Bibliometric Study of IoT in Security and Monitoring Systems

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

ABSTRACT

This study presents a bibliometric analysis of research trends on the Internet of Things in security and monitoring systems using publications indexed in the Scopus database. The objective is to map the intellectual structure, thematic evolution, and collaboration patterns that shape the development of this research field. Bibliographic data were analyzed using VOSviewer to visualize keyword co-occurrence, temporal trends, density distribution, co-authorship networks, institutional collaboration, and country partnerships. The findings indicate that the internet of things serves as the central research hub, closely linked with machine learning, cybersecurity, authentication, and monitoring system architectures. Temporal analysis shows a transition from foundational intrusion detection and network security topics toward intelligent, application-oriented solutions supported by blockchain and data privacy frameworks. Density mapping highlights the convergence of AI-driven analytics with real-time monitoring environments, while collaboration analysis reveals strong research contributions from India and expanding global partnerships involving the United States, United Kingdom, China, and European countries. The results suggest that the field is evolving toward adaptive and context-aware security frameworks embedded within domain-specific monitoring applications such as healthcare and smart agriculture. This study contributes by providing a comprehensive overview of the knowledge structure and future research directions in IoT-based security and monitoring systems.

Keywords: *Internet of Things, Cybersecurity, Monitoring Systems, Machine Learning, Intrusion Detection, Data Privacy, Blockchain*

1. INTRODUCTION

The Internet of Things (IoT) has emerged as one of the most transformative technological paradigms of the 21st century, promising unprecedented connectivity between physical devices, systems, and data platforms. By enabling embedded sensors, processors, and communication modules to exchange information autonomously, IoT has revolutionized how systems operate across industry, healthcare, transportation, agriculture, and urban infrastructure [1]. This rapid integration has propelled the development of smart environments, where real-time data streams facilitate adaptive decision-making, predictive maintenance, and resource optimization. As the number of connected devices is projected to reach tens of billions globally within the next decade, IoT's influence has expanded far beyond its early applications to become a foundational pillar for modern digital ecosystems [2].

In parallel with this growth, security and monitoring systems have evolved from conventional analog or standalone digital solutions to highly interconnected, intelligent networks. Traditional security systems primarily relied on human intervention and manual oversight, which limited their responsiveness and scalability [3]. With the advent of IoT, security mechanisms have been augmented with sensor networks, automated alerts, and cloud-enabled analytics that significantly enhance situational awareness. Monitoring systems, once bound to fixed infrastructures, now leverage mobile, distributed, and adaptive IoT frameworks to capture environmental, behavioral, and operational data across diverse contexts [4]. For example, IoT-enabled surveillance in smart cities uses edge analytics to detect anomalies and trigger proactive responses, whereas industrial IoT systems monitor equipment health to prevent failures.

The synergy between IoT and security monitoring has generated a research surge, driven by the need for real-time responsiveness, remote accessibility, and scalability. Research has explored diverse applications such as intrusion detection systems using machine learning-enabled IoT sensors, smart home security frameworks that integrate biometric and environmental data, and intelligent surveillance networks that optimize bandwidth and storage through edge computing [5]. Furthermore, the proliferation of low-cost sensor technologies and advances in wireless communication protocols have democratized access to IoT-based security solutions, facilitating both large-scale deployments and community-level adoption [5]. These innovations underscore not only the technical feasibility of IoT in security contexts but also its potential to redefine standards of safety and operational efficiency.

Despite its transformative impact, the integration of IoT into security and monitoring infrastructures presents multifaceted challenges. From hardware limitations and interoperability concerns to issues of data privacy and system reliability, the complexity of IoT ecosystems demands rigorous research and standardized frameworks [6]. Researchers have responded with a diverse body of literature exploring architectural models, protocol optimizations, artificial intelligence integration, and risk mitigation strategies. As such, the scholarly output in this domain has grown at an exponential pace, encompassing journals, conference proceedings, technical reports, and industry whitepapers. Identifying trends, influential works, collaborative networks, and thematic focus areas within this broad literature is critical for both academic and practical advancements.

