West Science Interdisciplinary Studies
Vol. 4, No. 03, March 2026: pp. 506-512

Fraud Detection Research Trends: A Bibliometric Analysis

Loso Judijanto
IPOSS Jakarta, Indonesia and losojudijantobumn@gmail.com

ABSTRACT

This study examines the development and intellectual structure of fraud detection research through a bibliometric analysis. Using data extracted from a major scientific database and analyzed with bibliometric visualization tools, the study maps publication trends, influential contributors, and thematic evolution within the field. The findings reveal that fraud detection research is strongly centered on machine learning and increasingly shaped by advances in deep learning, neural networks, and data-driven approaches. At the same time, the field has expanded beyond traditional financial contexts into broader digital ecosystems, including cybersecurity, blockchain, and data privacy. The analysis also highlights a clear shift from conventional statistical methods toward more adaptive and complex models capable of handling large-scale and interconnected data. In addition, emerging themes such as predictive analytics, risk management, and decentralized finance indicate a growing orientation toward real-world application and decision-making. Overall, the study provides a comprehensive overview of the research landscape, identifies key trends and gaps, and offers directions for future research, particularly in integrating technological innovation with practical, ethical, and system-level considerations.

Keywords: *Fraud Detection, Bibliometric Analysis, Machine Learning, Deep Learning, Cybersecurity*

1. INTRODUCTION

Fraud has become a critical global issue affecting financial institutions, governments, and individuals, particularly with the rapid advancement of digital technologies and financial systems. The increasing complexity of financial transactions, coupled with the expansion of digital platforms, has created new opportunities for fraudulent activities that are more sophisticated and difficult to detect. As a result, fraud detection has evolved into a multidisciplinary field involving accounting, finance, computer science, and data analytics. Traditional rule-based detection systems are gradually being replaced by more advanced analytical techniques that are capable of identifying complex patterns and anomalies in large datasets. This shift reflects the growing necessity for more effective and adaptive fraud detection mechanisms in modern economies [1].

In recent years, there has been a significant increase in academic interest in fraud detection research. Studies indicate that the number of publications in this field has grown steadily since the mid-2000s, highlighting its rising importance in both academic and practical domains. This growth is driven by the increasing incidence of financial crimes such as credit card fraud, money laundering, and cyber fraud, which pose substantial risks to economic stability. Moreover, the globalization of financial systems has further amplified these risks, requiring collaborative and cross-border research efforts. The expanding body of literature reflects the need to better understand fraud mechanisms and develop more robust detection strategies [2].

Another important development in fraud detection research is the integration of advanced technologies such as artificial intelligence (AI) and machine learning (ML). These technologies have significantly improved the ability to analyze large volumes of transactional data and detect hidden patterns that may indicate fraudulent behavior. Bibliometric studies reveal that AI and ML have become dominant themes in recent fraud detection research, particularly in the banking and financial sectors. The adoption of these technologies enables real-time fraud detection, enhances predictive accuracy, and reduces false positives, making them essential tools in combating modern financial crimes [3].

In addition to technological advancements, the field of fraud detection has also become increasingly interdisciplinary. Research now incorporates insights from forensic accounting, behavioral science, and network analysis to better understand the motivations and methods of fraudsters. For instance, forensic accounting has emerged as a key area in fraud prevention and detection, emphasizing the importance of investigative techniques and regulatory frameworks. This interdisciplinary approach allows researchers to address fraud from multiple perspectives, leading to more comprehensive and effective solutions [4].

Bibliometric analysis has gained prominence as a methodological approach for examining the development of research fields, including fraud detection. By analyzing publication patterns, citation networks, and keyword trends, bibliometric studies provide valuable insights into the evolution, structure, and future directions of research. Previous bibliometric analyses have identified key contributors, influential journals, and emerging research themes in fraud detection, highlighting the dynamic nature of this field. Despite these contributions, there is still a need for updated and comprehensive analyses that capture recent developments and emerging trends, particularly in the context of rapidly evolving technologies.

