

Bibliometric Analysis of Fraud Detection in the Fintech Sector

Loso Judijanto¹, Adih Supriadi²

¹IPOSS Jakarta, Indonesia and losojudijantobumn@gmail.com

²Fakultas Ekonomi dan Bisnis, Universitas Sultan Ageng Tirtayasa and adihs84@untirta.ac.id

ABSTRACT

The rapid growth of financial technology (fintech) has transformed the delivery of financial services while simultaneously increasing exposure to various forms of digital fraud and cybersecurity threats. As fintech platforms continue to expand globally, fraud detection has emerged as a critical research area aimed at enhancing the security, reliability, and sustainability of digital financial ecosystems. This study conducts a bibliometric analysis to examine the intellectual structure, research trends, influential publications, and collaborative networks within the field of fraud detection in the fintech sector. Bibliographic data were collected from the Scopus database and analyzed using VOSviewer to visualize keyword co-occurrence, author collaboration, institutional collaboration, country collaboration, overlay visualization, and density mapping. The findings reveal that fintech serves as the central theme connecting major research areas such as fraud detection, artificial intelligence, machine learning, cybersecurity, blockchain, and risk management. Keyword analysis indicates that artificial intelligence and machine learning have become dominant technological approaches for detecting and preventing fraudulent activities in digital financial services. Overlay visualization demonstrates a shift from traditional concerns related to cybercrime, regulatory compliance, and financial risk management toward emerging topics such as blockchain security, financial inclusion, and AI-driven fraud detection systems. Citation analysis identifies studies on artificial intelligence, fintech security frameworks, and cybersecurity as the most influential contributions to the field. Furthermore, collaboration analysis shows that research activities are concentrated within a limited number of author groups, institutions, and countries, with India emerging as the leading contributor to international collaboration.

Keywords: Fintech, Fraud Detection, Artificial Intelligence, Machine Learning, Cybersecurity

1. INTRODUCTION

Growth and advancement in FinTech have led to major changes in the world of finance, as new digital financial products provide fast and efficient solutions. FinTech refers to technological innovation in financial operations such as payment processing, electronic banking, peer-to-peer financing, crowdfunding, crypto trading, and mobile wallets. Digital financial systems have provided better conveniences and opportunities for financial inclusiveness across different countries, particularly in developing economies [1]. Nevertheless, besides these benefits, FinTech also experiences significant problems related to security breaches and criminal activities. As the number of digital transactions and the use of online financial systems expand, there is greater potential for cybercriminals to misuse their vulnerabilities, engage in transaction manipulation and identity theft, as well as carry out different types of fraud schemes. Research shows that fraud in the digital financial domain keeps becoming increasingly complex due to the advanced technologies employed by criminals [2], [3]. Thus, it is crucial to focus on fraud detection in the FinTech sphere.

It is for this reason that fraud detection has become one of the most critical areas of study in finance technology and digital banking. More and more, financial institutions and FinTech companies depend on sophisticated analytics, machine learning algorithms, artificial intelligence, blockchain technology, and big data analytics to detect any form of suspicious activity to avoid any potential financial losses [4], [5]. Intelligent fraud detection technology makes it possible for organizations to observe transactions in real-time, detect any form of irregular behavioral pattern,

and enhance their ability to prevent any form of fraud. Prior literature reveals that machine learning methods such as neural networks, decision trees, support vector machines, and deep learning methods have been widely employed to improve the performance of fraud detection in financial systems [6].

The trend towards fraud detection in FinTech has also garnered much attention from academics in a range of disciplines such as finance, accounting, information systems, computer science, and cybersecurity [7], [8]. Consequently, there has been a remarkable increase in the number of scientific publications regarding the use of technology in detecting fraud in recent years. According to bibliometric analyses, there is a rising number of scientific publications, international collaborations, and diversity of topics in research related to fraud. Research trends show that there is an apparent link between fraud detection research and artificial intelligence, data mining, blockchains, and risk management systems [9]. Some studies carried out in the field have tried to investigate and analyze the intellectual structure of the field and its future research directions and leading scholars and coauthorship relationships in this field [9]–[11].

