Google Scholar Crossref doi scopus

Impact factor 6.2

Geoscience Journal

ISSN:1000-8527

Indexing:

- Scopus
- Google Scholar
- DOI, Zenodo
- Open Access

www.geoscience.ac

Registered

INTEGRATING INTERNET OF THINGS SOLUTIONS INTO RESEARCH INFORMATION SYSTEMS

Kumutha D[1], R. Dhivya [2], P. Latha [3], P. Geetha [4], Renuka.B. Jiddagi[5], Swetha.C. S[6]

[1]Department of ECE, AMC Engineering College, Bangalore, India-*600 119*
[2]Department of ECE, Adhiparasakthi College of Engineering
[3]Department of IT, Panimalar Engineering College, Chennai, India
[4]Department of Electronics and Communication Engineering, Sathyabama Insitute of Science and Technology, Chennai, Tamil Nadu, India
Department of ECE, Global Academy of Technology, Bangalore, India-560098
[6] Department of MCA, Bangalore Institute of Technology, Bangalore, India-560004

Abstract: The network of research collaborations within a certain academic topic is mapped using bibliometric analysis in this study, which identifies important contributors and the structure of their links. Through data analysis from reputable academic databases, the study visualizes author clusters and evaluates their impact using metrics related to publications and citations. The results highlight key authors and possible areas of cooperation while providing strategic insights into the primary research communities. There is discussion of the practical consequences for academic highlighting how these organizations may use the analysis to improve research output and innovation through financing methods, research networks, and institutions. The study's concentration on quantitative metrics, which might not adequately reflect the dynamic and qualitative components of human contributions, and possible database biases are among its limitations. Not withstanding these difficulties, bibliometric analysis offers insightful advice for academic and research communities' strategic decision-making.

Keywords: Information System, Internet of Things (IoT), Bibliometric Analysis VOSviewer

1. INTRODUCTION

The privacy and safety of IoT have become a critical concern in today's world. As Internet of Things (IoT) gadgets more frequently occurring in our residences, organizations, and neighbourhoods, the necessity for effective privacy and security protections is more and more essential. The purpose of this research paper is to examine the present status of IoT security and privacy, emphasising important obstacles and possible remedies. One key difficulty in IoT security includes the absence of device standardization. Most IoT gadgets are built by smaller or growing enterprises with limited assets, making good safety precautions hard to install. Furthermore, these gadgets frequently employ exclusive protocols and networking mechanisms, making it harder for security experts to find and resolve problems.

The sheer number of internet-connected gadgets is also a huge challenge. By 2022, there will probably be trillions of Internet of Things (IoT) gadgets in usage, making it increasingly difficult to ensure that every one of them is secure. The reality that a lot of Internet of Things devices prioritise ease and functionality over security twists matters further. Several ideas have been presented to overcome these difficulties. One option would be to create standard procedures for IoT privacy and security, including the Internet of Things (IoT) Security Foundation's "Code of Practice for the Internet of Things Security." This would make sure that every one of the Internet of things gadgets satisfy a basic standard of security. Furthermore, there have also been requests for higher government oversight of internet of things security, which includes the suggested IoT Cybersecurity Enhancement Act in the United States of

America. Another technique involves safeguarding communication routes among IoT devices. This might involve employing cryptography along with safe protocols to safeguard information while in transit, as well as safe enrollment as well as network management techniques to guarantee that only authorized devices can join to a network.

Artificial intelligence and machine learning are becoming increasingly popular for improving IoT security. Algorithms based on machine learning are capable of identifying and reacting to odd network behaviour, while AI can find and address issues in IoT devices.

In general, IoT privacy and safety is a difficult and quickly changing topic. Although issues remain, there are potential methods to improve IoT device security and confidentiality.

As the Internet of Things continues to technology advances, researchers, business executives, and government officials must collaborate to assure device security and user confidentiality. The Internet of Things is gaining traction in all aspects of the modern world. As technology advances, the Internet of Things (IoT) is becoming a worldwide network that connects everything to the internet. The Internet of Things (IoT) is a rapidly expanding field of research. The expanse of minds has gotten us near to changing the present internet into an altered and organised version.

Connecting every one of the internet service providers' gadgets, whether wired or via the internet, will enable easy access to a breakthrough source of information. Connecting intelligent gadgets is a novel concept.[1].

A smart community is a complex system that uses data as well as ICT to enhance the attractiveness and sustainability of urban areas. IoT technology has significant economic opportunities due to its evolving nature. Crucial stakeholders include programme designers, expert organisations, inhabitants, governmental and public sector organisations, the evaluation area, as well as level engineers. The intelligent city cycle includes developments in ICT, amenities, support, and apps for citizens.

IoT frameworks are crucial for organising large-scale diverse networks [2]. The "Smart City" concept has gained popularity in academic writing and worldwide plans. This proposal addresses rapid IT breakthroughs to improve urban areas for citizens. Urban settlements and metropolitan regions account for a significant share of the total population. The recent metropolitan population growth has had a negative impact on the quality and quantity of services provided to citizens. As the population grows rapidly, administrative services are insufficient to meet present needs. Certain amenities still waste resources and time. In today's technological age, Smart Cities offer effective solutions for residents facing these issues. Smart cities are large-scale projects initiated by local governments. In certain nations, governments and private partnerships collaborate to create smart cities that benefit inhabitants. ICT is the primary technology utilised in smart cities [3].