Bibliometric analysis has therefore become a valuable approach for mapping the evolution and structure of scientific knowledge in IoT and security monitoring research. Through quantitative metrics such as publication counts, citation patterns, co-authorship networks, keyword co-occurrence, and cross-disciplinary linkages, bibliometric studies offer insights that transcend individual papers [6]. By analyzing patterns of research output over time, researchers can identify emerging themes, influential authors and institutions, and gaps that warrant further inquiry. In fields characterized by rapid technological evolution—such as IoT in security and monitoring—bibliometric analyses are particularly useful for synthesizing large volumes of literature and guiding future research directions.

Despite the rapid growth of literature on IoT applications in security and monitoring systems, the field lacks a comprehensive bibliometric overview that systematically maps publication trends, thematic concentrations, collaborative structures, and emerging research fronts. Existing literature reviews tend to focus on specific applications or technical aspects, such as security protocols, machine learning integration, or smart city case studies, while overlooking broader scientific trends and influence patterns across disciplines [7], [8]. This fragmentation inhibits the ability of researchers, industry practitioners, and policymakers to gain a holistic understanding of how the field has evolved, where activity is concentrated, and which areas may represent opportunities or challenges for future exploration. The primary objective of this study is to conduct a comprehensive bibliometric analysis of research on the application of IoT in security and monitoring systems.

2. METHODS

This study employs a bibliometric research design to systematically evaluate the development of scholarly publications related to the application of the Internet of Things (IoT) in security and monitoring systems. Bibliometric analysis is a quantitative approach that examines patterns in scientific literature using statistical and visualization techniques. The study focuses on identifying publication trends, influential authors, institutional contributions, and thematic structures within the selected research domain. Data for the analysis were obtained from Scopus. The selection of these databases ensures high-quality and reliable bibliographic records. The search strategy utilized keyword combinations including "Internet of Things," "IoT," "security systems," and "monitoring systems," applied to titles, abstracts, and keywords of publications. Inclusion criteria consisted of English-language publications, peer-reviewed articles, and conference papers relevant to IoT-based security and monitoring applications, while unrelated fields and duplicate records were excluded.

After data collection, the retrieved bibliographic records were exported in standardized formats for preprocessing and analysis. The preprocessing stage involved data cleaning procedures such as removing duplicates, standardizing author names, and harmonizing keyword variations to ensure consistency in analysis. Bibliometric indicators including publication year, citation count, author productivity, institutional affiliations, and country contributions were then extracted. Science mapping techniques were applied to reveal intellectual structures and relationships among research topics. Keyword co-occurrence analysis was conducted to identify dominant research themes and emerging trends, while co-authorship analysis was used to examine collaboration patterns among researchers and institutions. To support visualization and network analysis VOSviewer was employed.

