Industrial IoT cybersecurity: a bibliometric analysis

Ignacio J. Dasso, Sébastien Maudet, Renzo E. Navas, Guillaume Andrieux

▶ **To cite this version:**

Ignacio J. Dasso, Sébastien Maudet, Renzo E. Navas, Guillaume Andrieux. Industrial IoT cybersecurity: a bibliometric analysis. SpliTech 2025: 10th International Conference on Smart and Sustainable Technologies, IEEE, Jun 2025, Split, Croatia. pp.#1571125762, ⟨10.23919/SpliTech65624.2025.11091687⟩. ⟨hal-05039566⟩

HAL Id: hal-05039566

https://hal.science/hal-05039566v1

Submitted on 14 May 2025

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

HAL Authorization

Industrial IoT cybersecurity: a bibliometric analysis

Ignacio J. Dasso[†], Sébastien Maudet[†], Renzo E. Navas[‡], Guillaume Andrieux[†]
[†] *Nantes Université, CNRS, IETR, UMR 6164, F-85000 La Roche-sur-Yon, France*
{ignacio.dasso, sebastien.maudet, guillaume.andrieux}@univ-nantes.fr
[‡]*IMT Atlantique, IRISA, UMR CNRS 6074, F-35700 Rennes, France*
renzo.navas@imt-atlantique.fr

***Abstract*—Industrial Internet of Things (IIoT) cybersecurity has become critical to our societies as industrial systems increasingly rely on interconnected devices. Several literature studies exist regarding cybersecurity for IoT or security topics in Industry 4.0. Still, very few are exclusively dedicated to cybersecurity for IIoT—and they approach the subject non-systematically. In this study, we conduct a systematic bibliometric analysis of over 12,000 academic publications from 2014 to 2024 to map the research landscape of IIoT cybersecurity. Guided by eight Research Questions and a methodological approach, we examine publication types, key venues, and dominant topics to highlight trends and research clusters within the field. Our findings show that conference papers and journal articles are equally predominant, with IEEE and Springer serving as the leading publishers. Among the most cited works, "blockchain" is the most popular topic. A keyword co-occurrence analysis identifies four thematic clusters led by: (1) "blockchain" and "security," (2) "network security" and "industrial IoT," (3) "embedded systems" and "cyber-physical systems," and (4) "automation" and "network architecture." The first two clusters are the most prominent grouping 80% of the top 20 keywords. Regarding future trends, the growing prominence of "machine learning" and "intrusion detection," and a slight deceleration of "blockchain" in 2024, suggests shifting research priorities. We publicly share the bibliographic data and source code used to create this bibliometric analysis.**

***Index Terms*—IoT, Industry 4.0, IIoT, cybersecurity, review, survey.**

I. Introduction

The Internet of Things (IoT) blends sensors, embedded systems, computing capabilities, communication technologies, and the Internet [1]. IoT developments provide solutions for a wide variety of applications. It has been more than 15 years since IoT merged with the Industry, starting what is know as the Industrial Internet of Things (IIoT).

Compatible with low latency communications, intelligent response, autonomous access, and administration of information [2], IIoT solutions are implemented in production environments (e.g., water plants, oil & gas refineries, energy plants, food processing plants, etc). Even more, production environments are linked with managing financial resources, and complying with local and international regulations. The combination of financially rich stakeholders and Internet-accessible industrial systems raises both the interest in attacking and defending IIoT systems.

A panorama to better understand IIoT cybersecurity is needed: available publications address cybersecurity either from the standpoint of IoT, which results in a broad view, or from the standpoint of specific applications or technologies, which results in a narrow view. For this reason, the goal of this work is to build a comprehensive view of IIoT cybersecurity. This study is based on a systematic bibliometric methodology, supported by eight Research Questions and evidence obtained from peer-reviewed articles.

The remainder of this work is structured as follows. Related work is presented in Sec. II. The bibliometric analysis methodology is defined in Sec. III, while Sec. IV presents the results. Finally, Sec. V concludes this work.

II. Related work

Cybersecurity in the IIoT has been approached from different perspectives and with multiple levels of depth in the scientific literature.

