West Science Information System and Technology
Vol. 4, No. 02, August 2026, pp. 245~257

Internet of Things Infrastructure Research Mapping

Loso Judijanto
IPOSS Jakarta, Indonesia

Article Info

Article history:

Received Aug, 2026
Revised Aug, 2026
Accepted Aug, 2026

Keywords:

Internet of Things
IoT Infrastructure
Bibliometric Analysis
Research Mapping
Edge Computing
Cybersecurity

ABSTRACT

The fast pace of developing the concept of digital transformation made the Internet of Things infrastructure a crucial basis for connected systems, intelligent applications, and sustainable technological ecosystems. The purpose of this study is to conduct a bibliometric analysis and identify the patterns of development, intellectual structure, collaboration, and current research trends in the IoT infrastructure. Scientific publications related to the topic were gathered and analyzed using the software VOSviewer in order to investigate citation performance, co-authorship network, collaborations between institutions and countries, co-occurrence of keywords, thematic dynamics, and patterns of research density. It was found out that there has been a considerable increase in the amount of IoT infrastructure research, with cybersecurity, secure communication, edge computing, fog computing, smart cities, and intelligent infrastructure being identified as leading research topics. Citation analysis suggests that papers dedicated to IoT security framework, intrusion detection system, critical infrastructure protection, and distributed computing architecture have had a significant impact on this field. Collaboration analysis has indicated the presence of strong international research networks with China, India, USA, Germany, and the UK being recognized as the key contributors. Finally, it has been found out that the research has evolved from addressing connectivity challenges to advanced research which includes artificial intelligence, machine learning, privacy protection, energy efficiency, and autonomous IoT systems.

Corresponding Author:

Name: Loso Judijanto
Institution: IPOSS Jakarta, Indonesia
Email: losojudijantobumn@gmail.com

1. INTRODUCTION

With the swift development of digital technologies, new forms of interaction between people, businesses, and the government with physical spaces have been created. Among these technologies, IoT is one of the paradigms that gained high influence due to providing means for communication between physical items, sensors, computational systems, and digital technologies through interconnected networks. IoT provides an opportunity for embedded devices to exchange data and process it via communication and sensing capabilities, which contributes to automation and intelligent decision making in many areas, such as healthcare, industry, agriculture, transportation, smart cities and industry [1], [2]. The development of IoT is tightly connected with the process of digital transformation, when the organization creates connected infrastructure and uses it for developing data-driven systems and services. Thus, the IoT infrastructure is becoming one of the crucial areas for research as the success, scalability, and sustainability of the IoT applications highly depend on technological infrastructure [3], [4].

The IoT infrastructure development encompasses several connected layers, which include sensors, communication networks, cloud and edge computing platforms, database systems, cybersecurity and data privacy measures, and applications. While the design and operation of traditional information systems are simpler than that of IoT, the latter require constant interaction between heterogeneous devices that operate using various protocols and under varying computational and operating conditions. All these factors cause a number of difficulties associated with the issues of interoperability, scalability, energy consumption, latency reduction, data privacy, and cybersecurity [5], [6]. Moreover, due to the rapid increase in the number of connected devices, there has emerged a need for more sophisticated infrastructure models, which can provide support for huge numbers of devices as well as for the real-time data processing. The new trends in the area of infrastructure development, such as edge computing, fog computing, 5G communication networks, and the use of AI, have made even greater expansion of the research area due to the movement of computations towards data sources [7].

During the last decade, there has been significant progress in the area of IoT infrastructure research and industrialization. Several studies have explored a variety of issues related to IoT infrastructure, among which include network architecture, communication protocols, cloud computing in IoT, IoT security framework, resources management in IoT, and intelligent IoT data analysis. Early research was mainly concerned with definition of IoT terminology and establishment of IoT architectures, whereas the latest studies have been dedicated to infrastructure optimization, autonomous systems and integration with novel technologies like artificial intelligence, blockchain, digital twins, and machine learning [8], [9]. These changes show that research in the area of IoT infrastructure evolves and reflects advances and needs of modern society. Nevertheless, the increase in the number of articles leads to knowledge fragmentation since different research areas, methods, applications and technologies are covered in literature. Thus, it becomes hard to understand the evolution and research trends of the field.

In the case of growing numbers and diversity of publications on IoT infrastructure, it is necessary to implement systematic approaches to researching development of the sphere. Although traditional literature review offers a valuable theoretical approach, it might face certain drawbacks when it comes to recognizing large-scale publication patterns, identifying important studies, collaboration networks, emerging topics, and structures of knowledge. The research mapping approach including bibliometric analysis and science mapping is one of such methods for evaluating the evolution of scientific knowledge through analyzing publication trends, citation patterns, keyword relations, and author/collaborative relationships [10]. This method is widely used in technology researches to discover dominant topics, research gaps, and opportunities for future studies. In the case of IoT infrastructure, research mapping might give an idea about its development, technological areas attracting considerable attention, and emerging topics.

While significant advances have been made in the development of IoT literature, there is a lack of studies that focus on the development of research on IoT infrastructure in a comprehensive way. In fact, some reviews have investigated issues related to IoT security, IoT communication technologies, IoT applications, or IoT architecture; yet a review that encompasses the entire intellectual structure of IoT infrastructure has not been developed. It is crucial to conduct such a study to identify research clusters, key papers, conceptual relationships, and future research topics. This is especially important because IoT infrastructure is evolving due to the advent of new computing paradigms such as edge intelligence, decentralized paradigm, sustainable IoT, and next generation communication.