1.1 Privacy

Solove defines security as a broad term that encompasses a variety of related concepts. The organisation Privacy International defines security as a multifaceted concept with four key components: 1) Body, 2) Correspondences, 3) Domain, 4) Data. Genuine security prioritises protecting individuals from external threats. Interchange security relies on the secure transmission of data via any channel. This involves phone calls, letters, and emails.

Establishing borders on real estate, including homes, workplaces, and public spaces, is crucial for security in the region. Security of data protects confidential data collected and handled by a body, including healthcare data and linked cards. [4]

1.2 Privacy Threats

As the Internet of Things takes authority over our daily lives, maintaining security has become increasingly challenging. The Internet of Things (IoT) will exacerbate conflicts over access to specific data. Ziegeldorf's writing audit [84] identifies the most common security risks in IoT:

Authentication is a threat that binds a particular component to an identification, such as an individual's identity or location.

Using techniques like GPS, web traffic, or mobile phones to track an individual's approximate location has concerns, including localization and monitoring.

Profiling is commonly used in online business to customise content, such as announcements and advertising. Organisations use data pertaining to individuals to identify their interests based on biographies and statistics.

Interaction along with introduction relate to effective techniques and approaches for connecting with individuals and providing information to consumers. The flow of confidential information between frameworks and clients might compromise security.

The lifecycle of an IoT device includes its acquisition, use, and eventual disposal. Smart gadgets often keep track of their own experiences throughout their lives, despite the assumption that all data is deleted. Specific recordings and pictures may not be available indefinitely.

Inventory assaults include unauthorised entry to and gathering of information about the status and attributes of certain goods. Offenders can use inventory data to plan a break-in at a safe time.

Linking structures that incorporate data sources can lead to unauthorised utilisation and privacy violations.

1.3 Security

Data security (DS) refers to the methods and approaches utilised to protect data, information, as well as frameworks. Security of data includes avoiding unauthorised utilisation, consumption, impact, and dissemination. Modification or destruction. Consider the three fundamental safeguarding data principles. They involve respect, ease of access, and confidentiality. Responsibility has become a widespread criterion, often cited as one of the three basic principles by security organisations for corporations such as Combitech AB.[5]

There are significant issues in a variety of domains, including the healthcare industry, transportation systems, educational systems, electricity systems for management, garbage management, criminal prevention and management, etc. The Internet of Things (IoT) offers practical answers to challenges in smart cities. There are several difficulties to creating a smart urban environment, among them the most important of which is money for smart city initiatives, as well as other administrative and regulatory concerns such as approvals from relevant authorities. Educating the residents of cities that are smart is also a problem that must be addressed efficiently. [6]

"The World Wide Web Application Safety Project" (OWASP) [7] has provided a thorough list of the top ten serious vulnerabilities. Safety difficulties with web user interfaces, inadequate permission or authorization, unstable network connectivity, an inadequate level of transportation encryption, and more. There are a total of five issues with privacy, five cloud user interface protection faults, seven MII imperfections eight insufficient security set up flaws, nine software/firmware flaws, and ten poor physical protection flaws.[8]

The primary goals of this research are to comprehend the fundamental ideas of IoT, as well as the applicable areas where it may be used to benefit city dwellers. This article focuses on the use of IoTs in smart cities. This article covers IoT ideas, smart city environments, main components, applications, concerns, challenges, and opportunities for further development. Web-based user interfaces are designed to connect with monitors and IoT devices which have been inspected.

2. LITERATURE REVIEW

According to Ruchi Parashar and others, the Internet of Things (IoT) concept enables items to interact securely with one another and other devices through differentiating, detecting, networking, and handling capabilities. The Internet enables a wide range of services. The internet allows us global connectivity with a simple click. This article summarises current research on IoT systems. The researchers employ many methodologies, including a thorough review of literature and current IoT developments.

They also highlight obstacles in IoT that may hinder its spread in certain areas. Researchers discussed IoT system's architecture. There are a total of five distinct levels: processing layer, application layer, business layer, , and authentication layer. The company's layer is the initial layer. Layers are primarily responsible for determining whether apps are compatible with the Internet of Things.

The scientists discuss the technologies that enables the Internet of Things. They differentiate three forms of technology: OT and QRC, NFC, RRFID, and Bluetooth connectivity low energy, which is considered the most recent. According to the authors, internet usage has significantly impacted our daily lives. A lot of study is needed in the realm of IoT. [9]

According to the article, the Internet of Things (IoT) is an innovative technology that allows for digital communication.

This research focuses on IoT applications in urban areas. Effective Internet of Things (IoT) services and big data visualisation are driving global smart city ambitions.[2] In this work, the author emphasises on a city-wide Internet of Things system. This can be a common use case for IoT technology. The Urban IoT System (UIoTS) aims to create and study the concept of Smart Cities. This study aims to improve communication technologies and provide value-added services to the municipal government and residents.[10]

The authors suggest that modern cities are faster, safer, greener, and more adaptable, leading to increased satisfaction and comfort among residents. The researchers go on to address the primary elements of Smart Cities. Key factors include design, structures, healthcare, transportation, electrical power, technological advances, government, educational institutions, and citizens. These aspects combine to make the town a Smart City. ICT is efficiently employed to accomplish this.[11]