Despite the growing volume of research on fraud detection, the literature remains fragmented across different disciplines, methodologies, and application areas, making it difficult to obtain a holistic understanding of the field. Many studies focus on specific aspects such as machine learning techniques, forensic accounting, or particular types of fraud, without providing an integrated view of overall research trends. Furthermore, the rapid expansion of publications has created challenges in identifying key themes, influential works, and emerging directions. Existing bibliometric studies, while valuable, are often limited in scope, time period, or dataset, and may not fully capture the latest developments in fraud detection research. Therefore, there is a need for a comprehensive bibliometric analysis that systematically maps the research landscape, identifies trends, and highlights gaps to support future research and practical applications. This study aims to conduct a comprehensive bibliometric analysis of fraud detection research in order to identify key trends, patterns, and developments within the field.

2. METHODS

This study employs a bibliometric analysis approach to systematically examine the development and trends in fraud detection research. Bibliometric analysis is a quantitative method used to evaluate scientific literature through statistical and mathematical techniques, enabling the identification of patterns in publications, citations, and research collaborations. This approach is particularly suitable for mapping the intellectual structure of a research field and uncovering emerging themes over time. The study adopts a descriptive and exploratory research design, focusing on published academic works related to fraud detection across multiple disciplines. By using bibliometric techniques, the research aims to provide an objective and comprehensive overview of the evolution of fraud detection studies.

The data for this study are collected from a reputable academic database, such as Scopus or Web of Science, which are widely recognized for their extensive coverage of high-quality scholarly publications. The search process is conducted using specific keywords, including "fraud detection," "financial fraud," "fraud analytics," and "fraud prevention," applied to titles, abstracts, and keywords. The inclusion criteria consist of peer-reviewed journal articles and conference papers published within a defined time frame, for example from 2000 to 2025, to capture both early developments and recent advancements in the field. After the initial retrieval, the dataset is refined by removing duplicates, irrelevant documents, and non-English publications to ensure data consistency and reliability. The final dataset is then exported in a compatible format for further bibliometric analysis.

