West Science Interdisciplinary Studies
Vol. 03, No. 06, June and 2025: pp. 990-1000

Bibliometric Review on Infrastructure Monitoring with IoT

Loso Judijanto[1], Justam[2], Ardi Azhar Nampira[3]
[1] IPOSS Jakarta, Indonesia and losojudijantobumn@gmail.com
[2] Universitas Mega Buana Palopo and justam@umegabuana.ac.id
[3] Institute Teknologi Sepuluh November and ardi.azhar@gmail.com

ABSTRACT

The integration of the Internet of Things (IoT) into infrastructure monitoring has transformed how built environments are observed, maintained, and managed. This study conducts a comprehensive bibliometric review to map the research landscape, thematic trends, and collaboration patterns in the domain of IoT-based infrastructure monitoring. Using data retrieved from the Scopus database (2010–2024) and analyzed through VOSviewer, the study identifies key research clusters, influential authors, prolific countries, and the evolution of core topics over time. Results show that the research focus has shifted from basic sensor deployment and data acquisition to advanced topics such as machine learning, edge computing, data privacy, and cybersecurity. India, China, and the United States emerge as leading contributors, with dense global collaboration networks. The study highlights both the maturity of core research areas and the emergence of new directions such as blockchain integration and privacy-preserving infrastructure systems. These findings provide valuable insights for academics, policymakers, and practitioners aiming to enhance infrastructure resilience and efficiency through IoT technologies.

Keywords: *Internet of Things (IoT), Infrastructure Monitoring, Structural Health Monitoring, Machine Learning, Bibliometric Analysis*

1. INTRODUCTION

In recent years, the integration of the Internet of Things (IoT) into infrastructure monitoring has revolutionized how critical assets such as bridges, buildings, railways, and pipelines are maintained and managed. IoT facilitates real-time, continuous, and automated data collection from various sensors embedded within infrastructure components, enabling predictive maintenance and early detection of potential failures [1]. The use of IoT in this context offers unprecedented efficiency and cost-saving opportunities compared to traditional manual inspection methods. With the rapid development of smart cities and Industry 4.0, infrastructure monitoring has become a pivotal area for implementing IoT solutions to ensure safety, sustainability, and resilience [2], [3].

The convergence of IoT and infrastructure systems has led to an increasing number of studies focusing on structural health monitoring (SHM), environmental sensing, and asset management [4]. These studies have explored how IoT technologies such as wireless sensor networks (WSNs), edge computing, cloud-based analytics, and machine learning can be deployed to collect, transmit, and analyze large volumes of data from infrastructure systems. The digital transformation of infrastructure monitoring has also improved decision-making processes in urban planning, maintenance scheduling, and risk assessment [5]. Governments and industries alike are investing in IoT-powered monitoring systems to improve public safety, reduce downtime, and optimize asset lifecycles.

As this field matures, researchers are investigating various types of sensors, communication protocols, and architectures suitable for diverse environmental conditions and infrastructure types. For example, vibration sensors are frequently used in bridge monitoring, while temperature and

humidity sensors are vital for tunnel and pipeline monitoring. Furthermore, low-power wide-area networks (LPWANs) such as LoRaWAN and NB-IoT have gained popularity for ensuring long-range, energy-efficient communication among distributed sensors. These technical developments are complemented by advances in data analytics, including anomaly detection, predictive modeling, and visualization tools [6]. The synergy between IoT and these analytical frameworks supports proactive maintenance strategies and risk mitigation.

Despite the proliferation of IoT-based infrastructure monitoring systems, the landscape of research in this domain is highly fragmented, with numerous studies focusing on specific applications, sensor types, or monitoring objectives. A wide range of case studies has been conducted globally, yet there is a lack of systematic consolidation and mapping of these scholarly outputs. In this context, bibliometric analysis serves as a powerful tool to identify research trends, influential publications, prominent authors, and key research clusters. It can help synthesize the evolution of this interdisciplinary field and uncover gaps for future investigation [7].

