edges indicate the frequency of co-occurrence between keyword pairs (Donthu et al., 2021). The size of each node reflects the frequency with which a keyword appears in the literature, and the thickness of the connecting lines represents the strength of the relationship between keywords (Castro-Espin & Agudo, 2022; Donthu et al., 2021; Heersmink et al., 2011). The proximity between nodes signifies the degree of thematic association, and node colors represent clusters of frequently co-occurring keywords, which can help identify broad areas for further fieldwork and research development (Pathak et al., 2022). The results of the VOSviewer analysis indicate that "machine learning" is the most frequently occurring keyword, while the most prominent domains of fraud detection research are in the finance and banking sectors.

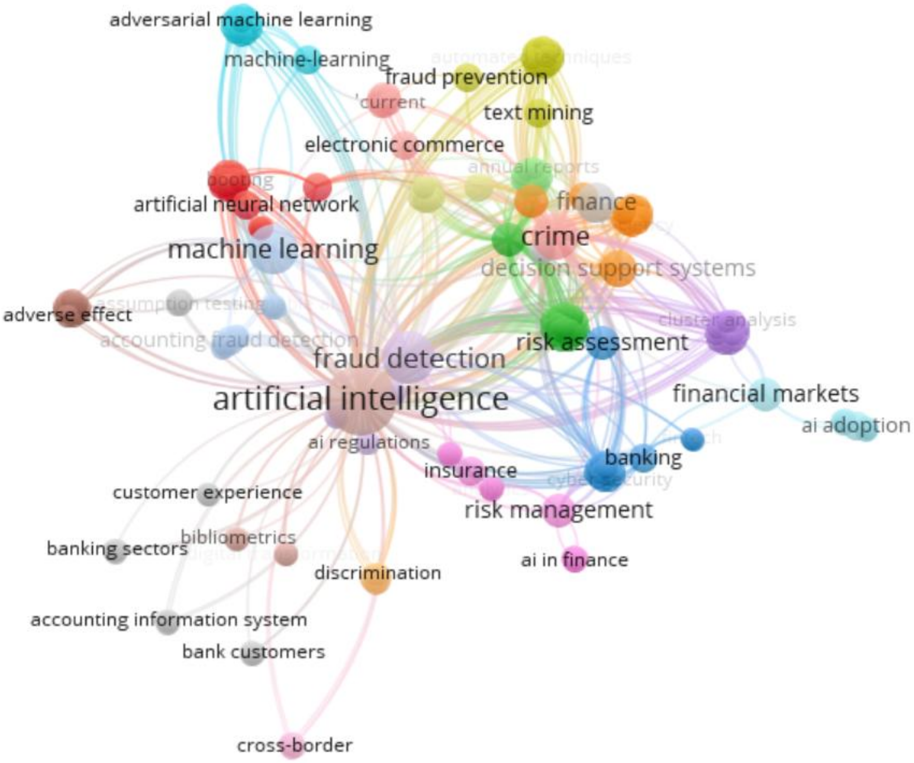

Figure 4. Co-occurrence Network Analysis

Source: VOSviewer analysis based on Scopus data, 2025

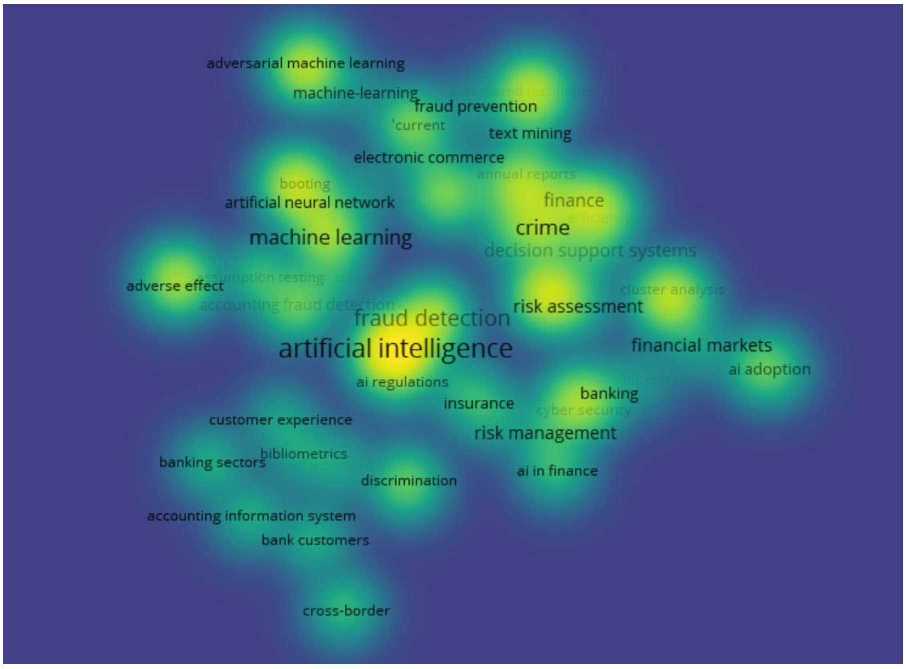

Figure 5. Keyword Density Visualization

Source: VOSviewer analysis based on Scopus data, 2025

Figure 5 presents the keyword density visualization, where the visualization labels each keyword in a manner consistent with the previous network representation. This view illustrates the spatial distribution of keyword density within the literature, using a default color gradient of blue, green, and yellow to represent varying levels of density at specific locations. Yellow areas indicate the highest density of items, while blue areas indicate the lowest density. The color tone at each point corresponds to the number of surrounding keywords and their associated weight. Brighter, yellow hues denote higher density and keyword weight. In contrast, darker blue tones suggest fewer neighboring items and lower weight (Widyantoro & Arief, 2022).

The visualization reveals that fraud detection and artificial intelligence occupy the central position with the highest density, reaffirming their dominance as the primary research foci in the field. In contrast, keywords such as adversarial machine learning, text mining, electronic commerce, insurance, and crime are positioned in low-density areas, indicating that although they are relevant, these topics remain underexplored. For instance, 'adversarial machine learning' is crucial for developing robust AI models that can withstand sophisticated fraud attacks designed to evade detection. However, research in this specific sub-field within fraud detection is still in its early stages. Similarly, 'text mining' holds immense potential for analyzing unstructured data (e.g., fraud reports, social media) to uncover hidden patterns, which is currently underutilized. Expanding research into 'electronic commerce' and 'insurance' fraud using AI is also vital, given the significant financial losses in these sectors.