Although an increase in the number of research works in the sphere of fraud detection can be observed, the number of researches devoted to bibliometrics in the field of FinTech frauds is relatively small. The majority of the existing bibliometric analyses concern fraud accounting, banking fraud, forensic accounting, and other spheres without analyzing FinTech specifically. FinTech differs from traditional financial systems due to its specific nature characterized by the use of decentralized technologies, mobility in operations, electronic identification, algorithms as well as cross-border financial services provided. Such features cause the development of new types of fraud and demand a better approach to their detection. Moreover, the fast changes experienced in financial technologies influence the research directions in FinTech fraud detection, which explains why there is a need in a comprehensive mapping of the available literature in order to see the direction of its development, major areas and the most authoritative scientists along with the opportunities for further research.

Also, a bibliometric analysis of fraud detection in the FinTech industry should be conducted from both academic and practical standpoints. From an academic perspective, the bibliometric analysis could help clarify the historical progress made so far in the area, identify key articles, and uncover issues that have not yet been examined. Practically speaking, the results obtained could help financial institutions, regulators, policy makers, and technology developers understand the directions of current research efforts and new approaches towards preventing frauds. In addition, through the bibliometric analysis, some innovative technologies related to fraud mitigation in the FinTech industry could be identified and used as inputs for developing better collaboration among researchers and organizations involved. Given the continuous growth of digital financial services today, a bibliometric analysis of the literature on fraud detection in the FinTech industry would become more important than ever before. Hence, in this paper, I aim to conduct a comprehensive bibliometric analysis of the literature on fraud detection in the FinTech industry.

The quick growth of the FinTech industry has created new challenges and made the problem of frauds more complex and risky in the realm of financial transactions. As a result, more attention from scholars is paid to studying fraud detection techniques and ways. Even though the problem of frauds and ways of detecting them through the help of artificial intelligence, machine learning, and data analytics has been discussed extensively, there is no complete overview of the current research status in the area under consideration. While many bibliometric analyses of scientific achievements

in the field of fraud detection have been conducted, they mostly focused on general fraud detection, forensic accounting, and banking fraud. Little information can be found about the intellectual structure of the field, publications, collaboration, and topics related to fraud detection in FinTech. The lack of information about the key topics and issues investigated in the field, main authors, most productive countries, and future research directions makes the topic of special concern. This paper attempts to conduct an examination and mapping of fraud detection research in the FinTech industry from a bibliometric analysis perspective.

2. METHODS

The chosen approach of research in this paper involves the use of a bibliometric methodology for investigating the evolution and development of scientific researches regarding fraud detection within the FinTech industry. Bibliometric analysis refers to the quantifiable method of assessment that uses citation analysis, author analysis, keyword analysis, and collaboration network analysis for evaluating and mapping scientific publications. This research technique is extensively used in literature analysis for revealing trends in scientific publications, important papers, key researchers, and promising topics in particular research areas. In the present paper, descriptive and evaluative research will be conducted to investigate the growth and changes experienced by academic literature about fraud detection in financial technology.

The data analyzed in this study were obtained from internationally acclaimed scientific databases like Scopus and Web of Science. The literature relevant to this study was determined by using the keywords "fraud detection," "financial technology," "FinTech," "artificial intelligence," "machine learning," and "digital finance." Data collection was constrained to peer-reviewed journal articles, conference papers, and review papers written in English within a defined period to achieve data consistency and relevancy. Following the search process, duplicates and unrelated documents were excluded based on title, abstract, and research focus in a filtering step. The relevant publications were subsequently imported into compatible files for bibliometric analysis. Several bibliometric indicators have been adopted in this study, which include growth in publications, citations, co-authorship, co-citation, and keyword co-occurrence.

The bibliometric analysis was carried out through VOS viewer for mapping connections between authors, organizations, countries, and research topics. The VOS viewer tool was employed for visualizing authorship, citation, and keyword networks, while the Biblioshiny software helped in statistical analysis and topic mapping. The results were analyzed descriptively to elucidate the progress of fraud detection studies within the FinTech domain and reveal emerging areas and potential research directions. This technique has allowed this study to offer an organized insight into the intellectual history of fraud detection research and shed light on technology developments and future research trends in digital finance security.