3. RESULTS AND DISCUSSION

3.1 Network Visualization

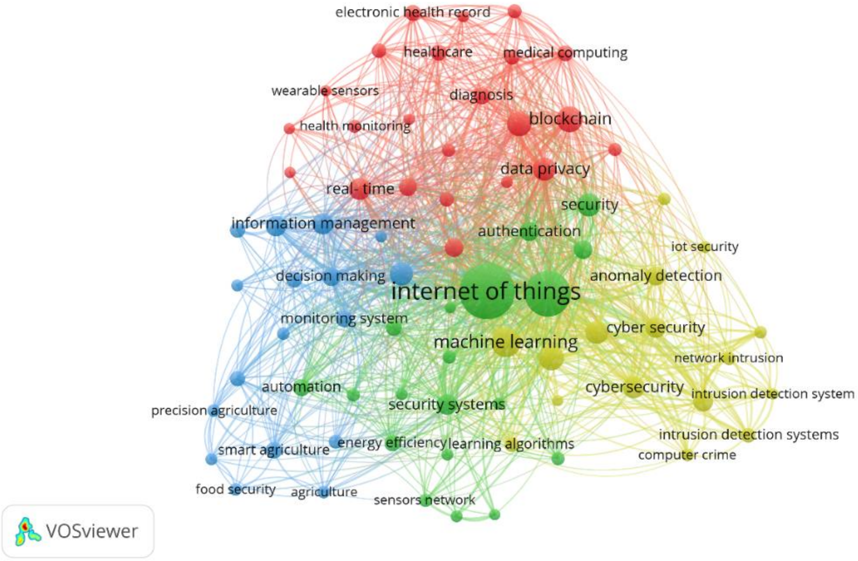

Figure 1. Network Visualization

Source: Data Analysis Result, 2026

Figure 1 network reveals that "internet of things" functions as the central and most dominant node, indicating its role as the conceptual backbone of research on security and monitoring systems. Its strong connections with terms such as machine learning, cybersecurity, monitoring system, and blockchain suggest that IoT studies are highly interdisciplinary, integrating data analytics, intelligent automation, and secure communication technologies. The density of links surrounding the central node reflects a mature research structure where IoT acts as a technological platform rather than a standalone topic.

The red cluster highlights the integration of IoT within healthcare monitoring and digital medical ecosystems, shown by keywords like healthcare, electronic health record, diagnosis, and data privacy. The presence of blockchain within this cluster indicates growing scholarly attention toward secure medical data management and trusted decentralized infrastructures. This suggests that IoT security research is not limited to technical infrastructure but extends to sensitive application domains where privacy protection and ethical data handling are critical. The green cluster emphasizes machine learning–driven security mechanisms and automation capabilities. Terms such as learning algorithms, security systems, energy efficiency, and sensors network indicate that many studies focus on optimizing monitoring performance through intelligent analytics. This cluster shows a technological shift toward predictive monitoring and adaptive systems, where algorithms play a crucial role in detecting threats and improving operational efficiency within IoT environments.

Meanwhile, the yellow cluster represents the core cybersecurity and intrusion detection domain, including keywords like cyber security, network intrusion, intrusion detection system, and anomaly detection. The tight interconnections within this group indicate that intrusion detection remains a central research stream in IoT security literature. The coexistence of traditional cybersecurity terms with IoT-specific keywords highlights the evolution of classical network security frameworks into more complex, distributed IoT ecosystems. The blue cluster reflects application-oriented monitoring and information management contexts, including agriculture, precision monitoring, and decision-making systems. The presence of terms such as smart agriculture, precision agriculture, and information management shows that IoT security research is expanding into sectoral applications where monitoring reliability is essential.