Furthermore, integrating insights from 'criminology' could provide a deeper understanding of fraudster behavior, leading to more proactive detection strategies. The yellow color, which bridges fraud detection, artificial intelligence, and machine learning, highlights the strong conceptual linkage among these core themes. Furthermore, the density map also reveals interconnected terms such as finance, banking, risk management, and insurance, indicating that the application of artificial intelligence in fraud detection spans multiple integrated domains and highlights the need for cross-disciplinary collaboration in future research efforts.

Co-Authorship Analysis

Based on the VOSviewer analysis presented in Figures 6 and 7, the visualizations offer insights into the density and collaborative relationships among authors who contribute to research on the application of Artificial Intelligence in fraud detection. The results reveal that Scorsatto, Rodrigo occupies the highest and most concentrated area of the network, indicating substantial productivity and influence in this field. Other prominent contributors, such as Antunes, Rodolfo Stoffel, and Da Rosa Righi, Rodrigo, also appear in high-density zones, reflecting their significant roles in advancing this area of study. The visualization places authors such as Barbosa, Jorge Luis Victória; Da Silveira, Diórgenes Eugênio; Arcot, Tanuj; Da Costa, Cristiano André; Rodrigues, Vinicius Facco; and Policarpo, Lucas Micol in lower-density areas, yet they still make meaningful contributions to the research network. Overall, the visualization highlights a core group of dominant authors, with Scorsatto and Rodrigo emerging as a central figure. This strong clustering around specific authors suggests the formation of influential research groups or 'schools of thought' that are driving significant portions of the research agenda in AI-based fraud detection. These central figures likely play a crucial role in mentoring new researchers, securing funding, and shaping the methodological approaches within the field. Nonetheless, the presence of additional contributors underscores the diversity and collaborative nature of scholarly efforts in expanding the body of knowledge related to Artificial Intelligence in fraud detection. The interconnectedness of these authors, even those in lower-density areas, indicates a healthy collaborative ecosystem where knowledge is shared and built upon, fostering interdisciplinary approaches to complex fraud challenges.