3. RESULT AND DISCUSSION

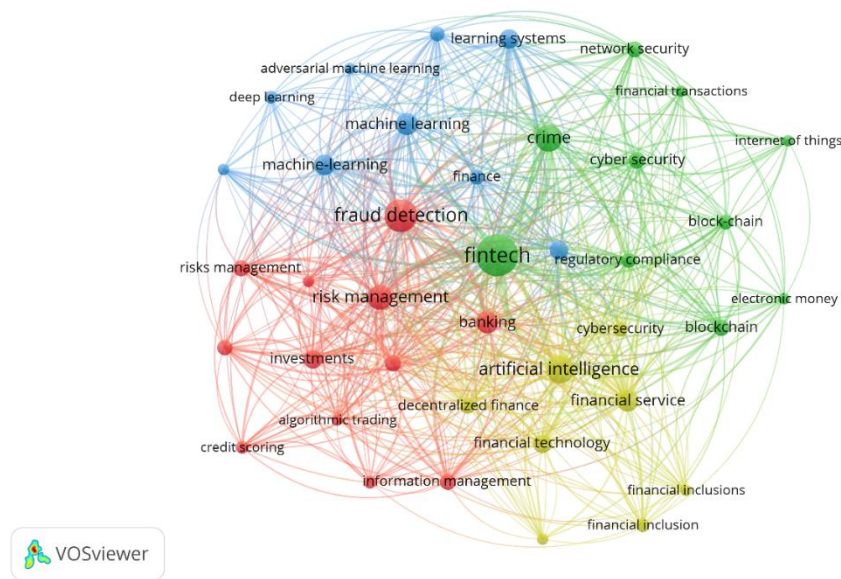


Figure 1. Network Visualization

Source: Data Analysis Result, 2026

According to the keyword co-occurrence network, fintech emerges as the most important and dominant theme of research within the field of fraud detection in fintech. Being located at the very center of the network and having ties to almost all the other keywords, fintech functions as the core node that connects research streams in technology, finance, and security domains. The close relations among fintech, fraud detection, artificial intelligence, machine learning, blockchain, cybersecurity, and risk management confirm that fraud prevention has now evolved into a multi-domain topic involving experts from the fields of finance, information technology, and data analysis.

This group is centered on words such as fraud detection, machine learning, machine-learning, deep learning, adversarial machine learning, and learning systems. This group can be said to symbolize the technological and scientific backbone of research on fraud detection. The dominance of machine learning-related keywords shows that the scholars in this area have started to use sophisticated techniques to analyze and spot abnormal transaction behaviors. Furthermore, the mention of adversarial machine learning points out to an increasing need to ensure that the fraud detection model cannot be fooled by smart attackers trying to bypass it.

Security and criminality issues in relation to financial operations in a digital environment are the main concerns discussed under the green cluster. Keywords like crime, cyber security, network security, financial transaction, internet of things, electronic money, and block chain show how important security issues related to digital finance infrastructure have become. The correlation of fintech with cyber crime-related terms shows that while digital financial service delivery has grown, there have been increased levels of cyber crime, frauds, and other criminal issues. The use of IoT and block chain indicates that the area of fraud detection studies has expanded to include new technological areas.

Red-colored clustering focuses on issues relating to financial governance as well as fraud detection risk-based aspects. The inclusion of keywords such as risk management, banking, investment, credit scoring, algorithmic trading, information management, and DeFi indicates that there is research being conducted in regards to fraud detection based on financial decision-making and risk management processes. The close relation between fraud detection and risk management points to the fact that fraud prevention is becoming an integral part of enterprise risk management

systems. In addition, the occurrence of decentralized finance shows that researchers are starting to study fraud risks associated with Decentralized Financial platforms.

As can be seen from the yellow cluster, current research interests revolve around artificial intelligence, financial service, financial technology, financial inclusion, financial inclusions, and cybersecurity. The placement of the terms shows that there will be a movement toward researching the possibilities through which intelligent technologies will be able to achieve both improved security and increased accessibility of financial products and services. In addition, the association between artificial intelligence and financial inclusion shows that there will be increasing attention paid to achieving balance and innovation without compromising the effectiveness of the fraud-prevention mechanism. Overall, the network shows that there is a trend towards a comprehensive research agenda, in which artificial intelligence, cybersecurity, blockchain technology, risk management, and financial inclusion are intertwined to build more secure and efficient fintech systems.