RESULT AND DISCUSSION

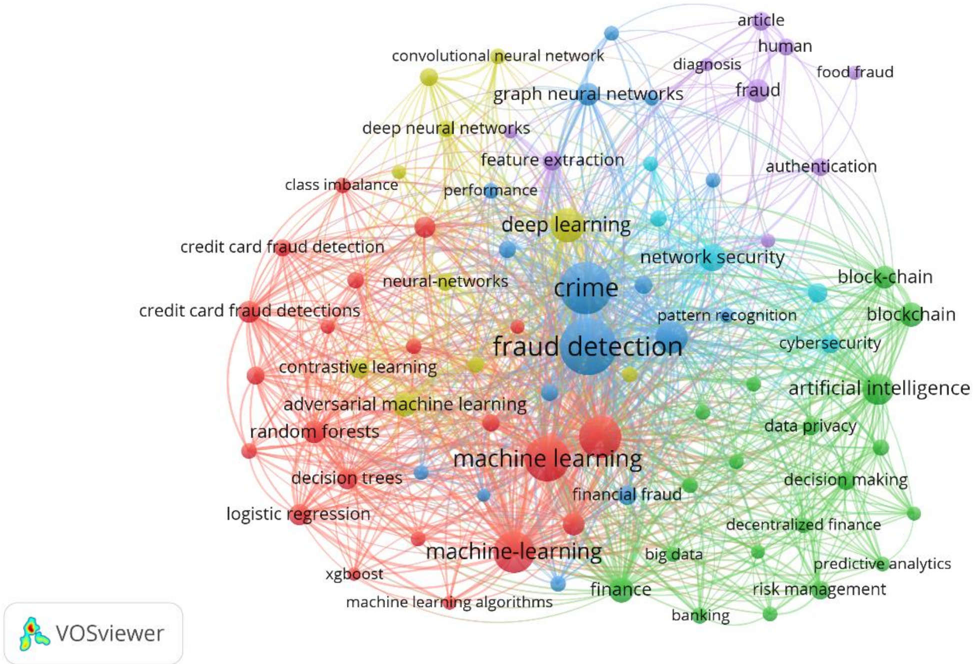

Figure 1. Network Visualization
Source: Data Analysis Result, 2026

Figure 1 reveals that "fraud detection" occupies a central and highly connected position, indicating its role as the core theme that integrates multiple research streams. Closely linked to it are terms such as machine learning, deep learning, and crime, suggesting that contemporary fraud detection research is strongly driven by computational approaches. The density of connections around these nodes reflects an active and evolving research area where technological methods are increasingly used to address complex fraud patterns. A prominent cluster (red) is dominated by machine learning techniques, including random forests, logistic regression, decision trees, and XGBoost. This indicates that a large portion of the literature focuses on predictive modeling for fraud detection, particularly in structured financial data contexts such as credit card fraud. The presence of terms like class imbalance and adversarial machine learning shows that researchers are not only applying models but also addressing methodological challenges, especially those related to data distribution and model robustness.

Another cluster (yellow and blue overlap) highlights the transition toward more advanced computational paradigms, particularly deep learning and neural networks. Terms such as convolutional neural networks, graph neural networks, and feature extraction suggest a shift toward handling complex, high-dimensional, and relational data. This reflects how fraud detection research is moving beyond traditional tabular data into more sophisticated representations, including network-based fraud (e.g., fraud rings or transaction networks). The green cluster emphasizes the intersection between fraud detection and broader digital ecosystems, including blockchain, cybersecurity, data privacy, and artificial intelligence. This suggests that fraud is increasingly studied within the context of digital platforms and decentralized systems. The inclusion of decentralized finance (DeFi) and risk management indicates an emerging research direction where fraud detection is integrated with financial innovation and regulatory concerns, rather than being treated as a standalone technical problem. The purple cluster reflects more applied and domain-specific contexts, such as authentication, diagnosis, and food fraud. This indicates that fraud detection research is expanding across sectors, from finance to healthcare and supply chains.