This study emphasises the necessity to thoroughly investigate privacy issues and problems in IoT. We break down this complicated issue into four steps: To discuss privacy in the IoT, we offer an accurate description of privacy and utilise an illustration model. A quick review of privacy rules highlights flaws and emphasises the need for a detailed investigation of privacy concerns. The second stage acknowledges that the Internet of Things is a dynamic field that can't be defined solely by its technological capabilities. Our explanations of evolving IoT characteristics as well as technologies offer a thorough as well as privacy-focused overview of current, past, and forthcoming developments. subsequently academics summarise their findings. [14]

The Internet of Things (IoT) plays an important role in the rapid development of modern technologies. Technology makes it easier to share data. Consequently, it is vital to address user information security. This article focuses mostly on the security of IoT technology. As previously noted, the Internet of Things is subject to several attacks, such as DDoS, credential guessing, rewind, and threats from insiders. We have reviewed authentication techniques for IoT, which are crucial for meeting basic security needs. Common approaches to authentication include unique passwords, mutual authorization using ECC, ID validation, certificate confirmation, and blockchain. After comparing recent authentication solutions, we discovered that most rely on block-chain technology. [15]

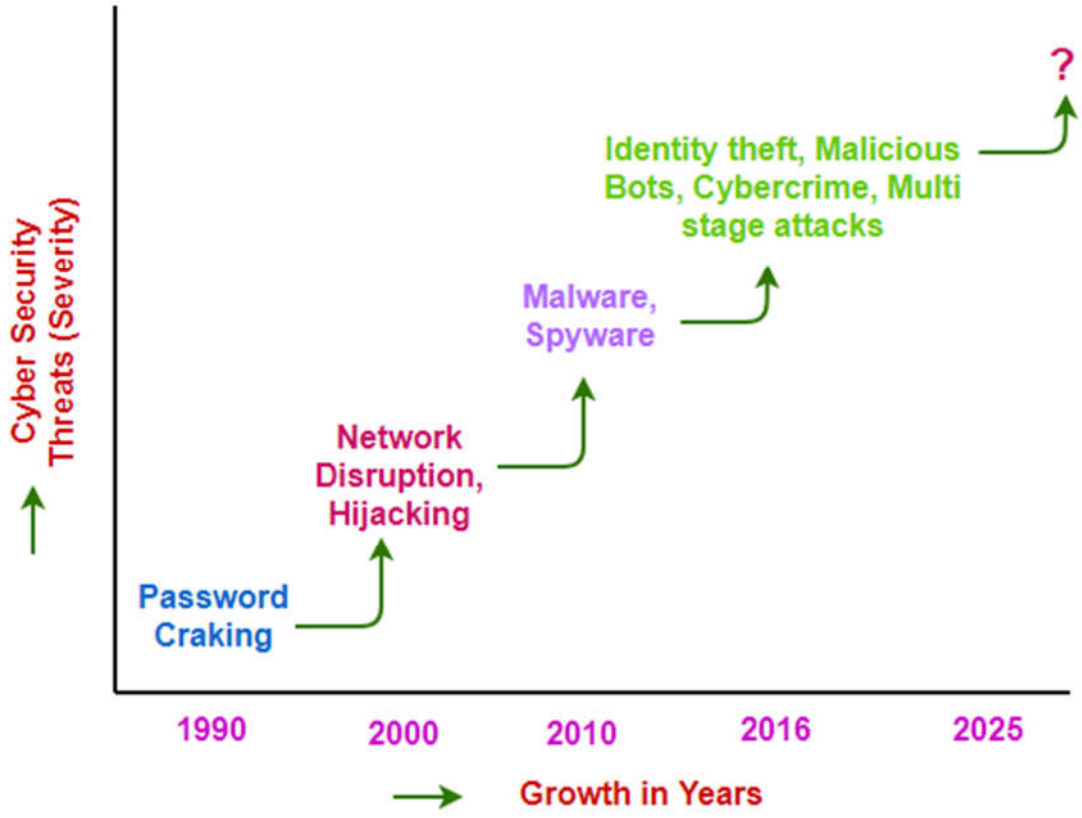

Figure 1: The development of multiple threats.

The increasing accessibility and responsiveness of data poses an obstacle to the privacy and security of data in today's linked world. The use of diverse innovations, services, and standards across the web and cloud sectors may lead to increased security risks in the future. Figure 1 shows how security threats have increased over time due to the introduction of new attack tools

in secure cyberspace. As security attacks get increasingly sophisticated, the amount of information needed to launch them is steadily reducing. Effective safeguarding of information requires balancing privacy and security safeguards. [16]

3. METHODOLOGY

This article uses the SLR technique and the PRISMA [12] approach to analyse IoT applications in smart towns and cities. The study consists of three primary steps: preparation, execution, and summarising. Figure 2 has detailed explanations of each step.