While the field of IoT infrastructure has developed into a very fast-growing research domain, the literature that has been accumulated in this area so far has proven to be quite scattered in nature. Due to the lack of an appropriate research mapping methodology, there are certain problems associated with gaining an understanding of the entire development process, finding out the main topics that were covered in the literature, pinpointing influential papers, and highlighting the areas that should be further explored. In the past, previous studies have paid attention to some parts of IoT infrastructure, which implies limited knowledge about the overall scientific context.

This research intends to undertake a systematic research map regarding the development of IoT infrastructure through studying scientific papers on IoT infrastructure development. More specifically, the purpose of this research is to identify patterns in publications, influential authors and papers, important themes of research, collaboration among authors and new trends in the field. Through undertaking a systematic research map, this paper intends to give an account of the intellectual evolution of IoT infrastructure research and the way forward for future research.

2. METHODS

The present study uses a bibliometric research methodology to systematically analyze the growth, structure, and trends in research related to IoT infrastructure. The bibliometric research methodology is chosen for the present study as it offers an objective quantitative method to assess scientific works using statistical and network analysis methodologies. Through such methods, researchers can determine publication patterns, influential works, research clusters, and evolution of knowledge in a particular field of science [10]. As opposed to qualitative analysis of literature review articles, bibliometric research methodology helps in carrying out a thorough analysis of vast amounts of academic literature through citations, co-word analysis, collaboration among authors, and institutional affiliations of works. It is appropriate to use this methodology in the field of IoT infrastructure research as the field has rapidly expanded into various academic disciplines, leading to fragmentation of knowledge.

The data collection procedure was performed according to the systematic search approach by employing the Scopus database as the main source of scientific publications. The reason why Scopus was chosen is that it covers peer-reviewed journals and conferences on the topics of engineering, computer science, information systems, and emerging technologies. The process of search entailed identifying the scientific documents associated with the concept of IoT infrastructure through the application of specific keywords such as "Internet of Things," "IoT infrastructure," "IoT architecture," "IoT network," "IoT platform," and "connected devices." The documents were analyzed based on the pre-established inclusion/exclusion criteria, such as the topic relevance, document type, language, and others. Only those documents which addressed the topic of IoT infrastructure were included in the final sample. The bibliographic data, such as the publication year, authors, affiliations, keywords, citations, and references, were further exported for the analysis purposes.

Bibliometric mapping methods were employed at the analysis stage to trace out the development and structure of IoT infrastructure research. Visualization and network analysis methods like VOSviewer were employed to develop scientific maps on the basis of relationships between co-authors, citations, bibliographic coupling, and co-occurrences of keywords. Publication trend analysis was conducted to trace the development patterns of researches, whereas citation analysis was done to find out influential works and scientific contributions. Keyword co-occurrence analysis was conducted to find out research themes dominating in the literature and emerging research areas associated with IoT infrastructure. Cluster analysis was also performed to classify related research areas and to develop the conceptual structure of the subject under consideration. This study offers an insight into the development of research on IoT infrastructure from the bibliometric point of view.