3.2 Overlay Visualization

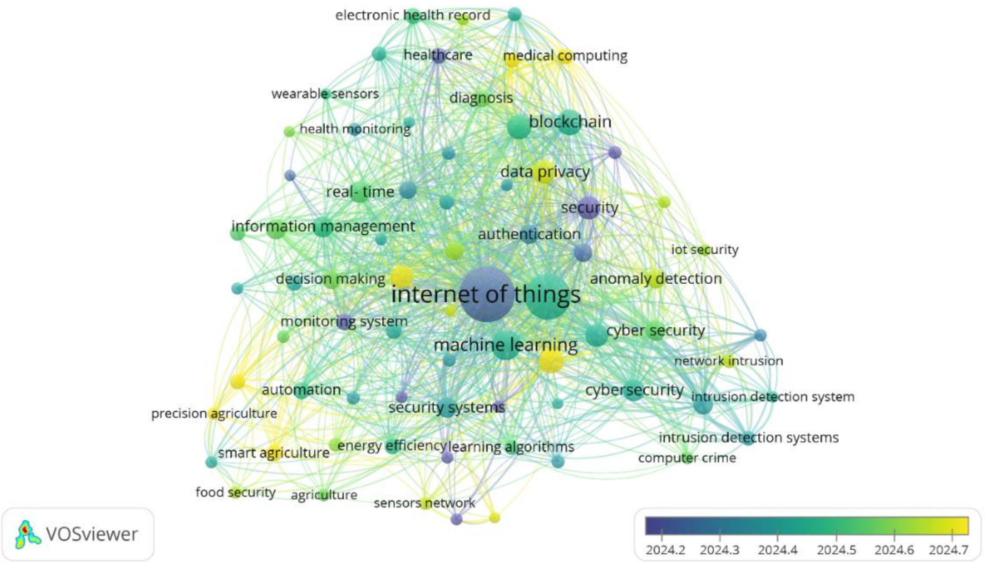

Figure 2. Overlay Visualization

Source: Data Analysis Result, 2026

Figure 2 shows the temporal evolution of research themes within the IoT security and monitoring systems literature. Keywords colored in darker blue tones represent earlier research phases, where foundational topics such as internet of things, security systems, and intrusion detection systems dominated the field. These early studies primarily focused on establishing basic cybersecurity frameworks and monitoring architectures, reflecting the initial stage of integrating IoT into secure digital infrastructures. As the color gradient moves toward green, the research trajectory shifts toward intelligent and data-driven approaches. Keywords such as machine learning, authentication, data privacy, and cyber security indicate a growing emphasis on adaptive security mechanisms and automated monitoring processes. This transition suggests that scholars began integrating artificial intelligence techniques to address the complexity of distributed IoT networks, emphasizing predictive analytics and anomaly detection rather than purely reactive security strategies. The most recent topics, highlighted in yellow, reveal an expansion toward applied and interdisciplinary domains, including precision agriculture, smart agriculture, automation, and medical computing. These emerging areas indicate that IoT security research is moving beyond technical system design into sector-specific monitoring applications.

3.3 Citation Analysis

Table 1. The Most Impactful Literatures

Citations	Authors and year	Title
1340	[9]	A Survey on the Edge Computing for the Internet of Things
1024	[10]	Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach
919	[11]	A survey of intrusion detection in Internet of Things
859	[12]	Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare
825	[13]	Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring
805	[14]	Digital Twins: A Survey on Enabling Technologies, Challenges, Trends and Future Prospects
739	[15]	IoT Considerations, Requirements, and Architectures for Smart Buildings-Energy Optimization and Next-Generation Building Management Systems
725	[16]	Review of Internet of Things (IoT) in Electric Power and Energy Systems
723	[17]	Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges
715	[18]	IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices

Source: Scopus, 2025

3.4 Density Visualization

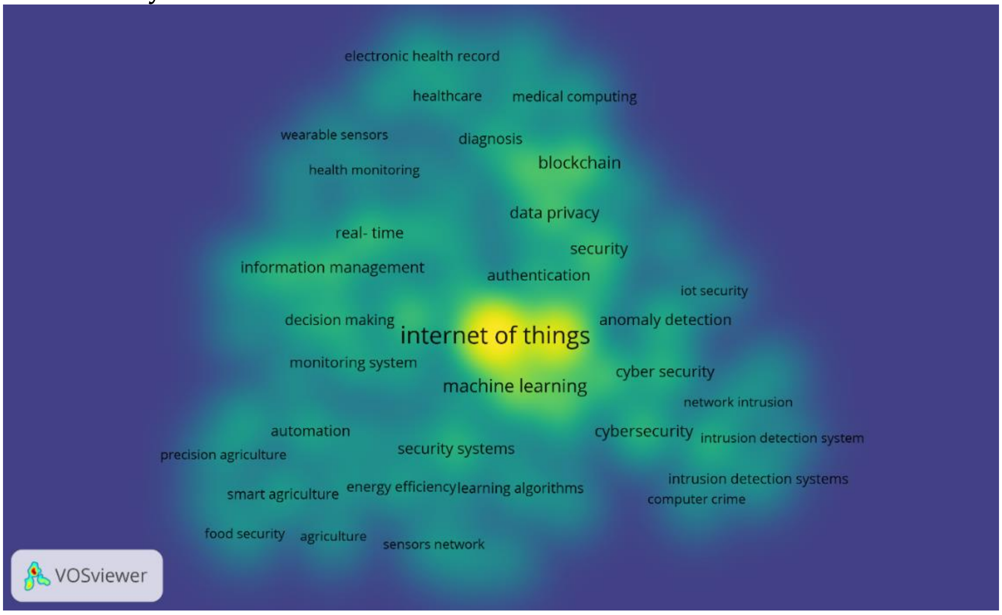

Figure 3. Density Visualization

Source: Data Analysis Result, 2026

Figure 3 highlights the intellectual concentration within the IoT security and monitoring systems literature, where "internet of things" appears as the brightest and most dominant hotspot. Its strong proximity to machine learning, cybersecurity, authentication, and security systems indicates that these themes form the core foundation of current research. The intensity around these keywords suggests that scholars heavily focus on integrating intelligent algorithms with secure IoT architectures, emphasizing real-time monitoring, anomaly detection, and adaptive protection mechanisms as central research priorities. Beyond the central hotspot, moderate-density areas emerge around healthcare monitoring and sectoral applications such as blockchain, data privacy, medical computing, and smart agriculture. These surrounding zones illustrate expanding interdisciplinary directions where IoT security is applied to specific domains requiring reliable monitoring and data protection. The gradient from high-density central themes toward more dispersed application keywords reflects a research landscape that is both technically grounded in cybersecurity and increasingly diversified into practical monitoring environments across healthcare, agriculture, and automated systems.

3.5 Co-Authorship Network

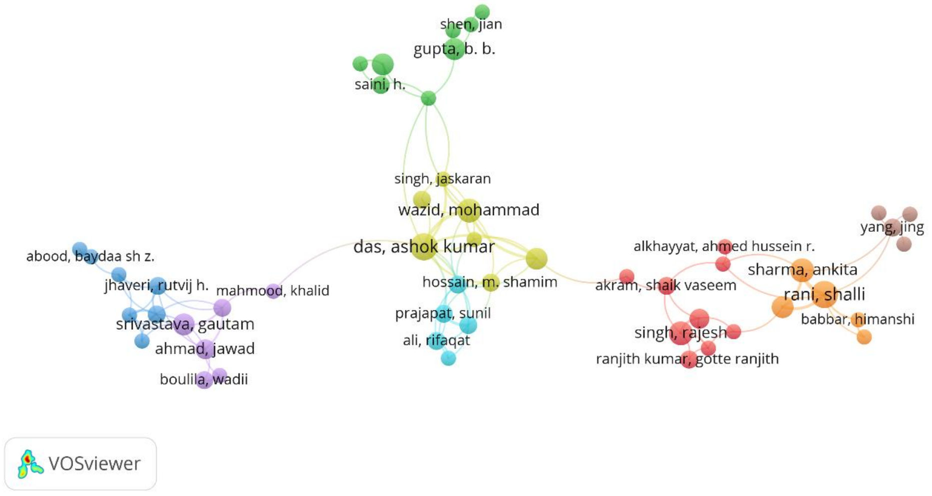

Figure 4. Author Visualization

Source: Data Analysis Result, 2026

Figure 4 illustrates several distinct collaboration clusters, indicating that research on IoT in security and monitoring systems is organized around regional or thematic research groups rather than a single dominant global network. Authors such as Das, Ashok Kumar and Wazid, Mohammad appear as central connectors, linking multiple collaborators and suggesting their strong influence within the field. On the right side, another active cluster formed by Rani, Shalli, Sharma, Ankita, and related co-authors reflects consistent teamwork within cybersecurity-focused studies, while smaller isolated clusters on the left indicate localized collaborations with fewer cross-group connections.