Moreover, the global push for sustainable development goals (SDGs), particularly Goal 9 on industry, innovation, and infrastructure, has amplified the importance of robust infrastructure systems supported by smart monitoring technologies. The integration of IoT into infrastructure monitoring aligns with the broader goals of enhancing urban resilience, promoting innovation, and enabling data-driven governance. This macro-level agenda further justifies the need to understand the trajectory of research in this area through a comprehensive bibliometric study that traces its intellectual structure and thematic directions.

Although numerous studies have explored various aspects of IoT applications in infrastructure monitoring, there is a paucity of bibliometric reviews that comprehensively map the development, trends, and thematic concentrations within this research domain. Most existing reviews are either narrative in nature or limited to specific case studies, sensor technologies, or infrastructure types, thereby failing to capture the broader intellectual landscape. Consequently, there is a knowledge gap in understanding the research evolution, collaboration patterns, and influential contributors in the field of IoT-based infrastructure monitoring. This study aims to conduct a bibliometric review of the research landscape on infrastructure monitoring using the Internet of Things (IoT).

2. METHODS

This study employed a bibliometric analysis approach to systematically map the intellectual structure and research development in the field of infrastructure monitoring using the Internet of Things (IoT). Bibliometric analysis is a quantitative method that evaluates patterns of scientific publications, co-authorship, citation networks, and keyword trends within a specific area of research [7]. By using this method, the study aims to reveal the most influential authors, journals, institutions, and countries, identify emerging themes, and detect collaborative research patterns in the domain. The bibliometric approach was selected for its ability to handle large volumes of academic data and uncover latent trends that may not be visible through traditional literature reviews.

The data for this study were collected from the Scopus database, which was selected due to its comprehensive coverage of peer-reviewed journals and high-quality metadata suitable for bibliometric analysis. The search query was formulated using a combination of keywords such as “infrastructure monitoring”, “IoT”, “structural health monitoring”, “smart infrastructure”, and

"Internet of Things", applied to the article title, abstract, and keywords fields. The search was limited to the period between 2010 and 2024, aligning with the emergence and growth of IoT technologies. Only articles, conference papers, and reviews written in English were included in the dataset. After applying the inclusion criteria and manually screening irrelevant records, a total of 689 publications were finalized for analysis.

For the analytical process, the study utilized VOSviewer, a software tool specifically designed for constructing and visualizing bibliometric networks. The software was used to create maps of co-authorship, keyword co-occurrence, citation patterns, and institutional collaboration. Co-occurrence analysis of keywords was performed to identify research hotspots and thematic clusters within the field. Additionally, citation analysis was conducted to determine the most influential documents and authors. Network visualizations were generated to interpret the relationships among countries, institutions, and authors contributing to IoT-based infrastructure monitoring research.

