Journal of Theoretical and Applied Information Technology
15th May 2022. Vol.100. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SYSTEMATIC DESCRIPTION OF THE INTERNET OF THINGS: A BIBLIOMETRIC ANALYSIS

M. IZHAM JAYA, *MOHD FAIZAL AB RAZAK, DANAKORN NINCAREAN EH PHON, SYIFAK IZHAR HISHAM, AHMAD FIRDAUS

Faculty of Computing, College of Computing and Applied Sciences, Universiti Malaysia Pahang,

26600 Pekan, Malaysia

Corresponding Author: [1]faizalrazak@ump.edu.my

ABSTRACT

The explosive progress of the Internet of Things (IoT), such as smart watches, medical implants, and smart refrigerators, has empowered researchers to view these developments of science and technology from the research perspective. The breakthrough of accelerated technologies has helped to reshape global research patterns in IoT. Despite the many articles published in research, there is, however, still a lack of bibliometric reports that demonstrate the comprehensive research patterns of the IoT. This study seeks to assess the world's research activities on the IoT by observing the gaps through a thorough research pattern of the IoT research practices. The analysis of more than 1000 articles that were published between 2009 to 2019 in the ISI Web of Science (WoS) database was performed through the bibliometric approach. The outcome showed the global research pattern of the activities in the following forms: notable journals, foremost articles, research areas, influential institutions, most prolific countries, authors productivity, keywords and network collaborations. A closer inspection of the bibliometric analysis also showed that a comprehensive analysis is significant for measuring the degree of activity in research patterns.

Keywords: *Bibliometric, Internet of Things, Security, Review, Web of Science*

1. INTRODUCTION

The Internet of Things (IoT), as a unique platform, has drawn significant considerations, with its ability to connect users to "Things" using the network infrastructure. By connecting devices or "Things" through the Internet, users have the potential to control and administer their devices from a distance. This has advanced the evolution of the IoT internet-connected technologies, such as the execution of persons and assets tracking, as well as a secure smart home implementation. As an example, [1] has utilizes the IoT based coordinate locator to track persons based on the user determined geofence area. On the other hand, [2] has enhanced the security of IoT devices in smart home environments using the G2F authentication framework. In an attempt to show the growth of the IoT technologies, this study highlights some statistics drawn from various reports and documents.

Gartner Inc. had forecasted that the global government IoT revenue would grow to $21 billion in 2022, an increment of 22% when compared to the projected total in 2021 [3]. The IoT technology holds a significant potential in the infrastructure and assets monitoring as well as to improve citizens' safety. In the present context of Covid-19 spread, control measure and quarantine compliance has demanded a secure and reliable IoT's technology, making it the most challenging topic today.

With the proliferation of the IoT comes the danger of the IoT devices becoming a potentially powerful platform for cyberattacks. Confidentiality, Integrity and Availability (CIA) triads have been well discussed in a number of literature reviews. This phenomenon seems to be immature for the IoT but there are challenges in the compromising of the critical system because not all possible attack paths have been fully assessed [4], [5]. With cyberattacks on the IoT, researchers need to find ways to protect the confidential data from being leaked or harmed. Some notable cyberattacks are traced to the Denial of Service (DoS), man in the middle, malicious insider, and session hijacking attacks. These cyberattacks demonstrate that there is a potential for research to be conducted. Nonetheless, despite so many articles being published in support of such cyberattacks, many of the bibliometric articles, until today, have not really dealt with the research patterns.

Bibliometric analysis is a technique used to uncover evidence that would reveal the research patterns of issues being examined. For the computer security community, uncovering similar studies and their research patterns would be beneficial for the

progress of the research community. In that regard, this study aims to provide a bibliometric analysis on IoT research particularly from the perspective of IoT security. Various interests and potential perspectives of literature survey are presented in the visualization and interpretation phase. Using the bibliometric analysis method offers several advantages: (1) Readers are able to focus on the research trend and innovation; (2) Authors are able to show their productivity in publishing research articles; (3) Institutions are able to access the intellectuals of such research, thereby attracting institution collaborations; and (4) Others are able to assess the research activities of specific active fields, and the country's leading in such research.

With the intention of highlighting the growth of the IoT domain, this study sets out to implement a comprehensive assessment of the domain by evaluating the IoT research published in the Web of Science (WoS), from 2009 to 2019. The method includes the assessment of the IoT study, the publication patterns, the research topics, and the assessment of the network traffic. To achieve the aim of this study, the research questions were formulated as follows: (a) What is the trend of the IoT publications in the global context? and (b) How would this uncovered trend assist in demonstrating the future direction of the IoT study?

Table 1 describe recent literature that is related to the IoT and employs a bibliometric approach to outline the progress of specific fields in the IoT, such as irrigation in agriculture [6], smart cities [7], and edge computing [8].

Table 1: Recent Literature That Related to IoT and Employed a Bibliometric Approach.

References	Title	Aim
[9]	Bibliometric and content analysis of the internet of things research: a social science perspective	To identify current trends in IoT research
[6]	An overview of the internet of things (IoT) and irrigation approach through bibliometric analysis	To outline the progress of IoT implementation in irrigation approaches.
[7]	Internet of Things and Smart Cities: A Bibliometric Analysis	To gain a broad perspective, using bibliometric data on IoT in smart city implementation.
[8]	Bibliometric Analysis of Scientific Productivity around Edge Computing and the Internet of Things	To identify the progress and review the performance of edge computing in the IoT research.

As compared to the previous literature in Table 1, this paper provides a comprehensive bibliometric analysis to highlight the changes in the IoT research landscape. Nevertheless, the bibliometric approach in this study extensively covers the following:

i. This study extracted 1,731 studies from the WoS database which comprised ISI-indexed papers, for the IoT bibliometric assessment.

ii. The experiment considers the IoT research effort which was documented in numerous types of documents.

iii. This study examines the IoT research among countries and the respective continents rather than any specific location or region. This was done by analysing the total number of articles and publications within each continent.

iv. This study highlights three significant network connections: (a) Author collaboration network; (b) Keyword occurrence network; and (c) Affiliation collaboration network. The network connection variable was applied to highlight the relationship between the authors, the keywords, and their affiliations.

The organization of this paper is as follows. Section 2 describes the related bibliometric studies. Section 3 demonstrates the research methodology. Section 4 provides the growth and finding of the IoT, and Section 5 highlights the network collaborations among institutions throughout the world.

2. RELATED WORKS

The construction of scientific knowledge can be estimated, analyzed, and visualized by using the bibliometric approach [10], [11]. Several lines of evidence also suggest that the bibliometric approach can be used to study the growth of the desired field in a specific area of knowledge [11]. Using this approach, several features are essential for evaluating the publication components including: the impact factor, citations, publishers, and countries of publication [12], [13]. Table 2 highlights the various studies which had employed the bibliometric approach, nevertheless, there are differences between previous studies and the current study especially on the field of interest.

Table 2: Previous Studies That Employed a Bibliometric Approach.

Authors	Fields	Year
[14]	IoT	2021
[15]	IoT	2021
[16]	Blockchain	2019
[17]	Malware	2016

3. METHODOLOGY

Bibliometric is a technique used to analyse the evolution of academic literature within a particular research area in a certain period using quantitative methods. Since the research topic is limited, the quality criteria should be clearly determined beforehand by selecting suitable empirical metrics and statistical methods for the analysis. As such, the bibliometric approach used in this study involves a thorough investigation of the articles, focusing on specific indicators such as citations, leading journals, publishers, impact factors, institutions, and countries of publication. Centering on the security domain of the IoT, this study aims to deliver a comprehensive analysis of this field. Figure 1 presents the methodology and the phases employed.

3.1 Selection Criteria

At the data collection stage of this study, the ISI WoS database was considered as the main source of collection. The vital aspects of the data collection encompassing details about the author, the leading journals, the articles published, and the countries involved were then sourced from the WoS Core Collection, a database that has been considered by the research community to be of reputation and recognition. The keywords used to identify the related articles include "IoT" and "network security". To widen the analysis and to have the most relevant information, the most frequently used keywords appearing in the titles and abstracts of those retrieved publications were also considered and searched for in the database. During the search, the publication period was limited from the year 2009 to 2019. From this search, we net a total of 13,375 articles from several journals, books, articles, and conferences. To remove the unrelated articles, such as non-English articles, an exclusion was performed, following which, a total of 1,731 articles remained for further analysis. The exclusion criteria performed in this study is outlined from [18] and described below:

a) Articles published in language other than English.
b) Articles that are not related to IoT domain.
c) Duplicate and erroneous entries.

The validity of chosen articles is confirmed by cross-checking among participating researchers. In a group discussion among the researchers, a random sample of collected articles was confirmed based on the stated criterial. In the instance of contradictory opinion, a dialogue had taken place, and mutual agreement had been reached.