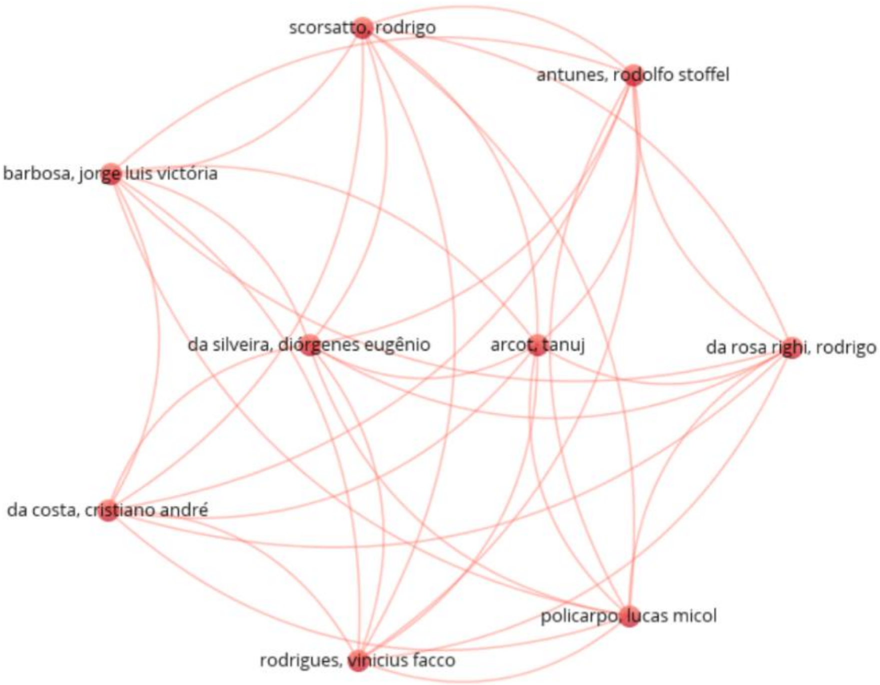
scorsatto, rodrigo
antunes, rodolfo stoffel
barbosa, jorge luis victória
da silveira, diórgenes eugênio
arcot, tanuj
da rosa righi, rodrigo
da costa, cristiano andré
policarpo, lucas micol
rodrigues, vinicius facco

Figure 6. Co-authorship Network Analysis

Source: VOSviewer analysis based on Scopus data, 2025

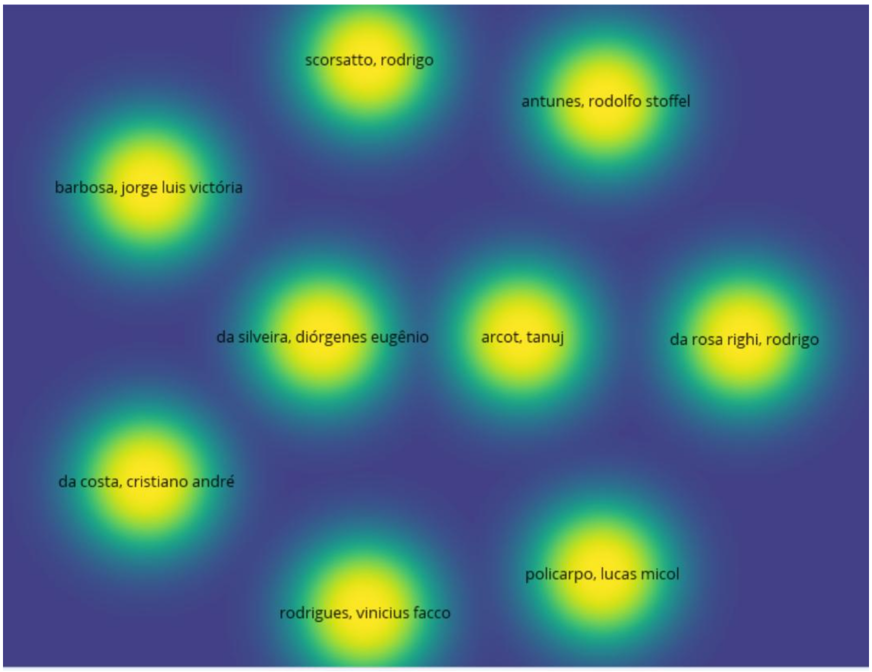

Figure 7. Writers Density Visualization
Source: VOSviewer analysis based on Scopus data, 2025

5. CONCLUSION

This study demonstrates the pivotal role of Artificial Intelligence (AI) in combating increasingly sophisticated digital fraud through a comprehensive bibliometric analysis of literature published between 2013 and 2024. The findings reveal a substantial rise in scholarly attention toward AI-driven fraud detection, with 75% of publications concentrated in 2023 and 2024, predominantly led by the United States, China, India, and the United Kingdom, countries with robust AI infrastructure and public funding. The financial sector emerges as the dominant application area, while underexplored domains such as adversarial machine learning and cross-sector implementations highlight opportunities for further research. This work not only contributes to theoretical development by illustrating how AI intersects with computer science, risk management, and organizational studies but also uncovers pressing challenges, including the need for higher-quality datasets, algorithmic transparency, and ethical frameworks surrounding privacy and accountability. Addressing these issues requires collaborative governance models that engage researchers, industry practitioners, and policymakers in a shared effort to address these issues. To advance the field, we recommend developing attack-resistant AI models for dynamic fraud environments, expanding research into neglected domains like e-commerce fraud using text mining techniques, and establishing international consortia to address resource disparities between developed and developing nations. Ultimately, this study advocates for ethically grounded, cross-sector collaboration to transform AI innovations into practical fraud prevention solutions that reinforce trust in digital ecosystems, a critical need as financial crimes grow in complexity and scale.