3. RESULTS AND DISCUSSION

3.1 Network Visualization

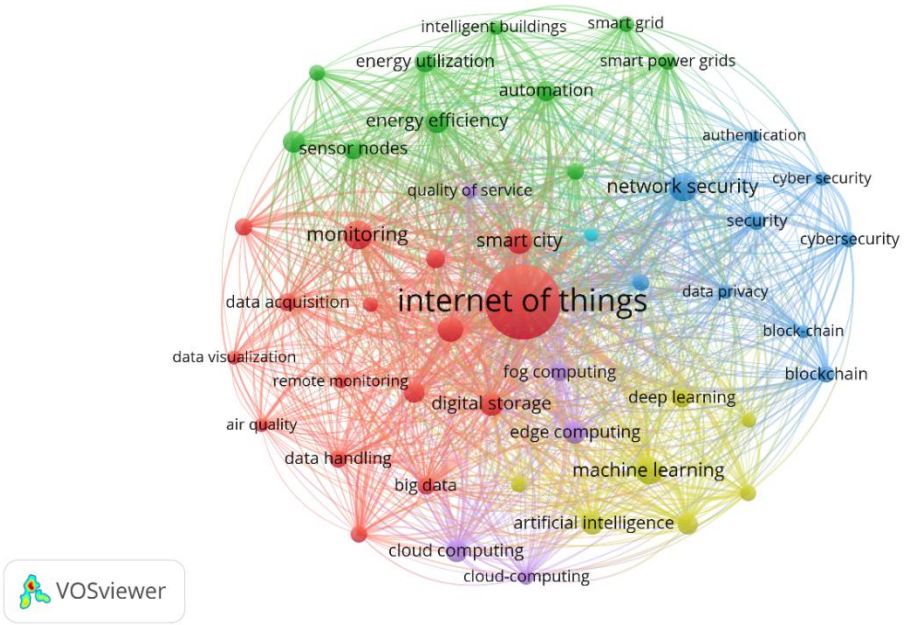

Figure 1. Network Visualization
Source: Data Analysis Result, 2025

Figure 1 above presents a keyword co-occurrence network related to the topic of Infrastructure Monitoring with IoT. Each node represents a keyword from the dataset, with node size indicating frequency of occurrence, and the lines (edges) representing co-occurrence strength between keywords. The colors represent different thematic clusters generated through VOSviewer's clustering algorithm. At the center of the map, the term "internet of things" appears as the most dominant node, indicating its centrality and high frequency across the analyzed literature.

The red cluster is largely concerned with *monitoring and data handling*. Keywords such as "monitoring," "data acquisition," "data handling," "remote monitoring," and "big data" are prominent in this group. This suggests a strong focus on the technical backbone of infrastructure monitoring—specifically, how data is sensed, collected, and transmitted. The presence of terms like "data visualization" and "air quality" indicates that this cluster also touches on environmental

sensing and the interpretation of sensor-generated data, underscoring the operational side of IoT deployment in real-world infrastructure.

The green cluster covers topics related to *energy efficiency and smart systems*. Terms such as "sensor nodes," "energy utilization," "energy efficiency," "intelligent buildings," and "automation" signify research focused on sustainable smart infrastructure. The inclusion of "smart power grids" and "smart grid" shows how IoT is utilized for improving energy systems and infrastructure performance. This cluster likely captures research that bridges IoT with green technology and smart building management, reflecting an emphasis on sustainability in infrastructure monitoring.

The blue cluster centers on *network and information security*, including terms like "network security," "cybersecurity," "authentication," "security," and "data privacy." This highlights growing scholarly attention to the vulnerabilities and risks associated with IoT-based monitoring systems. As infrastructure becomes increasingly digitized, the protection of data and the secure transmission of sensor information are crucial. This cluster indicates a substantial body of research addressing how to safeguard critical systems from cyber threats in IoT environments.

The yellow cluster focuses on computational intelligence and processing technologies. Keywords such as "machine learning," "deep learning," "artificial intelligence," "cloud computing," "edge computing," and "fog computing" reflect an interest in enhancing infrastructure monitoring using advanced analytics. These technologies allow for real-time, decentralized data processing and decision-making, supporting predictive maintenance and anomaly detection. This cluster also illustrates the convergence of IoT with AI-driven solutions, indicating an evolution toward intelligent, adaptive infrastructure systems.