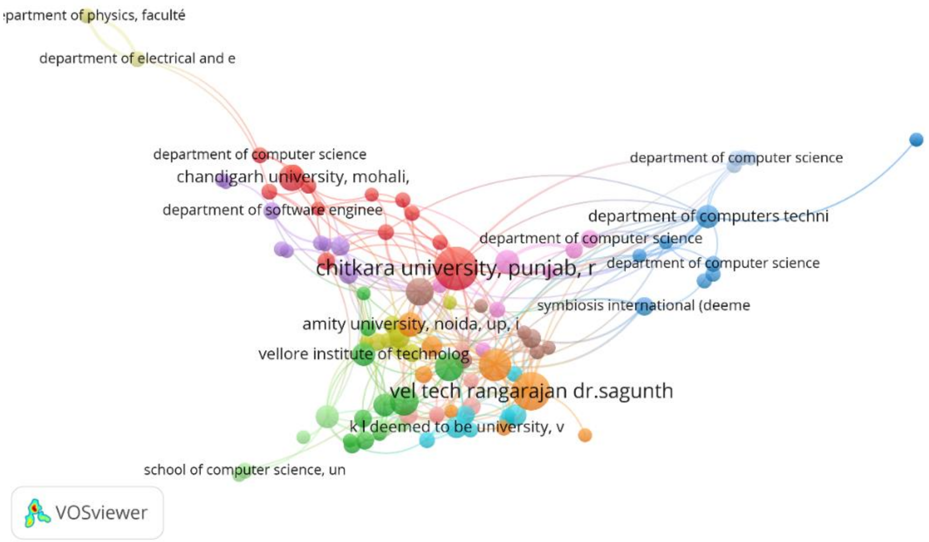
partment of physics, faculté
department of electrical and e
department of computer science
chandigarh university, mohali,
department of software enginee
chitkara university, punjab, r
department of computer science
department of computers techni
department of computer science
department of computer science
symbiosis international (deeme
amity university, noida, up, i
vellore institute of technolog
vel tech rangarajan dr.sagunth
k l deemed to be university, v
school of computer science, un
VOSviewer

Figure 5. Affiliation Visualization

Source: Data Analysis Result, 2026

Figure 5 shows that research on IoT in security and monitoring systems is strongly centered around a few leading universities, with Chitkara University Punjab and Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology appearing as prominent hubs connected to multiple departments and partner institutions. The dense clustering among Indian universities such as Amity University, Chandigarh University, and Symbiosis International indicates a regional research concentration, where collaborations are largely formed within interconnected academic networks in engineering and computer science fields. Peripheral nodes, including departments of computer science from other institutions, suggest emerging participation but with fewer collaborative ties.