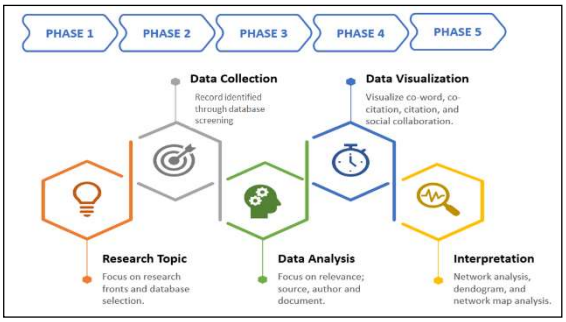

Figure 1: The Methodology Phases.

3.2 Data Analysis

To accomplish the analysis, this study takes into account several additional indicators, such as h-index, number of articles published by the author, total number of citations, and citations per article. These indicators were essential as they were always associated with the significance of the authors, journals, articles, institutions, and countries. As such, the cumulative impact of an author is evaluated using the h-index. In addition, the total number of citations is considered as the sum number of citations received by the articles in a certain period and somehow depended on the contributions made by those articles. The selected indicators also facilitated a complete analysis of the main authors, journals, articles, institutions, and countries. Information related to the selected indicators were then extracted from the articles and analysed to examine the knowledge structure, authors productivity and development of the research area. Moreover, the growth of the research area was demonstrated by emphasizing on the authors, institutions, and countries that had made major contributions to the development.

Lastly, the mapping technique was implemented to visualise the bibliometric maps and illustrate the quantitative data systematically. To visualize the results, this study used an open-source statistical application known as R tool which also provides numerous methods of data visualisation. This software has been widely used for evaluating research information.

4. BIBLIOMETRIC ANALYSIS

This section deliberates on the growth of the IoT research area. The emergence of Industrial Revolution 4.0 (IR 4.0) has significantly increased the number of research in IoT especially within the

scientists and universities community. As one of the nine principal technologies that drive the IR 4.0, research in IoT is mostly centered on the communication between devices, process automation, and analytics targeted to improve operational efficiencies. Therefore, analysis of the most notable article, author, journal, institution, and country, would further expand the growth of IoT research by providing insights and evidence-based description of the impact from the existing research. The category of publication that was analysed in this study is described in Table 3.

Table 3: Category of Publication.

Publication	Results
Article	1,584
Review	111
Proceeding article	25
Editorial material	11
Total	**1,731**

It is noted that the article-type had the highest number of publications, with a total of 1,584 articles. The next in line was the review-type publications with 111 publications followed by the proceeding article-type publications (25) and the editorial materials (11). The diverse number of publications may be due to several factors. For instance, the small number of editorial materials is expected due to the nature that these publications provide less scientific views of a specific person, group, or organization. Its low frequency is also related to the fact that this publication only includes material derived from a small number of invited authors and preface from the editorial board.

4.1 The Most Notable Journals in the IoT Research

Journal publishers provide the researchers with a platform to share their findings with the society, with hope that the findings will improve the body of knowledge on a particular research area. In this context, the substance of IoT research can be traced to the number of articles that were published in the impactful journals. Metrics such as quartile, impact factor, impact metrics, rank, and number of citations determine the impact of a particular journal and how influential the journal is. Based on the numbers of publication involved in this study, Table 4 describes the top-20 journals that had

Table 4: 20 Most Notable Journals in IoT.

Journal	Publications	Quartile	Impact Factor	Impact Metrics	Rank	Reference	Citation
IEEE Access	232	Q1	4.098	20,879	50/893	253,013	5,521
IEEE Internet of Things Journal	168	Q1	9.515	6,119	63/413	17,720	784
Sensors	163	Q1	3.031	46,222	44/527	177,731	8,326
Future Generation Computer Systems-The International Journal of Escience	89	Q1	5.768	10,230	31/413	30,805	1,592
Security And Communication Networks	49	Q2	1.376	2,025	145/413	9,313	104
Journal Of Network and Computer Applications	45	Q1	5.273	6,959	58/413	12,908	547
Computer Networks	41	Q1	3.03	10,122	32/413	13,546	342
International Journal of Distributed Sensor Networks	38	Q1	1.614	4,131	83/413	8,611	144
Wireless Personal Communications	36	Q1	0.929	5,256	68/413	23,552	658
Ad Hoc Networks	29	Q1	3.49	5,084	70/413	5,365	145
IEEE Transactions on Industrial Informatics	29	Q1	7.377	13,187	83/893	17,639	1,484
IEEE Communications Surveys and Tutorials	26	Q1	22.973	16,408	16/413	21,366	822
International Journal of Communication Systems	25	Q2	1.278	1,863	419/893	10,466	245
Wireless Communications & Mobile Computing	25	Q1	1.396	3,421	99/413	19,176	229
IEEE Communications Magazine	24	Q1	10.356	24,753	9/413	4,380	397
IEEE Sensors Journal	24	Q1	3.076	18,838	57/893	36,945	2,320
Computers & Security	21	Q1	3.062	3,684	90/413	10,370	253
Journal of Supercomputing	20	Q1	2.157	3,374	101/413	11,227	402
Applied Sciences- Basel	19	Q1	2.217	5,955	211/893	109,246	1,378
Transactions on Emerging Telecommunications Technologies	18	Q3	1.258	1,013	230/413	5,532	168

published research related to the IoT from 2009 until 2019.

Among the top 20 journals listed, 17 journals are in the first quartile of WoS database with the highest impact factor of 22.973 (IEEE Communications Surveys and Tutorials) and the lowest impact factor of 0.929 (Wireless Personal Communications). The IEEE Access journal (impact factor of 4.098) published the highest number of publications on the IoT. A total of 232 articles were published in this journal with the total number of citations accumulated to 5,521. On the second rank is the IEEE Internet of Things Journal which published a total of 168 publications and held an impact factor of 9.515 which remarked the significant impact of the published articles towards the research area. It is worth noting that the articles published in these journals have undergone rigorous quality assessment to maintain journals reputation. Nonetheless, the Applied Sciences - Basel and Transactions on Emerging Telecommunications Technologies, had the lowest number of publications, 19 and 18 publications, respectively. Further description on the growth of publications from 2009 to 2019 is illustrated in Figure 2.

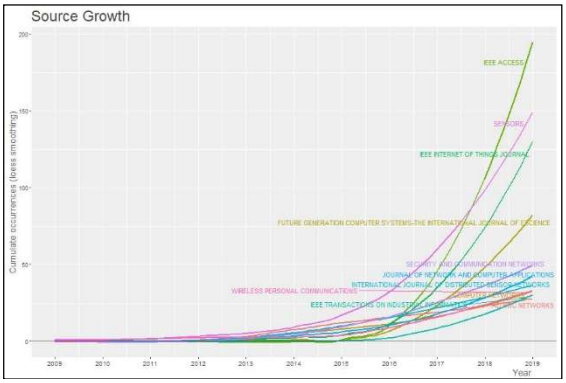

Figure 2: The Growth of Publications From 2009 to 2019

4.3 The Most Notable Articles in the IoT Research

Contributions made by several researchers have notably influence the growth of the IoT

Table 5: Top-20 Publications in IoT Research.

Title	Journal	Time cited	Year	Ref.
Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions	Future Generation Computer Systems-The International Journal of EScience	3,433	2013	[19]
The Internet of Things for Health Care: A Comprehensive Survey	IEEE Access	574	2015	[20]
Security, Privacy and Trust in Internet of Things: The Road Ahead	Computer Networks	474	2015	[21]
Internet of Things: Applications and Challenges in Technology and Standardization	Wireless Personal Communications	456	2011	[22]
Implementing Smart Factory of Industries 4.0: An Outlook	International Journal of Distributed Sensor Networks	453	2016	[23]
A Survey on Trust Management for Internet of Things	Journal Of Network and Computer Applications	393	2014	[24]
Security of the Internet of Things: Perspectives and Challenges	Wireless Networks	367	2014	[25]
On The Features and Challenges of Security and Privacy in Distributed Internet of Things	Computer Networks	365	2013	[26]
A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications	IEEE Internet of Things Journal	352	2017	[27]
Securing the Internet of Things	Computer	285	2011	[28]
The Promise of Edge Computing	Computer	213	2016	[29]
Mobile Edge Computing: A Survey	IEEE Internet of Things Journal	197	2018	[30]
Multimedia Traffic Security Architecture for The Internet of Things	IEEE Network	195	2011	[31]
SVELTE: Real-Time Intrusion Detection in the Internet of Things	Ad Hoc Networks	192	2013	[32]
A Novel User Authentication and Key Agreement Scheme for Heterogeneous Ad Hoc Wireless Sensor Networks, Based on the Internet of Things Notion	Ad Hoc Networks	181	2014	[33]
State-Of-The-Art, Challenges, And Open Issues in the Integration of Internet of Things and Cloud Computing	Journal Of Network and Computer Applications	174	2016	[34]
Anonymous Authentication for Wireless Body Area Networks with Provable Security	IEEE Systems Journal	169	2014	[35]
IoT Security: Review, Blockchain Solutions, and Open Challenges	Future Generation Computer Systems-The	167	2018	[36]

Secure Integration of IoT and Cloud Computing	International Journal of Escience Future Generation Computer Systems-The International Journal of Escience	155	2018	[37]
A Survey On 5G Networks for the Internet of Things: Communication Technologies and Challenges	IEEE Access	154	2018	[38]

research since 2009 until 2019. Table 5 shows the influential articles generated from the analysis which contributed significantly to the progress of the IoT research.