3.2 Overlay Visualization

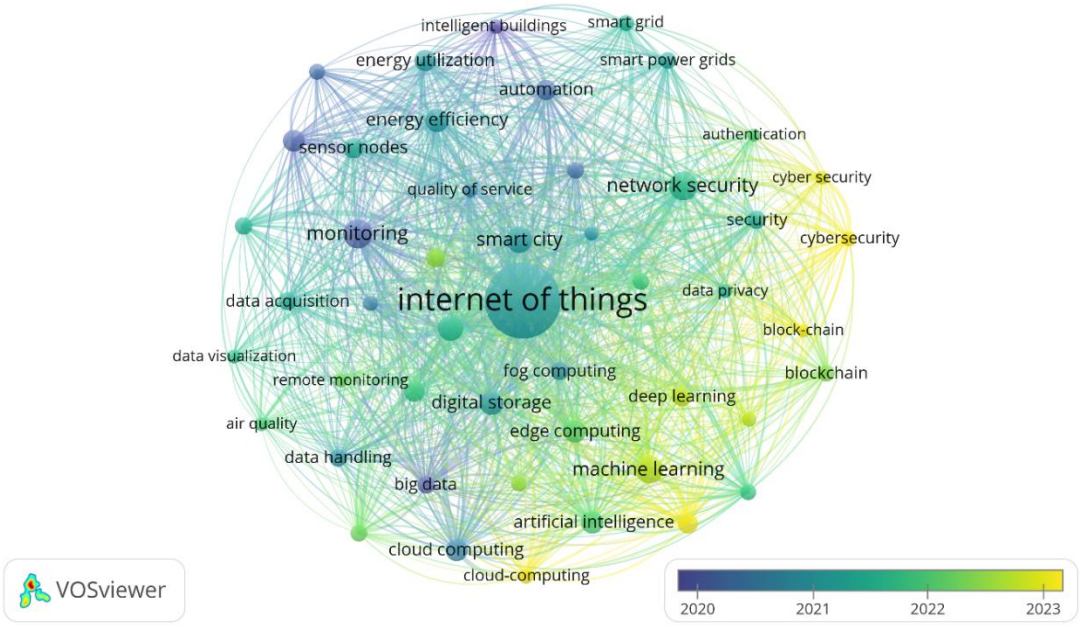

Figure 2. Overlay Visualization

Source: Data Analysis Result, 2025

Figure 2 displays the temporal evolution of keywords in the domain of infrastructure monitoring using IoT, with colors indicating the average publication year (from 2020 to 2023). Keywords shaded in blue to purple represent concepts more prominent in earlier years, while green to yellow keywords indicate more recent research attention. The central keyword, "internet of

things," remains consistently relevant across the timeline, showing it as a foundational concept throughout the dataset. Earlier studies (2020–2021) emphasized technical aspects like "sensor nodes," "energy efficiency," "data handling," and "monitoring," as seen by their darker shades.

In contrast, more recent developments (2022–2023) are indicated by yellow-toned keywords clustered on the right side of the map. These include "machine learning," "blockchain," "cybersecurity," "deep learning," "data privacy," and "edge computing." This shift suggests that current research is increasingly focusing on enhancing data intelligence, security, and distributed computing architectures for IoT-based infrastructure systems. The emergence of "blockchain" and "data privacy" reflects rising concerns over secure and trustworthy data management, particularly as smart infrastructures become more interconnected and exposed to cyber threats. This evolution illustrates a transition from hardware and data acquisition challenges to intelligent analytics and secure architecture. As the field matures, there is a clear movement from deploying basic sensing and networking infrastructure toward optimizing these systems using advanced technologies like AI, privacy-preserving protocols, and edge/fog computing.

3.3 Citation Analysis

Table 1. The Most Impactful Literatures

Citations	Authors and year	Title
1252	[8]	iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments
1205	[9]	A Survey on the Edge Computing for the Internet of Things
1008	[10]	An IoT-Aware Architecture for Smart Healthcare Systems
962	[11]	Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach
681	[12]	IoT Considerations, Requirements, and Architectures for Smart Buildings-Energy Optimization and Next-Generation Building Management Systems
644	[13]	Cloud-assisted Industrial Internet of Things (IIoT) - Enabled framework for health monitoring
624	[14]	State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing
550	[15]	Securing Fog Computing for Internet of Things Applications: Challenges and Solutions
519	[16]	Digital Twins: A Survey on Enabling Technologies, Challenges, Trends and Future Prospects
494	[17]	The internet of things for ambient assisted living