On the one hand, many articles explore general aspects of IoT security. Raimundo et al. [3], present a literature review of 70 articles on IoT security technologies and cyber risk management in industry, including the definition of concepts and identification of challenges. In [4], the authors evaluate 774 publications through a bibliometric analysis in the field of IoT security protocols, depicting research clusters, countries, and continents at the forefront of research. Lee et al. [5] systematically map 1,365 publications identifying researchers, key topics, and 10 research clusters. These articles focus on IoT security in general but not on IIoT as the main topic.

On the other hand, Industry-focused IoT security surveys study specific applications. Chevtchenko et al. [6] conduct a systematic review of 84 studies on anomaly detection for industrial machines using IoT devices and machine learning algorithms. In [7], the authors conduct a survey describing attacks, and evaluating the qualities and flaws of industrial IoT systems based on a proposed IoT protocol stack. Reyes Domínguez et al. [8] evaluate through a bibliometric analysis 1,069 documents related to Industry 4.0 in the manufacturing sector.

To the best of our knowledge, no study has addressed the cybersecurity of IIoT as a main topic by means of a bibliometric analysis. In this article, we conduct a study with the same level of abstraction as some of the previously cited publications, but with a methodological approach.

III. Methodology

This bibliometric analysis is inspired by known methodologies [9] which propose a research path by answering Research

Questions (RQs). The answers to the RQs are based on metadata and data extracted from peer-reviewed articles.

The raw information from the articles and the scripts used for this bibliometric study are available here [10]: https://github.com/idasso/bibliometricAnalysisIIoTCybsec .

A. Research Questions

This "IIoT cybersecurity" bibliometric study is guided by the following RQs:

RQ1. What are the top publication types?
RQ2. What are the top publishers?
RQ3. What are the top publication venues?
RQ4. What publications are the most cited?
RQ5. What recent surveys are the most cited?
RQ6. Which are the main research clusters?
RQ7. What are the most popular topics?
RQ8. What are the publication trends of popular topics?

B. Literature search and selection

Keywords chosen to describe "IIoT cybersecurity" are: "industry," "iiot," "internet of things," "iot," "cybersecurity," and "security". The database selected is Scopus. The publication period from 2014 to 2024 provides research material from a complete decade.

The result of applying these ideas leads to Query #1 (Q#1) presented in Lis. 1. The selected parameters to export are: "document title," "year," "source title," "citation count," "source and document type," "publisher," and "indexed keywords". The indexed keywords provide the core information to establish links between different publications.

C. Most cited publications and surveys

The articles are sorted by average citations per year. Our reference year is 2025. The normalizing factor is obtained by subtracting the year of publication. For example, publications from 2024 have a normalizing factor of 1 ($2025 - 2024 = 1$), while publications from 2014 have a normalizing factor of 11 ($2025 - 2014 = 11$).

The results sought are the top cited articles based on Q#1 and the top cited surveys based on a new Query #2 (Q#2), shown in Lis. 2. Q#2 has added lines of code that limit the corpus to surveys and similar studies, select publications stating "IIoT" or "cybersecurity" in the title, and limit publications from 2022 to 2024 for recent results.

D. Cluster identification

Keywords and keyword co-occurrences are the building blocks of the network map [11], [12]. The software VOSviewer supports the map creation by processing the information exported from Scopus.

The network map plots each keyword as a node. The higher the amount of times a keyword occurs, the greater the size of the node on the network map. The lines linking the different keywords represent the co-occurrences within a publication. The thicker the line, the higher the amount of co-occurrences.

The exported keywords from the databases are not standardized. This leads to keywords representing the same topic being processed as different and reducing its importance (i.e., "iot" and "internet of things" in different co-occurrence groups). The keywords need processing for the network map to become a more reliable representation. The proposed steps are to identify and group the keywords, choose a reference keyword for the group, and define a mapping function. The mapping function standardizes the keywords and generates a new file that is used for the network map creation.

IV. Results

In the following subsections, we present the results of our bibliometric analysis. The corpus consists of 12,573 articles provided by Q#1 (query executed on January 22nd, 2025).

A. RQ1. What are the top publication types?

Benefiting from the information extracted from Scopus with Q#1, Table I presents the publication types. Results show that conference paper is the main publication type, followed in second place by journal article[1]. Both concentrate close to 80% of the publications.