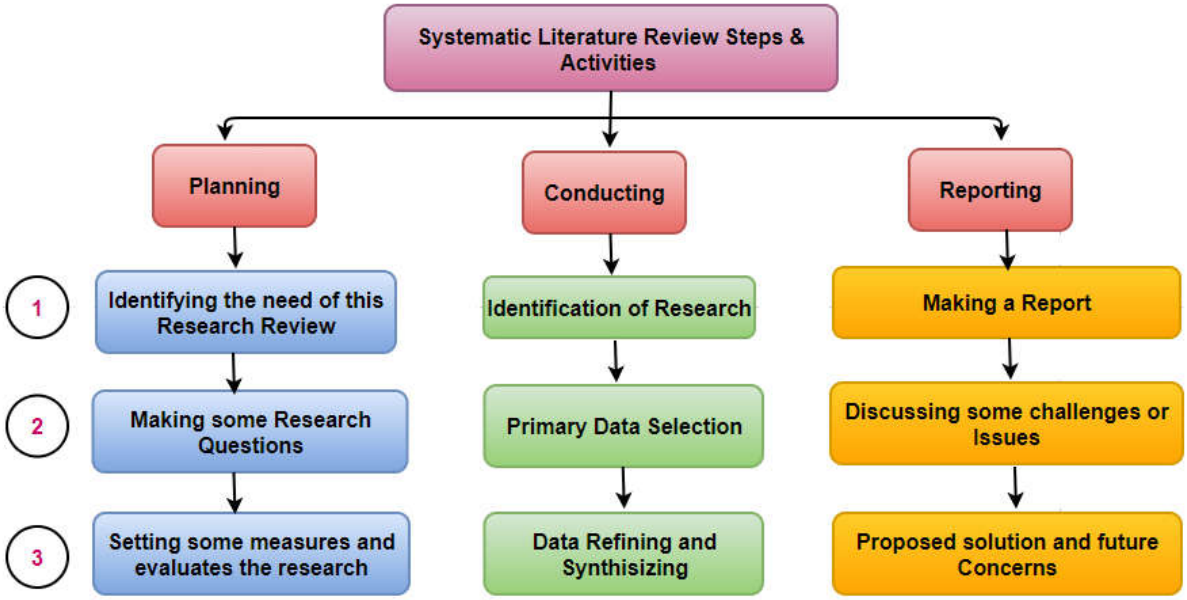

Figure 2: Systematic Literature Review Steps & Activities

3.1 Step-1 Planning

During this stage, we identified the main point of the review and completed activities to clarify each advancement in depth. This STR aims to assess security and privacy in smart cities that are utilising IoT technology. We developed study questions to analyse the Smarts Cities environment.

The most important study research questions are as follows.

RQ-1. Definition of Security and Privacy IoT in Smart City Settings?

RQ-2. How do you safeguard the IoT facilities?

RQ-3. What are the main difficulties or problems with IoT technology?

RQ-4. How can IoT be used effectively in a given region in terms of security?

3.2 Step-2 Conducting Review

To conduct this research, I searched for relevant publications using generic keywords in existing literature. A few internet data sets were used to represent a wide range of scholastic

distributions. The Online data sources used include Springer, Google Scholar, Research Gate, IEEE Explorer Access, ACM online Digital Library, as well as the Web of Science. The aforementioned data sets are considered appropriate and have an elevated impact factor distribution. The automated search focused on "Security and Confidentiality of the Internet of Things IoT" and associated concerns based on the review's assessment question. Figure 3 shows how data from research publications were obtained from a digital database.

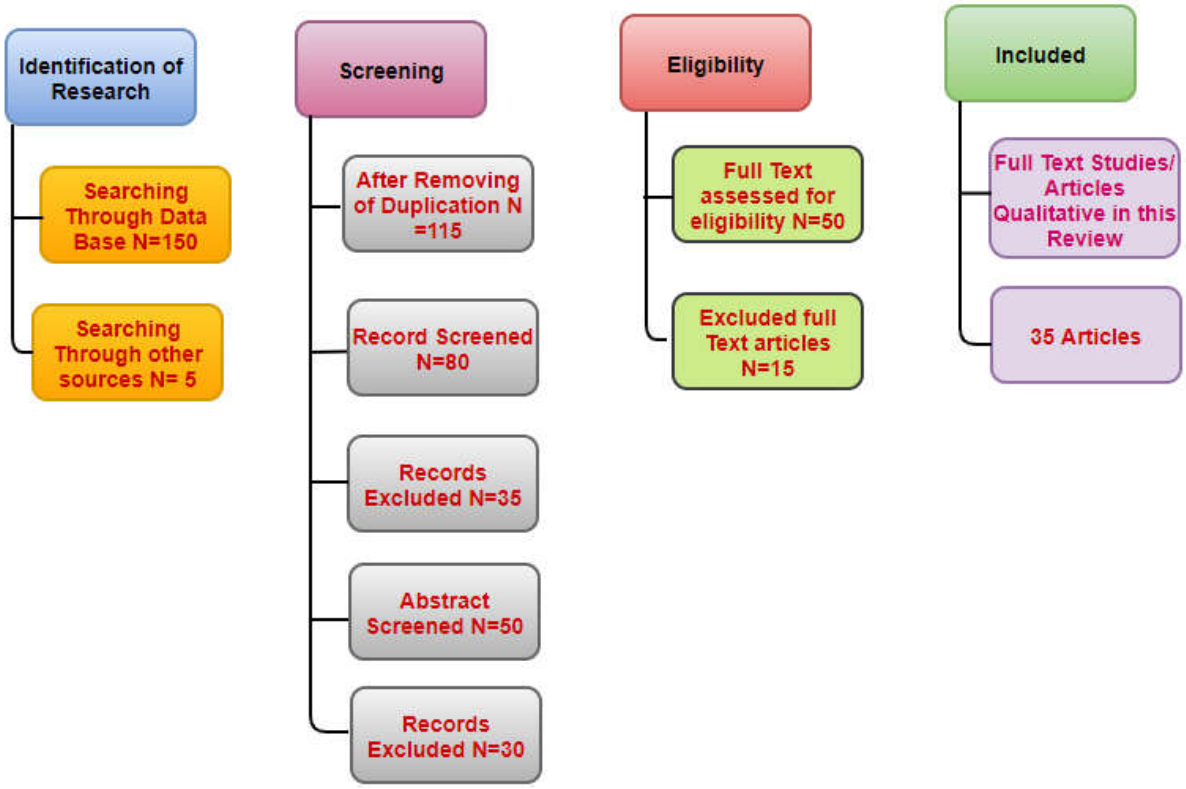

Figure 3: Flow Representation of PRISMA Technique

Table 1 summarises the final examination of research articles, book chapters, and associated materials, including citations, publication years, and publishers/data sources. We picked 40 items that are particularly relevant to our analysis of the prominent digital database.