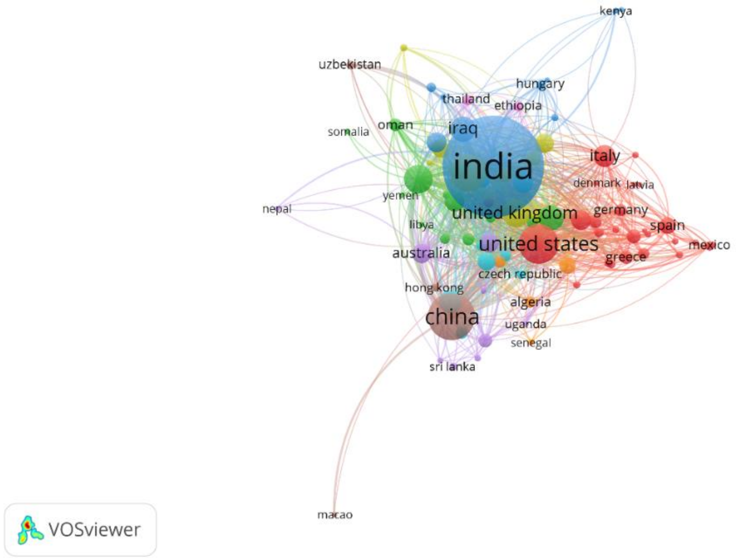

Figure 6. Country Visualization

Source: Data Analysis Result, 2026

Figure 6 indicates that research on IoT in security and monitoring systems is heavily dominated by India, which appears as the largest and most central node, reflecting high publication output and extensive international collaboration. Strong linkages with countries such as the United States, United Kingdom, China, Italy, and Germany show that the field is supported by cross-regional partnerships between Asia, Europe, and North America. European countries form a tightly connected cluster, suggesting collaborative projects focused on cybersecurity and advanced monitoring technologies, while emerging connections with nations in the Middle East, Africa, and Southeast Asia highlight the gradual globalization of IoT research. The network structure implies that although a few countries lead in productivity, the research landscape is increasingly interconnected, promoting knowledge exchange and collaborative innovation across diverse geographical regions.

Discussion

The bibliometric findings reveal that research on IoT in security and monitoring systems has evolved into a multidisciplinary field that integrates cybersecurity, intelligent analytics, and real-time monitoring infrastructures. The keyword co-occurrence analysis shows that the "internet of things" acts as the conceptual nucleus, strongly connected with machine learning, cybersecurity, authentication, and monitoring systems. This pattern indicates that current scholarly attention is no longer limited to device connectivity but is increasingly directed toward intelligent threat detection and adaptive security architectures. The dominance of machine learning within the network also suggests a transition from traditional rule-based monitoring approaches toward data-driven predictive security models that can respond dynamically to complex cyber-physical environments.

The overlay visualization highlights a temporal shift in research priorities. Early studies primarily emphasized foundational cybersecurity frameworks and intrusion detection systems, reflecting the initial phase of securing distributed IoT infrastructures. Over time, the literature has moved toward integrating advanced technologies such as blockchain, anomaly detection, and data privacy mechanisms. Recent research trends, represented by newer keywords, demonstrate growing attention to application-oriented domains including smart agriculture, healthcare monitoring, and automated industrial systems. This progression suggests that IoT security research is transitioning from conceptual system development to domain-specific implementations, where security becomes embedded within operational monitoring processes rather than functioning as a separate technical layer.

Density analysis further confirms that the intellectual core of the field revolves around the convergence of IoT, cybersecurity, and machine learning. High-density areas indicate a strong concentration of studies focusing on secure data transmission, authentication, and intelligent monitoring frameworks. Meanwhile, moderate-density zones related to healthcare, blockchain, and precision agriculture illustrate emerging interdisciplinary directions that extend beyond purely technical discussions. These patterns imply that researchers are increasingly addressing the societal and operational implications of IoT monitoring systems, particularly in environments where data privacy and real-time decision-making are critical.

Collaboration analyses provide additional insight into the structural development of the research landscape. The co-authorship network shows that scholarly production is largely organized around several active research groups, with a few influential authors acting as central connectors within their clusters. Institutional collaboration maps reveal that universities in India play a prominent role, forming dense research hubs linked to engineering and computer science departments. Similarly, the country collaboration network demonstrates that India leads publication output, supported by strong partnerships with the United States, United Kingdom, China, and several European nations. Although the field exhibits increasing internationalization, the presence of regionally concentrated clusters suggests opportunities for broader global collaboration to enhance knowledge diversity and methodological innovation.

CONCLUSION

This bibliometric study demonstrates that research on IoT in security and monitoring systems has developed into a dynamic and interdisciplinary domain centered on the integration of cybersecurity, machine learning, and intelligent monitoring technologies. The analysis reveals that IoT functions as the primary research hub, with growing emphasis on data privacy, authentication, anomaly detection, and application-driven solutions in sectors such as healthcare and smart agriculture. Collaboration patterns show strong contributions from India and increasing global partnerships, indicating expanding international engagement despite the presence of regional research clusters. Overall, the field is progressing toward adaptive, intelligent, and context-aware security frameworks, suggesting that future studies should prioritize cross-sector integration, scalable protection mechanisms, and collaborative innovation to address the evolving challenges of IoT-based monitoring environments.