TABLE I
Top publication types 2014 to 2024[a]

Document Type	Quantity	Percentage
Conference paper	5,236	41.6%
Journal article	4,840	38.5%
Book chapter	1,178	9.4%
Review	547	4.3%
Conference review	408	3.2%
Others	367	2.9%

[a]Retrieved January 24th, 2025.

B. RQ2. What are the top publishers?

The most prolific publishers are IEEE (39.0%) and Springer (16.8%), concentrating more than 55% of the total publications. The list of publishers, the number of publications, and

[1]Scopus uses the term "article" to indicate "journal article".

Listing 1. Main search query (Q#1).

```
TITLE-ABS-KEY ( industr* OR iiot ) AND (
TITLE-ABS-KEY ( "internet of things" OR iot )) AND (
TITLE-ABS-KEY ( cybersecurity OR security )) AND (
PUBYEAR > 2013 ) AND ( PUBYEAR < 2025 ) AND (
LIMIT-TO ( LANGUAGE , "English" ))
```

Listing 2. Survey and related studies search query (Q#2)

```
TITLE-ABS-KEY ( industr* OR iiot ) AND (
TITLE-ABS-KEY ( "internet of things" OR iot )) AND (
TITLE-ABS-KEY ( cybersecurity OR security )) AND (
PUBYEAR > 2021 ) AND (PUBYEAR < 2025 ) AND (
TITLE (review OR survey OR map* OR bibliometric OR
analysis ) ) AND ( TITLE (iiot OR cybersecurity ))
AND ( LIMIT-TO ( LANGUAGE,"English" ) )
```

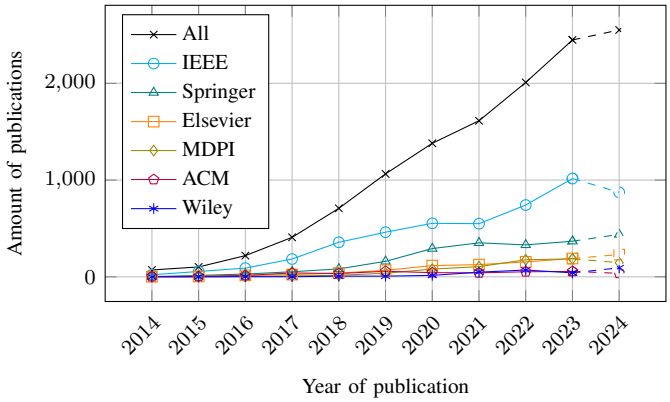

Fig. 1. Amount of publications per main publisher per year based on Q#1 results (retrieved January 23rd 2025).

each percentage are presented in Table II (publishers with at least 2%).

TABLE II
TOP PUBLISHERS IN IIOT CYBERSECURITY FROM 2014 TO 2024[a]

Publisher	Quantity	Percentage
IEEE	4901	39.0%
Springer	2118	16.8%
Elsevier	964	7.7%
MDPI	760	6.0%
ACM	379	3.0%
Wiley	284	2.3%
Others	3167	25.2%

[a]Retrieved January 23rd, 2025.

We also calculated the contribution of each publisher per year. The results are in Fig. 1. The last portion of each plot (2023 to 2024) is presented with a dashed line since there are yet unavailable publications corresponding to 2024. IEEE is the dominant publisher of the last decade, followed in second place by Springer. The publications are growing year after year, yet with a slower ratio for 2024.

C. RQ3. What are the top publication venues?

Table III presents the top 10 publication venues based on Q#1 results. The top 5 publication venues accumulate $\approx 12.7\%$ of the total publications. IEEE (positions #1, #2, #3) and Springer (positions #4, #5) are the top related publishers. Journals lead the publication venues being present in the first three positions.

D. RQ4. What publications have been highly cited?

In Table IV, we present the top 10 publications based on citations per year. Results show that surveys are among the most cited (5 publications from the top 10); the most cited publications concern Machine Learning; "IIoT" is mentioned in 3 publications, while "cybersecurity" is not mentioned in the top 10.