3.1 Overlay Visualization

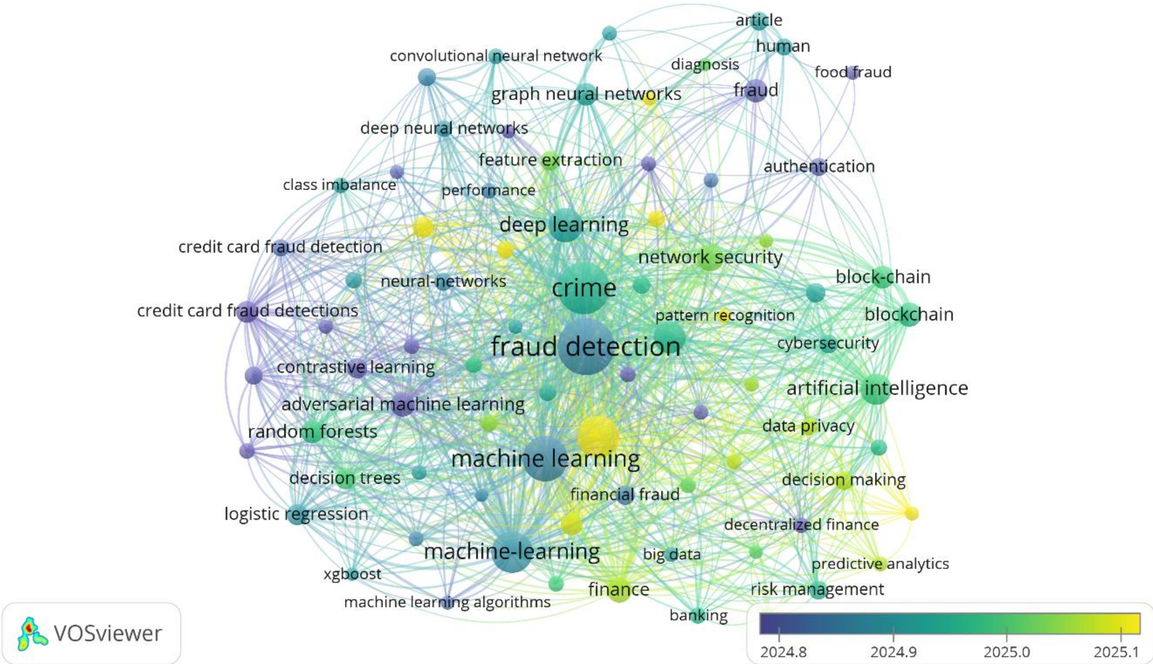

Figure 2. Overlay Visualization
Source: Data Analysis Result, 2026

Figure 2 highlights the temporal evolution of fraud detection research, where color gradients represent the average publication year of keywords. Central terms such as fraud detection, machine learning, and crime appear in green to yellow tones, indicating that these topics remain actively studied and continue to evolve in recent years. Their dense interconnections suggest that the field is not static but continuously integrating new methods and perspectives, particularly driven by advances in data-driven technologies. More recent topics, shown in yellow shades, include financial fraud, decision making, big data, and predictive analytics. This pattern reflects a growing shift toward applied and real-time fraud detection systems, especially in financial and digital environments. The emergence of decentralized finance, risk management, and data privacy also indicates that research is increasingly responding to the complexities of modern financial ecosystems, where fraud risks are embedded in rapidly evolving technological infrastructures. In contrast, earlier or more established topics, indicated by blue to teal colors, include logistic regression, decision trees, and traditional credit card fraud detection. These methods form the methodological foundation of the field but are gradually being complemented or replaced by more advanced approaches such as deep learning and graph neural networks.

3.2 Citation Analysis

Table 1. The Most Impactful Literatures

Citations	Authors and year	Title
2835	[5]	A survey of outlier detection methodologies
2478	[6]	Survey on deep learning with class imbalance

Citations	Authors and year	Title
2475	[7]	A few useful things to know about machine learning
2128	[8]	Deep learning applications and challenges in big data analytics
2068	[9]	How the machine 'thinks': Understanding opacity in machine learning algorithms
1259	[10]	Graph based anomaly detection and description: A survey
1226	[11]	Mining concept-drifting data streams using ensemble classifiers
1206	[12]	Who blows the whistle on corporate fraud?
1180	[13]	Outlier analysis
1084	[14]	Distance-based outliers: Algorithms and applications