Source: Scopus, 2025

3.4 Density Visualization

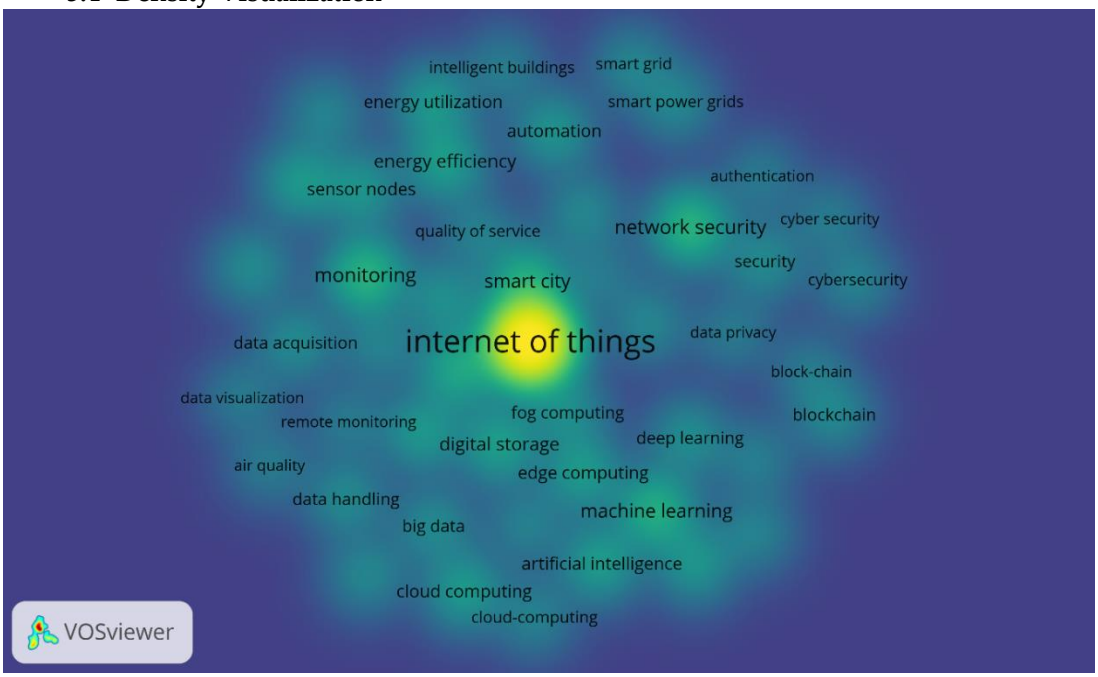

Figure 3. Density Visualization

Source: Data Analysis Result, 2025

Figure 3 illustrates the density of keyword occurrences in the field of IoT-based infrastructure monitoring. Areas with brighter colors (yellow to green) indicate higher concentrations of publications, while darker zones (blue to violet) reflect sparser activity. The term "internet of things" appears as the most intensely concentrated keyword, positioned at the center of the map, highlighting its fundamental and ubiquitous role across all research in this domain. Closely associated terms such as "monitoring," "smart city," "data acquisition," and "network security" also show high density, indicating their frequent co-occurrence with IoT in the scholarly literature. In contrast, peripheral keywords such as "air quality," "block-chain," and "data visualization" exhibit lower density, suggesting that although these topics are present, they are either emerging or niche in their research contributions. The map suggests that current scholarly focus is heavily centered on core IoT technologies and their integration into infrastructure systems, while advanced analytics, environmental monitoring, and blockchain-related aspects are still developing areas.