TABLE III
TOP PUBLICATION VENUES 2014 TO 2024[a]

Publication venue (publisher)	Quantity	Percentage
IEEE Access (IEEE)	389	3.09%
IEEE Internet of Things Journal (IEEE)	368	2.93%
IEEE Transactions on Industrial Informatics (IEEE)	288	2.29%
Lecture Notes in Computer Science (Springer)	287	2.28%
Lecture Notes in Networks and Systems (Springer)	263	2.09%
ACM International Conference Proceeding Series (ACM)	202	1.61%
Sensors (MDPI)	182	1.45%
Communications in Computer and Information Science (Springer)	153	1.22%
Electronics - Switzerland (MDPI)	118	0.94%
Advances in Intelligent Systems and Computing (Springer)	110	0.87%
Others	10,216	81.23%

[a]Retrieved January 24th, 2025.

TABLE IV
TOP 10 CITED PUBLICATIONS FROM 2014 TO 2024[a]

Average citations per year	Citation count	Publication title
615	2,461	Machine Learning: Algorithms, Real-World Applications and Research Directions [13]
255	1,788	Industrial internet of things: Challenges, opportunities, and directions [14]
253	1,266	A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems [15]
230	2,302	The internet of things for health care: A comprehensive survey [16]
211	1,480	On blockchain and its integration with IoT. Challenges and opportunities [17]
183	1,468	DDoS in the IoT: Mirai and other botnets [18]
179	719	Federated Learning for Internet of Things: A Comprehensive Survey [19]
175	876	Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT [20]
160	961	Blockchain for Internet of Things: A Survey [21]
150	1,055	The industrial internet of things (IIoT): An analysis framework [22]

[a]Retrieved January 23rd, 2025.

E. RQ5. What recent surveys are the most cited?

The recent surveys of IIoT cybersecurity have been retrieved by means of Query #2 (see Lis. 2). From the outcome of 68 publications, we chose the top 10 highest cited in terms of average citation per year and presented them in Table V.

The top cited recent surveys focus separately on "cybersecurity" and "IIoT". Only one publication mentions both "cybersecurity" and "IIoT" in the title. "Blockchain" appears 4 times being the most recurrent topic, while machine-learning-related terms appear 3 times. Chaotic-map-related terms appear 2 times.

TABLE V
TOP 10 CITED SURVEYS FROM 2022 TO 2024[a]

Average citations per year	Citation count	Publication title
64	194	Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review [23]
45	135	Cybersecurity Awareness in the Context of the Industrial Internet of Things: A Systematic Literature Review [24]
35	70	Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects [25]
21	63	Analysis of ToN-IoT, UNW-NB15, and Edge-IIoT Datasets Using DL in Cybersecurity for IoT [26]
16	32	CMAF-IIoT: Chaotic Map-Based Authentication Framework for Industrial Internet of Things [27]
15	46	Secure Blockchain Middleware for Decentralized IIoT towards Industry 5.0: A Review of Architecture, Enablers, Challenges, and Directions [28]
14	44	IIoT implementation challenges: analysis and mitigation by blockchain [29]
13	26	Cybersecurity for Blockchain-Based IoT Systems: A Review [30]
12	36	Enhancing Cybersecurity Policies with Blockchain Technology: A Survey [31]
8	25	Secure Smart Healthcare Monitoring in Industrial Internet of Things (IIoT) Ecosystem with Cosine Function Hybrid Chaotic Map Encryption [32]

[a]Retrieved February 11th, 2025.

F. RQ6. Which are the main research clusters?

The network map presented in Fig. 2 is based on the keyword co-occurrence analysis. The identified clusters are:

- Cluster 1 (15 items): blockchain, security, cryptography, authentication, decision processes, data administration, and computing technologies.
- Cluster 2 (14 items): network security, industrial IoT, intrusion detection, and machine learning.
- Cluster 3 (13 items): embedded systems and cyber-physical systems, artificial intelligence, security of systems and data, and big data.
- Cluster 4 (8 items): automation, network architecture, intelligent buildings, wireless sensor networks, and energy usage.

It can be seen that cluster 1 deals mainly with data and access security; cluster 2 , with attacks and security breaches; cluster 3 , with systems and failures in the industry; and cluster 4 , with use cases and network architectures. However, boundaries are porous and some words are shared between different clusters.