3. RESULTS AND DISCUSSION

3.1 Co-Authorship Analysis

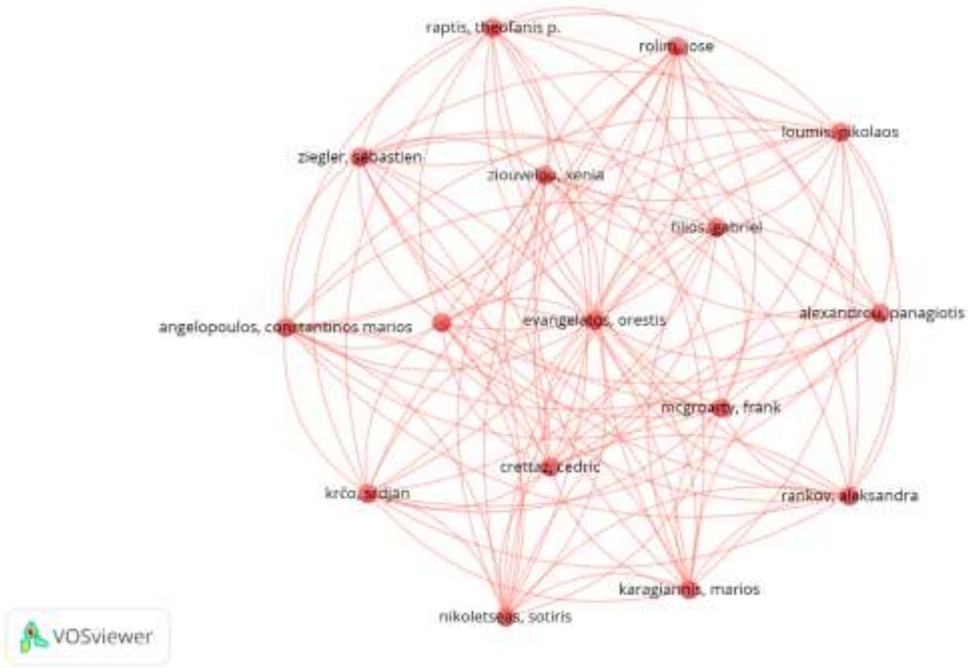

Figure 1. Author-Level Visualization
Source: Data Analysis

Figure 1 shows the collaboration among the top productive authors in the field of Internet of Things (IoT) Infrastructure research. As can be seen from the network, there is only one dominant cluster made up of red colored nodes, showing that the authors in this group are highly interconnected in terms of joint publications. Big nodes show highly productive or influential authors in the selected dataset, and the linking edges show the level of collaboration between these authors. Researchers such as Theofanis P. Raptis, Nikolaos Loumis, Sebastian Ziegler, Orestis Evangelatos, and Gabriel Filios appear to be central researchers due to their connectivity with other researchers in the research, and this indicates their crucial role in shaping the IoT infrastructure body of knowledge. The highly interconnected network suggests that the research field is collaborative in nature, where knowledge creation is largely based on researcher collaboration. It is because IoT infrastructure research involves different fields including communication networks, embedded systems, cybersecurity, edge computing, and smart applications.

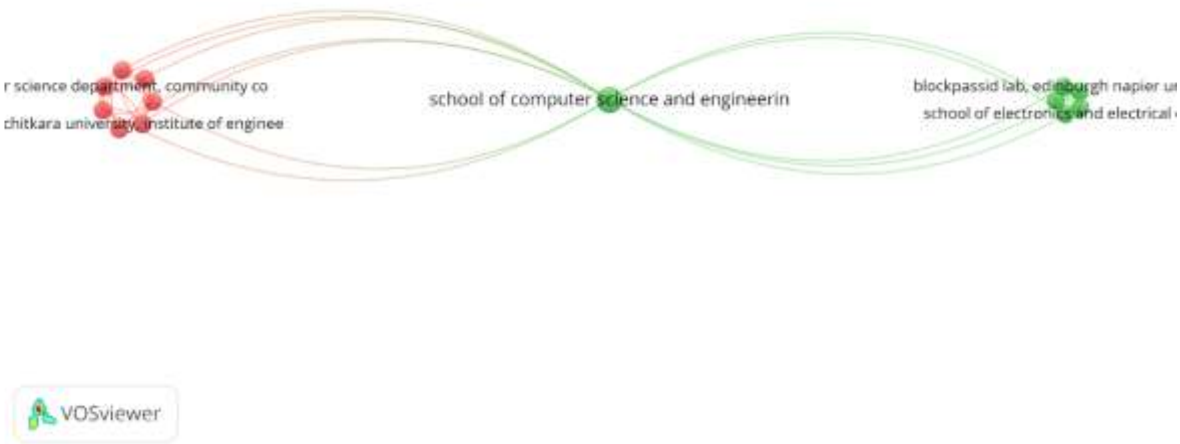

Figure 2. Institution-Level Visualization
Source: Data Analysis

Figure 2 represents the institutional interactions involved in the IoT infrastructure research. The graph shows the existence of several institutional groups that collaborate through joint papers, whereby nodes show institutions while links show collaborations between organizations. The institutional network is relatively sparse compared with author collaboration networks, which implies that institutional collaboration is focused among few research institutions. The School of Computer Science and Engineering comes out as an important institution that acts as a link between various institutional communities. Such position of the institution indicates the importance of this institution in the knowledge transfer and collaborative research processes. The interaction between institutions such as Chitkara University Institute of Engineering, computer science institutions, and Blockpass ID Lab and School of Electronics and Electrical Engineering at Edinburgh Napier University represents international collaboration and interdisciplinary collaboration among the institutions in IoT infrastructure studies. The above collaboration pattern represents the fact that IoT infrastructure research involves cooperation among computer science, engineering, and emerging technology laboratories, which shows the multi-disciplinary nature of IoT development, including networking, hardware systems, cybersecurity, and digital platforms.

