# The evolution of the Internet of Things (IoT) over the past 20 years

Wang, J., Lim, M., Wang, C. & Tseng, M.



**Original citation & hyperlink:**
Wang, J, Lim, M, Wang, C & Tseng, M 2021, 'The evolution of the Internet of Things (IoT) over the past 20 years', Computers & Industrial Engineering, vol. 155, 107174. https://dx.doi.org/10.1016/j.cie.2021.107174

DOI 10.1016/j.cie.2021.107174
ISSN 0360-8352

Publisher: Elsevier

# The evolution of the Internet of Things (IoT) over the past 20 years


## Abstract

To reveal the origin of the IoT, evaluate its mainstream research topics, and discuss the challenges facing the IoT in the future, this paper conducts a bibliometric study of the IoT from 2000 to 2019. First, this paper presents a basic bibliometric overview of the IoT. Second, co-citation, coupling and cluster analysis methods are used to analyse collaboration networks, and VOSviewer® is used to visualize the networks. Third, biblioshiny® is used to analyse the thematic trends of IoT. Finally, this paper discusses IoT challenges and provides some suggestions to address them. The limitations of this paper are also summarized. Research results show that, the mainstream studies in this field mainly focus on IoT security, wireless sensor networks, IoT management, IoT challenges and privacy. In addition, the thematic evolution of keywords shows that security and algorithm issues have become basic themes in the field of IoT research in recent years.



**Keywords**: Internet of things; Bibliometric; Network analysis; Thematic trends analysis; VOSviewer; Biblioshiny.

## 1. Introduction

The Internet of Things (IoT) is an extended and expanded system network based on the Internet, and its ultimate goal is to achieve real-time interaction among things, machines and humans through various advanced technological means. The earliest literature on the IoT was published in 2002; Schoenberger (2002) first designed the application of the IoT in stores, and he stated that tiny wireless chips enable stores to have eyes. After nearly 20 years of development, increasing numbers of government officials, corporate executives and researchers tend to believe that the IoT is an important technology for improving our living environment and quality of life (Atzori, Iera, & Morabito, 2010; Gubbi, Buyya, Marusic, & Palaniswami, 2013; Lim, Xiong, & Lei, 2020; Su, Bai, Sindakis, Zhang, & Yang, 2020). A market research report showed that the global IoT market reached $1.90 billion in 2018, and this number is expected to reach $11.03 billion in 2026 (Panetta, 2016). The European Union (EU), the United States (USA), China and other countries have also formulated IoT-related action plans. These policies and plans mainly include the IoT-An action plan for Europe and IoT development plans 2016-2020.

The concept of the IoT usually refers to achieving smart connections among different people, machines, tasks and knowledge by using the Internet and sensors (Dang, Piran, Han, Min, & Moon, 2019; Tu, Lim, & Yang, 2018a). IoT-related research has been extended by some scholars to the Internet of Service (Kwak, Cho, Shin, & Yang, 2020), Internet of Machine (Gazis, 2017), Internet of People (Li, 2017) and Internet of Knowledge (Lim, Tseng, Tan, & Bui, 2017; Santoro, Vrontis, Thrassou, & Dezi, 2018). With the progress of science and technology, the IoT is expected to achieve large-scale applications in the home and public service markets (Bouzembrak, Kluche, Gavai, & Marvin, 2019). IoT applications make important contributions to reducing environmental pollution caused by human activities and increasing the economic development of countries (Lim, Wang, Wang, & Tseng, 2020; Su, Yang, & Yang, 2018; Tseng, Lim, & Wu, 2019).

To achieve this potential growth, the innovative growth of various emerging technologies and services needs to keep pace with market demand growth (Li, Lim, Tan, Lee, & Tseng, 2020; Lim & Jones, 2017; Zhang, Yang, Zheng, & Su, 2019). Several review articles have covered different aspects of the IoT. For example, Atzori, Iera, & Morabito (2010) summarized the IoT from the

aspects of technology, application scenarios and major challenges and believed that the multidisciplinary collaboration of telecommunications, informatics, electronics and society promotes the IoT to achieve multidisciplinary comprehensive development. Gubbi, Buyya, Marusic, & Palaniswami (2013) reviewed the basic concepts, architectural elements and future development trends of the IoT and proposed a cloud-centric framework for the global IoT. However, the above article did not review the protocols that are used for the IoT. Hence, Al-Fuqaha, Guizani, Mohammadi, Aledhari, & Ayyash (2015) further analysed the technologies, protocols and application scenarios of the IoT. All these research results provide an important reference for researchers and programmers to design innovative IoT application scenarios.

After over 20 years of development, IoT-related research has been extended to different fields, including smart medical care (Al-Turjman, Nawaz, & Ulusar, 2020; Tu, Lim, & Yang, 2018b), smart agriculture (Sinha, Shrivastava, & Kumar, 2019), smart supply chains (Manavalan & Jayakrishna, 2019; Munuzuri, Onieva, Cortes, & Guadix, 2020), smart transportation (Babar & Arif, 2019; Wang, Lim, Zhan, & Wang, 2020) and smart cities (Liu, Bi, & Liu, 2020). The IoT concept has been widely recognized and applied in different fields. However, the IoT-related research results do not explore the inherent development rules and research trends of the IoT. In particular, few studies have been conducted to reveal the origin of the IoT, evaluate its mainstream research topics and discuss the challenges that will be faced by the IoT in the future based on a bibliometric method. In addition, the progress of IoT technology is inseparable from the support of related theories and methods, and increasingly scholars and practitioners are eager to learn more about the development status of the IoT by reading publications. Hence, it is time for a systematic review and outlook for IoT development over the past 20 years. To achieve this goal, this study mainly addresses the following four urgent issues:

1) What is the main bibliometric overview of the IoT?

2) What are the collaboration networks of IoT research?

3) What are the thematic trends of IoT development?

4) What are the main challenges and solutions for the IoT?

To address the above four core concerns of academic researchers, in this paper, co-citation, coupling and cluster analysis methods are used to evaluate the development and research trends of the IoT, and VOSviewer® and biblioshiny® are used to outline a profile of the IoT. The findings of this research help relevant researchers, entrepreneurs and governments have a clearer understanding of the development of the IoT in the last 20 years and in the future. For researchers, the results are helpful for understanding the thematic trends and important journals in the field of the IoT. For entrepreneurs, the results are helpful for finding well-known research institutions and developing a competitive IoT market after understanding the collaboration networks of the IoT. For governments, the results are helpful for formulating more professional action plans based on the development trends of the IoT. The sections of this paper are structured as follows: Section 2 presents the methodology and data sources. Section 3 shows a basic bibliometric overview of the IoT. Section 4 shows the collaboration network analysis of the IoT. Section 5 presents the thematic trends of the IoT. Section 6 discusses the challenges of the IoT. Section 7 presents the conclusion.

## 2. Methodology and data sources

### 2.1 Methodology

Structured literature review methods have been used to analyse and review scientific publications. These methods have some advantages, including that authors use them to conduct in-depth analysis for publications (Egger & Masood, 2020; Wang, Ghadimi, Lim, & Tseng, 2019). However, a limitation of these methods is that the time spent by authors increases exponentially as the number of studies increases (Wang, Zhao, Vilela, & Lim, 2019). In addition, it is difficult to eliminate the influence of author subjective factors on the analysis results (Addo-Tenkorang & Helo, 2016). In contrast, bibliometric analysis methods enable objectively processing thousands or even tens of thousands of scientific studies; in particular, visualization functions enable authors to clearly understand the trends of publications (Wang, Lim, Zhao, Tseng, Chien, & Lev, 2020; Ghadimi, Wang, & Lim, 2019). Bibliometric analysis methods have been applied successfully in different fields, including technology foresight evaluation (Gibson, Daim, Garces, & Dabic, 2018), cloud computing research evaluation (Cai, Lu, Wang, & Xing, 2015), and journal evaluation (Wang,

Lim, & Lyons, 2019). Hence, three bibliometric methods, co-citation, coupling, and cluster methods, are applied here.

a) Co-citation method. Co-citation was put forward by Henry Small, an American intelligence scientist, in 1973 (Small, 1973). The necessary condition for two articles to form a co-citation relationship is that both articles appear in the references of a third article.

b) Coupling method. The concept of publication coupling was first proposed by Kessler in 1963. Publication coupling refers to the existence of at least two publications that jointly refer to the same publication; then, the relationship between two or more publications is named coupling.

c) Cluster method. Clustering refers to dividing a certain number of elements into different groups according to those elements' degrees of similarity; the different groups are named clusters (Lee & Lee, 2018). After clustering, the elements distributed in the same cluster have higher similarity, and the elements distributed in different clusters have lower similarity.

Several tools enable visualization in this study, such as VOSviewer®, which is a professional visualization software developed by Nees & Waltman (2020), and biblioshiny®, which is a Java software developed by Massimo Aria from the University of Naples Federico (Aria, 2020). In this paper, co-citation, coupling, and cluster analysis methods based on VOSviewer ® and biblioshiny® are used to analyse IoT-related publications.

### 2.2 Data sources

Web of Science (WoS), Scopus, and Google Scholar are some of the most famous academic resource systems in the word (Hu, Wang, Ni, & Liu, 2020). Most of the publications included in the Google Scholar database are automatically retrieved by machines, and this process leads to the loss of key information of some publications. The three main evaluation indicators used in the Scopus database are Source Normalized Impact per Paper (SNIP), Impact per Publication (IPP), and SCImago Journal Rank (SJR), and the two main evaluation indicators used in the WoS database are impact factor (IF) and 5-year IF. The IF indicator is recognized by an increasing number of scientific research institutions. In addition, the WoS database includes SCI & SSCI documents. SCI & SSCI are citation index publications published and edited by the USA Institute of Scientific

Information (ISI). This retrieval system was founded in 1964, and the publications are divided into print, CD and online versions, containing more than 8,700 core academic journals that have the most influence in various fields, including natural sciences and engineering technology. Based on consideration of the advantages of the WoS database, this paper uses WoS as the main database for the literature evaluation of IoT publications.

As of March 28, 2020, the total number of IoT-related publications that belong to SCI or SSCI in WoS-Core Collections between 2000 and 2019 was 9,589, including conference papers (5589, 58.29%), research articles (3330, 34.73%), editorial materials (360, 3.75%), review articles (193, 2.01%), meeting abstracts (41, 0.43%), news items (26, 0.27%), book reviews (24, 0.25%), corrections (16, 0.17%), letters (6, 0.06%), retracted publications (3, 0.03%), and a book chapter (1, 0.01%). Considering the completeness of the research content, methods, and results of different types of publications, research articles and review articles (3,523) are analysed. These publications were drawn from a total of 10,210 authors, 2,851 institutions, and 94 countries. Notably, institutions from Hong Kong and mainland China are combined into one group named China, and institutions from Northern Ireland, Wales, Scotland and England are combined into one group named the UK.

## 3. Bibliometric overview

### 3.1 Journal overview

A total of 3,523 IoT-related publications published in 2000-2019 are analysed. In terms of the number of IoT publications, the top 20 journals are shown in Table 1. The IFs in Table 1 are from the annual Journal Citation Reports (JCR). The following two features are obtained from Table 1:

a) The journal with the highest 5-year IF is *IEEE Communications Magazine* with 12.091, followed by *IEEE Internet of Things Journal* with 11.216. The journal with the largest number of IoT articles is *IEEE Access* (375, 8.05%), followed by *IEEE Internet of Things Journal* (363, 7.79%). The journal with the most total citations is Sensors, with 46,222 citations. *IEEE Communications Magazine* tends to accept papers on hot topics.

b) *IEEE Internet of Things Journal* is the youngest journal and was launched in 2014. This journal mainly publishes IoT-related articles on topics including communication protocol design

and optimization, innovative practices and application, major technological innovation, system framework and architecture of the IoT, social management system innovation, etc.

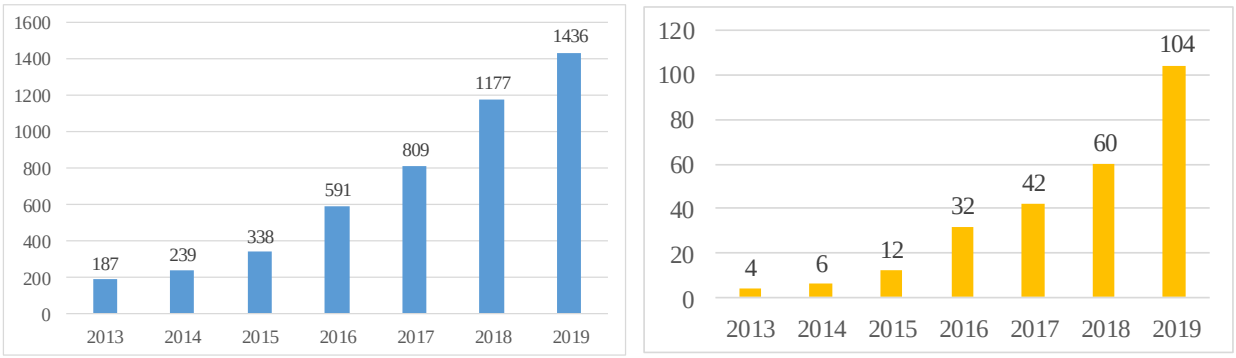
Table 1. Top 20 journals by the number of publications