Table 1: Important IoT Security Concerns

Sr. No.	Main Data Sources	Publisher Name	Publish Year	Ref. #
1	Web of Science, Google Scholar, IEEE Access Scopus, Resarchgate Academia, Websites E-books, Internet, books chapters, E-libraries	ACM	2023	[31]
2		AETiC	2021	[7]
3		Elsevier	2021	[13]
4		Elsevier	2019	[18]
5		Elsevier	2023	[20]
6		Elsevier	2023	[23]
7		Elsevier	2019	[24]
8		Elsevier	2022	[28]
9		Elsevier	2019	[32]
10		Elsevier	2022	[33]
11		Elsevier	2017	[1]
12		Elsevier	2023	[15]

13		Elsevier	2019	[12]
14		Elsevier	2019	[2]
15		FCS	2018	[6]
16		ICITSI	2015	[10]
17		Hindawi	2017	[12]
18		IEEE	2016	[17]
19		IEEE	2016	[11]
20		IEEE	2022	[17]
21		IEEE	2021	[14]
22		IEEE	2022	[21]
23		IEEE	2023	[26]
24		IEEE	2022	[15]
25		IEEE	2017	[29]
26		IJTRA	2016	[8]
27		IJSRCSEIT	2020	[17]
28		John Wiley & Sons, Ltd.	2019	[27]
29		Jaypee University of Information Technology	2018	[17]
30		MDPI	2016	[9]
31		MDPI	2017	[5]
32		MDPI	2014	[14]
33		Routledge	2022	[19]
34		Springer	2023	[25]
35		Springer	2023	[34]
36		Springer	2019	[3]
37		Springer	2014	[4]
38		IEEE	2016	[16]
39		IEEE	2022	[22]
40		IEEE	2022	[30]
		IEEE	2022	[35]

Figure 4 depicts the information from Table 1 in the form of a graph. Publication names are displayed horizontally, followed by the year of publication vertically. The investigation covers materials from 2008 to 2024.

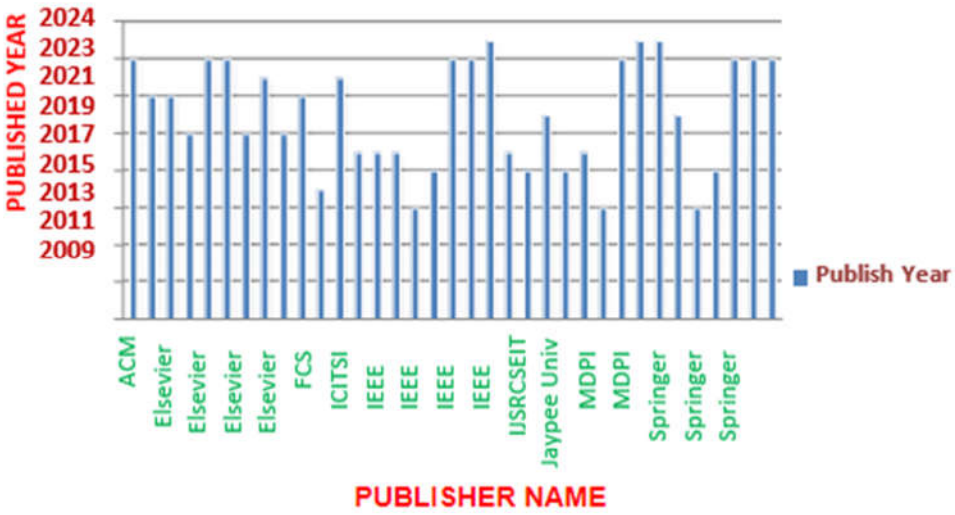

Figure 4: Graph Representation for Publisher and year

Table 2 shows a summary of the number of publications examined by publishers. The article covers 14 distinct publishers. IEEE and Elsevier have the optimum number of 9 and 8, correspondingly.

Table 2: Summary of inclusion

Sr. No.	Publisher Name	No. Publication
1	ACM	2
2	Hindawi	2
3	IJSRCSEIT	9
4	FCS	2
5	ICITSI	2
6	IJTRA	2
7	IEEE	8
8	John Wiley & Sons, Ltd.	2
9	MDPI	2
10	Jaypee University of Information Technology	2
11	Springer	2
12	Elsevier	4
13	Routledge	2
14	AETiC	6

Figure 5 depicts the information from Table 2. Publishers names are shown horizontally, followed by the total number of the appropriate publications in the vertical direction. IEEE ranks top on the graph owing to its bigger value.