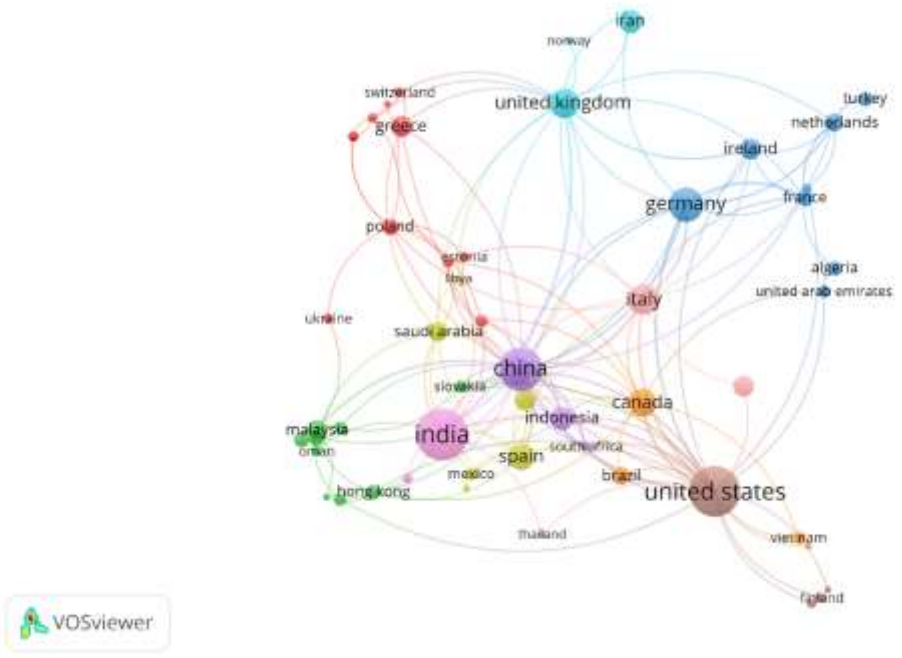

Figure 3. Country-Level Visualization
Source: Data Analysis

As shown in Figure 3, there are many examples of research cooperation on IoT infrastructure globally. The network shows that IoT infrastructure research is characterized by significant international collaboration with some countries being major contributors and collaboration centers. The size of the node reflects the research contribution or publications made. Connecting lines reflect the degree of collaboration between countries. Countries like China, India, the US, Germany, and the UK come out as the major countries since they have large nodes and many connections with other countries. Research conducted in China and India is high in terms of research collaboration with Asian, European, and North American countries, and they are playing an increasingly important role in IoT technology research. On the other hand, the US serves as the main international collaboration center for researchers from different parts of the world including Europe, Asia, and IoT researchers. Furthermore, the structure of the network provides some regional collaborative groups. European countries like Germany, the UK, France, Italy, and the Netherlands possess highly interconnected relations, suggesting the existence of regional research collaboration in IoT infrastructure, communication, and digital transformation. Countries from Asia such as China, India, Indonesia, Malaysia, and Hong Kong also represent a collaborative group, proving that the IoT research is developing fast in digital economies. Countries like Brazil, Saudi Arabia, South Africa, and Vietnam suggest that research in IoT infrastructure is becoming a global topic.

3.2 Citation Analysis

Table 1. The Most Impactful Literatures

Citations	Authors and year	Title
175	[11]	Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure
158	[12]	Intrusion Detection System to Advance Internet of Things Infrastructure-Based Deep Learning Algorithms

Citations	Authors and year	Title
136	[13]	Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities
115	[14]	Softwarization of internet of things infrastructure for secure and smart healthcare
107	[15]	Indie Fog: An Efficient Fog-Computing Infrastructure for the Internet of Things
100	[16]	Practical Lessons from the Deployment and Management of a Smart City Internet-of-Things Infrastructure: The SmartSantander Testbed Case
98	[17]	Early infrastructure of an Internet of things in spaces for learning
97	[18]	A programmable and virtualized network & IT infrastructure for the internet of things: How can NFV & SDN help for facing the upcoming challenges
95	[19]	PKI4IoT: Towards public key infrastructure for the Internet of Things
82	[20]	Recent advances in internet of things (IoT) infrastructures for building energy systems: A review

Source: Scopus, 2026

Table 1 provides the most influential studies in IoT infrastructure development in terms of citation counts. It includes the leading studies which have contributed to the formation of this research field in particular. The leading cited study is [11] with 175 citation counts. This study focuses on emerging cybersecurity concerns with IoT infrastructures as the study shows that security issues have become a major consideration in the use of IoT. In a similar way, [12] and [13] received a lot of citation counts as their work contributed to intrusion detection systems, deep learning approaches to security, and IoT infrastructures.

Furthermore, highly cited studies also reveal the evolution of IoT infrastructure from basic connectivity frameworks toward intelligent, scalable, and application-oriented ecosystems. Research by [14] and [15] highlights the importance of software-defined infrastructure, fog computing, and distributed architectures in supporting secure healthcare and efficient IoT services. Meanwhile, studies such as [16] and [17] demonstrate practical implementations of IoT infrastructure through smart city platforms and educational environments, reflecting the transition from conceptual frameworks to real-world deployment. Recent contributions, including [19]on public key infrastructure and [20] on IoT applications in building energy systems, further show the growing integration of security, sustainability, and intelligent management into IoT ecosystems.