As can be noted, the influential study presented by [19] in 2013, had garnered a total of 3,433 citations in the WoS Core Collection. [19] had provided the cloud centric vision for the worldwide implementation of the Internet; they also discussed the future directions of the IoT as propelled by the various applications and convergences noted in several interdisciplinary technologies. The proposed cloud implementation, known as Aneka, was based on the interaction of the private and public clouds. In this article, the authors also established a taxonomy of the IoT with IoT vision and technologies.

Another study conducted by [20] in 2015 titled "The Internet of Things for Health Care: A Comprehensive Survey" analysed the distinction of the IoT security and its privacy features which consisted of threat models, attack taxonomies, and security requirements. They further presented an intelligent collaborative security model which can reduce security risks. They then deliberated on the different innovations of the IoT from the health care perspective, including ambient intelligence, big data, and wearable devices. The question raised by this study was on the open issues and the challenges of the IoT based on health care. Their contributions were characterized by their extensive survey of the IoT based on healthcare services and applications.

Similarly, [21] presented survey-based research on the challenges and the existing solutions of IoT security. They also discussed the future research of the IoT and its open issues. This study had focused on access control, policy enforcement, authentication, confidentiality, and integrity. They also focused on privacy and trust issues in the IoT field as well as middleware and security solutions for mobile devices. The study also highlighted the importance of stable data transfer and reliable data sharing.

Interesting topics for investigating the IoT field can be traced from the influential articles with significant contributions published in the WoS Core Collection. It is vital to highlight these publications as the contributions are later expanded and published by other researchers in high impact journals. Moreover, all the published articles focusing on the IoT field as noted in the WoS Core Collection were considered vital documents because they also generate new ideas and new knowledge for the research community. The following section discusses the most influential authors detected from the analysis.

4.4 The 20 Most Influential Authors

A number of authors have contributed to the growth of IoT research. As researchers, these authors were required to publish their research discoveries to disseminate their findings as well as to stay relevant within the research community. The word "publish or perish" is a mutual phrase used to demonstrate the importance of writing and publishing. This, therefore, shows that the authors were simultaneously dealing with the increased pressure to publish besides conducting research. Table 6 lists the most influential researchers in the field of IoT.

It can be noted that the most productive researcher, Choo KKR, was from the Beijing University, and he had published in the Posts and Telecommunication journal which originated from the United States. Choo KKR has 27 articles written about the IoT. Another author, Rodrigues JJPC, had also achieved considerable high productivity, but lesser in comparison to Choo KKR. Rodrigues JJPC was from Brazil, but his affiliation was based at the Soonchunhyang University, South Korea. Other authors with a similar number of publications (15 articles) were Kumari S, Park JH, You I, and Zeadally S.

Table 6: Foremost 20 authors in IoT.

Authors	Articles	Authors-Fractionalized	Articles Fractionalized	Countries	Affiliation
Choo KKR	27	Wang Y	18.04	US	Beijing Univ Posts and Telecommunication
Rodrigues JJPC	22	Li J	5.0	Brazil	Soonchunhyang Univ
Li X	18	Li X	22.0	China	King Saud Univ
Kumar N	16	Chen J	25.19	India	Hunan Univ Sci. and Technology
Zhang Y	16	X Xu	25.13	US	Arizona State University
Kumari S	15	X Li	27.4	India	Ch. Charan Singh University
Park JH	15	Liu X	10.67	Korea	Xi An Jiao Tong Univ
You I	15	Zeadally S	5.27	Korea	Soonchunhyang University
Zeadally S	15	You I	27.93	USA	University of Kentucky
Das AK	14	M Wazid	12.5	India	International Institute of Information Technology Hyderabad
Guizani M	13	Kim S	9.23	Qatar	Huazhong Univ Sci and Technol
Conti M	12	S Roy	16.5	Italy	University of Padua
Liu Y	11	Zhang J	2.27	US	Tsinghua Univ
Lopez J	11	J Zhou	79.55	Spain	Universidad de Malaga
Ma JF	11	JH Wang	11.64	China	Changzhou University
Ning HS	11	H Liu	21.0	China	University of Science & Technology Beijing
Yan Z	10	P Zhang	50.3	China	Xidian University
He DB	9	MK Khan	33.89	China	Wuhan University
Khan MK	9	K Alghatbar	16.0	Saudi Arabia	King Saud University

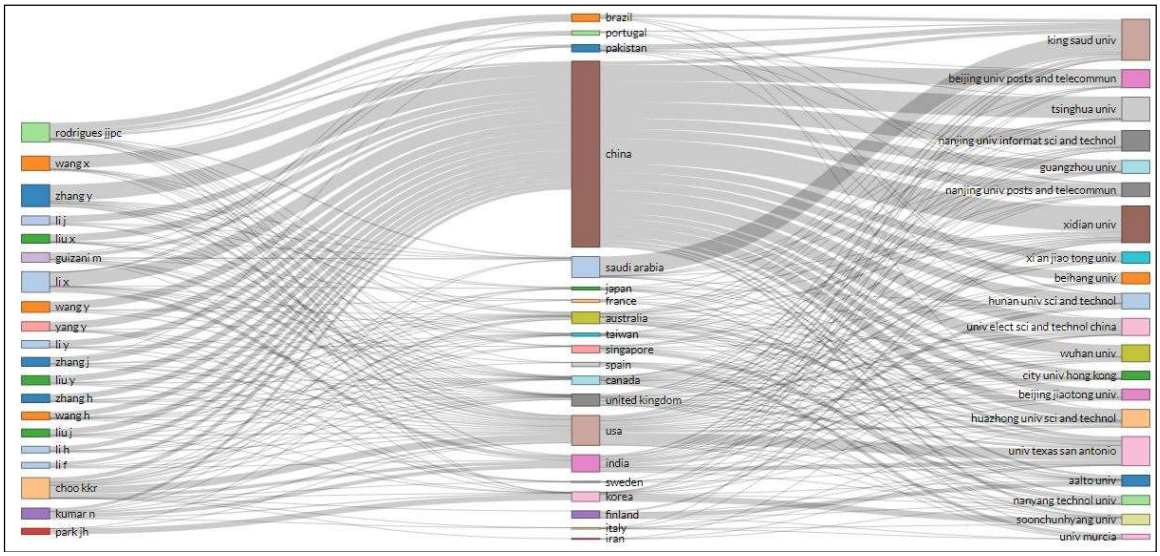

Figure 3: Relationship Between Author, Country, and Affiliation.

As Figure 3 and Table 6 demonstrate, China was noted to be considerably active in publishing articles since most of the authors were from China. It can be seen that the Asian continent of China and India were capable of contributing to numerous publications in the IoT field. The growth aspect also showed that authors from China and the United States had been the most productive in generating publications when compared to others. This prolific output showed the extensive contribution of the authors towards generating research thereby leading to article publications.

4.5 Author Productivity

To analyse the productivity of the authors, this study extracted data, such as the number of articles written, the number of authors, and the proportion of authors because rarely one article is written by a single or two authors. For every research article, it was observed that there are five authors on average. The number of authors is increased in a collaborative research project, and this raises noteworthy questions. For example, the authors' order for research articles, such as who would be the first author or the corresponding author in the articles. This is because the first or corresponding author's

list in a research article has a big impact on the good perceptions of readers and their institution, especially for the promotion and ranking. On the other hand, it would be unfair to rank authors by their relative contributions because these authors may have contributed to the research equally. Thus, in good faith, every author listed in the article ought to be credited equally since the group partnership had successfully completed a project. Table 7 lists author productivity in terms of publications.

Table 7: Author Productivity.

Articles written	Number of Authors	Proportion of Authors
1	2,813	0.754762544
2	494	0.132546284
3	160	0.04292997
4	96	0.025757982
5	55	0.014757177
6	25	0.006707808
7	22	0.005902871
8	13	0.00348806
9	11	0.002951435
10	10	0.002683123
11	3	0.000804937
12	4	0.001073249
13	6	0.001609874
14	3	0.000804937
15	2	0.000536625
16	1	0.000268312
17	1	0.000268312
18	3	0.000804937
22	1	0.000268312
23	2	0.000536625

Table 7 highlights the number of authors who have written articles in the field of IoT security. Among these authors, 2,813 authors had only published one article. 912 authors had published more than two articles within the year 2009 until 2019. All these authors contributed less than 500 articles to the IoT security field; they had produced 0.96% of publications or 10 articles on average dealing with the security of the IoT, from the year 2009 to 2019. Author productivity, as noted in the publications, showed the results of the literature growth.