| R | Journal | N | IF-2010 | IF-2015 | IF-2018 | IF-5Y | FY | TC | TC/N | TC/Y | > 500 | [300, 500] | [100, 300] | < 100 | Y |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | *IEEE Access* | 375 | - | 1.270 | 4.098 | 4.540 | 2014 | 20,879 | 55.68 | 3479.83 | 2 | 0 | 6 | 367 | 2013 |
| 2 | *IEEE Internet of Things J.* | 363 | - | - | 9.515 | 11.216 | 2014 | 6,119 | 16.86 | 1019.83 | 2 | 2 | 7 | 352 | 2014 |
| 3 | *Sensors* | 217 | 1.452 | 1.570 | 2,295 | 3.302 | 2012 | 46,222 | 213.00 | 5777.75 | 0 | 0 | 1 | 216 | 2001 |
| 4 | *Future Generation Computer Systems-the Int. J. of eScience* | 151 | 2.371 | 2.430 | 5.768 | 5.670 | 2013 | 10,230 | 67.75 | 1461.43 | 1 | 0 | 0 | 150 | 1995 |
| 5 | *Int. J. of Distributed Sensor Networks* | 142 | 0.067 | 0.906 | 1.614 | 1.461 | 2012 | 4,131 | 29.09 | 516.38 | 0 | 0 | 1 | 141 | 2004 |
| 6 | *IEEE Communications Magazine* | 88 | 2.837 | 5.125 | 10.356 | 12.091 | 2011 | 24,753 | 281.28 | 2750.33 | 0 | 0 | 10 | 78 | 1995 |
| 7 | *IEEE Transactions on Industrial Informatics* | 68 | 1.627 | 4.708 | 7.377 | 8.423 | 2013 | 13,187 | 193.93 | 1883.86 | 1 | 1 | 5 | 61 | 2004 |
| 8 | *Wireless Personal Communications* | 62 | 0.507 | 0.701 | 0.929 | 0.959 | 2009 | 5,256 | 84.77 | 477.82 | 0 | 1 | 2 | 59 | 2000 |
| 9 | *J. of Network and Computer Applications* | 53 | 0.660 | 2.331 | 5.273 | 4.744 | 2012 | 6,959 | 131.30 | 869.88 | 0 | 1 | 5 | 47 | 1995 |
| 10 | *Computer Networks* | 49 | 1.176 | 1.446 | 3.030 | 2.989 | 2010 | 10,122 | 206.57 | 1012.20 | 1 | 3 | 2 | 43 | 1997 |
| 11 | *Wireless Communications Mobile Computing* | 47 | 0.810 | 0.922 | 1.396 | 1.364 | 2016 | 3,421 | 72.79 | 855.25 | 0 | 0 | 0 | 47 | 2002 |
| 12 | *Computer* | 44 | 1.812 | 1.115 | 3.564 | 2.833 | 2011 | 7,260 | 165.00 | 806.67 | 0 | 0 | 3 | 41 | 1995 |
| 13 | *Int. J. of Advanced Computer Science and Applications* | 44 | - | - | - | - | 2015 | - | - | - | 0 | 0 | 0 | 44 | - |
| 14 | *IEEE Consumer Electronics Magazine* | 41 | - | - | 3.273 | 2.446 | 2012 | 636 | 15.51 | 79.50 | 0 | 0 | 1 | 40 | 2014 |
| 15 | *Computers Electrical Engineering* | 39 | 0.484 | 1.084 | 2.189 | 2.337 | 2011 | 3,855 | 98.85 | 428.33 | 0 | 0 | 1 | 38 | 1995 |
| 16 | *Cluster Comp. the J. of Networks Software Tools and App* | 37 | 0.679 | 1.514 | 1.851 | 1.359 | 2017 | 2,099 | 56.73 | 699.67 | 0 | 0 | 0 | 37 | 2005 |
| 17 | *Personal and Ubiquitous Computing* | 37 | 1.137 | 1.498 | 1.735 | 2.061 | 2011 | 2,371 | 64.08 | 263.44 | 0 | 0 | 2 | 35 | 2006 |
| 18 | *Ad Hoc Networks* | 36 | 1.592 | 1.660 | 3.490 | 3.336 | 2012 | 5,084 | 141.22 | 635.50 | 1 | 0 | 4 | 31 | 2007 |
| 19 | *IEEE Network* | 34 | 1.934 | 2.899 | 7.503 | 7.344 | 2011 | 4,228 | 124.35 | 469.78 | 0 | 0 | 3 | 31 | 1995 |
| 20 | *Multimedia Tools and Applications* | 34 | 0.914 | 1.331 | 2.101 | 1.876 | 2015 | 8,199 | 241.15 | 1639.80 | 0 | 0 | 0 | 34 | 1996 |

Note: R represents the quantity ranking. N represents the number of IoT articles indexed in WoS. IF represents the impact factor. FY represents the year when IoT articles were first indexed. TC represents total citations. > and [,] represent intervals of the number of citations of IoT articles, counted on March 18, 2020. Y represents the earliest year that is reported by InCites Journal Citation Reports (JCR).

### 3.2 Quantity distribution

The number of publications over the years indicates research results and trends in the IoT field. As of January 16, 2020, this paper classifies 3,523 publications from the WoS database; the published numbers of research and review articles from 2013 to 2019 are shown in Fig 1.




a) Research articles b) Review articles

Fig 1. The change trends of the numbers of different types of publications

The first article in the IoT field appeared in 2002, when Schoenberger (2002) mainly introduced application scenarios of the IoT in future smart supermarkets, including how to use sensors for detection in the operation of a supermarket. After 2009, these publications showed a growing trend. In contrast, review articles appeared relatively late, and the first review article appeared in 2012. The change trend of the number of publications is analysed and shown in Fig 2.

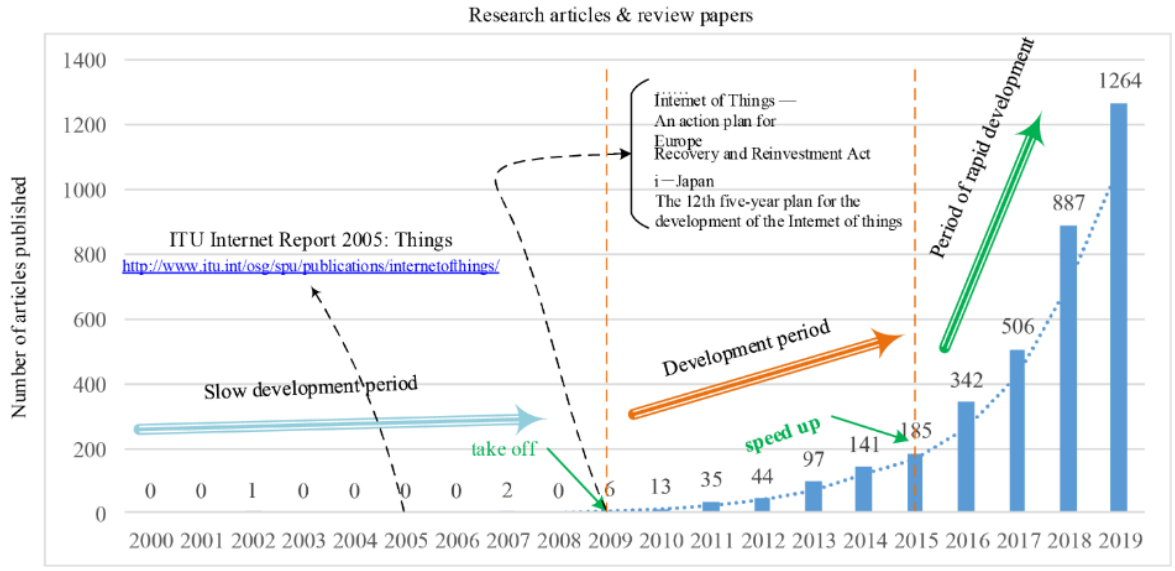



Fig 2. Analysis of the reasons for the changes in the number of IoT articles

Fig 2 shows that the development of the IoT has gone through three stages. The first stage was (2002, 2009], when nine publications were published. The International Telecommunication Union (ITU) released a report on the IoT in 2005 (ITU, 2003); after that, the IoT gradually entered a slow development period. The second stage was (2009, 2015], and many countries issued action plans on the IoT during this stage. For example, the EU released the "Internet of Things - An action plan for Europe" in 2009 (Brussels, 2009). The Chinese government also published the "Twelfth Five-Year" Development Plan Report on the IoT in 2010 (Most, 2012); this report provided a detailed plan for the key development directions of the IoT from 2011 to 2015. The third stage was (2015, 2019], when 2999 publications were published in WoS, and the annual increase in publications reached more than 85.13% in this stage.

### 3.3 Citation structure

Table 2 shows the citation structure in terms of IoT-related publications, where the column of "≥300" represents the number of articles that have been cited more than 300 times. The statistical results show that these IoT-related publications have received 74,720 citations in the last 20 years, and the most-cited publications were published in 2014, with a total of 12,032 citations, accounting for 16.10%. The total number of citations showed a trend of first increasing and then decreasing around 2014. This phenomenon shows that academic research on the IoT made an influential breakthrough in 2014. Representative study results during this period are about the application of the IoT in smart cities and industries (Zanella, Bui, Castellani, Vangelista, & Zorzi, 2014). This is followed by 2016, with a total of 10,748 citations, accounting for 14.38%, but these data may change over time, as publications still take time to reach their highest citation levels (Wang, Lim, Zhao, & Tseng, 2020). In addition, the average number of citations per year is 21.21 from 2002 to 2019. The most-cited publication was published in 2010, with an average number of citations of 498.54. Moreover, 0.88% of these publications have obtained more than 300 citations in WoS, 1.39% of these publications have obtained over 200 citations, 3.35% of these publications have obtained over 100 citations, and 7.84% of these publications have obtained over 50 citations. Note that the single most-cited paper was published in 2010, with 5,153 citations. This was a review article that pointed out that the IoT comprises multiple technologies and gave a detailed introduction to the challenges faced in the development of the IoT (Atzori, Iera, & Morabito, 2010).

Table 2. Citation structure in terms of IoT-related papers according to WoS

| Year | ≥300 | ≥200 | ≥100 | ≥50 | ≥20 | ≥10 | N | TC | TC/N | h-index | CA |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Total | 31 | 49 | 118 | 276 | 670 | 1083 | 3523 | 74,720 | 21.21 | 109 | 37,095 |
| 2019 | 0 | 0 | 0 | 4 | 28 | 67 | 1264 | 2,958 | 2.34 | 23 | 2,393 |
| 2018 | 0 | 0 | 8 | 24 | 118 | 224 | 887 | 8,698 | 9.81 | 42 | 6,423 |
| 2017 | 1 | 2 | 11 | 45 | 131 | 239 | 506 | 9,303 | 18.39 | 48 | 6,999 |
| 2016 | 3 | 7 | 19 | 53 | 136 | 199 | 342 | 10,748 | 31.43 | 51 | 8,376 |
| 2015 | 6 | 7 | 17 | 48 | 81 | 123 | 185 | 9,755 | 52.73 | 48 | 7,662 |
| 2014 | 10 | 13 | 23 | 41 | 78 | 101 | 141 | 12,032 | 85.33 | 44 | 8,904 |
| 2013 | 4 | 5 | 11 | 24 | 49 | 66 | 97 | 7,869 | 81.22 | 35 | 6,629 |
| 2012 | 2 | 4 | 7 | 12 | 16 | 23 | 44 | 3,220 | 73.18 | 17 | 2,864 |
| 2011 | 1 | 5 | 13 | 13 | 17 | 22 | 35 | 2,796 | 79.89 | 18 | 2,336 |
| 2010 | 2 | 4 | 6 | 8 | 10 | 11 | 13 | 6,481 | 498.54 | 11 | 6,037 |
| 2009 | 1 | 1 | 2 | 3 | 5 | 6 | 6 | 569 | 94.83 | 6 | 545 |
| 2008 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2007 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2006 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2005 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2004 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 285 | 142.5 | 2 | 285 |
| 2003 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2002 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 6 | 6 | 1 | 6 |
| 2001 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2000 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

Note: N represents the number of IoT articles indexed in WoS. TC represents total citations. h-index represents that at most, h publications have been cited at least h times. CA represents the article citations; all of these data were counted on March 28, 2020.

### 3.4 Institutional structure

In terms of the quantity of journal articles published, the Chinese Academy of Sciences (CAS) has the largest number of IoT articles. The quantity statistics of institutions are shown in Table 3. Table 3 shows that the CAS has the most published journal articles, with 109 articles, 23 h-index articles, and 4,198 citations, and the average annual number of citations is 38.43. This is followed by Beijing University of Posts and Telecommunications, with 97 publications. It is worth mentioning that the CAS is the highest academic institution in China (Zhang & Zhao, 2019), is the highest scientific and technological institution and is a natural science and high-tech comprehensive research centre. At present, the CAS mainly focuses on the research of advanced sensors and modules, communication systems and devices, optical communication devices and modules, wireless information systems and networks.

Table 3. The statistical analysis of institutions

| Ranking | Institution | Article quantity | Proportion |
|---|---|---|---|
| 1 | Chinese Academy of Sciences | 109 | 3.09% |
| 2 | Beijing University of Posts Telecommunications | 97 | 2.75% |
| 3 | King Saud University | 72 | 2.04% |
| 4 | University of Electronic Science Technology of China | 61 | 1.73% |
| 5 | Dalian University of Technology | 47 | 1.33% |
| 6 | Vellore Institute of Technology | 46 | 1.31% |
| 7 | Huazhong University of Science Technology | 43 | 1.22% |
| 8 | University of California System | 39 | 1.11% |
| 9 | Shanghai Jiao Tong university | 38 | 1.08% |
| 10 | University of Science and Technology Beijing | 38 | 1.08% |

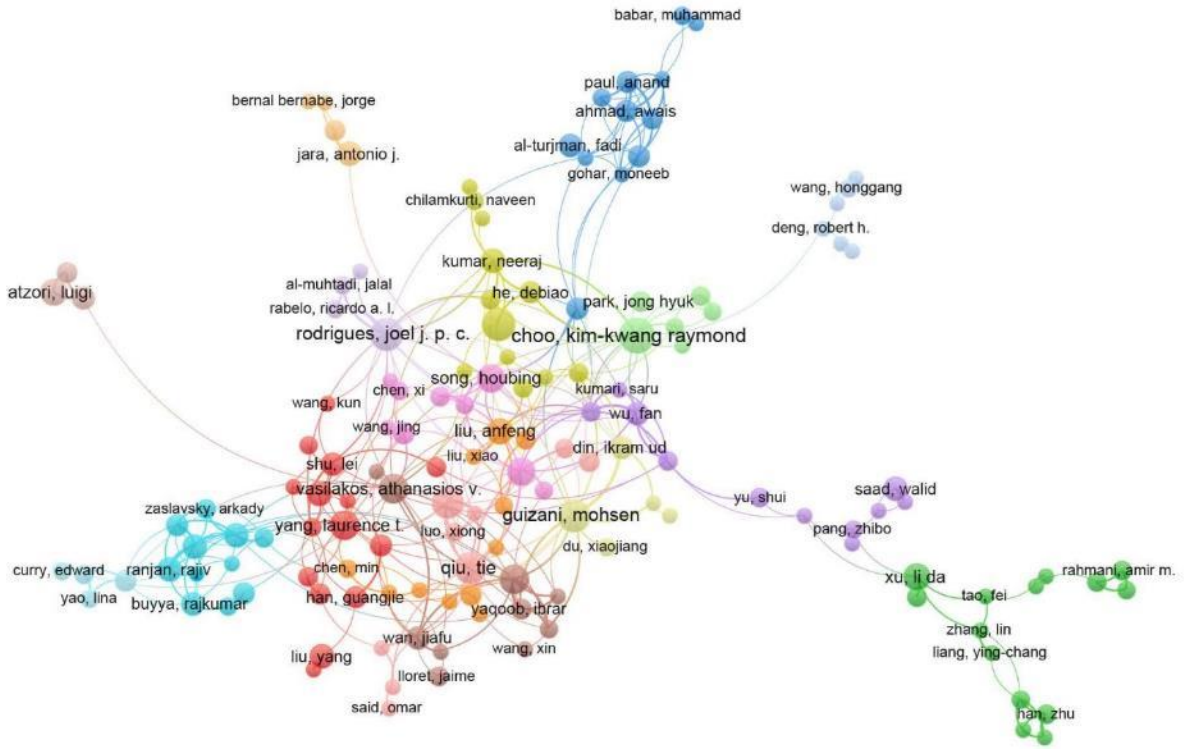
## 4. Network analysis

Network analysis is an important part of bibliometric analysis and mainly reflects the collaborative relationships among IoT publications. Next, analyses using co-authorship, citation and bibliographic coupling networks are presented.