3.3 Keyword Co-Occurrence Analysis

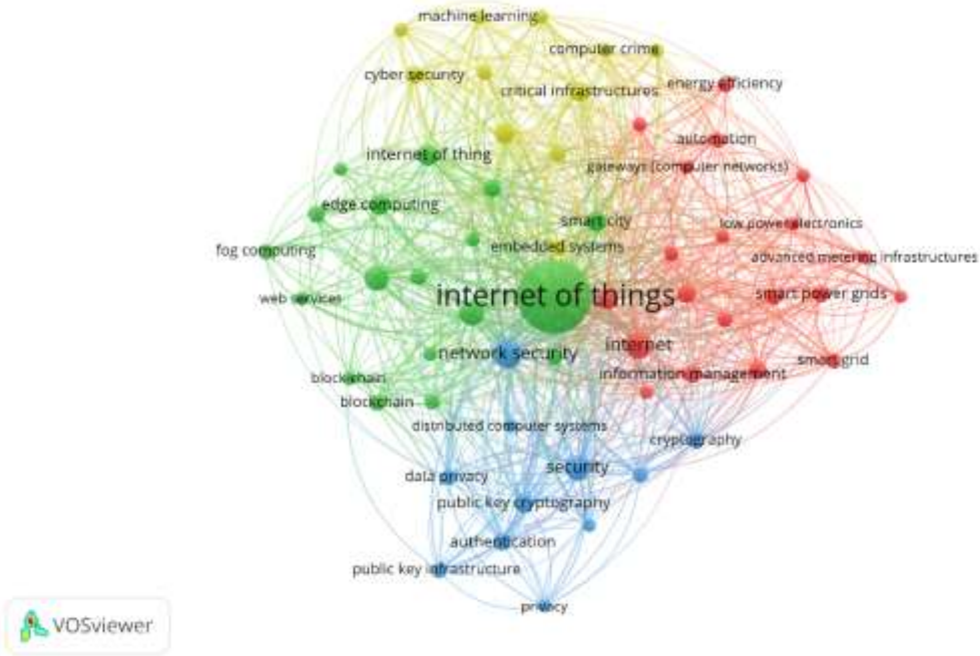

Figure 4. Network Visualization
Source: Data Analysis

Fig. 4 shows the conceptual framework and prominent themes in research on Internet of Things (IoT) infrastructure research. This network highlights the connections between frequently used keywords, where the size of the node denotes frequency of keyword use, while the link denotes the connection between keywords, and the color denotes thematic cluster. "Internet of things" is highlighted as the largest node in the network, which suggests its prominence in IoT infrastructure research as the core theme. Its numerous connections with other terms denote that the study of IoT infrastructure research is multidisciplinary.

The green cluster is associated with studies that deal with the IoT architecture, connectivity, and distributed computing infrastructure. Such keywords as edge computing, fog computing, embedded systems, web services, blockchain, and network security clearly point out a high level of research concerning the construction of efficient and scalable IoT ecosystems. This cluster is connected with the technological background that can be used for the development of large IoT ecosystems based on decentralized computing models, like edge computing and fog computing. The use of keywords connected with blockchain also shows an increasing trend.

The blue cluster emphasizes the significance of security, privacy, and authentication in the framework of IoT networks. Words such as security, cryptography, PKI, authentication, data privacy, and public key cryptography show that security measures for IoT networks and information systems have become the focal point of much research. Since IoT generates and transfers huge amounts of confidential data, it is becoming important for researchers to study security models that will guarantee privacy, integrity, and communication.

The cluster in red includes the literature on smart infrastructure applications and energy-focused IoT infrastructure applications. Key words like smart grid, smart power grids, advanced metering infrastructures, smart city, low power electronics, automation, and energy efficiency show the use of IoT technology for developing better urban and energy management practices. This cluster depicts the fact that IoT infrastructure research has come out of the domain of mere connectivity to more concrete implementation for sustainable development, intelligent energy distribution, and automation. The linkage between IoT and smart city concepts highlights the growing importance of IoT as an enabler of digital transformation in urban environments.

The yellow cluster reflects emerging integration between artificial intelligence, cybersecurity, and critical infrastructure management. Keywords such as machine learning, cyber security, computer crime, critical infrastructures, and energy efficiency indicate the growing adoption of intelligent approaches to enhance IoT performance and resilience. Machine learning techniques are increasingly explored for anomaly detection, predictive analysis, and automated decision-making in IoT environments.

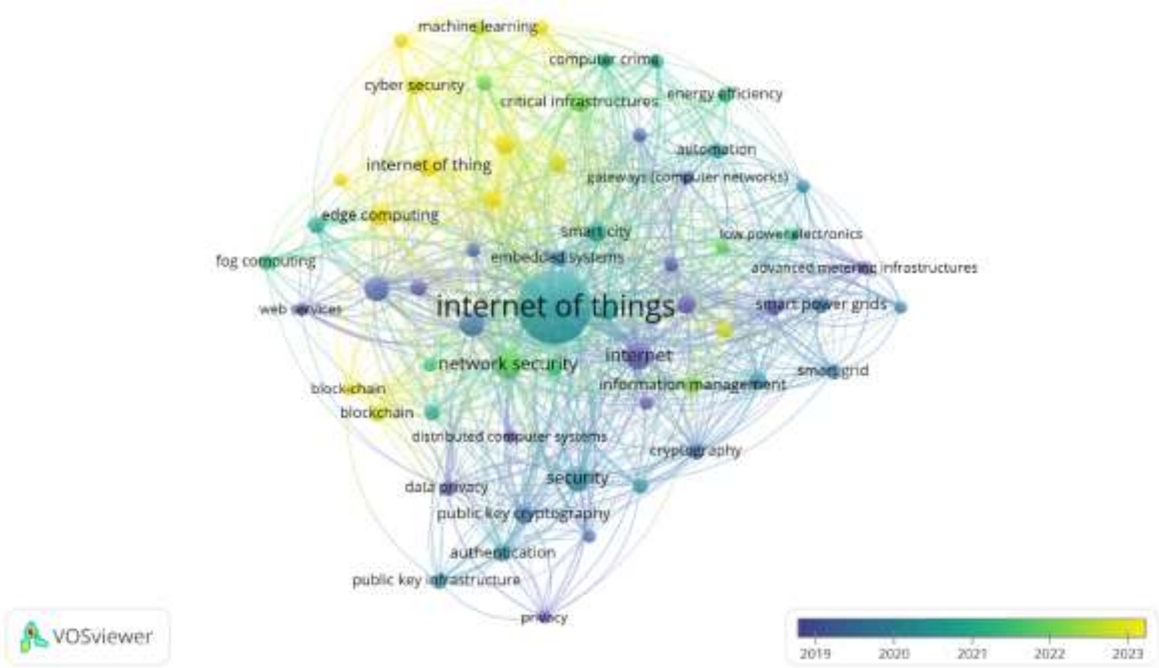

Figure 5. Overlay Visualization
Source: Data Analysis

Figure 5 demonstrates how the development of IoT infrastructure research has progressed over time from 2019 until 2023 depending on the distribution of key words. The color scale reflects the average publication year of key words; hence, dark blue means that the word attracted research attention at an earlier date, while green and yellow colors denote relatively new and emerging themes. Among all the words used, "internet of things" has been the most important one and has strong links with other research fields such as computing architecture, security, communications, and smart applications.