Source: Scopus, 2026

3.3 Density Visualization

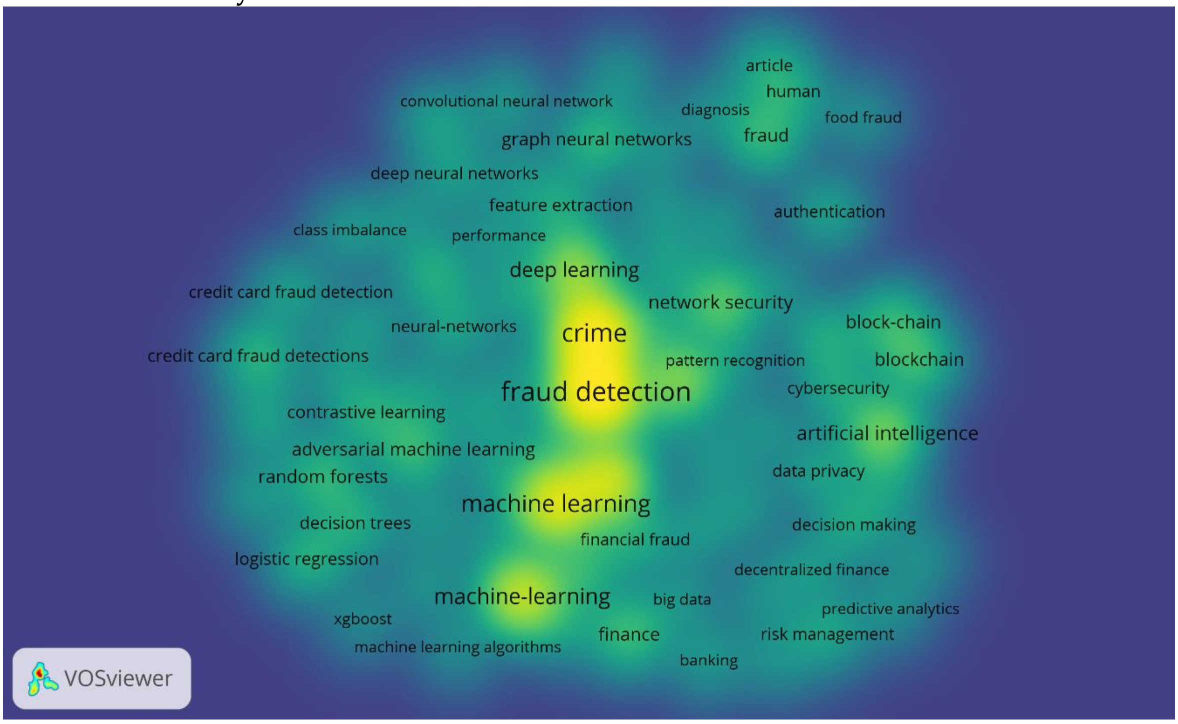

Figure 3. Density Visualization

Source: Data Analysis Result, 2026

Figure 3 shows that fraud detection, machine learning, and crime form the most concentrated and influential core of the research landscape, as indicated by the bright yellow areas. This suggests that the field is strongly centered on data-driven approaches to identifying fraudulent activities, with machine learning acting as the main methodological backbone. The close proximity of terms such as deep learning, neural networks, and feature extraction reflects a consolidation of advanced computational techniques around this central theme, indicating that researchers are increasingly focusing on improving detection accuracy through sophisticated modeling.

Beyond the core, surrounding areas with moderate density (green tones) reveal important but slightly less dominant themes, including cybersecurity, blockchain, data privacy, and financial fraud. These topics point to the expansion of fraud detection into broader digital and financial ecosystems, where issues of security, decentralization, and data governance become more prominent. Meanwhile, traditional techniques such as logistic regression and decision trees appear in lower-density zones, indicating their foundational role but reduced prominence in current research.

Discussion

The findings of this bibliometric analysis show that fraud detection research is anchored in a tightly connected core where fraud detection, machine learning, and crime intersect. This centrality reflects how the field has gradually shifted from a domain-specific concern—primarily within accounting and auditing—toward a broader computational problem shaped by advances in data science. The dominance of machine learning-related terms suggests that fraud is no longer approached as a static anomaly, but as a dynamic pattern embedded in complex and evolving data environments. In this sense, the literature captures a transformation in how fraud is conceptualized: from rule-based irregularities toward adaptive and data-driven phenomena.

The cluster structure further reveals a layered methodological evolution. Earlier approaches such as logistic regression and decision trees remain visible but occupy less dense areas, indicating their foundational role rather than their current dominance. In contrast, more recent emphasis on deep learning, neural networks, and graph-based models points to an increasing need to capture non-linear relationships and interconnected fraud behaviors. This progression reflects a broader methodological trajectory in which fraud detection research follows developments in artificial intelligence, adapting its tools to handle higher data complexity, larger volumes, and more sophisticated fraud schemes.

Another important pattern emerging from the visualization is the integration of fraud detection within wider digital ecosystems. Keywords such as cybersecurity, blockchain, data privacy, and decentralized finance suggest that fraud is increasingly examined in relation to digital infrastructures rather than isolated transactions. This shift indicates that fraud detection is becoming part of a larger system of digital risk management, where technological innovation simultaneously creates new opportunities and new vulnerabilities. As financial systems become more decentralized and data-intensive, the boundary between fraud detection, cybersecurity, and regulatory compliance becomes less distinct.

The density and overlay patterns also indicate a growing orientation toward application and real-time decision-making. Terms such as predictive analytics, risk management, and financial fraud highlight the movement toward operationalizing fraud detection models in practical settings. This suggests that the field is not only concerned with improving algorithmic performance but also with embedding these models into decision-making processes within organizations. The increasing attention to issues such as class imbalance, adversarial learning, and model performance further reflects an awareness of practical challenges that arise when deploying fraud detection systems in real-world environments.