4.6 The 20 Most Influential Institutions

Universities are institutions that provide the required resources for conducting research, for instance, finances and libraries. Finance has an important role to play in providing the necessary support, and in shaping the way forward for research projects. In addition to this, some universities tend to focus more on research because they want to increase the number of their publications, hence research would get more financial priorities by the authorities. Institutions may also provide research facilities such as laboratories for professional researchers, thereby assisting the way for research to be conducted, and this would bring the institutions towards becoming world-class academic institutions. Table 8 lists the institutions that had conducted the IoT related research.

Table 8: The Foremost 20 Institution in IoT.

Institutions	Articles	Countries
Xidian Univ	53	China
King Saud Univ	49	Saudi Arabia
Beijing Univ Posts and Telecommunication	34	China
Chinese Acad Sci	32	China
Univ Elect Sci and Tech. China	28	China
Univ Texas San Antonio	27	US
Soonchunhyang Univ	21	South Korea
Nanjing Univ Information Sci Technol	20	China
Wuhan Univ	20	China
Aalto Univ	19	Finland
Beijing Jiaotong Univ	19	China
Guangzhou Univ	19	China
Nanyang Technol Univ	18	Singapore
Univ Murcia	18	Spain
Univ Sci Technol Beijing	18	China
Dalian Univ Technol	17	China
Hunan Univ Sci and Technol	17	China
Tsinghua Univ	17	China
Univ Technol Sydney	17	Australia

As can be observed, all the institutions were located in seven (7) countries, encompassing: China, Saudi Arabia, the United States, South Korea, Finland, Spain, and Singapore. Institutions from China held the highest number of publications, followed by Saudi Arabia which held the second highest number of publications. It is worthy to note that Xidian University from China holds the highest number of publications comprising 53 articles which were listed in the WoS Core Collection with ISI ranking.

The subsequent institution with many publications was the King Saud University, with a total of 49 articles published under the IoT research field. Like China, all these articles were also ISI ranked. It is important to take note of the number of publications in the IoT because this raises the ranking of the university concerned. Nonetheless, it is vital to note the publication periods where most of the publications had focused on the IoT, with each period suggesting the institution's influence and contribution to the growth in the field of IoT research.

4.7 Most Influential Country Based on Continents

This section discusses the publications of the IoT in terms of countries on continents. The purpose was to observe the number of publications published between 2009 to 2019. Table 8 presents the list of continents with the number of publications. It is noted that the Asian continent was the main contributor, led by China contributing to 585 of the entire Asian continent's publications. The next prolific contributor was the continent of Europe, North America, the Middle East, Australia, and then South America. Among these continents, Africa had lesser research on the IoT.

As shown in Table 9, the continents of Asia and North America made considerable efforts in stimulating scientific research which contributed new knowledge in the IoT field that would be applicable and usable for solving society's issues. Such contributions made Asia and North America as leaders in achieving the forefront position in IoT research. While the proliferation of publications suggests achievements in the field of IoT, the lesser number of publications implied lesser research funding, and smaller number of researchers who specialised in such fields of research. Without a doubt, research funding and expertise in the form of professional researchers are important for the institution or country to make contributions.

Table 9: Continent with Publications in IoT.

List of continents	Year										
	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
Asia = 1,133 publications											
Bangladesh	0	0	0	0	0	0	0	0	0	3	1
China	0	0	3	4	8	11	18	31	73	190	247
India	0	0	1	0	0	0	3	5	24	47	100
Japan	0	0	0	0	1	1	3	2	5	16	13
Malaysia	0	0	0	0	1	0	2	1	1	6	20
Singapore	0	0	0	0	2	2	0	4	4	12	16
South Korea	1	1	0	0	1	4	6	14	27	51	65
Taiwan	0	0	1	1	2	2	4	10	11	22	17
Thailand	0	0	0	0	0	0	0	0	0	1	3
Vietnam	0	0	0	0	0	0	0	0	0	1	7
Total	1	1	5	5	15	20	36	67	145	349	489
North America = 449 publications											
Canada	1	0	0	0	1	3	5	5	13	20	38
Mexico	0	0	0	0	0	0	0	0	1	3	6
Russia	0	0	0	0	0	0	0	4	2	3	11
United States	0	0	0	0	2	5	13	16	44	118	135
Total	1	0	0	0	3	8	18	25	60	144	190
South America = 64 publications											
Brazil	0	0	0	0	0	0	0	3	6	10	30
Chile	0	0	0	0	0	1	0	0	1	1	4
Colombia	0	0	0	0	0	0	0	0	2	1	1
Ecuador	0	0	0	0	0	0	0	0	0	2	1
Uruguay	0	0	0	0	0	0	0	0	0	0	1
Total	0	0	0	0	0	1	0	3	9	14	37
Europe = 738 publications											
Austria	0	0	1	0	0	1	0	1	3	1	2
Azerbaijan	0	0	0	0	0	0	0	0	0	1	0
Belgium	0	0	0	0	0	2	1	0	3	4	5
Bosnia	0	0	0	0	0	0	1	0	0	0	0
Croatia	0	0	0	0	0	0	0	1	0	0	2
Cyprus	0	0	0	0	0	0	0	0	2	1	4
Czech	0	0	0	0	0	0	0	2	0	1	5
Denmark	0	0	0	0	0	0	0	0	1	4	6
England	0	1	1	2	2	4	4	12	20	37	48
Estonia	0	0	0	0	0	0	0	0	1	0	4
France	0	0	0	1	0	3	6	4	8	8	19
Finland	0	0	0	0	2	2	3	4	7	7	13
Germany	0	0	2	0	2	1	1	0	3	8	17
Greece	0	0	1	0	0	1	0	1	6	8	7
Hungary	0	0	0	0	0	1	0	0	2	1	0
Italy	0	0	1	0	4	1	3	9	15	27	41
Ireland	0	0	0	0	0	1	2	2	2	6	9
Lithuania	0	0	0	0	0	1	1	1	0	1	1
Luxembourg	0	0	0	0	0	0	0	0	1	2	0

Macedonia	0	0	0	0	0	0	0	0	0	0	1
Netherlands	0	0	1	0	0	1	1	1	0	0	0
Norway	0	0	1	0	0	3	1	2	1	8	7
North Ireland	0	0	0	0	0	0	0	0	0	1	2
Romania	0	0	0	0	0	0	0	0	1	0	7
Poland	0	0	0	0	0	0	2	0	2	1	7
Portugal	0	0	0	0	2	2	1	6	3	7	24
Spain	0	0	3	2	10	4	5	13	10	29	35
Slovakia	0	0	0	0	0	0	0	0	0	0	2
Slovenia	0	0	0	0	1	1	0	2	0	1	3
Switzerland	0	0	0	0	1	1	3	1	4	2	4
Sweden	0	0	0	0	4	2	1	4	7	9	7
Total	0	1	11	5	28	32	36	66	102	175	282
Australia = 123 publications											
Australia	0	0	0	0	2	0	1	4	11	33	60
New Zealand	0	0	0	0	0	0	0	1	3	5	3
Total	0	0	0	0	2	0	1	5	14	38	63
Middle East = 303 publications											
Algeria	0	0	0	0	0	0	2	0	2	2	8
Egypt	0	0	0	0	0	0	0	1	2	5	4
Iraq	0	0	0	0	0	0	0	0	0	2	6
Iran	0	0	0	0	0	0	2	1	2	8	18
Israel	0	0	0	0	0	0	0	0	2	0	0
Jordan	0	0	0	0	0	0	1	1	1	10	2
Lebanon	0	0	0	0	0	0	0	0	0	2	6
Morocco	0	0	0	0	0	0	0	0	0	0	2
Oman	0	0	0	0	0	0	0	0	0	0	3
Pakistan	0	0	0	0	0	0	2	3	6	18	44
Qatar	0	0	0	0	0	0	0	0	2	3	9
Saudi Arabia	0	0	0	0	0	0	2	9	4	18	46
Turkey	0	0	0	0	0	0	2	1	3	8	9
U.A.E	0	0	0	0	0	0	0	0	3	4	12
Total	0	0	0	0	0	0	11	16	27	80	169
Africa = 28 publications											
Kenya	0	0	0	0	0	0	0	0	0	0	1
Nigeria	0	0	0	0	0	0	0	0	0	1	2
South Africa	0	0	0	0	0	0	1	1	3	4	2
Tanzania	0	0	0	0	0	0	0	0	0	0	1
Tunisia	0	0	0	0	0	0	0	1	1	1	9
Total	0	0	0	0	0	0	1	2	4	6	15

4.8 Total Citations Based on Continents

This section discusses the citations received from the WoS Core Collection on IoT publications. Given the importance of citations to demonstrate research growth and research fronts, Table 10 presents the average citation per year. It shows that the IoT research has grown drastically as evidenced by the increasing number of citations every year, suggesting that authors from all over the world are interested in exploring the security of the IoT.