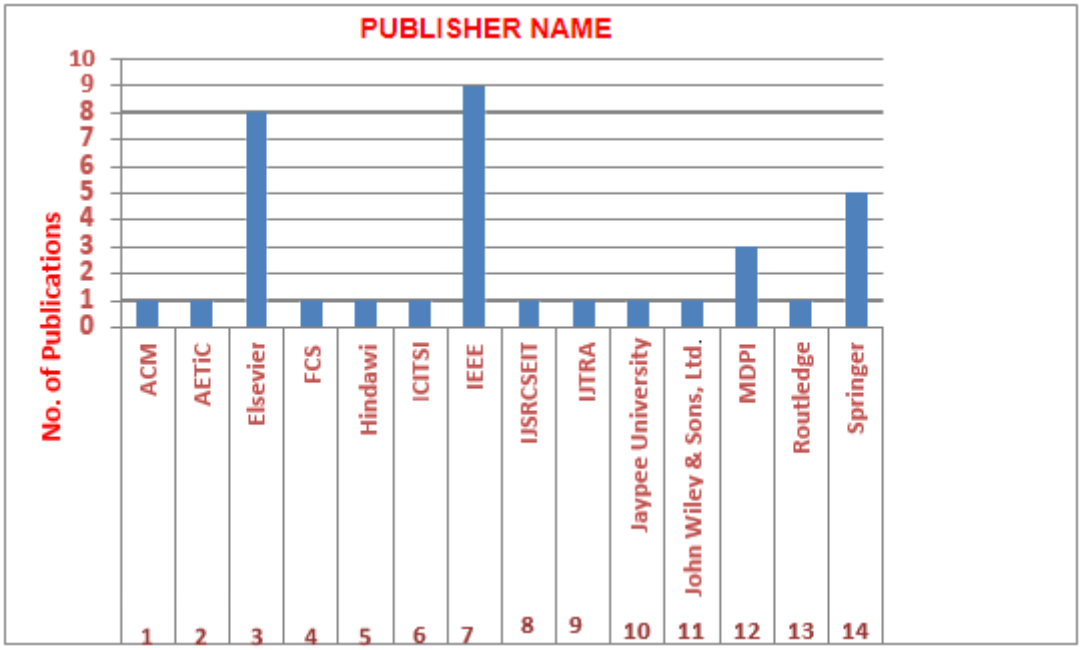

Figure 5: Graph Representation of No. Publication and Publishers

3.3 **Step-3 Reporting**

Thematic evaluation was used to identify areas of privacy, security, applications, and services related to the study topics. The research aims to establish a safe and trustworthy smart city infrastructure by addressing problems, dangers, and associated concerns. The report is aimed at responding to the investigation's questions.

4. RESULT AND DISCUSSION

This part presents findings from a comprehensive review of the literature on privacy and security in smart towns and cities, including security services and applications in the digital era. Table 3 highlights important security vulnerabilities identified in research publications on IoTs in smart cities [13].

Table 3: Important IoT Security Concerns

S.No	Reference Number	Data Privacy	Authentication	Availability of data	Data Integrity	Data Access	Data Confidentiality	Identification	Access Control	Device Security	Other Issue
1	[1]	C	N	C	C	C	C	C	C	N	C
2	[2]	C	C	N	C	N	C	C	C	C	C
3	[4]	C	C	C	C	C	N	C	N	C	C
4	[5]	N	C	C	C	C	C	C	C	C	C

5	[7]	C	N	N	C	C	C	N	C	C	N
6	[8]	c	C	C	C	C	C	C	C	C	N
7	[10]	C	C	C	C	C	C	C	N	C	N
8	[12]	C	C	C	N	N	C	N	C	C	N
9	[13]	C	N	N	C	C	C	C	C	N	C
10	[14]	C	C	C	C	C	N	C	C	C	C
11	[16]	C	C	C	C	C	C	C	C	C	C
12	[17]	N	C	C	C	C	C	C	N	C	C
13	[18]	C	C	C	C	C	C	C	C	N	N
14	[19]	C	C	C	N	C	C	N	C	C	C
15	[20]	N	N	N	C	N	N	C	C	C	C
16	[21]	C	C	C	C	C	C	C	N	C	C
17	[22]	C	C	C	C	C	C	C	N	C	C
18	[23]	N	C	N	C	C	C	C	C	C	N
19	[27]	C	C	C	N	C	C	N	C	N	N
20	[28]	N	C	C	C	C	N	C	N	C	N
21	[30]	C	C	C	C	C	C	C	C	C	C
22	[32]	C	C	C	C	N	C	C	C	C	C
23	[33]	C	C	N	C	C	C	C	C	C	C
24	[34]	C	N	C	C	C	N	N	C	N	C
25	[35]	C	C	C	C	C	C	C	C	C	N

*c indicates that the reference papers addressed security problems, whereas n indicates that they did not. Table 4 identifies security and privacy concerns, whereas table 5 lists the principal domains of the Internet of Things (IoT) privacy and security sections.