3.1 Overlay Visualization

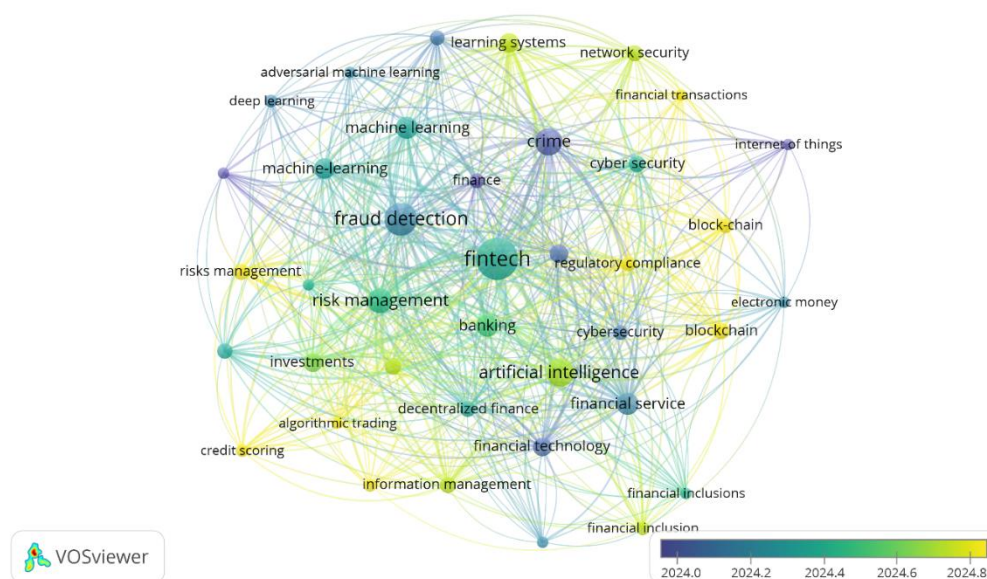


Figure 2. Overlay Visualization

Source: Data Analysis Result, 2026

The timeline visualization shows how research themes in fraud detection have evolved through time in the fintech industry. In this graph, the darker tones of blue and purple denote research themes that were introduced early into the literature, while lighter shades of green and yellow refer to themes introduced more recently. Fintech has been the hub keyword for all of the research themes explored in the literature and includes themes such as fraud detection, artificial intelligence, blockchain, cybersecurity, risk management, and financial services. This centrality proves that fintech is an important domain where technological developments and fraud prevention strategies meet.

A number of developed research themes could be spotted via darkened nodes, such as crime, regulation compliance, internet of things, financial technology, financial services, and fraud detection. These are the areas where a solid background of knowledge was built, which formed the correlation between the development of fintech and its associated security issues. In the early stages of research, scholars mostly concentrated on analyzing digital financial crimes, regulations, transactions, and application of basic machine learning approaches for detecting fraudulent activities. The significance of these developed themes indicates a shift in focus from the identification of fraud threats and regulatory issues to more advanced technological applications.

The more recent research trends are depicted with yellow nodes, including areas such as artificial intelligence, blockchain, financial inclusion, information management, credit scoring, financial transactions, and network security. The identification of these themes demonstrates that contemporary researchers are paying more attention to the development of innovative AI-based fraud detection methods, security based on blockchain technology, and intelligent risk management strategies that could facilitate financial inclusion. Financial inclusion as an important topic along with fraud detection implies that future security systems should not prevent people from accessing digital financial services.

3.2 Citation Analysis

Table 1. The Most Impactful Literatures

Citations	Authors and year	Title
288	[12]	Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance
94	[13]	Towards secure FinTech: A survey, taxonomy, and open research challenges
40	[14]	Advancements in Fin-Tech and Security Challenges of Banking Industry
37	[15]	Electronic Money Laundering, the Dark Side of Fintech: An Overview of the Most Recent Cases
28	[16]	Leveraging AI and FinTech: Driving Business Innovation in the Fourth Industrial Revolution
27	[17]	Novel Machine Learning Based Credit Card Fraud Detection Systems
25	[18]	Exploring Cutting-Edge Algorithms in FinTech: Leveraging Machine Learning and Artificial Intelligence for Achieving Sustainability
19	[19]	A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech
18	[20]	Banking Transformation Through FinTech and the Integration of Artificial Intelligence in Payments
18	[21]	Identity theft fraud- major loophole for FinTech industry in India

Source: Scopus, 2026

According to Table 1, the literature of significant impact is primarily represented by research articles on AI, security in fintech, banking risks, and fraud detection. [12] had the largest number of citations, meaning that their article presenting the opportunities and threats of AI implementation in banks, investments, and microfinance serves as a key source on the subject matter. Among other highly cited papers, there are those that focus on secure systems in fintech, taxonomies, and challenges related to banking security [13], [14]. This information, along with studies on electronic money laundering, credit card fraud detection, cybersecurity, identity theft, and payment transformation through AI, indicates that fraud detection in fintech relies on innovation and financial crime trends.