Table 10: Average citations per year.

Year	Total	Mean TCperArt	Mean TCperYear	Citable Years
2009	2	9.00	0.90	10
2010	4	90.25	10.03	9
2011	8	164.88	20.61	8
2012	11	10.45	1.49	7
2013	33	146.33	24.39	6
2014	47	35.96	7.19	5
2015	76	36.88	9.22	4
2016	137	21.05	7.02	3
2017	236	14.05	7.02	2
2018	508	7.40	7.40	1
2019	519	1.32	-	0

Notes: MeanTCperArt = average total citations per article; MeanTCperYear = average total citations per year

Table 11 tabulated countries based on the total number of citations, average article citations, the number of publications, and the overall percentages as compared to other countries. The highest ranking was steered by China from the continent of Asia, followed by Australia, the United States, South Korea, Spain, and Italy. The total citation levels that exceeded one thousand (1,000) citations in the field of IoT characterises these countries. Thus, the leading country has 4,178 total citations, followed by other countries with 3,507, 1,997, 1,508, 1,175 and 1,128 total citations, respectively. Another set of countries with high total citations level include India, England, and Canada. The total citations of

these countries were within five hundred (500) and one thousand (1,000) citations.

Table 11: A Total of Citations Based on Continent

List of Continents	Citation	Average Article Citations	Number of Articles	(%)
Asia				
China	8,051	13.72	586	17.90
India	2,301	12.78	179	5.10
Japan	332	8.1	41	0.74
Malaysia	517	16.68	31	1.15
Singapore	1,038	25.32	40	2.31
S. Korea	2,355	13.85	170	5.25
Taiwan	1,296	18.78	69	2.89
Thailand	36	1.5	4	0.08
Vietnam	56	7	8	0.12
North America				
Canada	1,403	16.13	87	3.12
Mexico	48	4.8	10	0.11
Russia	108	5.4	20	0.24
United States	5,848	17.51	334	13.0
South America				
Brazil	328	6.69	49	0.73
Chile	55	7.86	7	0.12
Colombia	22	5.50	4	0.04
Ecuador	4	1.33	3	0.01
Uruguay	1	1	1	0.01
Europe				
Austria	455	50.56	9	1.01
Azerbaijan	12	12	1	0.02
Belgium	205	13.67	15	0.45
Bosnia	74	74	1	0.16
Croatia	14	4.67	3	0.03
Cyprus	42	6	7	0.09
Czech Republic	73	9.13	8	0.16
Denmark	51	4.64	11	0.11
England	1,839	14.04	131	4.10
Estonia	20	4	5	0.04
France	580	11.84	49	1.29
Finland	1,005	26.45	38	2.24
Germany	522	32.625	34	1.16
Greece	497	20.71	24	1.10
Hungary	12	3	4	0.03
Italy	1,744	17.27	101	3.88
Ireland	159	7.23	22	0.35
Lithuania	26	5.2	5	0.05
Luxembourg	12	4	3	0.02
Macedonia	0	0	1	0
Netherlands	209	52.25	4	0.46
Norway	487	27.06	18	1.08
North Ireland	7	2.33	3	0.01
Romania	13	1.63	8	0.02
Poland	58	4.83	12	0.12
Portugal	515	11.44	45	1.14
Spain	1,938	17.46	111	4.32
Slovakia	4	2	2	0.01
Slovenia	314	39.25	8	0.70
Switzerland	291	18.19	16	0.64
Sweden	1,181	34.74	34	2.63
Australia				
Australia	4,620	41.62	111	10.30
New Zealand	185	15.42	12	0.41
Middle East				
Algeria	222	15.86	14	0.49
Egypt	66	5.5	12	0.14
Iraq	64	8	8	0.14
Iran	350	11.29	31	0.78
Israel	10	5	2	0.02
Jordan	202	13.47	15	0.45
Lebanon	39	4.88	8	0.08
Morocco	1	0.5	2	0.01
Oman	4	1.33	3	0.01
Pakistan	664	9.1	73	1.48
Qatar	174	12.43	14	0.38
Saudi Arabia	901	11.41	79	2.00
Turkey	185	8.04	23	0.41
U.A.E	257	13.53	19	0.57
Africa				
Kenya	3	3	1	0.01
Nigeria	161	53.67	3	0.35
South Africa	524	47.64	11	1.16
Tanzania	2	2	1	0.01
Tunisia	45	3.75	12	0.10

Two (2) countries were considered as highest in the number of article citations, with Nigeria from the continent of Africa being the first, comprising an average article citation of 53.67, followed by the Netherlands from the continent of Europe, with an average article citation of 50.25. An investigation of the total citations and average article citations based on the continents, noted some remarkable facts during several periods of time. Evidence shown in Table 11 indicates that these two (2) countries had received a significant amount in terms of average article citations worldwide for each article published in spite of the fact that these countries had published very few articles. This outcome indicates that these countries had published scientific research articles which contributed to new knowledge that is usable to address society issues. The data further suggest that Africa and the Netherlands had published in high impact journals, thereby drawing other researchers to read and cite their articles. In conclusion, it can be said that scientific research with contributions to new knowledge leads to an increase in total citations for the countries as well as continents.

5. NETWORK COLLABORATIONS

This section illustrates the bibliometric approach of the IoT in network form. It includes country collaborations and keyword co-occurrences network. The network demonstrates the collaboration movement that is related to each country around the world.

5.1 Country Collaboration Network

In order to observe the scientific development among the countries throughout the world, this study

analysed the trail of active networking collaboration. Here, collaboration is referred to as the network that specifies the contribution of authors across the country. This is noted by analysing the link between authors and co-authorships.

Figure 4 illustrates the collaboration of countries in the world, and their research connected to the IoT. The collaborations between countries are highlighted by the red line which indicates collaboration between authors across countries. The countries that actively worked with other countries were Australia, the United States, China, and Russia. The red line in the map also showed that the most active country in publishing collaborative research related to the IoT was China followed by the United States and Australia. As a result of collaborating, these countries were able to increase their publications' performance as well as their citations.

Table 12 tabulates the frequency of collaboration in research across countries. China was noted to be the highest in collaborating with 46 countries. This is followed by the United States and Australia collaborating with 40 and 27 countries, respectively. As can be seen in Table 12, China seemed to be collaborating more with the United States, having 113 frequencies. This showed that China and the United States have a good relationship in collaborating in research, and in publishing good quality research on the IoT. As a result of publishing good articles in high quality journal, more collaboration is expected between these countries.

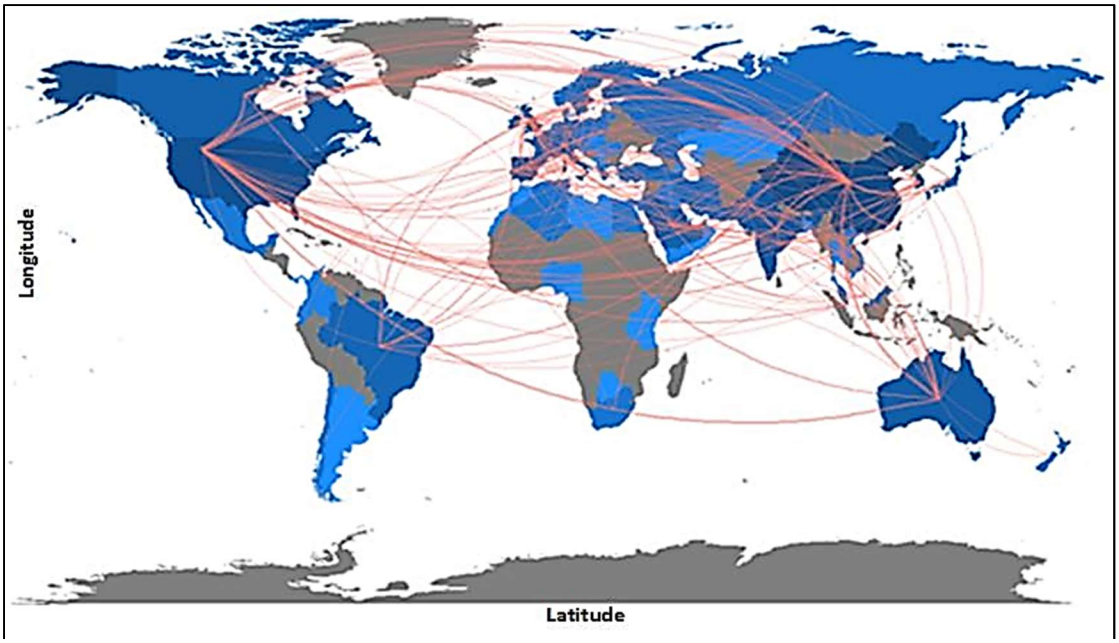

Figure 4: Collaboration Map Around the World

Table 12: List of Collaboration Country.