### 4.1 Co-authorship network analysis

Fig 3 shows the collaboration network of different authors in terms of publications. The nodes represent author names, the links represent the co-authorship relationships between different

authors, and the node sizes represent each author's number of publications. The co-authorship network analysis results show that Guizani, Mohsen is the most influential author in terms of the total link strength. Guizani, Mohsen mainly studies IoT technologies innovative and practices (Al-Fuqaha, Guizani, Mohammadi, Aledhari, & Ayyash, 2015). Atzori, Luigi is the most influential author, with 6,529 citations.

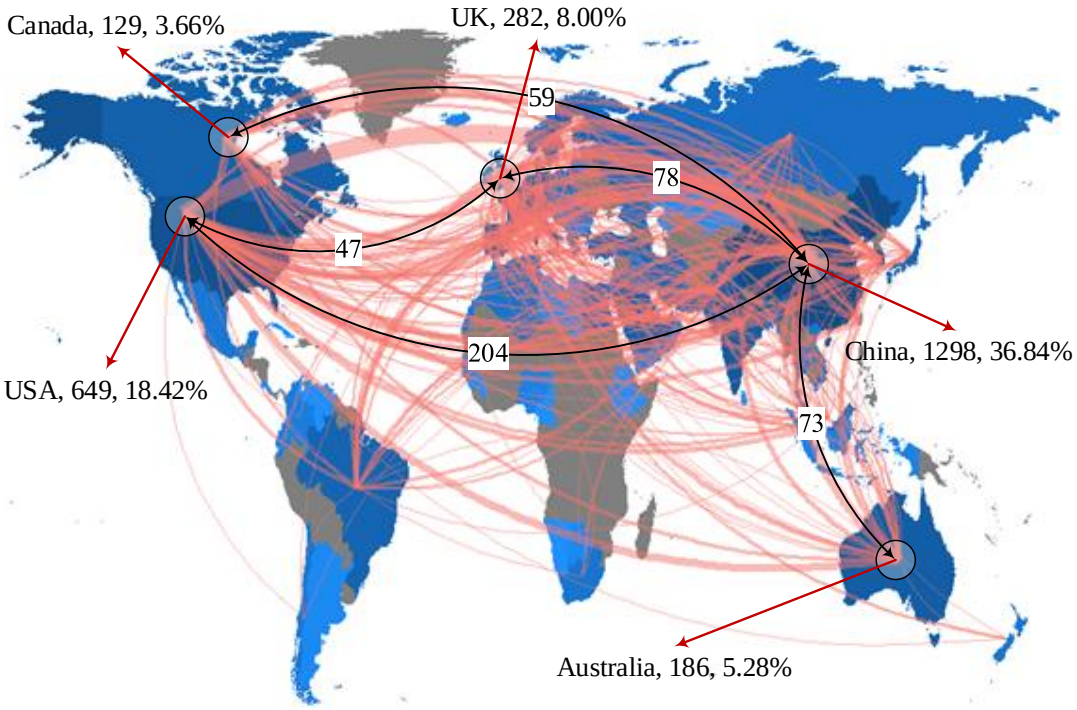



Note: The network is visualized by VOSviewer®. The whole network consists of 156 nodes, 17 clusters and 344 links. The total link strength value is 659.

Fig 3. The author co-authorship network

The data and network structure (Fig A1) show that collaborative relations between developing countries and other countries are becoming more frequent, which is one of the causes of the rapid development in developing countries. In contrast, institutions in developed economies rarely take the initiative to cooperate with institutions in other economies; they tend to choose institutions that are better than themselves as partners. The country co-authorship network is shown in Fig A2. The results show that the UK, Saudi Arabia, the USA, France and Iran are becoming research centres for the IoT. In addition, these countries include developed economies and developing economies,

which indicates that there is no theoretical leading region for the study of the IoT. The country collaboration map is shown in Fig 4.



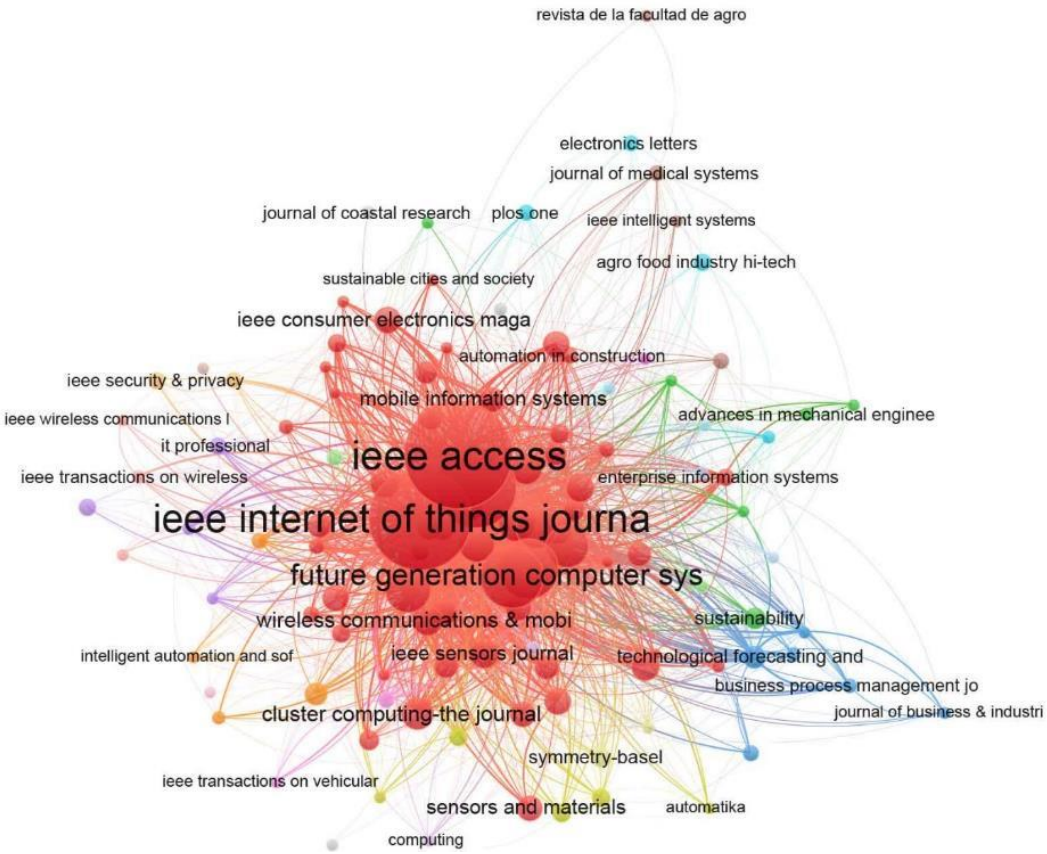

Note: The network is visualized by biblioshiny®. The red links represent the collaborative relationships between different countries. The blue colour represents the number of publications, where a darker colour indicates a greater number of publications.

Fig 4. Collaboration map of the top five countries

The collaboration map (Fig 4) shows that collaborative research between different countries has become a mainstream trend. The collaborative relationship between the USA and China is the most frequent, with 204 collaborations. This is followed by China and the UK, with 78 collaborations. In addition, the country collaboration map shows that China, the USA, the UK, Australia, Canada and Korea have extensive collaborative relations with other countries in the world. Notably, China, the USA, the UK, Australia and Canada have published 2,544 IoT-related papers, accounting for 72.21%. This also shows that cooperative research between countries is more easily able to achieve greater results than individual research.

### 4.2 Citation network analysis

In this subsection, the source citation network is constructed, as shown in Fig 5. This network shows that the top ten journals by the number of links are *Computer Networks* (106), *IEEE Internet of Things Journal* (105), *Future Generation Computer Systems-the International Journal of eScience* (97), *IEEE Access* (97), *IEEE Communications Surveys and Tutorials* (93), *Sensors* (92), *Ad Hoc Networks* (89), *Journal of Network and Computer Applications* (89), *IEEE Transactions on Industrial Informatics* (83), and *IEEE Communications Magazine* (80). These journals are the core journals that accept IoT-related papers.




Note: The network is visualized by VOSviewer®. The whole network consists of 116 nodes and 1,789 links, and the total link strength of this network is 8,035. Those journals marked in red tend to accept publications with general topics in the IoT. The nodes marked in blue pay more attention to the related topics of the integration of the IoT and business. The nodes marked with green tend to pay more attention to the application of the IoT in green and clean products. Nodes marked in yellow tend to focus on sensor topics.

Fig 5. The source citation network

From the source citation network results, some valuable conclusions can be obtained, including that these important journals maintain strong citation relationships with each other. The nodes representing these journals are mostly red, which indicates that the types of articles accepted by these journals have a certain similarity and that each journal has not formed a distinctive feature theme. The key indicator for judging whether different journals are similar is whether there is a relationship between citation intensity and citation direction among the publications they accept. This phenomenon may change with the passage of time, as different journals may tend to accept different types of research articles, including technology, applications and algorithms. Detailed information on these journals can be found in Table 1.

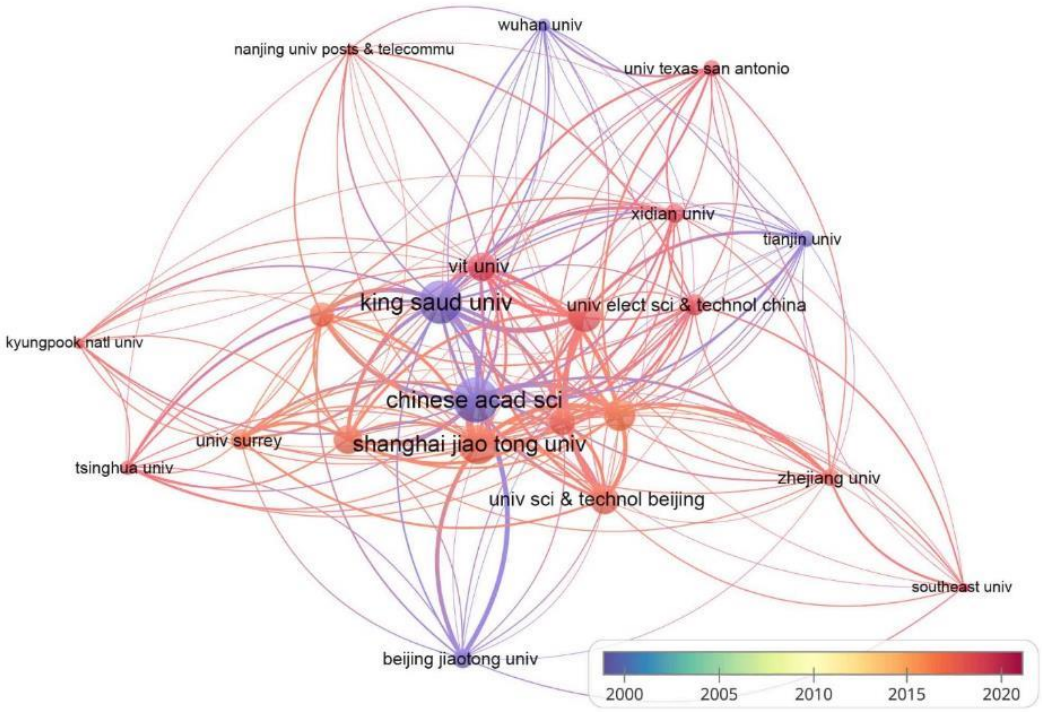
The author citation network is shown in Fig A3. The network analysis results (Fig A3) showed that the largest link is Atzori, Luigi from the University of Catania. His team mainly focuses on the social IoT (SIoT) (Atzori, Iera, & Morabito, 2011; Atzori, Iera, Morabito, & Nitti, 2012) and trustworthiness management (Nitti, Girau, & Atzori, 2014). The second-largest link is Iera, Antonio from the University of Reggio Calabria. His team shares the same research themes as the team of Atzori, Luigi, including the SIoT (Atzori, Iera, & Morabito, 2014; Atzori, Iera, Morabito, & Nitti, 2012). The detailed information of author citations is shown in Table 4.

Table 4. Detailed information for the authors citations

| R | Author | W1 | W2 | W3 | W4 | W5 | S1 | S2 | S3 |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Atzori, Luigi | 80 | 403 | 14 | 6529 | 34.13 | 2014 | 466.36 | 2.44 |
| 2 | Iera, Antonio | 79 | 365 | 10 | 6241 | 31.37 | 2014 | 624.10 | 3.14 |
| 3 | Morabito, Giacomo | 78 | 343 | 8 | 6135 | 26.82 | 2014 | 766.88 | 3.35 |
| 4 | Buyya, Rajkumar | 66 | 173 | 10 | 3933 | 61.87 | 2017 | 393.30 | 6.19 |
| 5 | Xu, Lida | 65 | 241 | 14 | 3617 | 66.41 | 2014 | 258.36 | 4.74 |
| 6 | Li, Shancang | 57 | 178 | 7 | 2410 | 44.25 | 2014 | 344.29 | 6.32 |
| 7 | Guizani, Mohsen | 71 | 302 | 22 | 2131 | 74.98 | 2018 | 96.86 | 3.41 |
| 8 | Vasilakos, Athanasios v. | 66 | 204 | 17 | 2084 | 59.15 | 2015 | 122.59 | 3.48 |
| 9 | Perera, Charith | 51 | 179 | 12 | 1861 | 29.11 | 2016 | 155.08 | 2.43 |
| 10 | Georgakopoulos, Dimitrios | 48 | 138 | 9 | 1589 | 23.17 | 2015 | 176.56 | 2.57 |

Note: W1 represents the weight<Links>; W2 represents the weight<Total link strength>; W3 represents the weight<Publications>; W4 represents the weight<Citations>; W5 represents the weight<Norm. citations>; S1 represents the score<Avg. pub. year>; S2 represents the score<Avg. citations>; S3 represents the score<Avg. norm. citations>.