In Fig. 2, the main connections related to "cybersecurity" are "network security," "machine learning," "intrusion detection," "embedded systems," "industry 4.0," and "cyber-attacks". While "industrial internet of things" is mainly linked with "network security," "blockchain," "cryptography," "authentication," "intrusion detection," and "deep learning". The following observations fall into place:

- "cybersecurity" and "industrial internet of things" belong to Cluster 2
- "cybersecurity" and "industrial internet of things" have strong links with "network security" and "intrusion detection"
- "cybersecurity" has higher intensity links with keywords from Cluster 3 than "industrial internet of things"
- "industrial internet of things" has higher intensity links with keywords from the Cluster 1 than "cybersecurity"
- "cybersecurity" and "industrial internet of things" establish a link with machine-learning-related keywords: "cybersecurity" with "machine-learning"; "industrial internet of things" with "deep learning"

The network map shows the top 50 keywords for clarity purposes. The remaining ones ($\approx 30,100$), while less representative, also hold information of current and potential promising research directions.

G. RQ7. What are the most popular topics?

We assume a semantic equivalence between topics and the processed keywords. The top 20 keywords are presented in Table VI. The information of the table has been acquired during the set up of the network map.

The keyword "internet of things" (6,697 occur.) tops the rank, followed in second place by "network security" (3,293 occur.). "industrial iot" (1,630 occur.), "blockchain" (1,614 occur.), "security" (1,498 occur.), "cybersecurity" (1,307 occur.) come along as those with over 1,000 occurrences.

TABLE VI
TOP 20 MOST RECURRENT TOPICS

Occur.	Topic	Occur.	Topic
6,997	1 internet of things	737	3 embedded systems
3,293	2 network security	724	2 deep learning
1,630	2 industrial iot	699	4 automation
1,614	1 blockchain	694	3 industry 4.0
1,498	1 security	642	1 data privacy
1,307	2 cybersecurity	638	1 digital storage
938	1 cryptography	625	2 learning systems
868	1 authentication	549	1 cloud-computing
858	2 machine-learning	543	4 network architecture
768	2 intrusion detection	527	1 information management

Out of the 20 topics, 16 are concentrated in 2 clusters: 9 in Cluster 1 , 7 in Cluster 2 .

H. RQ8. What are the publication trends of popular topics?

Fig. 3 illustrates the publication trends. The keywords selected for the analysis are: "blockchain," "cryptography," "authentication," "machine-learning," "intrusion detection," and "embedded systems". The non selected keywords are "internet of things," "network security," "industrial iot," "security," and "cybersecurity".

Every selected keyword has been used to identify publications per year. The results show "blockchain" as the most popular topic, while both "machine learning" and "intrusion