3.3 Density Visualization

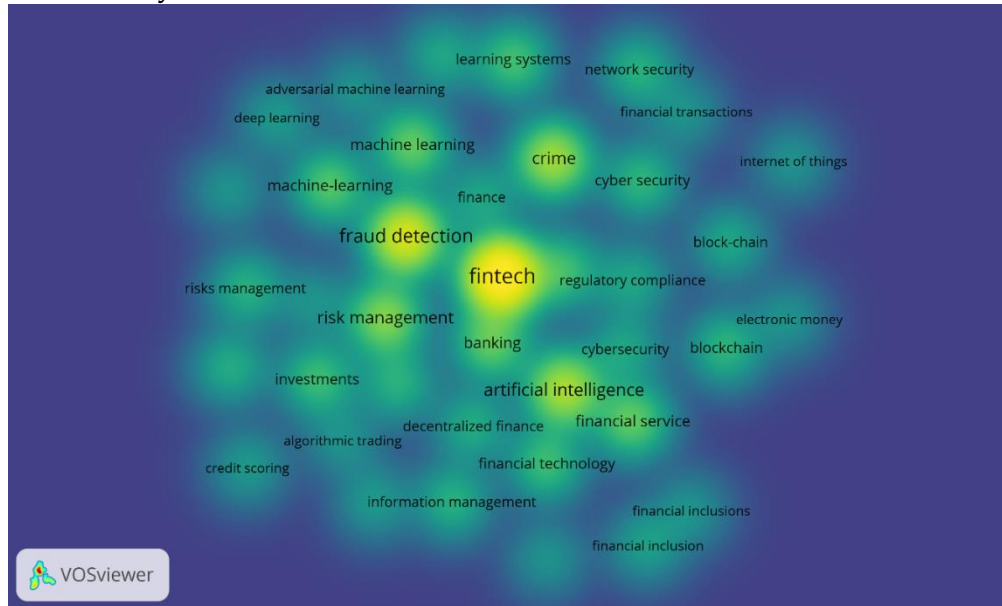


Figure 3. Density Visualization

Source: *Data Analysis Result, 2026*

Figure 3 highlights the most intensively studied topics in the field of fraud detection within the fintech sector. In VOSviewer, brighter yellow areas indicate keywords with higher frequency and stronger connections, whereas green and blue areas represent less-developed or more specialized topics. The map shows that fintech is the dominant research hotspot, occupying the brightest and most central position. Closely surrounding it are fraud detection, artificial intelligence, risk management, banking, and crime, indicating that the literature is heavily concentrated on developing technological and managerial approaches to identify, prevent, and mitigate fraud risks in digital financial environments. The strong density around these keywords suggests that fraud detection has become a core research stream within fintech, driven by the rapid expansion of digital banking, online transactions, and AI-powered financial services.

In contrast, topics such as financial inclusion, internet of things, electronic money, credit scoring, decentralized finance, algorithmic trading, and information management appear in less dense areas, indicating that they remain relatively underexplored despite their growing relevance. Similarly, keywords related to blockchain, cybersecurity, and network security exhibit moderate density, suggesting emerging but expanding research attention. This pattern implies that future studies may increasingly focus on integrating artificial intelligence with blockchain technologies, strengthening cybersecurity frameworks, and addressing fraud risks associated with financial inclusion initiatives and decentralized financial ecosystems. Therefore, the density map reveals both the established knowledge base centered on fintech, fraud detection, and risk management, as well as several promising avenues for future research in advanced digital finance security.