3.5 Co-Authorship Network

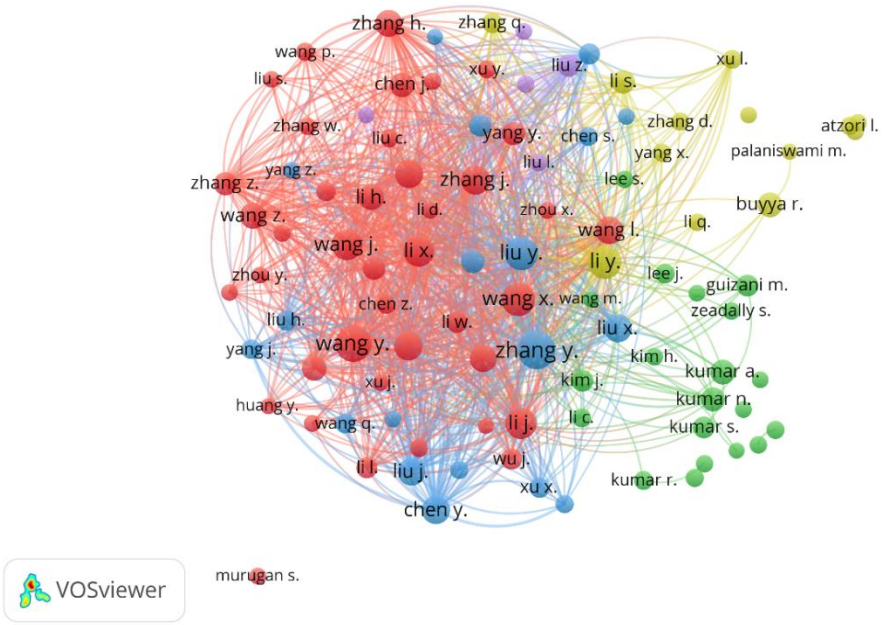

Figure 4. Author Visualization
Source: Data Analysis Result, 2025

Figure 4 above represents a co-authorship network of researchers in the field of IoT-based infrastructure monitoring. Each node denotes an individual author, and the node size corresponds to the author's publication frequency or co-authorship strength. The colors represent different collaborative clusters or author groups, indicating shared research interests or institutional affiliations. Notably, authors with the surname Zhang, Wang, Liu, Li, and Chen form the dense red cluster at the core, illustrating a highly interconnected network—likely indicative of prolific collaborations within institutions based in China. The green and yellow clusters on the right highlight other research communities, including scholars like Kumar R., Buyya R., and Atzori L., who appear more internationally oriented with connections across institutions.

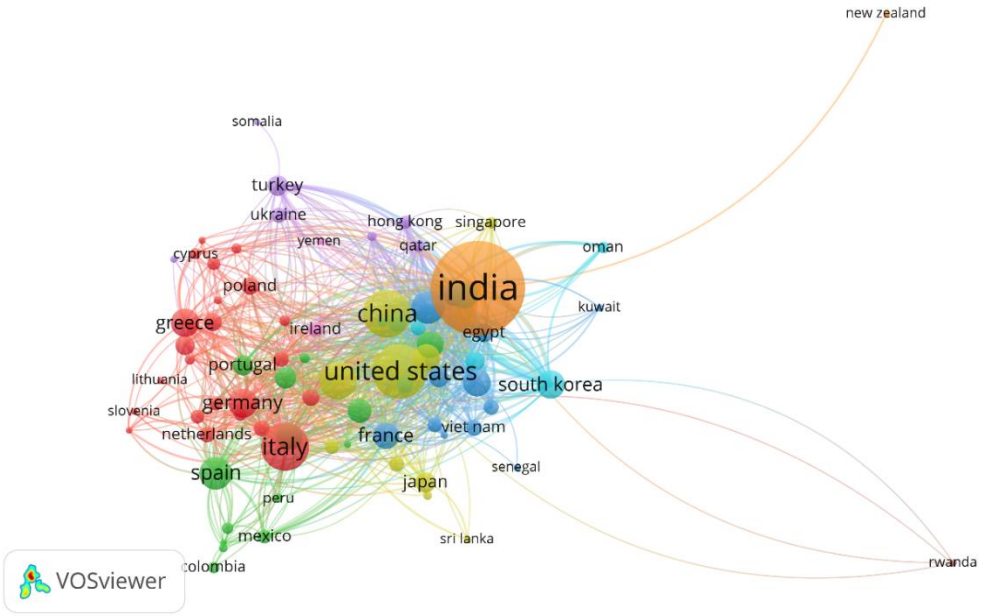

Figure 5. Country Visualization
Source: Data Analysis Result, 2025

Figure 5 illustrates the country collaboration network in the field of infrastructure monitoring using IoT. Each node represents a country, with node size corresponding to the number of publications, and lines (edges) indicating co-authorship or collaborative links. Notably, India appears as the largest and most central node, signifying its dominant contribution and high international collaboration in this research area. It is closely connected to China, the United States, South Korea, and Italy, forming a core of globally active contributors. European countries like Germany, France, Spain, and Portugal form a dense collaborative cluster, reflecting strong intra-European cooperation. Meanwhile, countries like New Zealand, Rwanda, and Somalia appear on the periphery, indicating limited but emerging participation.