The trends identified from the previous researches, depicted in blue and purple colors, have been concerned mostly with infrastructure and security aspects. The use of keywords like security, cryptography, public key infrastructure, authentication, data privacy, and distributed computer systems signifies that initial researches were centered on the creation of secure and dependable IoT ecosystems. The researches tackled important issues in relation to data security, network vulnerability, and secure communications between connected devices. In addition, topics like network security and information management reflect the significance of creating efficient means for supporting the IoT ecosystem.

The most recent research directions denoted in green and yellow colors emphasize how there has been a move towards intelligent, adaptive, and application-based IoT frameworks. The areas of research like machine learning, cyber security, edge computing, smart city, energy efficiency, and critical infrastructures suggest an increased convergence of IoT with computational technology. An increased emphasis on machine learning and edge computing demonstrates the move from traditional connected systems to intelligent IoT systems that can make autonomous decisions.

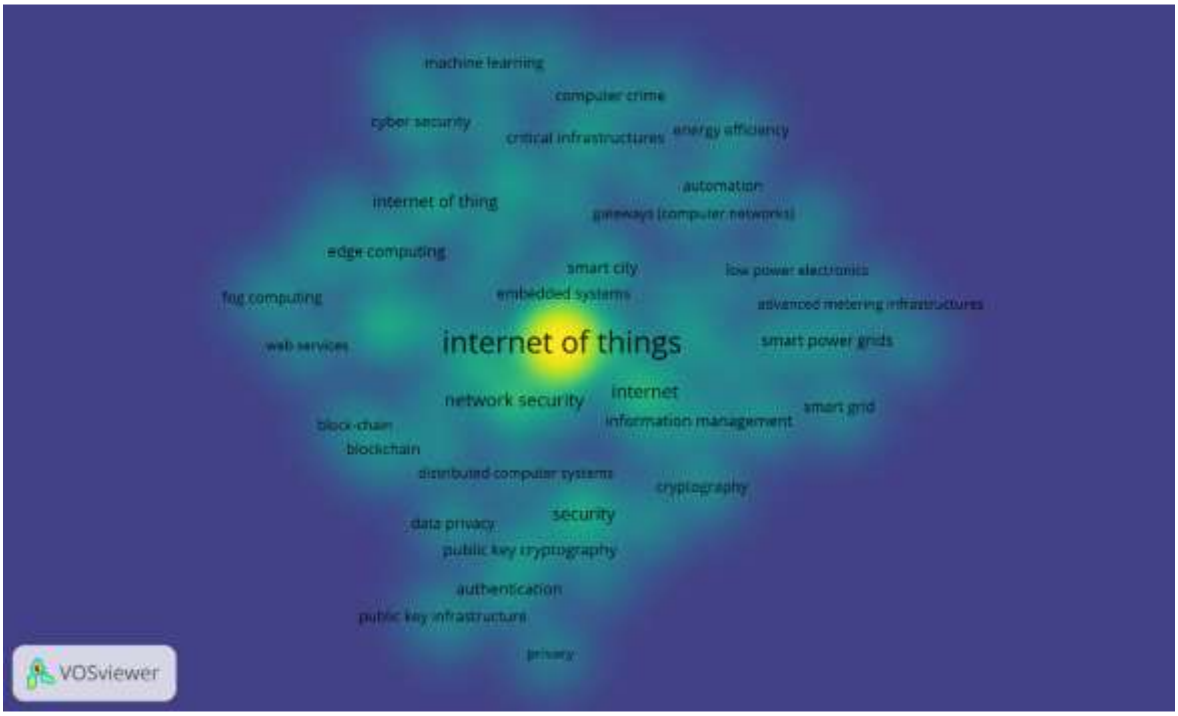

Figure 6. Density Visualization
Source: Data Analysis

Figure 6 shows the density and importance of topics in Internet of Things (IoT) infrastructure research studies. The bright color intensity of the figure shows the number of occurrences and importance of keywords, where the more colorful region shows the topic with higher density of research, and the less colorful region denotes lower density of research. The keyword "internet of things" can be seen to be the most dominating and dense topic located at the center of the diagram. The dense nature of the keyword shows that IoT forms the basic foundation of research for different technologies like networking, computing, security, and smart applications.

Some important theme clusters that the visualization shows include: Theme clusters that are located near high-frequency words like "edge computing", "network security", "security", "smart city", "smart grid" and "information management" suggest that these themes are some of the main concerns among the researchers in the IoT field. On the other hand, some of the new emerging themes include "machine learning", "cyber security", "critical infrastructures" and "energy efficiency". Thematic clusters involving the themes "cryptography", "authentication", "public key infrastructure" and "data privacy" continue to be some of the important secondary themes in the study.