6. REFERENCES

ACFE. (2024). The Nations Occupational Fraud 2024: 2 Foreword Occupational Fraud 2024: A Report to the Nations.

ACFE, I. C. (2019). Survei fraud Indonesia 2019.

Alatawi, I. A., Ntim, C. G., Zras, A., & Elmagrhi, M. H. (2023). CSR, financial and non-financial performance in the tourism sector: A systematic literature review and future research agenda. In International Review of Financial Analysis (Vol. 89). Elsevier Inc. https://doi.org/10.1016/j.irfa.2023.102734

Behl, A., Gaur, J., Pereira, V., Yadav, R., & Laker, B. (2022). Role of big data analytics capabilities to improve sustainable competitive advantage of

MSME service firms during COVID-19 – A multi-theoretical approach. Journal of Business Research, 148, 378–389. https://doi.org/10.1016/j.jbusres.2022.05.009

Borovykh, A., Bohte, S., & Oosterlee, C. W. (2018). Conditional time series forecasting with convolutional neural networks. http://arxiv.org/abs/1703.04691

Callon, M., Courtial, J. P., Turner, W. A., & Bauin, S. (1983). From translations to problematic networks: An introduction to co-word analysis. Colloquium on the Sociological Analysis of Scientific and Technical Research: Social Science Information, 22, 191–235.

Castro-Espin, C., & Agudo, A. (2022). The role of diet in prognosis among cancer survivors: A systematic review and meta-analysis of dietary patterns and diet interventions. Nutrients, 14(2). https://doi.org/10.3390/nu14020348

Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2024). A comprehensive study of artificial intelligence and cybersecurity on bitcoin, crypto currency and banking system. Annals of Data Science, 11(1), 103–135. https://doi.org/10.1007/s40745-022-00433-5

Cholakov, G., & Stoyanova-Doycheva, A. (2024). Extending fraud detection in students exams using AI. TEM Journal, 13(4), 3068–3078. https://doi.org/10.18421/TEM134-41

Desai, V. S., Crook, J. N., & Overstreet, G. A. (1996). A comparison of neural networks and linear scoring models in the credit union environment. European Journal of Operational Research, 95(1), 24–37. https://doi.org/10.1016/0377-2217(95)00246-4

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

Garza-Reyes, J. A. (2015). Lean and green-a systematic review of the state of the art literature. Journal of Cleaner Production, 102, 18–29. https://doi.org/10.1016/j.jclepro.2015.04.064

Harsanto, B., & Firmansyah, E. A. (2023). A twenty years bibliometric analysis (2002–2021) of business economics research in ASEAN. Cogent Business and Management, 10(1).

https://doi.org/10.1080/23311975.2023.2194467

Heersmink, R., Hoven, J. van den, Eck, N. J. van, & Berg, J. van den. (2011). Bibliometric mapping of computer and information ethics. Ethics and Information Technology, 13(3), 241–249. https://doi.org/10.1007/s10676-011-9273-7

Husnaningtyas, N., & Dewayanto, T. (2023). Financial fraud detection and machine learning algorithm (unsupervised learning): Systematic literature review. Jurnal Riset Akuntansi Dan Bisnis Airlangga, 8(2), 2023. https://e-journal.unair.ac.id/jraba

Nawaz, K., Saeed, H. A., & Sajeel, T. A. (2020). Covid-19 and the state of research from the perspective of psychology. International Journal of Business and Psychology, 2(1), 35–44.

Pathak, D., Sharma, J. P., & Patnaik, S. (2022). Twenty years of entrepreneurship and innovation research: A bibliometric analysis. Journal of Operations and Strategic Planning, 5(1).

Putra, E. F., & Kosala, R. (2011). Application of artificial neural networks to predict intraday trading signals. Proceedings of the 10th WSEAS International Conference on E-Activities, 174–179.

Sharifani, K., & Amini, M. (2023). Machine learning and deep learning: A review of methods and applications. World Information Technology and Engineering Journal, 10(7). https://ssrn.com/abstract=4458723

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

Tautiva, J. A. D., Rivera, F. I. R., Celume, S. A. B., & Rivera, S. A. R. (2024). Mapping the research about organisations in the latin american context: A bibliometric analysis. Management Review Quarterly, 74(1), 121–169. https://doi.org/10.1007/s11301-022-00296-3

Teng, H. W., & Lee, M. (2019). Estimation procedures of using five alternative machine learning methods for predicting credit card default. Review of Pacific Basin Financial Markets and Policies, 22(3). https://doi.org/10.1142/S0219091519500218

Widyantoro, T., & Arief, M. (2022). The current and future research on environmental, social, and governance (ESG) performance: A bibliometric analysis. Proceedings of the 2nd Indian International Conference on Industrial Engineering and Operations Management.

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