From	To	Frequency	From	To	Frequency	From	To	Frequency
China	Algeria	3	United	Albania	2	Australia	Brazil	3
	Australia	36	States	Algeria	1		Canada	5
	Austria	1		Australia	22		Denmark	1
	Belgium	2		Austria	2		Estonia	2
	Brazil	5		Belgium	1		France	1
	Canada	28		Brazil	5		Germany	3
	Chile	2		Canada	17		Greece	1
	Denmark	3		Chile	1		India	7
	Estonia	1		Czech	1		Iran	2
	Finland	8		Denmark	1		Ireland	3
	France	7		Egypt	2		Italy	2
	Germany	1		Estonia	1		Japan	2
	Greece	1		France	4		Korea	2
	India	30		Germany	5		Lebanon	1

Iran	2	India	20	Netherlands	1
Ireland	4	Iran	5	N. Zealand	2
Italy	6	Ireland	2	Pakistan	7
Japan	15	Italy	13	Portugal	2
Jordan	2	Japan	4	Russia	2
Kazakhstan	1	Jordan	6	S.Arabia	8
Korea	19	Korea	14	Singapore	3
Kuwait	2	Lebanon	2	Spain	1
Lebanon	1	Malaysia	1	Switzerland	1
Luxembourg	1	Mexico	1	Taiwan	1
Malaysia	2	Netherlands	1	Thailand	1
Netherlands	2	N.Zealand	1	U.A.E	2
New Zealand	2	Pakistan	10	Vietnam	1
Nigeria	1	Portugal	1		
Norway	8	Qatar	6		
Pakistan	12	Russia	2		
Portugal	4	S.Arabia	12		
Qatar	4	Singapore	5		
Russia	3	Spain	4		
Saudi Arabia	15	Sweden	4		
Singapore	14	Taiwan	8		
Slovenia	1	Tanzania	1		
South Africa	7	Tunisia	1		
Spain	1	Turkey	1		
Sweden	4	U.A.E	3		
Switzerland	2	Yemen	1		
Taiwan	20				
Tunisia	1				
Turkey	1				
United Kingdom	41				
United States	113				
Yemen	1				

5.2 Author's Keywords

This section discusses the findings related to the occurrence of terms linked to IoT and IoT Security in the keywords, abstracts and titles as specified in the articles. The analysis aims to analyse the research trend, and to identify the disciplinary field that applies to the IoT as well as the research gap. Author keywords are very important for improving the visibility of the articles, especially in helping other researchers to find the article of interest.

These unique keywords, abstracts and titles were derived from 1,731 articles for the period between 2009 until 2019. The top-ranking term used by authors was Internet, followed by Security, and Things. The Internet provides a communication platform that creates opportunities for people to connect things and to control them remotely. For example, smart appliances (coffee machines and smart refrigerators) can be monitored remotely through smartphones using the Internet. Table 13 lists the frequency of specific terms related to IoT and IoT Security occurrences in keywords, abstracts, and article titles.

The analysis suggests that most researchers tend to use Internet and Security as keywords in their abstracts and titles, for the sake of increasing their article's visibility. For instance, highly cited articles with titles "Internet of Things (IoT): A Vision, Architectural Elements, And Future Directions" [19] and "Security, Privacy and Trust in Internet of Things: The Road Ahead" [21] had also used the terms, Internet, and Security.

Figure 5 illustrates the relationship between the keywords, the abstracts, and the titles. It is worth noting that most researchers were more inclined in using these terms as compared to other terms in the IoT research. The link shown in Figure 5 had indicated the terms that normally related to each other.

Figure 6 illustrates the TreeMap of terms, which are usually used in IoT research. It reveals that Internet, Things, and Security were popular terms used by researchers in the IoT research field. Additionally, the analysis also suggested some interesting terms, such as Secure, Based, and Wireless. This shows that the researchers were

focused on communication security in the field of IoT, thereby proving that the IoT is a potential research ground, in terms of security, especially on data privacy, authentication, and communication between things and data.

Table 13: Keywords, Abstract and Title Occurrences

Keyword	Occurrences	Abstract	Occurrences	Title	Occurrences
Internet	386	IoT	3143	Internet	494
Security	299	Security	2912	Things	464
Things	248	Data	2115	IoT	333
Networks	134	Internet	1944	Security	251
Privacy	129	Network	1809	Networks	245
Wireless Sensor Networks	124	Things	1544	Secure	188
Challenges	116	Devices	1512	Wireless	154
Scheme	116	Networks	1070	Authentication	150
Protocol	103	Scheme	980	Scheme	147
IoT	102	Smart	931	Sensor	134
Architecture	95	System	871	Smart	123
Management	92	Communication	829	Data	118
System	69	Applications	810	Computing	101
Cloud	64	Systems	806	Survey	101
Framework	60	Attacks	773	Network	100
Authentication	58	Computing	762	Systems	99
Systems	57	Secure	745	System	95

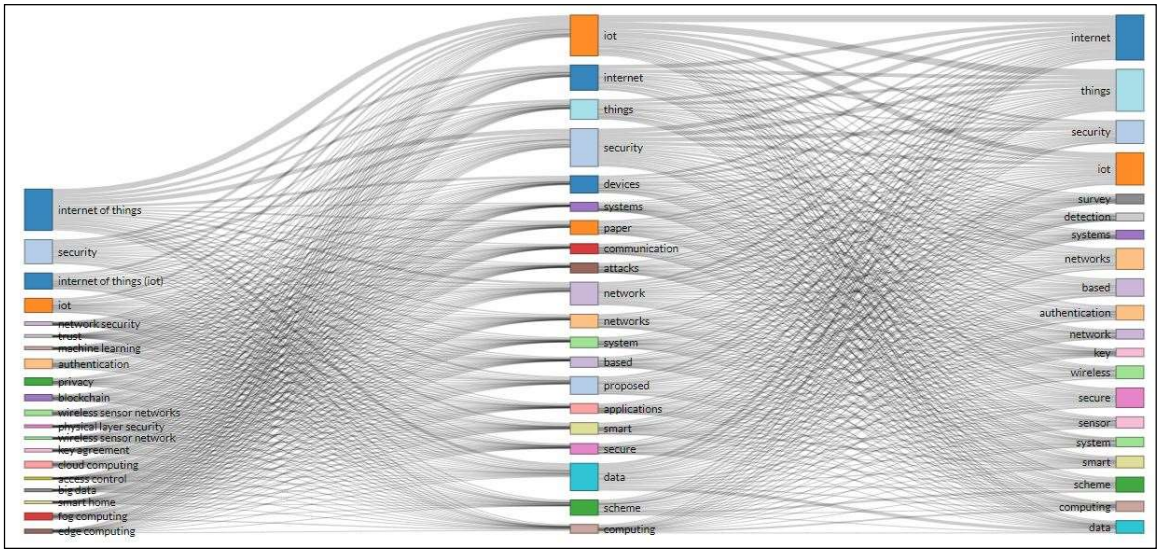

Figure 5: Relationship Between Keywords, Abstracts, and Titles.

Journal of Theoretical and Applied Information Technology
15th May 2022. Vol.100. No 9

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

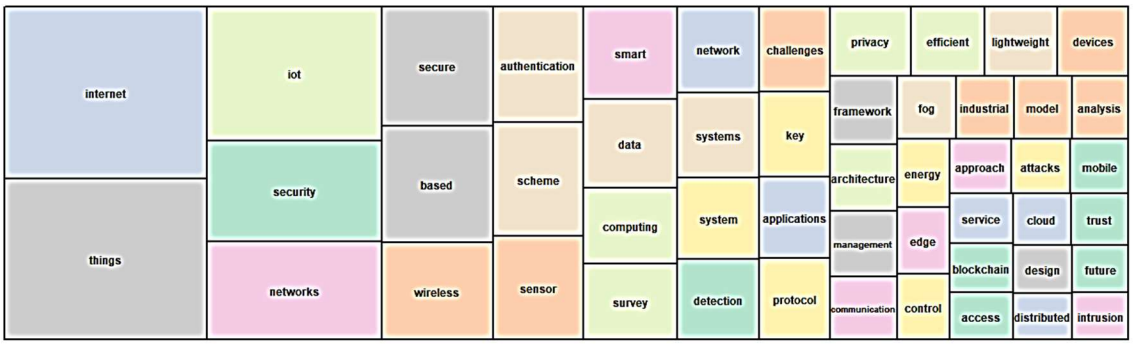

Figure 6: Word Treemap of Keywords.

Figure 7 depicts a dendrogram which is used to highlight the hierarchical association between keywords that were produced from the clustering process. It also represents the data, where each group is linked to two or more successor groups. This group is organised as a tree to illustrate the classification scheme. Figure 7 also provides the right and left branches, and at each dendrogram node, there is an individual cluster. For example, cloud and blockchain nodes have similar heights, showing that both have similarities. This means that the researchers implement the blockchain approach with cloud platforms in IoT research. The bigger the distance between the node, and the higher its height, the more general the cluster becomes.