3.4 Co-Authorship Visualization

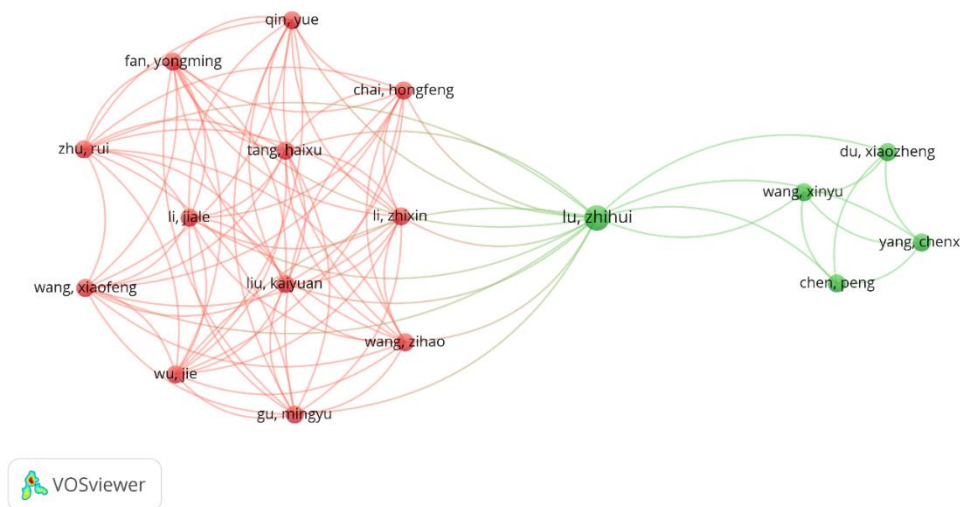


Figure 4. Author Visualization
 Source: Data Analysis Result, 2026

The figure below (Figure 4) shows two different research groups that are connected by a bridging author in the middle. The first cluster shown in red color is that of a group of closely connected authors, which includes Qin Yue, Fan Yongming, Zhu Rui, Li Jiale, Liu Kaiyuan, Wang Xiaofeng, Wu Jie, Gu Mingyu, Tang Haixu, Chai Hongfeng, Li Zhixin, and Wang Zihao. It should be noted that the highly connected nature of these authors implies that there are intensive collaboration and co-authorship activities taking place within the research community. In other words, the authors shown in the red color are considered as part of the dominant research group due to the close collaboration and knowledge exchange among each other. Moreover, it is highly likely that such authors form an established research team that makes great contributions towards developing a specific research domain. On the other hand, the second cluster in green color involves four authors, including Du Xiaozheng, Wang Xinyu, Yang Chenxi, and Chen Peng. The main characteristic of the network graph is the position of the author Lu Zhihui, who serves as a bridging link between these two clusters.

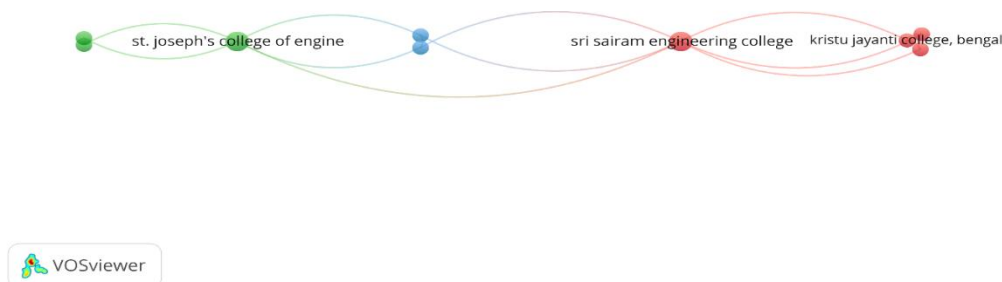


Figure 5. Institution Visualization
 Source: Data Analysis Result, 2026

As can be seen from Figure 5 below, there is a concentrated research collaboration among several institutes that have been working on research projects related to fraud detection in fintech industry. From the above network map, it is clear that the most prominent organizations include Sri Sairam Engineering College, Kristu Jayanti College, Bengaluru, and St. Joseph's College of Engineering. Since the organizations have strong connections with each other, it means that there have been collaborations among them. Specifically, one can note that Sri Sairam Engineering College is positioned centrally because it has connections with both Kristu Jayanti College and St. Joseph's College of Engineering. Furthermore, the networking model also exhibits some institutional connectivity, which means that collaboration occurs primarily among a small number of institutions. The presence of such institutional connectivity might imply that studies focusing on the issue of fraud detection within the fintech industry remain relatively nascent and could possibly be conducted by a few academic institutions whose research focus includes financial technologies, cybersecurity, artificial intelligence, and fraud detection. The centrality of Sri Sairam Engineering College can point out its contribution to establishing collaboration between academic institutions and conducting research work related to security and fraud detection in fintech.