Discussion

The results of this research offer a holistic view of the evolution and direction of the intellectual growth of the research domain of Internet of Things (IoT) infrastructure in relation to its bibliometric mapping. The bibliographic patterns reveal that the IoT infrastructure has become a fast-growing research field due to the ever-increasing demand for connections, digitalization, and intelligence. The top-cited sources show that the major issues in both the early and current research have always been related to the solution of the basic problems arising during the IoT deployment, including such aspects as cybersecurity, network stability, scalability, and management of the infrastructure. Top-cited literature dedicated to the development of secure IoT architecture, intrusion detection, fog computing, and smart infrastructure proves that the further development of IoT ecosystems depends on much more than just connectivity and involves secure, efficient, and sustainable operations. The findings prove that IoT infrastructure research has gone beyond the development of connections and is now aimed at the creation of technological ecosystems.

Collaboration analysis shows that research into IoT infrastructure is associated with high levels of international and interdisciplinary collaboration. Author collaboration analysis is used to show the presence of highly influential research communities making significant contributions to the field of IoT knowledge development. The country collaboration analysis helps in recognizing the important role played by countries like China, India, the USA, Germany, and the UK. These countries play a very significant role because IoT technologies have a strategic importance in various regions and economic sectors of the world. The participation of institutions from computer science, engineering, telecommunication, and technology laboratories means that multidisciplinary collaboration is necessary for the development of IoT infrastructure. Nevertheless, the fairly limited patterns of institutional collaboration mean that research collaboration is mainly done by technologically advanced institutions.

Through the analysis of co-occurrence and thematic evolution, several key research clusters are identified as the main directions of studies in IoT infrastructure. The first of them is concerned with computational and network infrastructure and includes edge computing, fog computing, embedded systems, and distributed computing systems. Such technologies can be considered crucial solutions to solve the problems related to latency and scalability issues as well as the challenges of processing because of the increasing number of connections. The second key research cluster is related to the issues of security and privacy; it is supported by the high correlation between IoT infrastructure and such keywords as cryptography, authentication, public key infrastructure, and data privacy. The reason for its importance is the increase of cyber threats associated with interconnected systems. The third cluster is associated with smart applications and sustainable infrastructure and includes such topics as smart city, smart grid, energy efficiency, and automation.

In addition, the temporal analysis along with the density analysis supports the shift of IoT infrastructure research from basic connectivity technology towards intelligent, secure, and adaptive ecosystem infrastructure. Recent trends in research reveal the integration of IoT with technologies such as machine learning, artificial intelligence, edge computing, and cybersecurity techniques. This implies that the future of IoT infrastructure will be towards developing self-decision making capabilities, real-time processing capabilities, energy efficient systems, and robust security infrastructures. The findings presented in the paper will add value to the literature on IoT infrastructure by presenting an organized framework of the developments, key themes, and future directions in IoT infrastructure research. Future research may explore the integration of IoT with technologies such as artificial intelligence, digital twins, sustainable technologies, and 5G and 6G communication networks.

4. CONCLUSION

The current research contributes to bibliometric mapping of the research on Internet of Things (IoT) infrastructure through exploring trends in publications, influential literature, cooperation networks, and research topics of this field. Results obtained show that IoT infrastructure has become an interdisciplinary research area that comprises computer science, engineering, cybersecurity, communication technologies, and smart applications. It is also shown that the research on IoT infrastructure is influenced by cybersecurity, infrastructure development, fog and edge computing, and smart systems. Collaboration analysis shows that the IoT infrastructure is characterized by considerable international cooperation with significant involvement of countries and institutions from Asia, Europe, and North America in this process. Keyword analysis allows us to conclude that the theme of IoT research has changed from connectivity and network establishment to more complex research problems like artificial intelligence, machine learning, privacy protection, energy efficiency, and intelligent infrastructure management. Such results give us an understanding of the intellectual structure and development of IoT infrastructure. In the future, it will be interesting to investigate how the IoT can be combined with such emerging technologies as artificial intelligence, digital twins, sustainable computing, and next-generation communication networks.

REFERENCES

[1] S. K. Gupta, N. Kohli, K. Bedi, P. K. Angra, P. Singh, and A. Sharma, "AI, IoT, and Cybersecurity in Last-Mile Delivery Systems: A Systematic Review and Conceptual Framework," in *2026 International Conference on Smart Multidomain Integrated Learning Environments, ICSMILE 2026*, Lincoln University College, Selangor, Petaling Jaya, Malaysia: Institute of Electrical and Electronics Engineers Inc., 2026. doi: 10.1109/ICSMILE69273.2026.11519312.

[2] R. Vijayalakskmi *et al.*, "ASIC-Based AI Accelerator with Quantum-Inspired Optimization for Blockchain Validation and Fraud Detection," in *International Conference on AI-Driven Innovations and Applications, IC-AIDA 2026 - Conference Proceedings*, Anna University, Rajalakshmi Institute of Technology, Department of Computer Science and Business System, Chennai, India: Institute of Electrical and Electronics Engineers Inc., 2026. doi: 10.1109/IC-AIDA68291.2026.11564453.

[3] A. Al Hadwer, M. Tavana, D. Gillis, and D. Rezania, "A Systematic Review of Organizational Factors Impacting Cloud-based Technology Adoption Using Technology-Organization-Environment Framework," *Internet of Things (Netherlands)*, vol. 15, 2021, doi: 10.1016/j.iot.2021.100407.

[4] G. Naeem, M. Asif, and M. Khalid, "Industry 4.0 digital technologies for the advancement of renewable energy: Functions, applications, potential and challenges," *Energy Convers. Manag. X*, vol. 24, 2024, doi: 10.1016/j.ecmx.2024.100779.