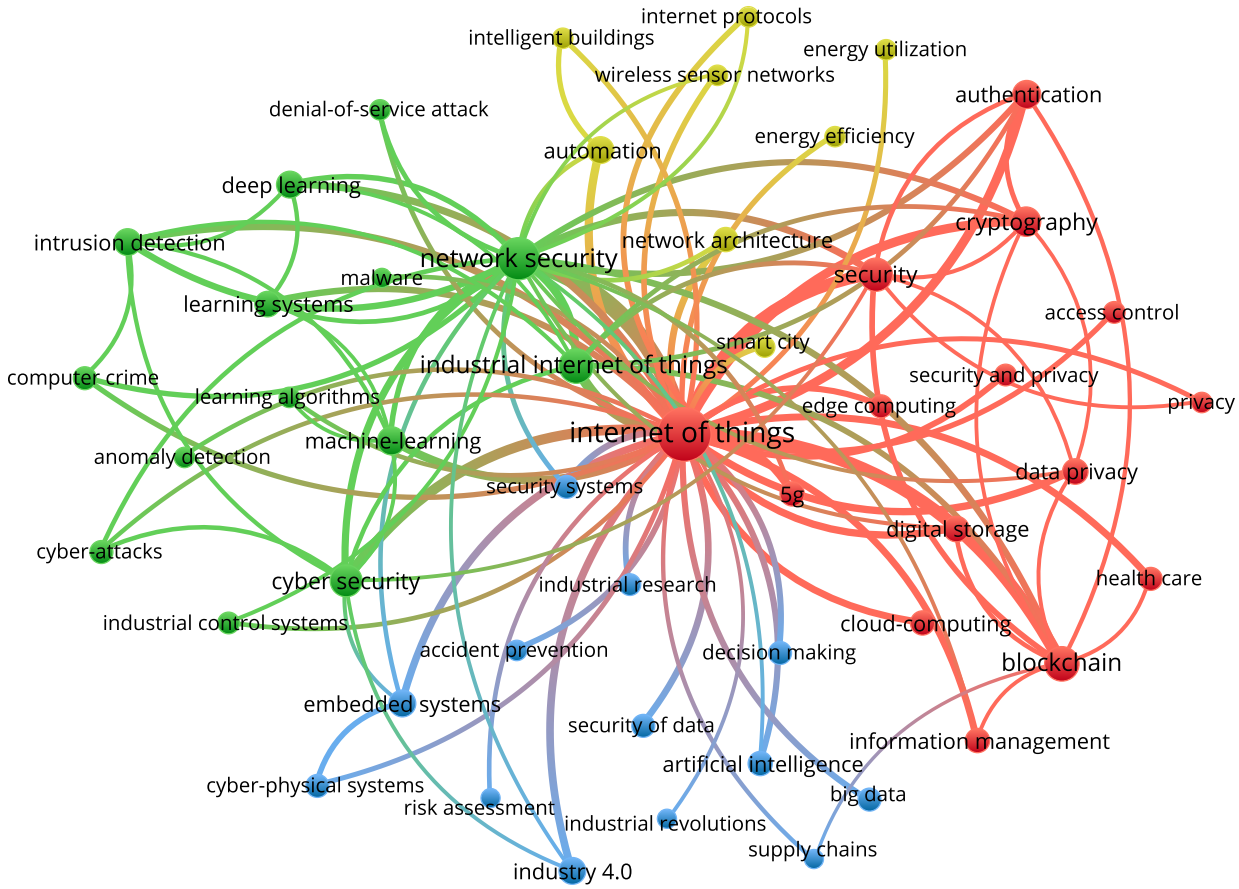

Fig. 2. Network map based on keyword co-occurrence.

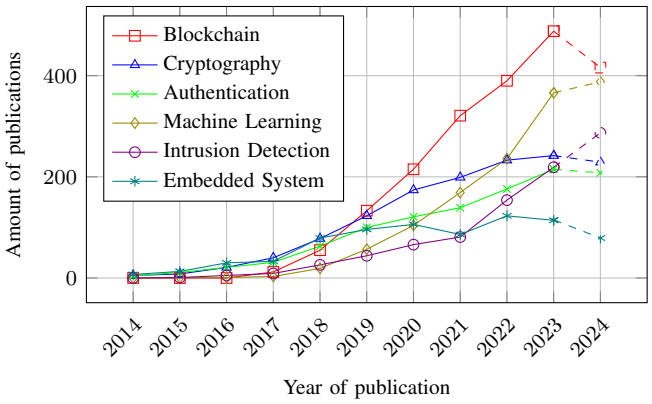

Fig. 3. Amount of publications per topic per year (retrieved Jan. 24th 2025)

detection" are the only ones that increase their publications per year.

Table VII shows the code used to tailor Q#1. Each line combined with an AND operator provides the specific combinations to retrieve the data for Fig. 3.

TABLE VII
TOPIC SPECIFIC QUERIES

Query focus	Code added to Q#1
Blockchain	`KEY ( block-chain OR blockchain )`
Cryptography	`KEY ( cryptograph* )`
Authentication	`KEY ( authentication )`
Machine learning	`KEY ( machine W/0 learning )`
Intrusion detection	`KEY ( intrusion W/0 detection )`
Embedded systems	`KEY ( embedded w/0 system* )`

V. CONCLUSIONS

In this article, we provided a bibliometric analysis of Industrial IoT cybersecurity. This work is based on a methodological approach, eight Research Questions, and the statistical analysis of over 12,000 publications from 2014 to 2024.

The research findings reveal that conference papers and journal articles are the equally dominant publication types (RQ1), with IEEE and Springer leading the way between publishers (RQ2, RQ3). Among the most cited publications, "blockchain" is the prevailing topic (RQ4, RQ5). Keyword co-occurrence analysis reveals four thematic clusters and their top keywords: 1 "blockchain," "security"; 2 "network security," "industrial IoT"; 3 "embedded systems," "cyber-physical systems"; and 4 "automation," "network architecture" (RQ6). Clusters 1 and 2 are the most prominent (RQ7); "machine learning" and "intrusion detection" are the only topics that show a positive publication rate over the whole

analysis period, dominated by "blockchain" despite having a decrease in 2024 (RQ8).