Discussion

1. Central Themes and Keyword Clusters

The keyword co-occurrence network illustrates that the term "internet of things" is the dominant and central concept, connecting diverse clusters of research activity. This prominence reflects the foundational role of IoT technologies across all aspects of infrastructure monitoring—from sensor deployment to intelligent data processing. Closely related keywords such as "monitoring," "data acquisition," "smart city," and "network security" demonstrate the field's focus on sensing, data transmission, and securing critical systems. The red cluster, which includes keywords like "monitoring," "remote monitoring," "data handling," and "air quality," signifies the operational and environmental aspects of infrastructure surveillance. This indicates a sustained interest in the practical implementation of IoT sensors for collecting environmental and structural data, particularly in smart urban environments. Meanwhile, the green cluster's focus on "sensor nodes," "energy efficiency," and "intelligent buildings" aligns with sustainable infrastructure objectives and shows growing awareness of the need to minimize energy consumption in large-scale monitoring deployments. The blue and yellow clusters represent evolving priorities. The blue cluster is focused on cybersecurity, including keywords such as "network security," "authentication," and "data privacy." As IoT devices become more embedded in critical infrastructure, concerns around

system vulnerabilities and data protection have intensified. Simultaneously, the yellow cluster highlights a shift toward intelligent data processing, with terms like "machine learning," "deep learning," "edge computing," and "artificial intelligence." These terms suggest the increasing integration of AI-based solutions to enhance predictive analytics, anomaly detection, and autonomous decision-making in infrastructure systems.

2. Temporal Evolution and Emerging Trends

The overlay visualization (color-coded by year) provides temporal context to the development of research themes. Early research efforts (darker tones) focused on basic infrastructure elements such as "sensor nodes," "energy utilization," and "data acquisition." These foundational topics formed the technical backbone for deploying IoT devices in the field. As IoT matured and the number of applications grew, recent research (yellow-toned keywords) began to explore more advanced themes such as blockchain integration, data privacy, machine learning, and edge computing. This evolution signifies a shift from implementation and deployment challenges toward enhancing the intelligence and autonomy of IoT systems. For instance, edge computing is gaining traction due to its ability to perform computations closer to the data source, thereby reducing latency and dependence on cloud infrastructure. Similarly, the rise of blockchain in this domain points to efforts in ensuring the integrity, traceability, and security of data transmitted from sensors, particularly in mission-critical infrastructure settings like bridges, pipelines, and power grids. Another notable trend is the increasing emphasis on smart cities as a research theme. The recurring appearance of this keyword in multiple clusters suggests its cross-cutting role in urban infrastructure monitoring, integrating elements of transportation, energy, environment, and public safety. Smart cities act as the testbed and application domain for many IoT innovations, making them central to this field's development.

3. Research Density and Focus Areas

The heatmap visualization further corroborates the centrality of "internet of things" in the research network. Surrounding high-density areas such as "monitoring," "smart city," "network security," and "machine learning" imply sustained attention and high publication output in these subfields. In contrast, peripheral keywords like "air quality," "data visualization," and "block-chain" indicate emerging or underrepresented areas, which may present opportunities for future exploration. These patterns suggest that while the field is rich in technical and architectural studies (e.g., data handling, sensor networks, system optimization), applied research in areas such as environmental impact, public health, and infrastructure resilience is comparatively sparse. This imbalance presents an opportunity for future interdisciplinary studies that link IoT data with policy-making, sustainability assessment, and social outcomes.

4. Author Collaboration Patterns

The co-authorship network reveals strong intra-regional and institutional collaborations, especially among researchers with the surnames Zhang, Wang, Liu, Li, and Chen. These authors form dense and highly interconnected clusters, most likely reflecting research groups based in Chinese institutions. The dominance of these networks suggests that China is a leading contributor to publication output in this field, particularly in the technical domains of IoT and structural health monitoring. In contrast, other author clusters—such as those involving Buyya R., Zeadally S., and Atzori L.—appear less dense but more globally distributed, indicating cross-institutional or international collaborations. These clusters likely represent research activity that bridges technical work with policy, governance, or emerging technologies like blockchain and AI. The structural separation of these clusters implies that while there is strong local collaboration in some regions, broader global integration in terms of co-authorship remains limited. Future efforts could benefit

from initiatives that encourage cross-cluster collaboration, especially between groups focused on system implementation and those working on data ethics, AI integration, and smart governance. Such collaboration would ensure that IoT-based monitoring systems are not only technologically sound but also socially responsible and contextually appropriate.