Table 4: Difficulties with Security and Privacy

Descriptions	Security and Privacy Challenges	References
Big Data	Securely managing large amounts of data on the Internet of Things	[11][14]
Interoperability	The functioning of numerous linked devices in an Internet of Things network system shouldn't be hampered by appropriate security measures.	[13]
Resource constraints	Many IoT nodes lack sufficient power, storage capacity, processing speed, and bandwidth due to their low-speed connections. Security measures that are difficult to implement.	[4][10]
Preserve privacy	Certain RFIDs lack an appropriate authentication method, making it vulnerable to assault and identification by other parties.	[14][15]
adaptability	The Internet of Things is made up of many nodes. The suggested security tools for IoT	[5]
Developing reliability	Trust management is an issue since IoT infrastructure lacks centrally managed administration.	[2][8]
autonomous management	The trust management of Internet of Things (IoT) networks is complicated by the lack of centrally regulated management.	[4][9]
Access management	The problem with IoT infrastructure trust management stems from the lack of centrally regulated administration.	[3][11][15]

Controlling of disruption or interruption	Keeping an eye out for any unusual network activity and being able to identify and prevent attacks are major issues.	[33]
Advanced Persistent Threats	Physical, Network, as well as application layer security	[35]
Designing Problem	Network layer security	[32]

Table 5: IoT Security and Privacy Domain

Main Domain	Sub area	Reference
Smart City	Architectural Design, element, modelling, and communication protocol IoT and SC relationships, management of waste, web-based services for urban IoT networks, stacking protocols, intelligent energy, healthcare systems, and big data	[3][7][12] [18][22] [23]
ICT	Information, mobile devices, confidentiality, harmful frauds, security, and detecting intrusions	[14][16] [20]
IoT security	Architectural design of security, threatens and confidentiality, encryption, security of information, susceptibility, dangers, attacks, safety concerns, risk as well as challenges, machine learning, permitted solution, determined threats, VPN security (end-to-end), SSL, IP security, Authentication system, challenges, limitations as well as difficulties	
SAST	Vulnerability mapping	[30][31]
IoT	IoT architecture, block chain technology for IoT security, and significant risks and weaknesses	[1][3][5] [9][11] [12]
IoT security and privacy	wearable technology, low energy, Bluetooth dangers, IoT security techniques, threats and assaults, and CPS	[3][4][12] [14][15]
IoMT Security	Privacy, risks, and smart health care services	[22][23] [24][25] [27][28]
IoT Intelligence	Machine learning solution	[29][30] [31]
Decentrilized IoT security	Using blockchain technology to enhance IoT and security	[32][33]
Cyber physical system (CPS)	Block chain technology, intelligent transportation, and 5G security	[28][31][3 3][34][35]

5. CONCLUSION

This bibliometric study highlights important contributors and the links between them, offering an organized representation of research collaboration and influence within a certain topic. In addition to facilitating a deeper comprehension of the collaboration networks, the study helps funding agencies, researchers, and academic institutions make well-informed decisions to promote productivity and innovation by identifying central authors and clusters. This study is useful for resource allocation and strategic planning in academic and research environments, despite certain drawbacks, including possible biases in database coverage and an emphasis on quantitative indicators. The knowledge gained from this study is crucial for directing future

lines of inquiry, encouraging productive teamwork, and raising the general influence of research in the community.

REFERENCES

1. Farooq, M., Waseem, M., Mazhar, S., Khairi, A., Kamal, T.: A Review on Internet of Things (IoT). Int. J. Comput. Appl. 113, 1–7 (2015). https://doi.org/10.5120/19787-1571

2. Mehmood, Y., Ahmad, F., Yaqoob, I., Adnane, A., Imran, M., Guizani, S.: Internet-of-Things-Based Smart Cities: Recent Advances and Challenges. IEEE Commun. Mag. 55, 16–24 (2017). https://doi.org/10.1109/MCOM.2017.1600514

3. Full article H. Samih (2019) Smart cities and internet of things, Journal of Information Technology Case and Application Research, 21:1, 3-12, DOI: 10.1080/15228053.2019.1587572

4. Hoepman, J.-H.: Privacy Design Strategies. In: Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A., and Sans, T. (eds.) ICT Systems Security and Privacy Protection. pp. 446–459. Springer, Berlin, Heidelberg (2014)

5. Sharma, M., Sehgal, V.: Security and Privacy Mechanism in IOT. (2017)

6. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., Zhao, W.: A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet Things J. 4, 1125–1142 (2017). https://doi.org/10.1109/JIOT.2017.2683200

7. Li, J. (2020). Vulnerabilities Mapping based on OWASP-SANS: a Survey for Static Application Security Testing (SAST). ArXiv, abs/2004.03216.

8. Stout, W.M.S., Urias, V.E.: Challenges to securing the Internet of Things. In: 2016 IEEE International Carnahan Conference on Security Technology (ICCST). pp. 1–8. IEEE, Orlando, FL, USA (2016)

9. Parashar, R., Khan, A.: A SURVEY: THE INTERNET OF THINGS. 4, 7 (2016)

10. Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: Internet of Things for Smart Cities. IEEE Internet Things J. 1, 22–32 (2014). https://doi.org/10.1109/JIOT.2014.2306328

11. Mohanty, S.P., Choppali, U., Kougianos, E.: Everything you wanted to know about smart cities: The Internet of things is the backbone. IEEE Consum. Electron. Mag. 5, 60–70 (2016). https://doi.org/10.1109/MCE.2016.2556879

12. Oktaria, D., Suhardi, Kurniawan, and N.B.: Smart city services: A systematic literature review. In: 2017 International Conference on Information Technology Systems and Innovation (ICITSI). pp. 206–213 (2017)

13. Ogonji, M.M., Okeyo, G., Wafula, J.M.: A survey on privacy and security of Internet of Things. Comput. Sci. Rev. 38, 100312 (2020). https://doi.org/10.1016/j.cosrev.2020.100312

14. Ziegeldorf, J. H., Morchon, O. G. and Wehrle, K. (2014), Privacy in the Internet of Things: threats and challenges, Security Comm. Networks, 7, pages 2728– 2742, doi: 10.1002/sec.795

15. Azrour, M., Mabrouki, J., Guezzaz, A., & Kanwal, A. (2021). Internet of things security: challenges and key issues. Security and Communication Networks, 2021, 1-11.