As Figure 7 demonstrates the growth of research that is related to IoT, it also shows the importance of the current and past research related to IoT. Linking this finding to Figure 8, it is worth noting that the most frequently used words in IoT research were IoT and Security. Besides these two terms, other terms used were Wireless sensor networks, Privacy, Blockchain, and Authentication. Evidently, most of the researchers had applied these terms in their research. Further to this were terms like Privacy, Network security, and Physical layer security, all of which were components that were equally important for protecting information during the communication of things.

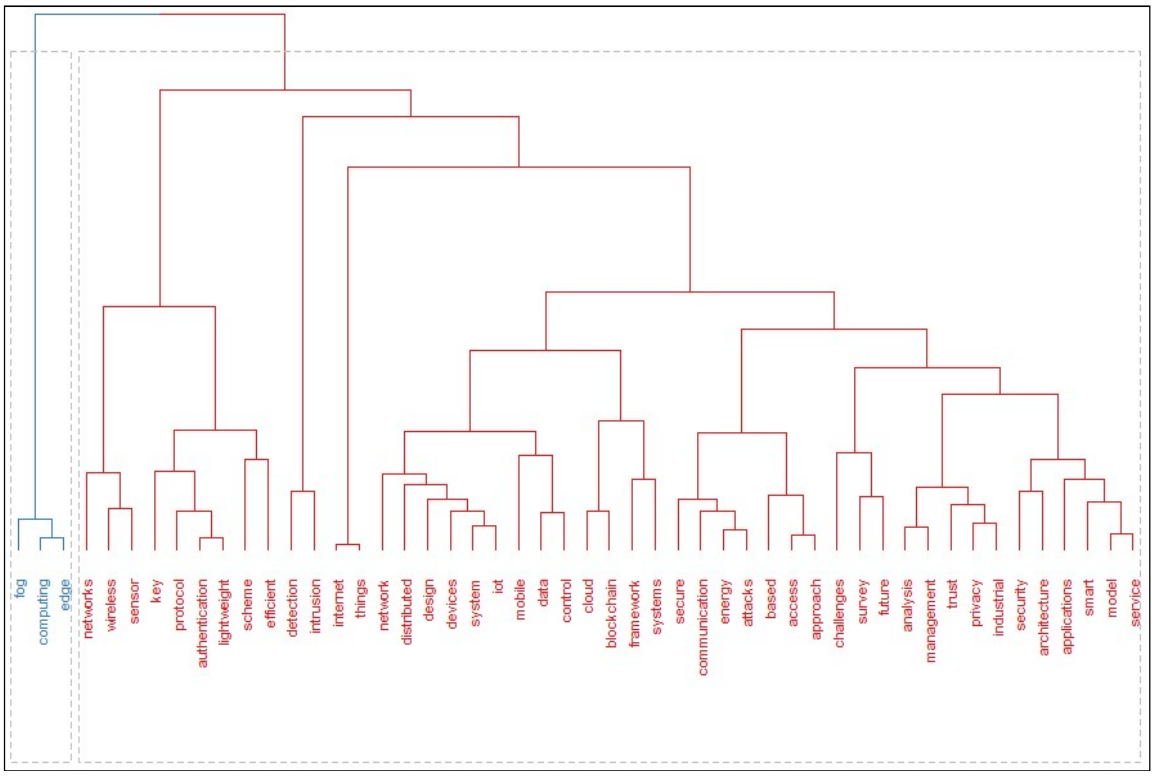

Figure 7: Term Dendrogram

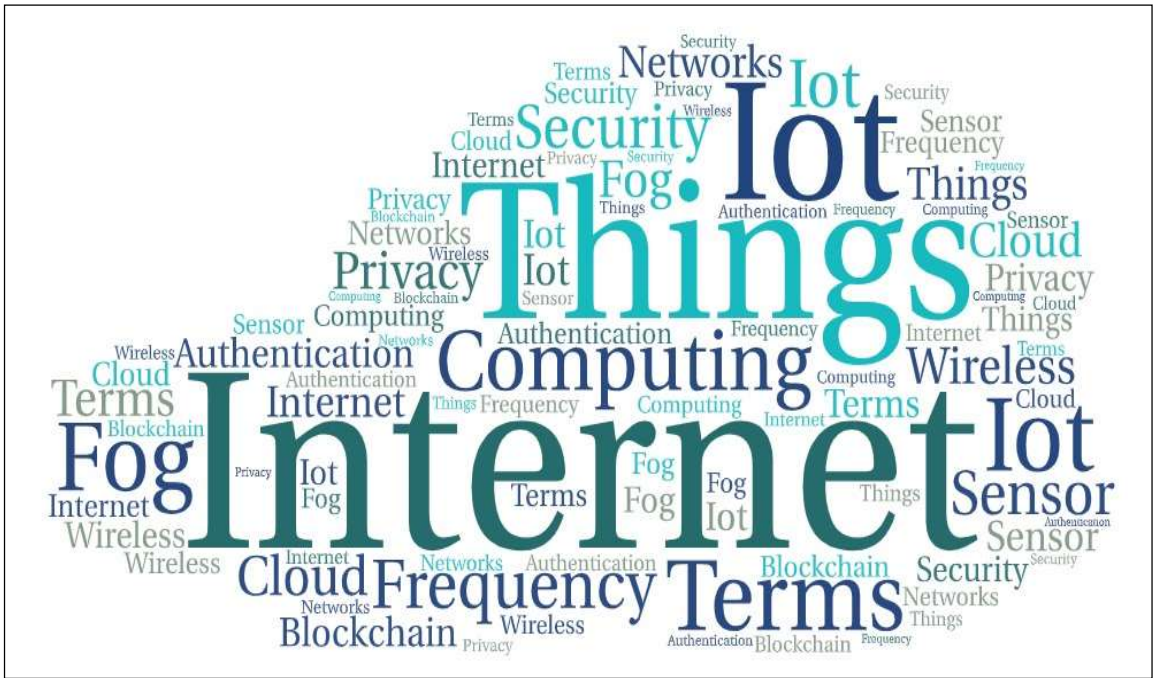

Figure 8: Word Cloud of Keywords

6. CONCLUSIONS

Given the importance of identifying the most popular, and the emerging specialty areas in the scientific research topic of IoT security, this study and its analysis had exhibited an in-depth research pattern that was drawn from research conducted between 2009 to 2019. In this regard, the development and growth of the research topics must be viewed from a global perspective. At present, major researchers around the world have reshaped the IoT research topic to support industrial technological transformation, and user demands. The findings of the research patterns analysed in this study were based on the evaluation of the research activity of the world's major countries, and an analysis of what researchers were focusing on in the face of global issues in innovation and technological advancement.

The comprehensive evaluation conducted by this study assessed the degree of activity in the research patterns in IoT. It comprised the most notable journals, highly cited articles, foremost authors, institutions, countries, citations, and network collaborations. Since notable journals were themselves composed of a group of impact factor, ranking number, and citations, together with subsequent and highly cited articles where the number of articles and citing articles and their respective citations were taken into account, it was worthy to note that these research patterns had experienced a rapid evolution with an increase in publications and citations. In general, it would be significant to publish articles in the foremost journals as this will increase article visibility and assure the research quality.

This study also highlighted the most influential and productive authors in terms of publication, thereby contributing to their respective countries. The list of countries also determined the degree of activity in research innovation and its pattern as reflected in research growth. In addition, this study had also revealed the sources of research vitality among the countries, where measures in two aspects, the number of publications, and citation influence, were noted through the years.

An analysis of the network collaboration and keyword frequencies was also employed to demonstrate the growth and research patterns for future studies. This study had also shown the collaborative publishing performed between authors; it also showed that the phenomenon has increased significantly. Overall, the present finding of this research reviewed the literature of IoT security by concentrating on several perspectives of the bibliometric analysis.

This study provides several research constraints, which are as follows:

i. The analysis was conducted based on the articles published from 2009 until 2019. Therefore, the results may not represent the actual number of recent articles published in the field of IoT.

ii. The criteria for analysis and discussions presented in this study are limited to the scope of this study. Thus, changes in the analysed data may result in varying presentations of the analysis, especially in figures and tables.

Upcoming research may consider adding more features and data to the development of the security-based research from a multiple viewpoint, especially the changes of technologies in IoT from a global perspective.

7. ACKNOWLEDGMENT

This work was funded by the Ministry of Higher Education, Malaysia via Fundamental Research Grant Scheme (FRGS) awarded under the RACER/1/2019/ICT03/UMP/2 Project ID: RDU192613.