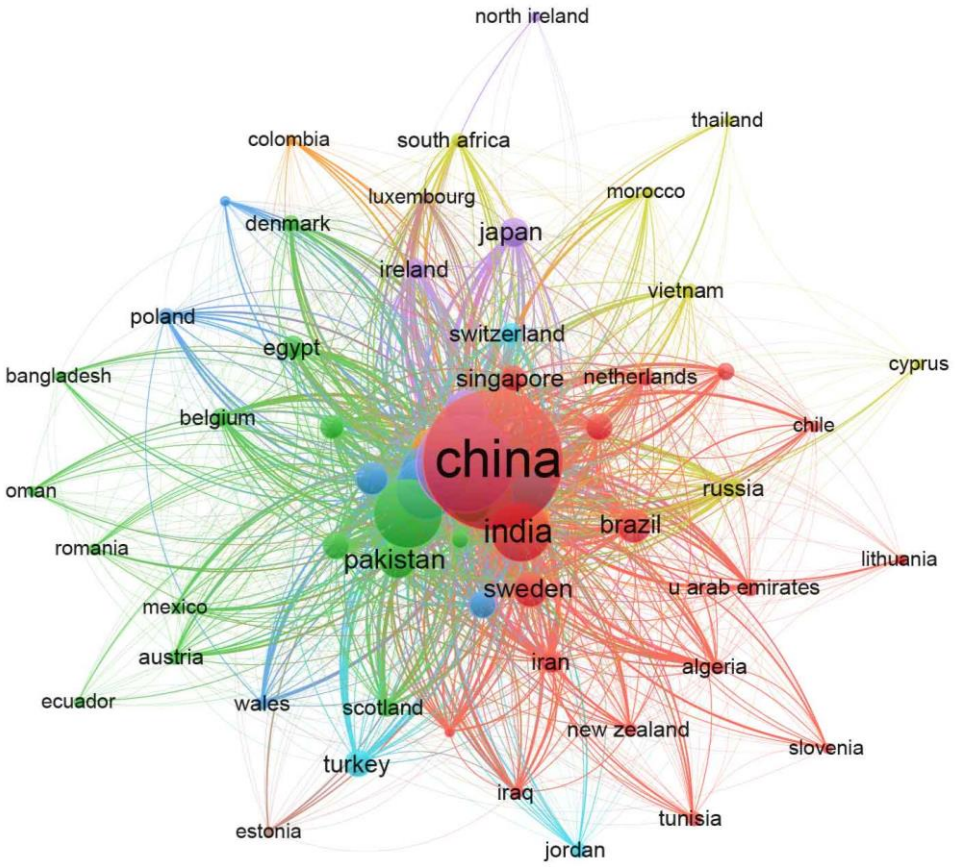
In terms of citations, the influential authors also often have collaborative relationships, such as Atzori, Luigi. Iera, Antonio and Morabito, Giacomo have a partnership, and the most impactful article they ever published was “The Internet of Things: A survey”, which was published in Computer Networks (Atzori, Iera, & Morabito, 2010). This article in the WoS database has been cited 5,153 times as of March 28, 2020. The citation analysis results are shown in Fig 6.




Note: The network is visualized by VOSviewer®. The maximum number of institutions per publication was set to 25, and 22 out of the 2,851 institutions met the thresholds.

Fig 6. The citation analysis results based on research institution

Fig 6 shows the related collaborative relationships between different research institutions. The clustering results show that the CAS and King Saud Univ have extensive collaborative relationships with research structures in other parts of the world. The CAS and King Saud Univ are located in developing economies, and these results show that developing economic regions play a key role in promoting collaborative research on the IoT. The country citation network is shown in Fig 7.




Note: The network is visualized by VOSviewer®. The whole network consists of 70 nodes, 4 clusters and 1,612 links, and the total link strength of this network is 34,994.

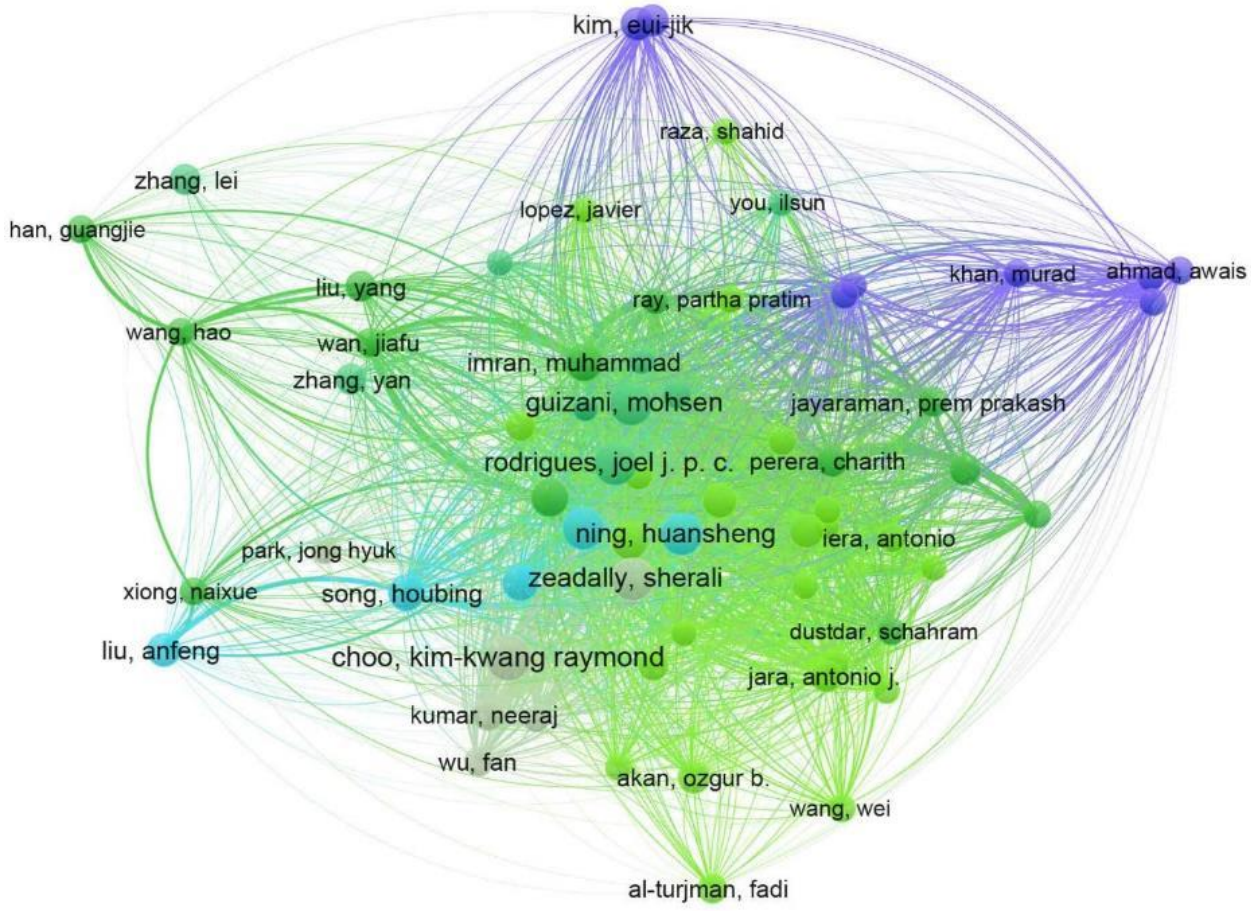
Fig 7. The country citation network

Fig 7 shows that the top ten countries by normalized number of citations are China (1,311), the USA (999), the UK (335), Australia (307), India (293), Italy (257), South Korea (245), Canada (184), Saudi Arabia (168), and France (153). Developed economies accounted for 70% of the top ten, and the sum total of IoT publications in developed economies was 2,480, accounting for 58%. This shows that developed economies play an important role in scientific research in the field of the IoT. In addition, developing economic regions are playing a key role in promoting collaborative study in the IoT field.

### 4.3 Bibliographic coupling network analysis

The coupling analysis results (Fig A4) based on sources show that the largest weight is obtained for *IEEE Internet of Things Journal*, followed by *IEEE Access*, *Future Generation Computer Systems-the International Journal of eScience*, *IEEE Transactions on Industrial Informatics*, and *Sensors*. Their weights are 561.41, 334.75, 329.86, 142.31, and 119.40, and their

shares of the total value reach 20.72%, 12.36%, 12.18%, 5.25%, and 4.41%, respectively. It should be noted that *IEEE Communications Surveys and Tutorials* is an online journal published by the IEEE Communications Association; its impact factor has reached 25.222 in the past five years, and its content covers all aspects of the communications field. The *IEEE Internet of Things Journal* and *IEEE Access* have many relationships with other journals, and these results show that they are playing an important role in influencing the future research trends of the IoT. The coupling of publications reflects the relationship between two cited publications. The author bibliographic coupling network is shown in Fig 8.




Note: The network is visualized by VOSviewer®. The nodes represent publications; the edges represent citation relationships between publications. The number of edges connected to a publication determines the size of the node. The larger the node is, the stronger the citation relationship between the publication and other publications.

Fig 8. The results of the coupling analysis based on authors

Fig 8 shows the coupling analysis results. These results show that the most influential article in the field of the IoT is Atzori, Iera, & Morabito (2010), which introduced the key technologies for implementing the IoT and the development direction of the IoT, and that article provides a good reference for the research of the IoT. The weight value of that article in the network is 11,810, and the proportion is 2.32%. This is followed by Gubbi, Buyya, Marusic, & Palaniswami (2013), which was published in *Future Generation Computer Systems*; that research mainly focuses on the constituent elements of the IoT and future development directions. Gubbi, Buyya, Marusic, & Palaniswami (2013) has a weight of 6,787 in the network, and the ratio is 1.33%. After co-citation analysis, these studies are divided into five categories, and the literature data with the highest weights in these five categories are shown in Table 5.

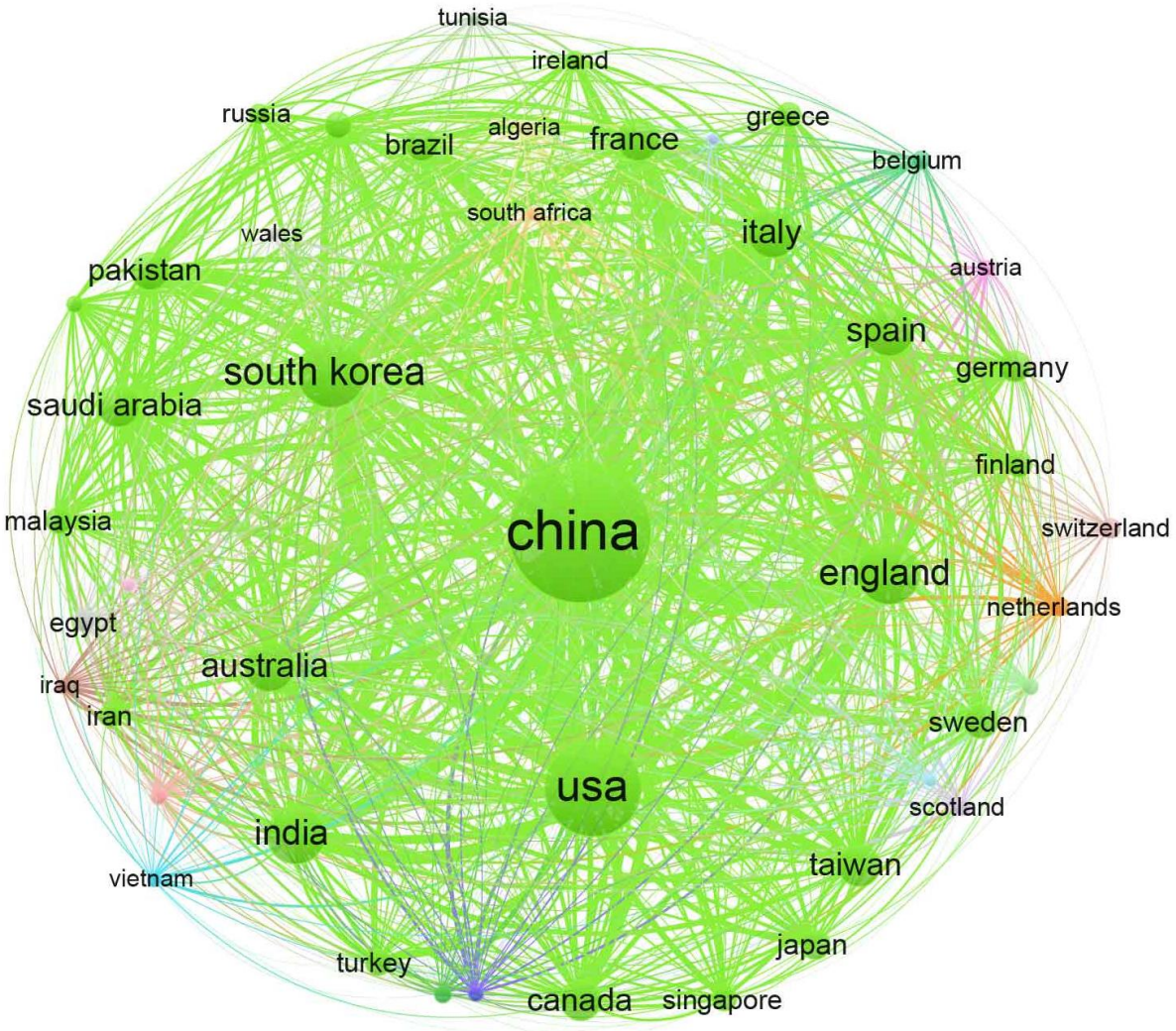
Table 5. The most weighted literature data in these five categories based on VOSviewer

| Label | X | Y | Cluster | T1 | T2 | T3 | T4 |
|---|---|---|---|---|---|---|---|
| Atzori, Iera, & Morabito (2010) | 0.3386 | 0.3515 | 2 | 676 | 11810 | 731 | 2.32% |
| Zhang & Wen (2017) | -0.1043 | -0.2659 | 1 | 617 | 3379 | 216 | 0.66% |
| Roman, Zhou, & Lopez (2013) | -0.2889 | 0.6223 | 3 | 601 | 4703 | 195 | 0.92% |
| Li, Lu,, Liang, Shen, Chen, & Lin (2011) | -0.593 | 0.3579 | 5 | 574 | 3326 | 166 | 0.65% |
| Lee & Lee (2015) | 0.8052 | 0.335 | 4 | 462 | 1724 | 102 | 0.34% |

T1: weight<Links>; T2: weight<Total link strength>; T3: weight<Citations>; T4: percentage.