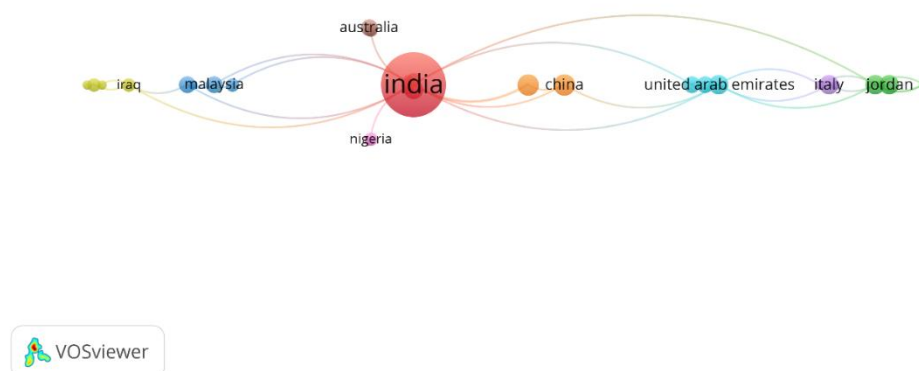


Figure 6. Country Visualization

Source: Data Analysis Result, 2026

Figure 6 demonstrates that India is the most dominant and influential contributor to research on fraud detection in the fintech sector. This is evident from its largest node size and extensive collaborative links with multiple countries, including China, Malaysia, Australia, Nigeria, the United Arab Emirates, Italy, Jordan, and Iraq. The central position of India suggests that it serves as the primary hub for international research cooperation, reflecting the country's growing fintech ecosystem, rapid digital financial adoption, and increasing scholarly interest in cybersecurity and fraud prevention. The strong connectivity also indicates that Indian researchers actively engage in cross-border collaborations, enhancing the dissemination of knowledge and technological innovation in fintech security. Beyond India, several regional collaboration groups can be observed. China and the United Arab Emirates occupy intermediary positions, facilitating connections between Asian and Middle Eastern research communities, while Italy and Jordan form another collaborative subgroup. Malaysia, Australia, Nigeria, and Iraq appear as smaller contributors that maintain direct links with India, indicating participation in broader international research networks despite lower publication volumes.

CONCLUSION

This bibliometric investigation gives an extensive insight into the evolution of the research in the domain of fraud detection within the fintech industry. According to the keywords' analysis, the fintech industry is recognized as the key research area and it is highly correlated with other aspects of the research including fraud detection, artificial intelligence, machine learning, risk management, cybersecurity, and blockchain technology. The overlay analysis and visualization by the network density imply that the research started with the exploration of such topics as cybercrime, compliance regulation, and financial risk management while evolving into such topics as the application of artificial intelligence, blockchain security measures, and financial inclusion. The citation analysis highlights that the most influential studies emphasize the opportunities and risks of artificial intelligence, fintech security frameworks, cybersecurity challenges, and fraud prevention mechanisms. Furthermore, the collaboration analyses reveal that scholarly contributions are concentrated within a limited number of author groups, institutions, and countries, with key actors serving as bridges between research communities. India emerges as the leading contributor to international collaboration, reflecting its significant role in the global fintech landscape.