Future research could focus on identifying industry-related communication technologies in IIoT cybersecurity, as 5G is the only communication technology present on the network map. Another research path could be assessing and correlating current network industry standards with technology requirements for the secure implementation of IIoT systems since no standards have arisen within the clusters.

ACKNOWLEDGMENT

This work was supported by Région Pays-de-la-Loire and La Roche-sur-Yon Agglomération and partially by the French National Research Agency under the France 2030 label (NF-HiSec ANR-22-PEFT-0009).

REFERENCES

[1] S. N. Swamy and S. R. Kota, "An Empirical Study on System Level Aspects of Internet of Things (IoT)," *IEEE Access*, vol. 8, pp. 188 082–188 134, 2020. doi:10.1109/ACCESS.2020.3029847

[2] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The Industrial Internet of Things (IIoT): An Analysis Framework," *Computers in Industry*, vol. 101, pp. 1–12, Oct. 2018. doi:10.1016/j.compind.2018.04.015

[3] R. J. Raimundo and A. T. Rosário, "Cybersecurity in the Internet of Things in Industrial Management," *Applied Sciences*, vol. 12, no. 3, p. 1598, Feb. 2022. doi:10.3390/app12031598

[4] G. Mwansa and N. Mabanza, "Review of Internet of Things Security Protocols – A Bibliometric Analysis," in *2023 25th International Conference on Advanced Communication Technology (ICACT)*. Pyeongchang, Korea, Republic of: IEEE, Feb. 2023, pp. 394–400. doi:10.23919/ICACT56868.2023.10079641

[5] J. Y. Lee and J. Lee, "Current Research Trends in IoT Security: A Systematic Mapping Study," *Mobile Information Systems*, vol. 2021, pp. 1–25, Mar. 2021. doi:10.1155/2021/8847099

[6] S. F. Chevtchenko *et al.*, "Anomaly Detection in Industrial Machinery Using IoT Devices and Machine Learning: A Systematic Mapping," *IEEE Access*, vol. 11, pp. 128 288–128 305, 2023. doi:10.1109/ACCESS.2023.3333242

[7] A. Alnajim, S. Habib, M. Islam, S. Thwin, and F. Alotaibi, "A Comprehensive Survey of Cybersecurity Threats, Attacks, and Effective Countermeasures in Industrial Internet of Things," *Technologies*, vol. 11, no. 6, p. 161, Nov. 2023. doi:10.3390/technologies11060161

[8] D. Reyes Domínguez, M. B. Infante Abreu, and A. L. Parv, "Main Trend Topics on Industry 4.0 in the Manufacturing Sector: A Bibliometric Review," *Applied Sciences*, vol. 14, no. 15, p. 6450, Jul. 2024. doi:10.3390/app14156450

[9] B. Kitchenham and S. Charters, "Guidelines for Performing Systematic Literature Reviews in Software Engineering," Keele University, United Kingdom, EBSE Technical Report EBSE-2007-01, Jul. 2007.

[10] I. Dasso, "Industrial IoT Cybersecurity: A Bibliometric Analysis (Code and Data)," Zenodo, Apr. 2025. Available: https://doi.org/10.5281/ZENODO.15305102. doi:10.5281/ZENODO.15305102

[11] L. Waltman, N. J. Van Eck, and E. C. Noyons, "A Unified Approach to Mapping and Clustering of Bibliometric Networks," *Journal of Informetrics*, vol. 4, no. 4, pp. 629–635, Oct. 2010. doi:10.1016/j.joi.2010.07.002

[12] A. Perianes-Rodriguez, L. Waltman, and N. J. Van Eck, "Constructing Bibliometric Networks: A Comparison between Full and Fractional Counting," *Journal of Informetrics*, vol. 10, no. 4, pp. 1178–1195, Nov. 2016. doi:10.1016/j.joi.2016.10.006

[13] I. H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," *SN Computer Science*, vol. 2, no. 3, p. 160, May 2021. doi:10.1007/s42979-021-00592-x

[14] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018. doi:10.1109/TII.2018.2852491

[15] L. Chettri and R. Bera, "A Comprehensive Survey on Internet of Things (IoT) Toward 5G Wireless Systems," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 16–32, Jan. 2020. doi:10.1109/JIOT.2019.2948888