[5] N. Kefalakis, A. Roukounaki, and J. Soldatos, "A configurable distributed data analytics infrastructure for the industrial internet of things," in *Proceedings - 15th Annual International Conference on Distributed Computing in Sensor Systems, DCOSS 2019*, IoT Group, Athens Information Technology, Marousi, Greece: Institute of Electrical and Electronics Engineers Inc., 2019, pp. 179–181. doi: 10.1109/DCOSS.2019.00048.

[6] Z. Grider and A. H. Nelson, "Solid-if-IoT: An Internet of Things Client Bridge to Interface with Solid Backend Infrastructure," in *IEEE Green Technologies Conference*, University of Arkansas, Electrical Engineering and Computer Science, Fayetteville, United States: IEEE Computer Society, 2024, pp. 227–231. doi: 10.1109/GreenTech58819.2024.10520357.

[7] I. Keshi, R. Daimon, Y. Takaoka, and A. Hayashi, "Integrated Evaluation of Semantic Representation Learning, BERT, and Generative AI for Disease Name Estimation Based on Chief Complaints," in *International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management, IC3K - Proceedings*, C. F., F. A., and B. J., Eds., AI & IoT Center, Fukui University of Technology, 3-6-1, Gakuen, Fukui, Japan: Science and Technology Publications, Lda, 2024, pp. 294–301. doi: 10.5220/0012927100003838.

[8] B. M. Kavya *et al.*, "An Efficient Machine Learning-Based Power Management System for Smart Grids Using Renewable Energy Resources," in *2nd IEEE International Conference on Networks, Multimedia and Information Technology, NMITCON 2024*, Ks Institute of Technology, Dept of Electronics and Communication Engineering, Bengaluru, India: Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/NMITCON62075.2024.10698819.

[9] M. Nayak, P. Patro, J. B. Awotunde, and S. K. Gupta, "IoT Security Architectures and Protocols," *Security Paradigms in 6G Smart Cities and IoT Ecosystems: Navigating the Future*. CRC Press, Department of

Computer Science and Engineering, NIST University, Odisha, Berhampur, India, pp. 52–71, 2025. doi: 10.1201/9781003564645-6.

[10] 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.

[11] A. Djenna, S. Harous, and D. E. Saidouni, "Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure," *Appl. Sci.*, vol. 11, no. 10, 2021, doi: 10.3390/app11104580.

[12] H. Alkahtani and T. H. H. Aldhyani, "Intrusion Detection System to Advance Internet of Things Infrastructure-Based Deep Learning Algorithms," *Complexity*, vol. 2021, 2021, doi: 10.1155/2021/5579851.

[13] X. Liu, C. Qian, W. G. Hatcher, H. Xu, W. Liao, and W. Yu, "Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities," *IEEE Access*, vol. 7, pp. 79523–79544, 2019, doi: 10.1109/ACCESS.2019.2920763.

[14] M. A. Salahuddin, A. Al-Fuqaha, M. Guizani, K. Shuaib, and F. Sallabi, "Softwarization of internet of things infrastructure for secure and smart healthcare," *Computer (Long. Beach. Calif).*, vol. 50, no. 7, pp. 74–79, 2017, doi: 10.1109/MC.2017.195.

[15] C. Chang, S. N. Srirama, and R. Buyya, "Indie Fog: An Efficient Fog-Computing Infrastructure for the Internet of Things," *Computer (Long. Beach. Calif).*, vol. 50, no. 9, pp. 92–98, 2017, doi: 10.1109/MC.2017.3571049.

[16] P. Sotres, J. R. Santana, L. Sanchez, J. Lanza, and L. Munoz, "Practical Lessons from the Deployment and Management of a Smart City Internet-of-Things Infrastructure: The SmartSantander Testbed Case," *IEEE Access*, vol. 5, pp. 14309–14322, 2017, doi: 10.1109/ACCESS.2017.2723659.

[17] G. R. González, M. M. Organero, and C. D. Kloos, "Early infrastructure of an Internet of things in spaces for learning," in *Proceedings - The 8th IEEE International Conference on Advanced Learning Technologies, ICALT 2008*, Carlos III University of Madrid, Leganes Campus, Madrid, Spain, 2008, pp. 381–383. doi: 10.1109/ICALT.2008.210.

[18] N. Omnes, M. Bouillon, G. Fromentoux, and O. Le Grand, "A programmable and virtualized network & IT infrastructure for the internet of things: How can NFV & SDN help for facing the upcoming challenges," in *2015 18th International Conference on Intelligence in Next Generation Networks, ICIN 2015*, Orange Labs IMT/OLN/CNC/NCA, Lannion, 22300, France: Institute of Electrical and Electronics Engineers Inc., 2015, pp. 64–69. doi: 10.1109/ICIN.2015.7073808.

[19] J. Höglund, S. Lindemer, M. Furuhed, and S. Raza, "PKI4IoT: Towards public key infrastructure for the Internet of Things," *Comput. Secur.*, vol. 89, 2020, doi: 10.1016/j.cose.2019.101658.

[20] W. Yaïci, K. Krishnamurthy, E. Entchev, and M. Longo, "Recent advances in internet of things (IoT) infrastructures for building energy systems: A review," *Sensors*, vol. 21, no. 6, pp. 1–40, 2021, doi: 10.3390/s21062152.