REFRENCES:

[1] M. I. Jaya, G. X. Tong, M. F. A. Razak, A. Zabidi, and S. I. Hisham, "Geofence Alerts Application with GPS Tracking for Children Monitoring (CTS)," *Proceedings - 2021 International Conference on Software Engineering and Computer Systems and 4th International Conference on Computational Science and Information Management, ICSECS-ICOCSIM 2021*, pp. 222–226, Aug. 2021, doi: 10.1109/ICSECS52883.2021.00047.

[2] H. Luo, C. Wang, H. Luo, F. Zhang, F. Lin, and G. Xu, "G2F: A Secure User Authentication for Rapid Smart Home IoT Management," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10884–10895, Jul. 2021, doi: 10.1109/JIOT.2021.3050710.

[3] "Global Government IoT Revenue for Endpoint Electronics and Communications to Total $21 Billion in 2022." https://www.gartner.com/en/newsroom/press-releases/2021-06-30-gartner-global-government-iot-revenue-for-endpoint-electronics-and-communications-to-total-us-dollars-21-billion-in-2022 (accessed Dec. 21, 2021).

[4] I. Stellios, P. Kotzanikolaou, and C. Grigoriadis, "Assessing IoT enabled cyber-physical attack paths against critical systems," *Computers & Security*, vol. 107, p. 102316, Aug. 2021, doi: 10.1016/J.COSE.2021.102316.

[5] I. Ullah and Q. H. Mahmoud, "Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks," *IEEE Access*, vol. 9, pp. 103906–103926, 2021, doi: 10.1109/ACCESS.2021.3094024.

[6] M. F. Jusoh, M. F. A. Muttalib, K. T. Krishnan, and A. Katimon, "An overview of the internet of things (IoT) and irrigation approach through bibliometric analysis," *IOP Conference Series: Earth and Environmental Science*, vol. 756, no. 1, p. 012041, May 2021, doi: 10.1088/1755-1315/756/1/012041.

[7] B. Yildiz, "Internet of Things and Smart Cities: A Bibliometric Analysis," *Quantrade Journal of Complex Systems in Social Sciences*, vol. 3, no. 1, pp. 27–44, 2021, Accessed: Dec. 21, 2021. [Online]. Available: http://www.dergipark.gov.tr/quantrade

[8] A.-J. Moreno-Guerrero, F.-J. Hinojo-Lucena, M. R. Navas-Parejo, and G. Gómez-García, "Bibliometric Analysis of Scientific Productivity around Edge Computing and the Internet of Things," *IoT 2020, Vol. 1, Pages 436-450*, vol. 1, no. 2, pp. 436–450, Nov. 2020, doi: 10.3390/IOT1020024.

[9] Y. R. Leong, F. P. Tajudeen, and W. C. Yeong, "Bibliometric and content analysis of the internet of things research: a social science perspective," *Online Information Review*, vol. 45, no. 6, pp. 1148–1166, Oct. 2021, doi: 10.1108/OIR-08-2020-0358/FULL/XML.

[10] S. Fosso Wamba, R. E. Bawack, C. Guthrie, M. M. Queiroz, and K. D. A. Carillo, "Are we preparing for a good AI society? A bibliometric review and research agenda," *Technological Forecasting and Social Change*, vol. 164, p. 120482, Mar. 2021, doi: 10.1016/J.TECHFORE.2020.120482.

[11] X. Chen, H. Xie, Z. Li, and G. Cheng, "Topic analysis and development in knowledge graph research: A bibliometric review on three decades," *Neurocomputing*, vol. 461, pp. 497–515, Oct. 2021, doi: 10.1016/J.NEUCOM.2021.02.098.

[12] S. Ratibah *et al.*, "Towards a systematic description of the field using bibliometric analysis: malware evolution," *Scientometrics 2021 126:3*, vol. 126, no. 3, pp. 2013–2055, Feb. 2021, doi: 10.1007/S11192-020-03834-6.

[13] F. J. Agbo, S. S. Oyelere, J. Suhonen, and M. Tukiainen, "Scientific production and thematic breakthroughs in smart learning environments: a bibliometric analysis," *Smart Learning Environments*, vol. 8, no. 1, pp. 1–25, Dec. 2021, doi: 10.1186/S40561-020-00145-4/FIGURES/12.

[14] W. Choi, J. Kim, S. E. Lee, and E. Park, "Smart home and internet of things: A bibliometric

study," *Journal of Cleaner Production*, vol. 301, p. 126908, Jun. 2021, doi: 10.1016/J.JCLEPRO.2021.126908.

[15] J. Wang, M. K. Lim, C. Wang, and M. L. Tseng, "The evolution of the Internet of Things (IoT) over the past 20 years," *Computers & Industrial Engineering*, vol. 155, p. 107174, May 2021, doi: 10.1016/J.CIE.2021.107174.

[16] A. Firdaus, M. F. A. Razak, A. Feizollah, I. A. T. Hashem, M. Hazim, and N. B. Anuar, "The rise of 'blockchain': bibliometric analysis of blockchain study," *Scientometrics*, vol. 120, no. 3, pp. 1289–1331, Sep. 2019, doi: 10.1007/S11192-019-03170-4/TABLES/14.

[17] M. F. A. Razak, N. B. Anuar, R. Salleh, and A. Firdaus, "The rise of 'malware': Bibliometric analysis of malware study," *Journal of Network and Computer Applications*, vol. 75, pp. 58–76, Nov. 2016, doi: 10.1016/J.JNCA.2016.08.022.

[18] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W. M. Lim, "How to conduct a bibliometric analysis: An overview and guidelines," *Journal of Business Research*, vol. 133, pp. 285–296, Sep. 2021, doi: 10.1016/J.JBUSRES.2021.04.070.

[19] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, Sep. 2013, doi: 10.1016/J.FUTURE.2013.01.010.

[20] S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak, "The internet of things for health care: A comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, Jun. 2015, doi: 10.1109/ACCESS.2015.2437951.

[21] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, Jan. 2015, doi: 10.1016/J.COMNET.2014.11.008.

[22] D. Bandyopadhyay and J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization," *Wireless Personal Communications 2011 58:1*, vol. 58, no. 1, pp. 49–69, Apr. 2011, doi: 10.1007/S11277-011-0288-5.

[23] S. Wang, J. Wan, D. Li, and C. Zhang, "Implementing Smart Factory of Industrie 4.0: An Outlook:," *http://dx.doi.org/10.1155/2016/3159805*, vol. 2016, Jan. 2016, doi: 10.1155/2016/3159805.

[24] Z. Yan, P. Zhang, and A. v. Vasilakos, "A survey on trust management for Internet of Things," *Journal of Network and Computer Applications*, vol. 42, pp. 120–134, Jun. 2014, doi: 10.1016/J.JNCA.2014.01.014.

[25] Q. Jing, A. v. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, Oct. 2014, doi: 10.1007/S11276-014-0761-7/FIGURES/3.

[26] R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, Jul. 2013, doi: 10.1016/J.COMNET.2012.12.018.

[27] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125–1142, Oct. 2017, doi: 10.1109/JIOT.2017.2683200.

[28] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, Sep. 2011, doi: 10.1109/MC.2011.291.

[29] W. Shi and S. Dustdar, "The Promise of Edge Computing," *Computer*, vol. 49, no. 5, pp. 78–81, May 2016, doi: 10.1109/MC.2016.145.

[30] N. Abbas, Y. Zhang, A. Taherkordi, and T. Skeie, "Mobile Edge Computing: A Survey," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 450–465, Feb. 2018, doi: 10.1109/JIOT.2017.2750180.

[31] L. Zhou and H. C. Chao, "Multimedia traffic security architecture for the internet of things," *IEEE Network*, vol. 25, no. 3, pp. 35–40, May 2011, doi: 10.1109/MNET.2011.5772059.

[32] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, Nov. 2013, doi: 10.1016/J.ADHOC.2013.04.014.

[33] M. Turkanović, B. Brumen, and M. Hölbl, "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion," *Ad Hoc Networks*, vol. 20, pp. 96–112, Sep. 2014, doi: 10.1016/J.ADHOC.2014.03.009.

[34] M. Díaz, C. Martín, and B. Rubio, "State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing," *Journal of Network and*

Computer Applications, vol. 67, pp. 99–117, May 2016, doi: 10.1016/J.JNCA.2016.01.010.

[35] D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous Authentication for Wireless Body Area Networks with Provable Security," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590–2601, Dec. 2017, doi: 10.1109/JSYST.2016.2544805.

[36] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Generation Computer Systems*, vol. 82, pp. 395–411, May 2018, doi: 10.1016/J.FUTURE.2017.11.022.

[37] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, "Secure integration of IoT and Cloud Computing," *Future Generation Computer Systems*, vol. 78, pp. 964–975, Jan. 2018, doi: 10.1016/J.FUTURE.2016.11.031.

[38] G. A. Akpakwu, B. J. Silva, G. P. Hancke, and A. M. Abu-Mahfouz, "A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges," *IEEE Access*, vol. 6, pp. 3619–3647, Dec. 2017, doi: 10.1109/ACCESS.2017.2779844.