[16] S. M. Riazul Islam, Daehan Kwak, M. Humaun Kabir, M. Hossain, and Kyung-Sup Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," *IEEE Access*, vol. 3, pp. 678–708, 2015. doi:10.1109/ACCESS.2015.2437951

[17] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On Blockchain and Its Integration with IoT. Challenges and Opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, Nov. 2018. doi:10.1016/j.future.2018.05.046

[18] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017. doi:10.1109/MC.2017.201

[19] D. C. Nguyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, and H. Vincent Poor, "Federated Learning for Internet of Things: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 3, pp. 1622–1658, 2021. doi:10.1109/COMST.2021.3075439

[20] Y. Lu, X. Huang, Y. Dai, S. Maharjan, and Y. Zhang, "Blockchain and Federated Learning for Privacy-Preserved Data Sharing in Industrial IoT," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4177–4186, Jun. 2020. doi:10.1109/TII.2019.2942190

[21] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for Internet of Things: A Survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, Oct. 2019. doi:10.1109/JIOT.2019.2920987

[22] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The Industrial Internet of Things (IIoT): An Analysis Framework," *Computers in Industry*, vol. 101, pp. 1–12, Oct. 2018. doi:10.1016/j.compind.2018.04.015

[23] M. Abdullahi *et al.*, "Detecting Cybersecurity Attacks in Internet of Things Using Artificial Intelligence Methods: A Systematic Literature Review," *Electronics*, vol. 11, no. 2, p. 198, Jan. 2022. doi:10.3390/electronics11020198

[24] A. Corallo, M. Lazoi, M. Lezzi, and A. Luperto, "Cybersecurity Awareness in the Context of the Industrial Internet of Things: A Systematic Literature Review," *Computers in Industry*, vol. 137, p. 103614, May 2022. doi:10.1016/j.compind.2022.103614

[25] I. H. Sarker, "Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects," *Annals of Data Science*, vol. 10, no. 6, pp. 1473–1498, Dec. 2023. doi:10.1007/s40745-022-00444-2

[26] I. Tareq, B. M. Elbagoury, S. El-Regaily, and E.-S. M. El-Horbaty, "Analysis of ToN-IoT, UNW-NB15, and Edge-IIoT Datasets Using DL in Cybersecurity for IoT," *Applied Sciences*, vol. 12, no. 19, p. 9572, Sep. 2022. doi:10.3390/app12199572

[27] M. Tanveer, A. Badshah, A. U. Khan, H. Alasmary, and S. A. Chaudhry, "CMAF-IIoT: Chaotic Map-Based Authentication Framework for Industrial Internet of Things," *Internet of Things*, vol. 23, p. 100902, Oct. 2023. doi:10.1016/j.iot.2023.100902

[28] J. Leng *et al.*, "Secure Blockchain Middleware for Decentralized IIoT towards Industry 5.0: A Review of Architecture, Enablers, Challenges, and Directions," *Machines*, vol. 10, no. 10, p. 858, Sep. 2022. doi:10.3390/machines10100858

[29] R. Kumar, R. Sindhwani, and P. L. Singh, "IIoT Implementation Challenges: Analysis and Mitigation by Blockchain," *Journal of Global Operations and Strategic Sourcing*, vol. 15, no. 3, pp. 363–379, Aug. 2022. doi:10.1108/JGOSS-08-2021-0056

[30] R. Alajlan, N. Alhumam, and M. Frikha, "Cybersecurity for Blockchain-Based IoT Systems: A Review," *Applied Sciences*, vol. 13, no. 13, p. 7432, Jun. 2023. doi:10.3390/app13137432

[31] A. Kumar and I. Sharma, "Enhancing Cybersecurity Policies with Blockchain Technology: A Survey," in *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*. Uttar Pradesh, India: IEEE, Dec. 2022, pp. 1050–1054. doi:10.1109/IC3I56241.2022.10072588

[32] J. Khan *et al.*, "Secure Smart Healthcare Monitoring in Industrial Internet of Things (IIoT) Ecosystem with Cosine Function Hybrid Chaotic Map Encryption," *Scientific Programming*, vol. 2022, pp. 1–22, Mar. 2022. doi:10.1155/2022/8853448