The number of studies published by scholars is one of the important indicators, that enables us to reflect whether scholar belong as experts in the IoT field. It has a positive effect for readers to quickly learn about experts in the IoT field by analysing the number of articles published. Table 5 shows that these authors have a considerable number of publications. As far as the number of articles cited is concerned, most of are from Atzori, Iera, & Morabito (2010) who comes from the University Cagliari; he has published 46 journal articles related to the IoT. In-depth mining of the author's relevant information, in this study showed that most of these authors are university professors. In addition, most authors have collaborative relationships and come from the same institution, for example, Atzori, Iera, & Morabito (2010) published an article entitled “The Internet of Things: A survey”.

In-depth collaboration between scientists and researchers from different countries in the IoT field has become a mainstream trend, and this in-depth collaboration phenomenon has a positive effect on promoting the rapid rise of IoT applications in different scenarios. The coupling analysis results based on countries are shown in Fig 9.




Note: The network is visualized by VOSviewer®. The nodes represent countries; a larger node indicates that the node has greater influence on other nodes. The lines represent the mutual relationships between those nodes; the different colours of the lines represent different clusters.

Fig 9. The results of coupling analysis based on countries

Fig 9 shows the results of the literature coupling. According to the weight ranking, the top five most influential countries are China, the USA, the UK, South Korea and India. The total link strength of these countries with other countries has reached 499,486; 409,396; 224,934; 202,134; and 179,176, respectively. It is important to note that the total connectivity is 3,432,852. Their

proportions are 14.55%, 11.93%, 6.55%, 5.89%, and 5.22%, respectively. The coupling results show that China, the USA, South Korea and India cite large numbers of the same literature, which indicates that the development of the IoT in these countries has the same literature reference foundation. Aiming to further analyse the mutual coupling relationships between those nodes and the characteristics, this sub-section selects several representative countries to further analyse the coupling of the literature. The publication coupling network is shown in Fig A5.

The following two features can be obtained from Fig A5: First, different countries tend to have coupling relationships with other countries that have a greater influence on the IoT, which has led to the emergence of widespread collaboration between countries that have greater influence and other countries that have less influence in the IoT field (Fig A5. a and b confirm this conclusion). Those countries with greater influence include the USA, China, the UK, and India. Second, countries with moderate influence tend to have coupling relationships with those countries that have a greater influence rather than with countries with less influence. As a result, countries that have moderate influence have more citation collaboration with countries that have a high relative influence (Fig A5. c and d confirm this conclusion). These regions include Japan and Singapore.

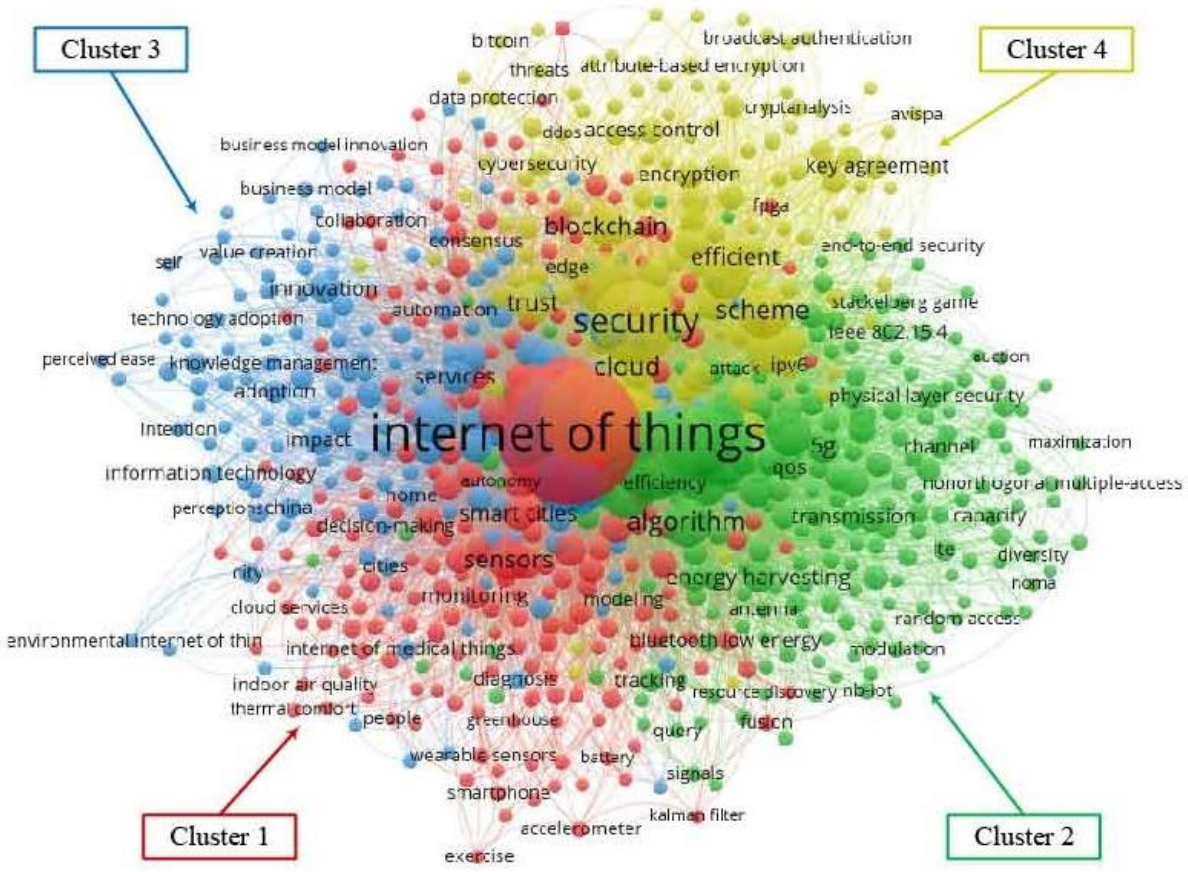
## 5. Thematic trend and challenge analysis results

A total of 11,899 keywords in 3,523 publications from 2000 to 2019 are analysed. A total of 2,531 keywords appeared twice, 1,401 keywords appeared three times, and 962 keywords appeared four times. The most frequently used keyword is “internet of things”, used 1,710 times, followed by “iot” 674 times, “security” 456 times, “internet of things (iot)” 557 times and “wireless sensor networks” 324 times. Next, the thematic trends and challenges are analysed.

### 5.1 Keyword co-occurrence network analysis

Based on the above keyword data, a cluster method is used to analyse the co-occurrence features of different keywords in the related IoT literature in this sub-section, which aims to show the main trends of keyword co-occurrence. The keyword co-occurrence network analysis results are shown in Fig 10. All keywords are divided into four main clusters. Based on these analysis

results, keywords with more than 20 occurrences in each cluster are selected, and the detailed information of each cluster is shown in Table 6.




Note: The network is visualized by VOSviewer®. The minimum number of occurrences of a keyword is set to 6.

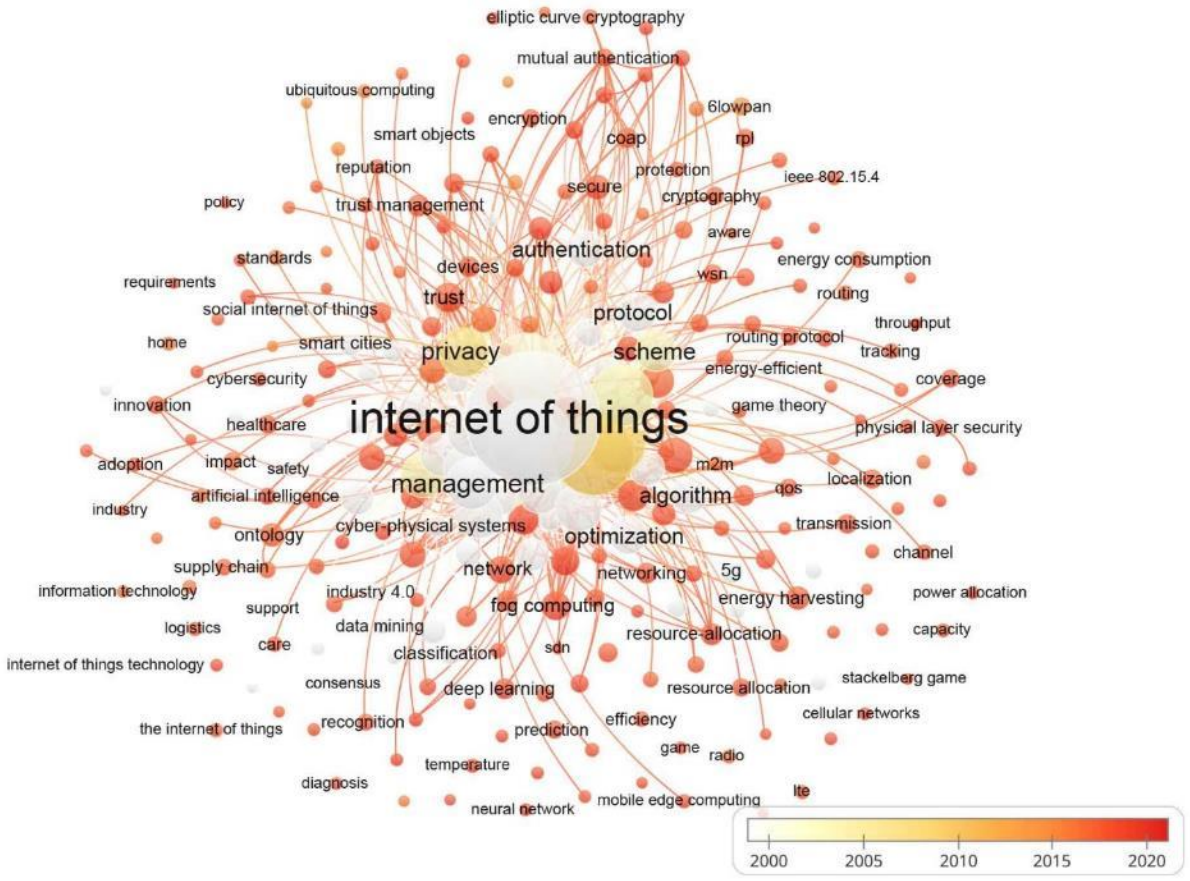
Fig 10. Keyword co-occurrence network

Cluster 1 mainly focuses on the IoT, big data, sensor research, and cloud computing. The most frequent keyword is “internet of things”, with 1,710 occurrences. Cluster 2 mainly focuses on algorithm and optimization research, including algorithm design for the IoT and routing protocols. Cluster 3 mainly focuses on IoT management issues related to performance management and supply chain management. Cluster 4 pays more attention to security and challenge issues, such as network attacks and privacy. The results are shown in Table 6.

Table 6. The main keywords identified based on a cluster method.

| Cluster | Cluster keywords (occurrences≥20) and the most frequent keywords |
|---|---|
| Cluster 1 | **35 keywords**: internet of things, cloud computing, sensors, big data, sensor, rfid, machine learning, smart city, wireless sensor network, middleware, smart cities, web, classification, ontology, interoperability, deep learning, artificial intelligence, internet, zigbee, smart objects, health, identification, prediction, anomaly detection, big data analytics, data mining, semantic web, data analytics, monitoring, quality of service, care, recognition, environment, network security, social IoT.<br>**The most frequent keyword**: internet of things, occurrences=1710. |
| Cluster 2 | **42 keywords**: wireless sensor networks, networks, design, systems, algorithm, optimization, sensor networks, communication, wireless, energy, network, energy efficiency, 5g, energy harvesting, access, resource allocation, selection, algorithms, networking, internet-of-things (iot), routing protocol, localization, transmission, discovery, sensor network, wireless networks, allocation, qos, resource allocation, cognitive radio, coverage, game theory, reliability, mobility, performance analysis, power, clustering, physical layer security, strategy, tracking, machine, routing.<br>**The most frequent keyword**: wireless sensor networks, occurrences=557. |
| Cluster 3 | **34 keywords**: management, system, model, framework, technology, performance, information, industrial IoT, technologies, service, integration, smart, services, future, platform, cyber-physical systems (CPS), innovation, industry 4.0, healthcare, implementation, mobile, smart grid, smart home, impact, vision, quality, supply chain, context, opportunities, adoption, analytics, knowledge, standards.<br>**The most frequent keyword**: management, occurrences=230. |
| Cluster 4 | **40 keywords**: security, challenges, privacy, architecture, scheme, protocol, cloud, authentication, blockchain, trust, fog computing, edge computing, efficient, industrial internet of things (iiot), secure, attacks, intrusion detection, protocols, trust management, wsn, coap, health-care, devices, access-control, issues, rpl, encryption, 6lowpan, cryptography, access control, lightweight, iot applications, mutual authentication, key agreement, low-power, cybersecurity, key agreement scheme, survey, of-the-art, user authentication.<br>**The most frequent keyword**: security, occurrences=456. |

To analyse the evolution of keywords in the last 20 years, the keyword co-occurrences with a timeline are shown in Fig 11. The red nodes represent the most recent emerging topics, which include block chain, wireless power transfer (WPT), fog, and intrusion detection. As an emerging topic in the field of the IoT, a block chain is a decentralized core system that has been used in digital cryptocurrencies (Carreno, Aguilar, Pacheco, Acevedo, Yu, & Acevedo, 2019; Li, Cai, Deng, Yao, & Wang, 2019). In addition, using radio-frequency WPT to achieve three-dimensional positioning of IoT devices has also become an emerging topic in research this year. Existing research results show that as long as a smart device is located in the radiating near-field area, the distance from the anchor point to the target can be estimated easily (Aziz, Ginting, Setiawan, Park, Tran, Yeon, Kim, & Choi, 2019).