16. Varadharajan, V., Bansal, S. (2016). Data Security and Privacy in the Internet of Things (IoT) Environment. In: Mahmood, Z. (eds) Connectivity Frameworks for Smart Devices. Computer Communications and Networks. Springer, Cham. https://doi.org/10.1007/978-3-319-33124-9_11

17. Ziegeldorf, Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and Solutions Survey. Sensors, 22(19), 7433.

18. Azrour, Hassan, W. H. (2019). Current research on Internet of Things (IoT) security: A survey. Computer networks, 148, 283-294.

19. M., Sadhu, P. K., Yanambaka, V. P., & Abdelgawad, A. (2022). Internet of Things: Security and Solutions Survey. Sensors, 22(19), 7433.

20. Shokry, M., Awad, A. I., Abd-Ellah, M. K., & Khalaf, A. A. (2022). Systematic survey of advanced metering infrastructure security: Vulnerabilities, attacks, countermeasures, and future vision. Future Generation Computer Systems.

21. Allifah, N. M., & Zualkernan, I. A. (2022). Ranking security of IoT-based smart home consumer devices. Ieee Access, 10, 18352-18369.

22. Rao, P. M., & Deebak, B. D. (2022). Security and privacy issues in smart cities/industries: Technologies, applications, and challenges. Journal of Ambient Intelligence and Humanized Computing, 1-37.

23. Keshta, I. (2022). AI-driven IoT for smart health care: Security and privacy issues. Informatics in Medicine Unlocked, 30, 100903.

24. Kumar, N. M., & Mallick, P. K. (2018). Blockchain technology for security issues and challenges in IoT. Procedia Computer Science, 132, 1815-1823.

25. Ziegeldorf, Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. Sensors, 23(2), 788.

26. Ashok, K., & Gopikrishnan, S. (2023). Statistical Analysis of Remote Health Monitoring Based IoT Security Models & Deployments from a Pragmatic Perspective. IEEE Access, 11, 2621-2651.

27. Perwej, Y., Parwej, F., Hassan, M. M. M., & Akhtar, N. (2019). The internet-of-things (IoT) security: A technological perspective and review. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN, 2456-3307.

28. Aversano, L., Bernardi, M. L., Cimitile, M., & Pecori, R. (2021). A systematic review on Deep Learning approaches for IoT security. Computer Science Review, 40, 100389.

29. Ziegeldorf, Deogirikar, J., & Vidhate, A. (2017, February). Security attacks in IoT: A survey. In 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC) (pp. 32-37). IEEE.

30. Sarker, I. H., Khan, A. I., Abushark, Y. B., & Alsolami, F. (2022). Internet of things (iot) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mobile Networks and Applications, 1-17.

31. Chen, Z., Liu, J., Shen, Y., Simsek, M., Kantarci, B., Mouftah, H. T., & Djukic, P. (2022). Machine learning-enabled iot security: Open issues and challenges under advanced persistent threats. ACM Computing Surveys, 55(5), 1-37.

32. Qian, Y., Jiang, Y., Chen, J., Zhang, Y., Song, J., Zhou, M., & Pustišek, M. (2018). Towards decentralized IoT security enhancement: A blockchain approach. Computers & Electrical Engineering, 72, 266-273.

33. M., Monem, A. A., & Shaalan, K. (2020). Hybrid end-to-end VPN security approach for smart IoT objects. Journal of Network and Computer Applications, 158, 102598.

34. Rajawat, A. S., Goyal, S. B., Bedi, P., Verma, C., Ionete, E. I., & Raboaca, M. S. (2023). 5G-Enabled Cyber-Physical Systems for Smart Transportation Using Blockchain Technology. Mathematics, 11(3), 679.

35. Khan, A., Ahmad, A., Ahmed, M., Sessa, J., & Anisetti, M. (2022). Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends. Complex & Intelligent Systems, 8(5), 3919-3941.

36. M. Jeyabharathi, D. Kumutha, S. Jeevitha, P. Geetha, Manjunathan Alagarsamy R. (2024).

A Massive 0.3 THz Bandwidth with High Gain 6G Antenna. Journal of Nano- and Electronics Physics, 16(4), 649

37. D. Kumutha, R. Delshi Howsalya Devi, M. Jeyabharathi, C. Priya, P. Geetha. (2024).Transit to 6G Spectrum with MIMO Antenna Model – A Review. Journal of Nano- and Electronics Physics, 16(4), 676

38. K. S. Balamurugan, Chinmaya Kumar Pradhan, A. N. Venkateswarlu, G. Harini, P. Geetha. (2024). An internet of things based smart agriculture monitoring system using convolution neural network algorithm. EAI Endorsed Transactions on Internet of Things, Vol. No. 10

39. M. Jeyabharathi, D. Kumutha, P. Geetha et al., (2024). Miniaturized T and Inverted T Slotted Ultra Wide Band Antenna with Defected Ground (DG) System for 5G Communication. Journal of Nano- and Electronics Physics, 16(3), 706.