5. Country Contributions and Global Collaboration

The country co-authorship map confirms that India, China, and the United States are the three most prolific contributors to research on IoT-based infrastructure monitoring. India stands out as the most central and collaborative node, indicating both high productivity and strong engagement with international partners. The prominence of India and China may be driven by their governmental investments in smart infrastructure, urbanization, and digital innovation programs. European countries such as Germany, Italy, Spain, and France form tightly-knit collaborative networks, reflecting strong intra-European cooperation. These collaborations are likely supported by EU-funded initiatives such as Horizon 2020 and regional smart infrastructure programs. Meanwhile, countries like New Zealand, Rwanda, and Somalia appear on the periphery, suggesting that while their contributions are limited in number, they may represent emerging participation or entry points for global inclusion. This geographic mapping suggests that while the field is global in scope, research is concentrated in a few leading countries, with many developing regions underrepresented. Enhancing research capacity in Africa, South America, and Southeast Asia could yield context-specific insights and support the localization of IoT solutions for infrastructure monitoring in diverse environments. It also opens the door to North–South collaboration frameworks that blend technological expertise with on-the-ground infrastructure challenges in underserved areas.

CONCLUSION

This bibliometric review has mapped the intellectual landscape, thematic evolution, and global collaboration patterns in the field of infrastructure monitoring using IoT. The findings reveal that research in this domain is growing rapidly, with central themes focused on real-time monitoring, sensor integration, intelligent data processing, and cybersecurity. Over time, the field has shifted from foundational sensor technologies toward advanced topics such as machine learning, edge computing, and blockchain, reflecting increasing complexity and maturity. Key contributors—both individual researchers and countries like India, China, and the United States—have played significant roles in shaping the field's development. The analysis also highlights emerging areas and underexplored topics, offering opportunities for future research. Overall, this study underscores the multidisciplinary and global nature of IoT-based infrastructure monitoring and provides a valuable foundation for guiding future investigations and fostering international collaboration.

REFERENCES

[1] Z. Lv, B. Hu, and H. Lv, "Infrastructure monitoring and operation for smart cities based on IoT system," *IEEE Trans. Ind. Informatics*, vol. 16, no. 3, pp. 1957–1962, 2019.

[2] 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.

[3] S. Jeong and K. Law, "An IoT platform for civil infrastructure monitoring," in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, IEEE, 2018, pp. 746–754.

[4] M. K. J. Ramphela, P. A. Owolawi, T. Mapayi, and G. Aiyetoro, "Internet of things (IoT) integrated data center infrastructure monitoring system," in *2020 international conference on artificial intelligence, big data, computing and data communication systems (icABCD)*, IEEE, 2020, pp. 1–6.

[5] G. Lu and Y. J. Yang, "IoT and smart infrastructure," *Internet Things Data Anal. Handb.*, pp. 481–493, 2017.

[6] E. Bertino, M. R. Jahanshahi, A. Singla, and R.-T. Wu, "Intelligent IoT systems for civil infrastructure health

monitoring: a research roadmap," *Discov. Internet Things*, vol. 1, pp. 1–11, 2021.

[7] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W. M. Lim, "How to conduct a bibliometric analysis: An overview and guidelines," *J. Bus. Res.*, vol. 133, pp. 285–296, 2021.

[8] H. Gupta, A. Vahid Dastjerdi, S. K. Ghosh, and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments," *Softw. Pract. Exp.*, vol. 47, no. 9, pp. 1275–1296, 2017.

[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] L. Catarinucci *et al.*, "An IoT-aware architecture for smart healthcare systems," *IEEE internet things J.*, vol. 2, no. 6, pp. 515–526, 2015.

[11] 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.

[12] 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.

[13] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring," *Comput. Networks*, vol. 101, pp. 192–202, 2016.

[14] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," *J. Netw. Comput. Appl.*, vol. 67, pp. 99–117, 2016.

[15] J. Ni, K. Zhang, X. Lin, and X. Shen, "Securing fog computing for internet of things applications: Challenges and solutions," *IEEE Commun. Surv. Tutorials*, vol. 20, no. 1, pp. 601–628, 2017.

[16] 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.

[17] A. Dohr, R. Modre-Opsrian, M. Drobics, D. Hayn, and G. Schreier, "The internet of things for ambient assisted living," in *2010 seventh international conference on information technology: new generations*, Ieee, 2010, pp. 804–809.