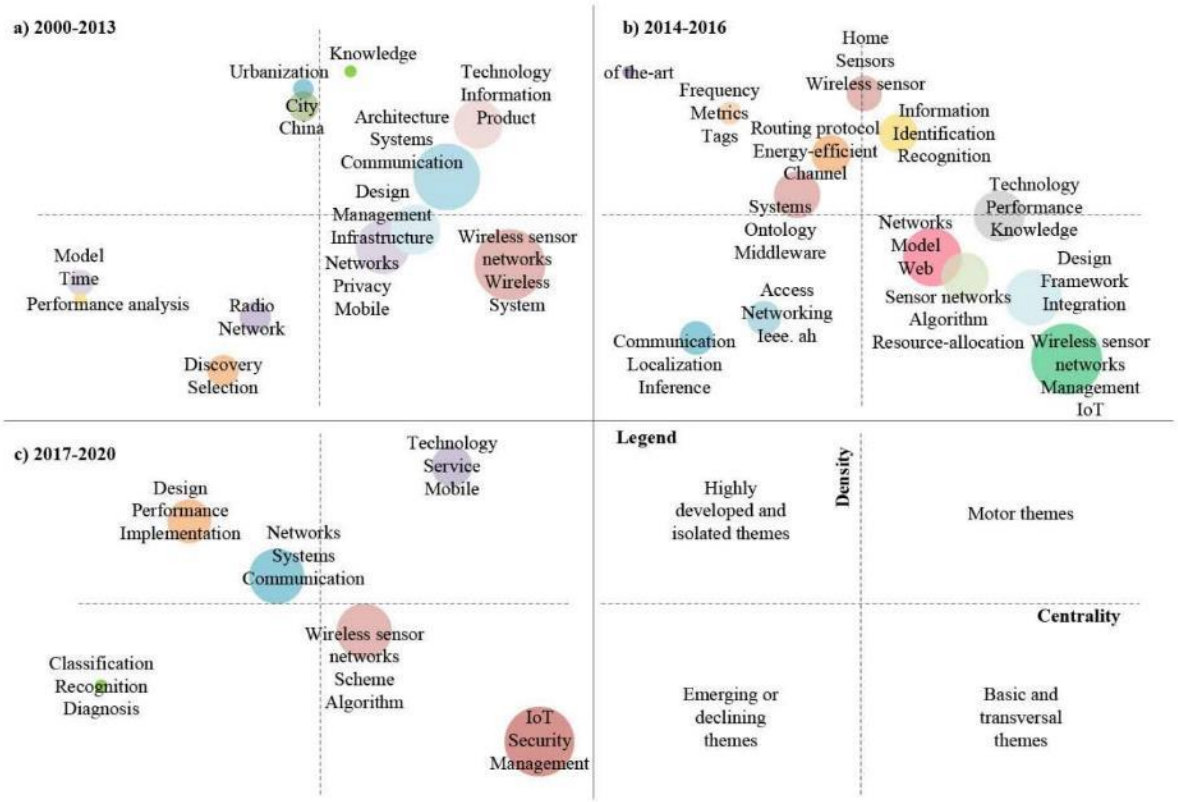



Note: The network is visualized by VOSviewer®. This network includes 268 nodes and 8,741 links; note that the different colours of the nodes represent different years.

Fig 11. The keyword co-occurrences with a timeline

## 5.2 Keyword evolution trends

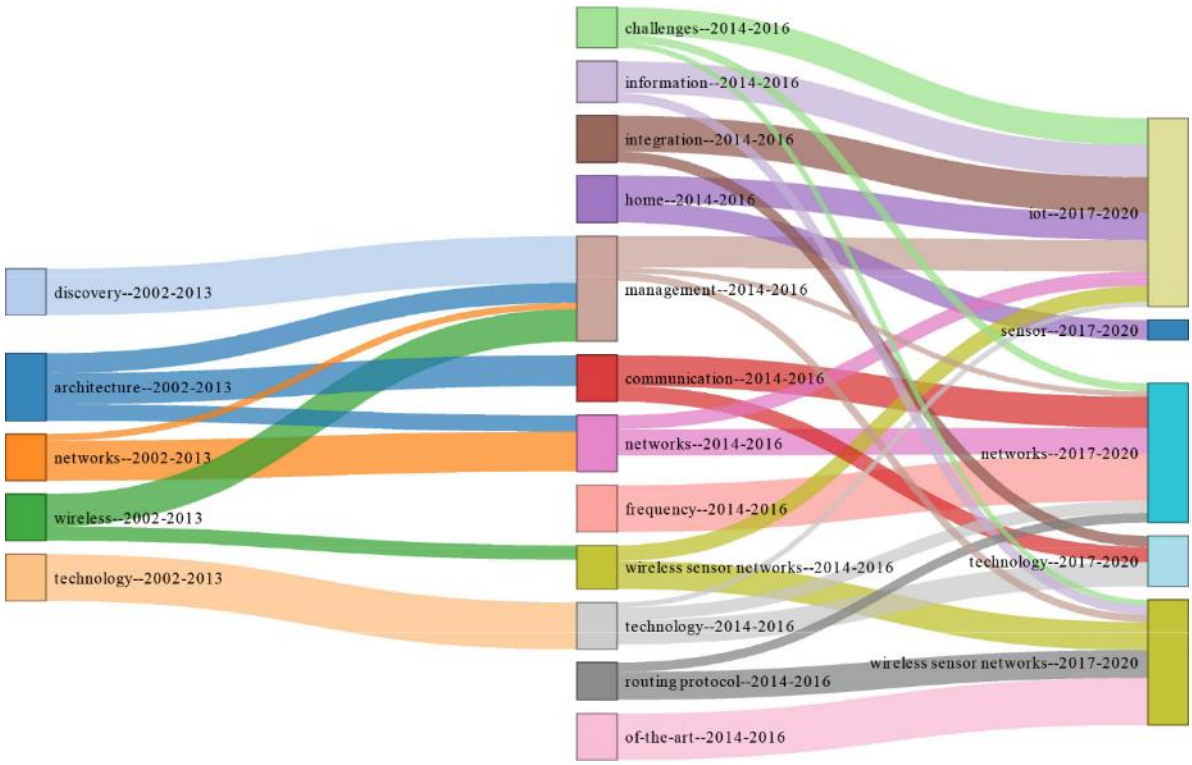
To reveal the evolution of keyword trends, strategic diagrams are constructed, as shown in Fig 12. The strategic diagrams include four quadrants: the first quadrant represents the thematic keywords belonging to motor themes; the second quadrant represents the thematic keywords belonging to highly developed themes; the third quadrant represents the thematic keywords belonging to emerging themes; and the fourth quadrant represents the thematic keywords belonging to basic and transversal themes.




Note: The network is visualized by biblioshiny®.

Fig 12. Keyword thematic map for IoT-related articles from 2000-2020

In Fig 12 (a)-(c), the motor area represents themes that have been well developed in the IoT field. The highly developed and isolated area represents themes that have good internal development. The emerging or declining area represents themes that have weakly developed. The basic and transversal areas represent themes that have weak internal development. Next, the thematic evolution is analysed based on keywords, and a Sankey diagram based on keyword thematic evolution is shown in Fig 13.




Note: The network is visualized by biblioshiny®. The number of keywords is set to 500, the minimum cluster frequency is set to 3, and the inclusion index is weighted by word occurrences.

Fig 13. Sankey diagram based on keyword thematic evolution from 2002-2020

According to the Sankey diagram (Fig 13) and keyword thematic map (Fig 12) analysis results, the following two features are valuable: a) The basic and transversal themes show that security and algorithm issues have become basic themes in the IoT field in recent years. From 2000-2013, the basic themes focused more on networks, design and wireless sensor networks. From 2014-2016, the basic themes focused more on IoT security and algorithms. Security and privacy challenges for the IoT and potential solutions are introduced in detail in the challenges and discussion section. b) The highly developed and isolated themes show that IoT networks and design have developed rapidly in recent years. From 2000-2016, IoT routing protocols and systems developed rapidly. Rank and Sybil attacks are the mainstream attack methods in the IoT. In recent years, research has aimed to provide more secure application scenarios for the IoT, and the design of a more secure and trustworthy routing protocol has become a main study hotspot and urgent issue (Airehrour, Gutierrez, & Ray, 2019).

### 5.3 Challenges and discussion

According to the keyword co-occurrence network and keyword thematic evolution results, IoT trust management, security and architecture have become challenging mainstream research topics. The security topic appears 456 times, architecture and framework topics appear 380 times, and trust and privacy topics appear 294 times. Hence, in this subsection, the challenges of IoT trust management, security and architecture are analysed and discussed in detail, and these challenges aim to transform the IoT from a hot concept into a good engineered viable technological paradigm.

**a) Trust challenges.** There are many nodes involved in an system composed of various intelligent devices and transmission protocols (Ding, Hu, Ke, Wang, & Chang, 2019; Zhang, Yang, Su, & Zheng, 2019; Zhang, Wang, Li, & Su, 2018). When a single node in the IoT network is attacked, it is easy to cause paralysis of the IoT system. One of the better ways to solve the collapse issue is to improve the robust performance and reliability of the IoT network, so the trust management (TM) issue in the IoT field has attracted the attention of many scholars (Ben, Olivereau, Zeghlache, & Laurent, 2013). Fig 14 shows a schematic diagram of the lack of IoT functions caused by some node failures.

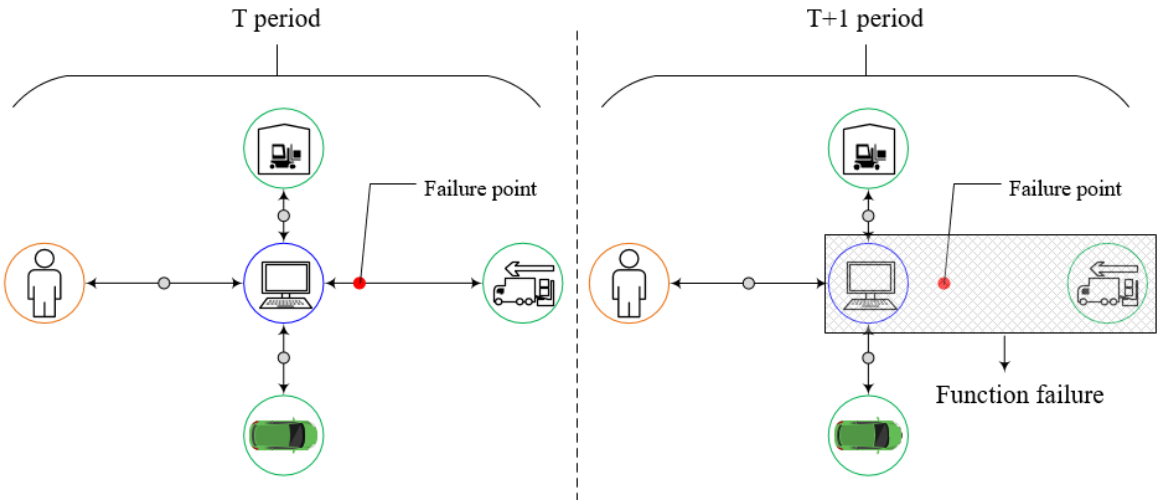



Fig 14. A schematic diagram of the lack of IoT functions caused by some node failures

Fig 14 shows an IoT system consisting of people, vehicles, warehouses and computers. Previous research results show that TM plays a positive role in building an IoT application service system based on the effective fusion of multisource isomerism data, qualified service quality, and

strong user privacy protection (Yan, Zhang, & Vasilakos, 2014). To solve the issues of TM in IoT management, Ning, Liu, & Yang (2013) provided an IoT system structure solution from four perspectives, including data, system, network and application security. However, those specific issues, including HCTI, SSR, DFMT, and TDR, have not been taken into account. Compared with previous research, Sun, Cai, Li, Liu, Fang, & Wang (2018) seemed to use a more micro-level approach in solving security management issues, and Sun, Li, Liu, Fang, & Wang (2018) briefly reviewed TM in the IoT from the aspects of authenticity and integrity of sensor data, lightweight encryption algorithms and protocols, and key protocols of the physical layer. However, as Li & Zhou (2011) described, the IoT architecture, the security of information processing and the protective management of personal privacy are unavoidable issues in the building process. Yan & Wang (2010) studied IoT TM from three aspects, the construction of heterogeneous network models, trust routing and TM design, and provided more detailed guidance for the design of a secure IoT.

**b) Security challenges**. The IoT also faces security challenges in its development. Previous investigations and research have fully described the security of the IoT, and they also provide common IoT attack methods and corresponding solutions (Lin, Yu, Zhang, Yang, Zhang, & Zhao, 2017). Harbi, Aliouat, Harous, Bentaleb, & Refoufi (2019) reported that because an IoT network enables access for a large number of devices, this also increases the risk of an attack on the network. These risks usually cause data loss in the IoT system; in a bad situation, attacks cause specific functions of the IoT to be lost. Table 7 shows the names of security risk attacks mentioned in the current literature, the potential consequences of those attacks, and the corresponding solutions.