REFERENCES

[1] D. C. Runtuwene, V. C. Poekoel, and P. D. K. Manembu, "Sistem Kontrol Dan Pemantauan Berbasis IoT untuk Kenyamanan Ternak Unggas: IoT Based Control And Monitoring System for Poultry Convenience," *J. Tek. Elektro dan Komput.*, vol. 13, no. 02, pp. 91–96, 2024.

[2] J. S. Raj, "A novel information processing in IoT based real time health care monitoring system," *J. Electron.*, vol. 2, no. 03, pp. 188–196, 2020.

[3] M. Alshamrani, "IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey," *J. King Saud Univ. Inf. Sci.*, vol. 34, no. 8, pp. 4687–4701, 2022.

[4] G. Manogaran *et al.*, "Wearable IoT smart-log patch: An edge computing-based Bayesian deep learning network system for multi access physical monitoring system," *Sensors*, vol. 19, no. 13, p. 3030, 2019.

[5] S. Kajornkasirat, N. Chanapai, and B. Hnusuwan, "Smart health monitoring system with IoT," in *2018 IEEE Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, IEEE, 2018, pp. 206–211.

[6] K. Micko, P. Papcun, and I. Zolotova, "Review of IoT sensor systems used for monitoring the road infrastructure," *Sensors*, vol. 23, no. 9, p. 4469, 2023.

[7] N. N. Pujianik, I. N. S. Parwata, I. M. O. G. Antara, K. Kazumi, and A. Rivai, "Development of an IoT-Based Real-Time Monitoring System and LFA to Improve the Efficiency and Performance of the Wastewater Treatment Plant at Udayana University Hospital," in *Journal of the Civil Engineering Forum*, 2023, pp. 109–116.

[8] S. Suganyadevi, D. Shamia, and K. Balasamy, "An IoT-based diet monitoring healthcare system for women," *Smart Healthc. Syst. Des. Secur. Priv. Asp.*, pp. 167–202, 2022.

[9] W. Yu *et al.*, "A survey on the edge computing for the Internet of Things," *IEEE access*, vol. 6, pp. 6900–6919, 2017.

[10] A. M. Rahmani *et al.*, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 641–658, 2018.

[11] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. De Alvarenga, "A survey of intrusion detection in Internet of Things," *J. Netw. Comput. Appl.*, vol. 84, pp. 25–37, 2017.

[12] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, "Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare," *Futur. Gener. Comput. Syst.*, vol. 78, pp. 659–676, 2018.

[13] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring," *J. Med. Syst.*, vol. 42, no. 7, p. 130, 2018.

[14] S. Mihai *et al.*, "Digital twins: A survey on enabling technologies, challenges, trends and future prospects," *IEEE Commun. Surv. Tutorials*, vol. 24, no. 4, pp. 2255–2291, 2022.

[15] D. Minoli, K. Sohraby, and B. Occhiogrosso, "IoT considerations, requirements, and architectures for smart buildings—Energy optimization and next-generation building management systems," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 269–283, 2017.

[16] G. Bedi, G. K. Venayagamoorthy, R. Singh, R. R. Brooks, and K.-C. Wang, "Review of Internet of Things (IoT) in electric power and energy systems," *IEEE Internet things J.*, vol. 5, no. 2, pp. 847–870, 2018.

[17] H. Feng, X. Wang, Y. Duan, J. Zhang, and X. Zhang, "Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges," *J. Clean. Prod.*, vol. 260, p. 121031, 2020.

[18] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, "IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8182–8201, 2019.