REFERENCES

- [1] Syifa Hasna Iftinan and Edi Sukarmanto, "Pengaruh Pengalaman Auditor dan Kompetensi terhadap Pendeteksian Kecurangan Laporan Keuangan," *J. Ris. Akunt.*, pp. 1–7, Jul. 2022, doi: 10.29313/jra.v2i1.666.
- [2] W. Andayani and M. Wuryantoro, "Good Corporate Governance, Corporate Social Responsibility and Fraud Detection of Financial Statements," *Int. J. Prof. Bus. Rev. Int. J. Prof. Bus. Rev.*, vol. 8, no. 5, p. 9, 2023.
- [3] H. O. Bello, A. B. Ige, and M. N. Ameyaw, "Deep learning in high-frequency trading: conceptual challenges and solutions for real-time fraud detection," *World J. Adv. Eng. Technol. Sci.*, vol. 12, no. 02, pp. 35–46, 2024.
- [4] A. Sohel, M. A. Alam, M. Waliullah, A. Siddiki, and M. M. Uddin, "Fraud Detection In Financial Transactions Through Data Science For Real-Time Monitoring And Prevention," *Acad. J. Innov. Eng. Emerg. Technol.*, vol. 1, no. 01, pp. 91–107, 2024.
- [5] W. Wahidahwati and N. F. Asyik, "Determinants of Auditors Ability in Fraud Detection," *Cogent Bus. Manag.*, vol. 9, no. 1, 2022, doi: 10.1080/23311975.2022.2130165.
- [6] P. Adhikari, P. Hamal, and F. B. Jnr, "Artificial Intelligence in fraud detection: Revolutionizing financial security," 2024.
- [7] H. Kryshstal, V. Tomakh, T. Ivanova, V. Metelytsia, M. Yermolaieva, and Y. Panin, "ECO-INNOVATIVE TRANSFORMATION OF THE URBAN INFRASTRUCTURE OF UKRAINE ON THE WAY TO POST-WAR RECOVERY," *Financ. Credit Act. Probl. Theory Pract.*, vol. 2, no. 55, pp. 391–408, 2024, doi: 10.55643/fcapter.2.55.2024.4281.
- [8] B. Lutsiv, O. Dziubliuk, Y. Chaikovskiy, P. Lutsiv, and Y. Chaikovskiy, "THE ROLE OF GREEN BANKING IN ENSURING THE GOALS OF SUSTAINABLE ECONOMIC DEVELOPMENT," *Financ. Credit Act. Probl. Theory Pract.*, vol. 1, no. 54, pp. 23–36, 2024, doi: 10.55643/fcapter.1.54.2024.4250.
- [9] B. Widagdo and C. Sa'diyah, "Business sustainability: Functions of financial behavior, technology, and knowledge," *Probl. Perspect. Manag.*, vol. 21, no. 1, pp. 120–130, 2023, doi: 10.21511/ppm.21(1).2023.11.
- [10] T. Gupta, "How are Emerging Financial Instruments Transforming Sustainable Infrastructure Finance in the Face of Climate Change?," *The BRICS Imperative: Confronting Climate Challenges and Advancing Sustainable Development*. Springer Nature, Jagannath International Management School, New Delhi, India, pp. 135–169, 2026. doi: 10.1007/978-3-032-05932-1_7.
- [11] S. Masruroh, E. Nanggur, and U. A. Ngamal, "Peran Wakaf dalam Pengembangan Ekonomi Berkelanjutan: Studi Kasus di Indonesia," *Indo-Fintech Intellectuals J. Econ. Bus.*, vol. 4, no. 2, pp. 490–500, 2024.
- [12] A. Ashta and H. Herrmann, "Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance," *Strateg. Chang.*, vol. 30, no. 3, pp. 211–222, 2021.
- [13] S. Mehrban *et al.*, "Towards secure FinTech: A survey, taxonomy, and open research challenges," *Ieee Access*, vol. 8, pp. 23391–23406, 2020.
- [14] S. Gopal, P. Gupta, and A. Minocha, "Advancements in fin-tech and security challenges of banking industry," in *2023 4th international conference on intelligent engineering and management (ICIEM)*, IEEE, 2023, pp. 1–6.
- [15] A. Faccia, N. R. Moşteanu, L. P. L. Cavaliere, and L. J. Mataruna-Dos-Santos, "Electronic money laundering, the dark side of fintech: An overview of the most recent cases," in *Proceedings of the 2020 12th international conference on information management and engineering*, 2020, pp. 29–34.
- [16] A. Y. Areiqat, "Leveraging AI and FinTech: driving business innovation in the fourth industrial revolution," in *Achieving Sustainable Business through AI, Technology Education and Computer Science: Volume 1: Computer Science, Business Sustainability, and Competitive Advantage*, Springer, 2024, pp. 703–709.
- [17] X. Feng and S.-K. Kim, "Novel machine learning based credit card fraud detection systems," *Mathematics*, vol. 12, no. 12, p. 1869, 2024.

-
- [18] M. Shehadeh, "Exploring cutting-edge algorithms in FinTech: Leveraging machine learning and artificial intelligence for achieving sustainability," 2025.
- [19] G. Ali, M. M. Mijwil, B. A. Buruga, and M. Abotaleb, "A comprehensive review on cybersecurity issues and their mitigation measures in FinTech," 2024.
- [20] O. Manta, V. Vasile, and E. Rusu, "Banking transformation through FinTech and the integration of artificial intelligence in payments," *FinTech*, vol. 4, no. 2, p. 13, 2025.
- [21] S. Saluja, "Identity theft fraud-major loophole for FinTech industry in India," *J. Financ. Crime*, vol. 31, no. 1, pp. 146–157, 2024.