Table 7. The names of security risk attacks, potential consequences and corresponding solutions

| No. | Name | Basic description | Potential consequences | Corresponding solutions |
|---|---|---|---|---|
| 1 | *Sleep deprivation attack* | Keep the node or device awake for a long time until it is forced to shut down | Some nodes fail and the network is down | Increase node energy storage capacity and adopt energy storage technology |
| 2 | *Sybil attack* | Malicious device has multiple legal identities in the system | Data leak, certain functions fail in IoT | Increase security identification mechanism |
| 3 | *Phishing attack* | Pretend to be a phishing website to trick user information | User account password leaked | Be alert when users go online |
| 4 | *False data injection attack* | Transfer fake data into IoT applications | Executes wrong feedback command | Detecting false or error data |
| 5 | *Malicious script attack* | Pretend to steal user confidential data in installation software | Confidential data leak | Add dynamic monitoring mechanism |
| 6 | *Sinkhole attack* | Infected device or node as a circular forwarding node | Damage to transmitted data, data leakage | Add multiple security protocols |
| 7 | *Man-in-the-middle attack* | Maliciously steal and control communication information between two normal devices | Loss of data integrity and accuracy | Deploying a secure communication protocol |
| 8 | *Deception attack* | Pretend to be a normal node or device to scam access | Specific functions fail in the IoT system | Add multi-factor authentication |
| 9 | *Worm attack* | Send malicious packets through two malicious nodes or devices | Cause network congestion and failure | Modify routing protocol |
| 10 | *Cryptanalysis attack* | Maliciously inferring encryption keys for IoT systems | Data leaks in systems, key functions fail | Set a secure encryption algorithm |
| 11 | *DDoS attack* | Bombs network with very large traffic, occupying available resources | Network paralysis | Increase network protection system |
| 12 | *Unauthorized attack* | Obtain information by accessing RFID without authentication | Information leakage | Add RFID authorized access mechanism |
| 13 | *Eavesdropping attack* | Eavesdropping on data transmitted over a wireless link | Information leakage | Set secret key to filter noise data |
| 14 | *Node capture attack* | Replace or tamper with nodes or devices in the IoT | Important information leakage | Monitor and detect malicious nodes |
| 15 | *Code injection attack* | Injecting malicious code into a node or device in the IoT | Attackers control specific functions | Verify the identity of the IoT code |
| 16 | *Routing information attack* | Controlling the spread of information by manipulating routing protocols | Data information is lost or some functions fail | Deploy a secure routing protocol |
| 17 | *Repetitive attack* | Gaining the trust of the IoT through multiple malicious inputs | Undermine the validity of the certificate | Set time and repeat threshold |
| 18 | *Malicious virus attack* | Attacks system by disguising itself as a self-propagating virus | System crash | Deploy a reliable firewall |

Table 7 shows the names of security risk attacks, the potential consequences of those attacks, and the corresponding solutions. The common feature of these attacks is to destroy or maliciously access the IoT system, thereby achieving the purpose of damaging the IoT system (Husain & Mohamed, 2019). Sleep deprivation attacks, phishing attacks and false data injection attacks have caused great challenges in the security of the IoT. Next, this subsection tries to give some effective solutions to these attacks. Sleep deprivation attacks cause the edge node functions of the IoT to fail and then affect the entire IoT system. An effective way to solve this issue is to improve the sustainable energy supply performance of edge devices, such as installing solar charging panels. Phishing attacks refer to an attacker who sends phishing websites via email or real-time chat windows (Spaulding, Mohaisen, & Ieee, 2018). In this scenario, customers are induced to click on links, and then the attacker uses them to obtain customers' personal accounts and passwords. One of the effective ways to solve this issue is to keep customers alert to unfamiliar links. A false data injection attack refers to an attacker entering false data in a node or edge device of the IoT (Liu, Qian, Hatcher, Xu, Liao, & Yu, 2019). These fake data induce the IoT control system to give wrong instructions, which is one of the attacker’s goals for destroying the IoT system. To solve a false data injection attack, it is necessary to add a data authenticity verification mechanism to IoT nodes.

**c) IoT architecture**. Service-oriented architecture (SOA) is a key technology for integrating heterogeneous systems or devices and has been successfully applied in the fields of cloud computing and vehicle networking (Da-Silva, Da-Costa, Crovato, & Righi, 2020; Paulraj, Swamynathan, & Madhaiyan, 2012). The key for SOA to be widely used in the IoT is that it supports the construction of a flexible multilayer SOA framework based on specific business needs. For example, the ITU proposes that an IoT framework should consist of five parts: sensing, access, middle, network and application layers. Domingo (2012); Li, Wang, Li, Li, Wang, & Du (2013) proposed a more simplified IoT layer framework that includes three parts: perception, network and service layers. Hossain & Muhammad (2016) proposed an IoT framework that consists of four parts: things and devices, communication gateways, clouds and data centres, and applications and services. With the aim of exploring the composition framework of the IoT, this paper conducts a

deep review of 20 highly cited papers related to the basic composition framework of the IoT. The composition framework of the IoT are shown in Table 8.

Table 8. Structure statistics of the IoT

| The structure of the IoT | Representative literature |
|---|---|
| Sensing, accessing, networking, middleware and application layers | ITU (2003) |
| Perception, network and service layers (or application layer) | Domingo (2012) |
| Application, network and sensing layers | Atzori et al. (2010) |
| Sensing, networking, service and interface layers | Xu et al. (2014) |
| Sensing, networking and application layers | Atzori et al. (2010) |
| Sensing, networking, service and interface layers | Li et al. (2015) |
| Topology, architecture, and platform layers | Islam et al. (2015) |
| Application, transportation and perception layers | Jing et al. (2014) |
| Smart objects/smart devices, hubs, cloud, third party | Stojkoska & Trivodaliev (2017) |
| Application, network, and device layers | Gazis (2017) |
| Perception, network and application layers | Lin et al. (2017) |
| Application, transportation and perception layers | Shin (2014) |
| Application, transport, network, MAC and physical layers | Jin et al. (2014) |
| Perception, network, middleware and application layers | Fang et al. (2014) |
| Devices, communication gateways, data centres and application layer | Hossain & Muhammad (2016) |
| Integrated services, applications and sensing entities layer | Tsai et al. (2014) |
| Open flow access switch, data plane, internet and cloud layer | Sun & Ansari (2016) |
| Smart device, edge/fog and cloud layers | Rahmani et al. (2018) |
| Collection station, data centre and observation station layer | Abawajy & Hassan (2017) |
| Wireless sensor networks, cloud computing and applications layer | Gubbi et al. (2013) |

The above statistical results (Table 8) show that the research results of 20 scholars have given 71 components of the IoT, but there are some overlapping and duplicate parts among them. Therefore, these 71 elements of the IoT are divided into five independent sets in this paper by using classification and summary methods, and the independent sets include smart device, perception, clouds, transportation and application layers. The research status statistics of these five parts of the IoT are shown in Table 9.

Table 9. Architecture classification of the IoT

| Literature | Smart devices | Perception | Cloud | Application | Transport |
|---|---|---|---|---|---|
| ITU (2003) | ☑ | ☑ | ☑ | ☑ | ☑ |
| Jin et al. (2014) | ☑ | ☑ | ☑ | ☑ | ☑ |
| Shamim & Hossain (2016) | ☑ | ☒ | ☑ | ☑ | ☒ |
| Fang et al. (2014) | ☒ | ☑ | ☑ | ☑ | ☑ |
| Sun & Ansari (2016) | ☑ | ☒ | ☑ | ☒ | ☒ |
| Xu et al. (2014) | ☑ | ☑ | ☒ | ☑ | ☑ |
| Li et al. (2015) | ☑ | ☑ | ☒ | ☑ | ☑ |
| Stojkoska & Trivodaliev (2017) | ☑ | ☒ | ☑ | ☒ | ☑ |
| Lin et al. (2017) | ☒ | ☑ | ☒ | ☑ | ☑ |
| Gubbi et al. (2013) | ☒ | ☒ | ☑ | ☑ | ☑ |
| Atzori et al. (2012) | ☒ | ☑ | ☒ | ☑ | ☑ |
| Rahmani et al. (2017) | ☑ | ☒ | ☑ | ☒ | ☒ |
| Gazis (2017) | ☑ | ☒ | ☒ | ☑ | ☑ |
| Abawajy & Hassan (2017) | ☒ | ☑ | ☑ | ☒ | ☒ |
| Jing et al. (2014) | ☒ | ☑ | ☒ | ☑ | ☑ |
| Islam et al. (2015) | ☑ | ☒ | ☒ | ☑ | ☑ |
| Tsai et al. (2014) | ☒ | ☑ | ☒ | ☑ | ☒ |
| Jia et al. (2012) | ☒ | ☑ | ☒ | ☑ | ☑ |
| Domingo (2012) | ☒ | ☑ | ☒ | ☑ | ☑ |
| Atzori et al. (2010) | ☒ | ☑ | ☒ | ☑ | ☑ |

According to the five independent sets (shown in Table 9), the current mainstream IoT system mainly includes five parts: a device layer, perception layer, cloud layer, transport layer and application layer. This IoT architecture has been applied to various fields, including multi-intelligent control systems (Hadipour, Derakhshandeh, & Shiran, 2020), cyber-physical systems (Silva & Jardim-Goncalves, 2019), business model renewal (Rocha, Narcizo, & Gianotti, 2019), and smart manufacturing systems (Jeong, Na, Kim, & Cho, 2018).

## 6. Conclusion

The IoT is permanently changing our world and has been applied in many fields, including smart healthcare, agriculture and manufacturing. Since the IoT was introduced, many academics and practitioners have begun to study this disruptive technique. However, there is still a lack of a systematic evaluation on this topic from a bibliometric perspective. In particular, the current literature does not answer the four questions well, including what is the basic bibliometric overview of the IoT, what are the collaboration networks of IoT research, what are the thematic trends of IoT

development, and what are the main challenges and solutions for the IoT? To address this gap, the systematic literature review method and data sources are described. Finding and insights are then illustrated through the bibliometric overview, network analysis, thematic trend and challenge analysis. Some valuable conclusions of this paper are as follows:

1) Developing economic regions are playing a key role in promoting collaborative research on the IoT through their ongoing search for cooperation with other countries. In addition, institutions in developed economies rarely take the initiative to cooperate with institutions in other economies, and they tend to choose institutions that are better than themselves as partners.

2) The mainstream study of the IoT mainly focuses on IoT security, wireless sensor networks, IoT management, IoT challenges, and privacy. In addition, the keyword thematic evolution shows that security and algorithm issues have become basic themes in the IoT field in recent years.

3) The *IEEE Internet of Things Journal* is the youngest journal and was launched in 2014. This journal mainly publishes IoT-related articles. In addition, the IEEE Internet of Things Journal is the most influential journal, with 3,043 citations, followed by IEEE Communications Magazine, with 2,468 citations.

4) China publishes the most articles and is the main productive country with 1,528 publications, followed by the USA with 896 publications. In terms of citation indicators, the USA has the largest global influence, with 21,910 citations. The USA and China have the strongest collaborative relationship, with 270 collaborations, followed by China and the UK, with 104 collaborations. Beijing University of Posts and Telecommunications is the most productive institution, with 101 publications. The University of Cagliari is the most influential institution, with 6,526 citations. Guizani, Mohsen is the most influential author in terms of the normalized citation index. Guizani, Mohsen mainly researches IoT technologies, protocols and applications. Atzori, Luigi is the most influential author, with 6,501 citations.

Moreover, this paper designs a general IoT architecture and analyses the challenges that the IoT will face in the future. In particular, trust and security challenges and potential solutions to these challenges are analysed and discussed in detail. In terms of TM, determining how to design a more trustworthy IoT system based on the effective fusion of multi-source data, qualified service

quality and strong user privacy protection has become one of the challenges in the IoT trust field. In terms of security, sleep deprivation attacks, phishing attacks and false data injection attacks are discussed in detail. In addition, this paper gives 18 common attacks on IoT systems and corresponding solutions to avoid them. The research results of this paper will help relevant researchers, entrepreneurs and governments have a clearer understanding of IoT systems.

Finally, the core difficulty of the IoT is how to realize dynamic optimization based on real-time data. Therefore, this paper suggests that researchers of the IoT should pay more attention to the dynamic optimization method of the IoT in various application scenarios in future research work, which is also one of the key components of this paper for the future. Practitioners should pay more attention to the security and reliability of the IoT in the future.

**Acknowledgements**

**Appendix A. supplementary data**

Appendix A1 shows the institutional co-authorship network. Appendix A2 briefly introduces the country co-authorship network. Appendix A3 presents the authors' citation network. Appendix A4 shows the coupling analysis results based on sources. Appendix A5 presents the publication coupling results between different countries. Appendix A6 shows the sensitivity analysis of different parameters to clustering results. Appendix A7 presents the bibliographic coupling analysis results.

**References**

Abawajy, J.H., & Hassan, M.M. (2017). Federated Internet of Things and Cloud Computing Pervasive Patient Health Monitoring System. IEEE Communications Magazine, 55(1), 48-53.

Addo-Tenkorang, R., & Helo, P.T. (2016). Big data applications in operations/supply-chain management: A literature review. Computers & Industrial Engineering, 101, 528-543.

Airehrour, D., Gutierrez, J.A., & Ray, S.K. (2019). SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. Future Generation Computer Systems-the International Journal of Escience, 93, 860-876.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. Ieee Communications Surveys and Tutorials, 17(4), 2347-2376.

Al-Turjman, F., Nawaz, M.H., & Ulusar, U.D. (2020). Intelligence in the Internet of Medical Things era: A systematic review of current and future trends. Computer Communications, 150, 644-660.

Aria, M. (2020). Bilionshiny biliomertrix. https://www.bibliometrix.org/biblioshiny/, 1, 1-2.

Atzori, L., Iera, A. & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805.

Atzori, L., Iera, A., & Morabito, G. (2011). SIoT: Giving a Social Structure to the Internet of Things. Ieee Communications Letters, 15(11), 1193-1195.

Atzori, L., Iera, A., & Morabito, G. (2014). From "Smart Objects" to "Social Objects": The Next Evolutionary Step of the Internet of Things. Ieee Communications Magazine, 52(1), 97-105.

Atzori, L., Iera, A., Morabito, G., & Nitti, M. (2012). The Social Internet of Things (SIoT) - When social networks meet the Internet of Things: Concept, architecture and network characterization. Computer Networks, 56(16), 3594-3608.

Aziz, A.A., Ginting, L., Setiawan, D., Park, J.H., Tran, N.M., Yeon, G.Y., Kim, D.I., & Choi, K.W. (2019). Battery-Less Location Tracking for Internet of Things: Simultaneous Wireless Power Transfer and Positioning. Ieee Internet of Things Journal, 6(5), 9147-9164.

Babar, M., & Arif, F. (2019). Real-time data processing scheme using big data analytics in internet of things based smart transportation environment. Journal of Ambient Intelligence and Humanized Computing, 10(10), 4167-4177.

Ben, S., Olivereau, Y., Zeghlache, D., & Laurent, M. (2013). Trust management system designs for the Internet of Things: A context-aware and multi-service approach. Computers & Security, 39, 351-365.

Bouzembrak, Y., Kluche, M., Gavai, A., & Marvin, H.J.P. (2019). Internet of Things in food safety: Literature review and a bibliometric analysis. Trends in Food Science & Technology, 94, 54-64.

Brussels. (2009). Internet of Things— An action plan for Europe. https://www.eesc.europa.eu/en/ourwork/opinions-information-reports/opinions/internet-things-action-plan-europe, 278, 1-15.

Cai, Y.Y., Lu, W., Wang, L.Q., & Xing, W.W. (2015). Cloud Computing Research Analysis Using Bibliometric Method. International Journal of Software Engineering and Knowledge Engineering, 25(3), 551-571.