These findings point to a research landscape that is both consolidating around advanced computational methods and expanding into interdisciplinary domains. The field appears to be moving toward more integrated frameworks that combine technical, organizational, and regulatory perspectives. Future research could benefit from bridging these dimensions more explicitly, particularly by addressing issues such as model interpretability, ethical implications, and contextual adaptation in different sectors. Rather than focusing solely on methodological advancement, there is room to develop a more holistic understanding of fraud detection as a socio-technical system embedded in evolving digital and institutional environments.

CONCLUSION

This study maps the development of fraud detection research as a field that has evolved from traditional statistical approaches into a data-driven, interdisciplinary domain centered on machine learning and advanced analytics. The bibliometric evidence shows a strong consolidation around computational methods, alongside a clear expansion toward digital ecosystems such as cybersecurity, blockchain, and decentralized finance. At the same time, the literature reflects a growing concern with practical implementation, including predictive decision-making and real-world deployment challenges. Overall, fraud detection research is moving toward more integrated and adaptive frameworks that combine technological capability with contextual awareness. This trajectory suggests that future work will benefit from not only advancing analytical techniques but also addressing issues of interpretability, ethics, and system-level integration within increasingly complex digital environments.

REFERENCES

[1] A. Z. Mansour, A. Ahmi, O. M. J. Popoola, and A. Znaimat, "Discovering the global landscape of fraud detection studies: a bibliometric review," *J. Financ. Crime*, vol. 29, no. 2, pp. 701–720, 2022.

[2] D. Hove, O. Olugbara, and A. Singh, "Bibliometric analysis of recent trends in machine learning for online credit card fraud detection," *J. Scientometr. Res.*, vol. 13, no. 1, pp. 43–57, 2024.

[3] H. Thakkar, S. Datta, P. Bhadra, H. Barot, and J. Jadav, "Artificial intelligence and machine learning in fraud detection: A comprehensive bibliometric mapping of research trends and directions," *Ann. Libr. Inf. Stud.*, vol. 72, no. 2, pp. 138–150, 2025.

[4] L. Zeng, Y. Li, and Z. Li, "Research hotspots, emerging trend and front of fraud detection research: A scientometric analysis (1984–2021)," in *International Conference on Data Mining and Big Data*, Springer, 2022, pp. 91–102.

[5] V. Hodge and J. Austin, "A survey of outlier detection methodologies," *Artif. Intell. Rev.*, vol. 22, no. 2, pp. 85–126, 2004.

[6] J. M. Johnson and T. M. Khoshgoftaar, "Survey on deep learning with class imbalance," *J. big data*, vol. 6, no. 1, p. 27, 2019.

[7] P. Domingos, "A few useful things to know about machine learning," *Commun. ACM*, vol. 55, no. 10, pp. 78–87, 2012.

[8] M. M. Najafabadi, F. Villanustre, T. M. Khoshgoftaar, N. Seliya, R. Wald, and E. Muharemagic, "Deep learning applications and challenges in big data analytics," *J. big data*, vol. 2, no. 1, p. 1, 2015.

[9] J. Burrell, "How the machine 'thinks': Understanding opacity in machine learning algorithms," *Big data Soc.*, vol. 3, no. 1, p. 2053951715622512, 2016.

[10] L. Akoglu, H. Tong, and D. Koutra, "Graph based anomaly detection and description: a survey," *Data Min. Knowl. Discov.*, vol. 29, no. 3, pp. 626–688, 2015.

[11] H. Wang, W. Fan, P. S. Yu, and J. Han, "Mining concept-drifting data streams using ensemble classifiers," in *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining*, 2003, pp. 226–235.

[12] A. Dyck, A. Morse, and L. Zingales, "Who blows the whistle on corporate fraud?," *J. Finance*, vol. 65, no. 6, pp. 2213–2253, 2010.

[13] C. Aggarwal, *Outlier Analysis*. 2013. doi: 10.1007/978-1-4614-6396-2.

[14] E. M. Knorr, R. T. Ng, and V. Tucakov, "Distance-based outliers: algorithms and applications," *VLDB J.*, vol. 8, no. 3, pp. 237–253, 2000.