Carreno, R., Aguilar, V., Pacheco, D., Acevedo, M.A., Yu, W., & Acevedo, M.E. (2019). An IoT Expert System Shell in Block-Chain Technology with ELM as Inference Engine. International Journal of Information Technology & Decision Making, 18(1), 87-104.

Da-Silva, F.S.T., Da-Costa, C.A., Crovato, C.D.P., & Righi, R.D. (2020). Looking at energy through the lens of Industry 4.0: A systematic literature review of concerns and challenges. Computers & Industrial Engineering, 143, 21.

Dang, L.M., Piran, M.J., Han, D., Min, K. ,& Moon, H. (2019). A Survey on Internet of Things and Cloud Computing for Healthcare. Electronics, 8(7), 49-59.

Ding, L., Hu, B., Ke, C.Y., Wang, T.T., & Chang, S. (2019). Effects of IoT technology on gray market: An analysis based on traceability system design. Computers & Industrial Engineering, 136, 80-94.

Domingo, M.C. (2012). An overview of the Internet of Things for people with disabilities. Journal of Network and Computer Applications, 35(2), 584-596.

Domingo, M.C. (2012). An overview of the Internet of Things for people with disabilities. Journal of Network & Computer Applications, 35(2), 584-596.

Egger, J., & Masood, T. (2020). Augmented reality in support of intelligent manufacturing - A systematic literature review. Computers & Industrial Engineering, 140, 22.

Fang, S., Xu, L.D., Zhu, Y., Ahati, J., Pei, H., Yan, J., & Liu, Z. (2014). An Integrated System for Regional Environmental Monitoring and Management Based on Internet of Things. IEEE Transactions on Industrial Informatics, 10(2), 1596-1605.

Fang, S.F., Xu, L.D., Zhu, Y.Q., Ahati, J., Pei, H., Yan, J.W., & Liu, Z.H. (2014). An Integrated System for Regional Environmental Monitoring and Management Based on Internet of Things. Ieee Transactions on Industrial Informatics, 10(2), 1596-1605.

Gazis, V. (2017). A Survey of Standards for Machine-to-Machine and the Internet of Things. Ieee Communications Surveys and Tutorials, 19(1), 482-511.

Ghadimi, P., Wang, C., & Lim, M.K. (2019). Sustainable supply chain modeling and analysis: Past debate, present problems and future challenges. Resources Conservation and Recycling, 140, 72-84.

Gibson, E., Daim, T., Garces, E., & Dabic, M. (2018). Technology Foresight: A Bibliometric Analysis to Identify Leading and Emerging Methods. Foresight and Sti Governance, 12(1), 6-24.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems-the International Journal of Escience, 29(7), 1645-1660.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. Future Generation Computer Systems, 29(7), 1645-1660.

Hadipour, M., Derakhshandeh, J.F., & Shiran, M.A. (2020). An experimental setup of multi-intelligent control system (MICS) of water management using the Internet of Things (IoT). Isa Transactions, 96, 309-326.

Harbi, Y., Aliouat, Z., Harous, S., Bentaleb, A., & Refoufi, A. (2019). A Review of Security in Internet of Things. Wireless Personal Communications, 108(1), 325-344.

Hossain, M.S., & Muhammad, G. (2016). Cloud-assisted Industrial Internet of Things (IIoT) - Enabled framework for health monitoring. Computer Networks, 101, 192-202.

Hossain, M.S., & Muhammad, G. (2016). Cloud-assisted Industrial Internet of Things (IIoT) – Enabled framework for health monitoring. Computer Networks, 101, 192-202.

Hu, G.Y., Wang, L., Ni, R., & Liu, W.S. (2020). Which h-index? An exploration within the Web of Science. Scientometrics, 9, 123.

Husain, A.J., & Mohamed, M.A.M. (2019). IMBF - Counteracting Denial-of-Sleep Attacks in 6LowPAN Based Internet of Things. Journal of Information Science and Engineering, 35(2), 361-374.

Islam, S.M.R., Kwak, D., Kabir, M.H., Hossain, M., & Kwak, K.S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access, 3, 678-708.

ITU. (2003). Internet of things reports. http://www.itu.int/osg/spu/publications/internetofthings/, 1, 1-5.

Jeong, S., Na, W., Kim, J., & Cho, S. (2018). Internet of Things for Smart Manufacturing System: Trust Issues in Resource Allocation. Ieee Internet of Things Journal, 5(6), 4418-4427.

Jia, X., Feng, Q., Fan, T., & Lei, Q. (2012). RFID technology and its applications in Internet of Things (IoT). In: International Conference on Consumer Electronics, Communications and Networks (pp. 1282-1285).

Jin, J., Gubbi, J., Marusic, S., & Palaniswami, M. (2014). An Information Framework for Creating a Smart City Through Internet of Things. IEEE Internet of Things Journal, 1(2), 112-121.

Jing, Q., Vasilakos, A.V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. Wireless Networks, 20(8), 2481-2501.

Jing, Q., Vasilakos, A.V., Wan, J.F., Lu, J.W., & Qiu, D.C. (2014). Security of the Internet of Things: perspectives and challenges. Wireless Networks, 20(8), 2481-2501.

Kwak, J.Y., Cho, C., Shin, Y., & Yang, S. (2020). IntelliTC: intelligent inter-DC traffic controller for the Internet of everything service based on fog computing. Iet Communications, 14(2), 193-205.

Lee, D., & Lee, H. (2018). IoT service classification and clustering for integration of IoT service platforms. Journal of Supercomputing, 74(12), 6859-6875.

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), 431-440.

Li, D.M., Cai, Z.M., Deng, L.B., Yao, X., & Wang, H.H. (2019). Information security model of block chain based on intrusion sensing in the IoT environment. Cluster Computing-the Journal of Networks Software Tools and Applications, 22, 451-468.

Li, H., & Zhou, X. (2011). Study on Security Architecture for Internet of Things. Applied Informatics and Communication, 224, 404-425.

Li, M.Z. (2017). Internet of People. Concurrency and Computation-Practice & Experience, 29(3), 3.

Li, Q., Wang, Z.Y., Li, W.H., Li, J., Wang, C., & Du, R.Y. (2013). Applications integration in a hybrid cloud computing environment: modelling and platform. Enterprise Information Systems, 7(3), 237-271.

Li, S., Xu, L.D., & Zhao, S. (2015). The internet of things: a survey: Kluwer Academic Publishers.

Li, S.C., Xu, L.D., & Zhao, S.S. (2015). The internet of things: a survey. Information Systems Frontiers, 17(2), 243-259.

Li, X., Lu, R.X., Liang, X.H., Shen, X.M., Chen, J.M., & Lin, X.D. (2011). Smart Community: An Internet of Things Application. Ieee Communications Magazine, 49(11), 68-75.

Li, Y., Lim, M.K., Tan, Y.S., Lee, S.Y., & Tseng, M.L. (2020). Sharing economy to improve routing for urban logistics distribution using electric vehicles. Resources Conservation and Recycling, 153, 13.

Lim, M.K., & Jones, C. (2017). Resource efficiency and sustainability in logistics and supply chain management. International Journal of Logistics-Research and Applications, 20(1), 20-21.

Lim, M.K., Tseng, M.L., Tan, K.H., & Bui, T.D. (2017). Knowledge management in sustainable supply chain management: Improving performance through an interpretive structural modelling approach. Journal of Cleaner Production, 162, 806-816.

Lim, M.K., Wang, J.X., Wang, C., & Tseng, M.L. (2020) A novel method for green delivery mode considering shared vehicles in the IoT environment. Industrial Management & Data Systems, 120(9), 1733-1757.

Lim, M.K., Xiong, W.Q., & Lei, Z.M. (2020). Theory, supporting technology and application analysis of cloud manufacturing: a systematic and comprehensive literature review. Industrial Management & Data Systems, 120(8), 1585-1614.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal, 4(5), 1125-1142.

Lin, J., Yu, W., Zhang, N., Yang, X.Y., Zhang, H.L., & Zhao, W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. Ieee Internet of Things Journal, 4(5), 1125-1142.

Liu, K., Bi, Y.R., & Liu, D. (2020). Internet of Things based acquisition system of industrial intelligent bar code for smart city applications. Computer Communications, 150, 325-333.

Liu, X., Qian, C., Hatcher, W.G., Xu, H.S., Liao, W.X., & Yu, W. (2019). Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study and Research Opportunities. IEEE Access, 7, 79523-79544.

Manavalan, E., & Jayakrishna, K. (2019). A review of Internet of Things (IoT) embedded sustainable supply chain for industry 4.0 requirements. Computers & Industrial Engineering, 127, 925-953.

Most. (2012). The 12th five-year development plan for the Internet of things. http://www.gov.cn/zwgk/2012-02/14/content_2065999.htm, 1(1), 1-5.

Munuzuri, J., Onieva, L., Cortes, P., & Guadix, J. (2020). Using IoT data and applications to improve port-based intermodal supply chains. Computers & Industrial Engineering, 139, 15.

Nees J.V.E., & Waltman, L. (2020). VOSviewer visualizing scientific landscapes. https://www.vosviewer.com/, 1, 1-8.

Ning, H.S., Liu, H., & Yang, L.T. (2013). Cyberentity Security in the Internet of Things. Computer, 46(4), 46-53.

Nitti, M., Girau, R., & Atzori, L. (2014). Trustworthiness Management in the Social Internet of Things. Ieee Transactions on Knowledge and Data Engineering, 26(5), 1253-1266.

Panetta, K. (2016). Market Research Report for internet of things. https://www.gartner.com/smarterwithgartner/7-technologies-underpin-the-hype-cycle-for-the-internet-of-things-2016/, 3(1), 12-19.

Paulraj, D., Swamynathan, S., & Madhaiyan, M. (2012). Process model-based atomic service discovery and composition of composite semantic web services using web ontology language for services (OWL-S). Enterprise Information Systems, 6(4), 445-471.

Rahmani, A.M., Gia, T.N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M., & Liljeberg, P. (2017). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. Future Generation Computer Systems, 78, 641-658.

Rahmani, A.M., Gia, T.N., Negash, B., Anzanpour, A., Azimi, I., Jiang, M.Z., & Liljeberg, P. (2018). Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things:A fog computing approach. Future Generation Computer Systems-the International Journal of Escience, 78, 641-658.

Rocha, C., Narcizo, C.F., & Gianotti, E. (2019). Internet of Management Artifacts: Internet of Things Architecture for Business Model Renewal. International Journal of Innovation and Technology Management, 16(8), 19.

Roman, R., Zhou, J.Y., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266-2279.

Santoro, G., Vrontis, D., Thrassou, A., & Dezi, L. (2018). The Internet of Things: Building a knowledge management system for open innovation and knowledge management capacity. Technological Forecasting and Social Change, 136, 347-354.

Schoenberger, C.R. (2002). The Internet of things. Forbes, 169(6), 155-185.

Shin, D. (2014). A socio-technical framework for Internet-of-Things design: A human-centered design for the Internet of Things. Telematics and Informatics, 31(4), 519-531.

Silva, E.M., & Jardim-Goncalves, R. (2019). Cyber-Physical Systems: a multi-criteria assessment for Internet-of-Things (IoT) systems. Enterprise Information Systems, 2019, 1698060.

Sinha, A., Shrivastava, G., & Kumar, P. (2019). Architecting user-centric internet of things for smart agriculture. Sustainable Computing-Informatics & Systems, 23, 88-102.

Small, H. (1973). Cocitation in scientific literature - new measure of relationship between 2 documents. Journal of the American Society for Information Science, 24(4), 265-269.

Spaulding, J., Mohaisen, A., & Ieee. (2018). Defending Internet of Things Against Malicious Domain Names using D-FENS. New York: Ieee. 10, 387-392.

Stojkoska, B.L.R., & Trivodaliev, K.V. (2017). A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production, 140, 1454-1464.

Su, J.F., Bai, Q., Sindakis, S., Zhang, X.F., & Yang, T. (2020). Vulnerability of multinational corporation knowledge network facing resource loss A super-network perspective. Management Decision, 20, 2019-0227.

Su, J.F., Yang, Y., & Yang, T. (2018). Measuring knowledge diffusion efficiency in R&D networks. Knowledge Management Research & Practice, 16(2), 208-219.

Sun, W.C., Cai, Z.P., Li, Y.Y., Liu, F., Fang, S.Q., & Wang, G.Y. (2018). Security and Privacy in the Medical Internet of Things: A Review. Security and Communication Networks, 9,1155.

Sun, X., & Ansari, N. (2016). EdgeIoT: Mobile Edge Computing for the Internet of Things: IEEE Press, 12, 22-29.

Tsai, C.W., Lai, C.F., Chiang, M.C., & Yang, L.T. (2014). Data Mining for Internet of Things: A Survey. IEEE Communications Surveys & Tutorials, 16(1), 77-97.

Tseng, M.L., Lim, M.K., & Wu, K.J. (2019). Improving the benefits and costs on sustainable supply chain finance under uncertainty. International Journal of Production Economics, 218, 308-321.

Tu, M.R., Lim, M.K., & Yang, M.F. (2018a). IoT-based production logistics and supply chain system - Part 1 Modeling IoT-based manufacturing IoT supply chain. Industrial Management & Data Systems, 118(1), 65-95.

Tu, M.R., Lim, M.K., & Yang, M.F. (2018b). IoT-based production logistics and supply chain system - Part 2 IoT-based cyber-physical system: a framework and evaluation. Industrial Management & Data Systems, 118(1), 96-125.

Wang, C., Ghadimi, P., Lim, M.K., & Tseng, M.L. (2019). A literature review of sustainable consumption and production: A comparative analysis in developed and developing economies. Journal of Cleaner Production, 206, 741-754.

Wang, C., Lim, M.K., & Lyons, A. (2019). Twenty years of the International Journal of Logistics Research and Applications: a bibliometric overview. International Journal of Logistics-Research and Applications, 22(3), 304-323.

Wang, C., Lim, M. K., Zhao, L.F., Tseng, M.L., Chien, C.F., & Lev, B. (2020). The evolution of Omega-The International Journal of Management Science over the past 40 years: A bibliometric overview. Omega-International Journal of Management Science, 93, 102098.

Wang, C., Zhao, L.F., Vilela, A.L.M., & Lim, M.K. (2019). The evolution of Industrial Management & Data Systems over the past 25 years A bibliometric overview. Industrial Management & Data Systems, 119(1), 2-34.

Wang, J.X., Lim, M.K., Zhan, Y.Z., & Wang, X.F. (2020). An intelligent logistics service system for enhancing dispatching operations in an IoT environment. Transportation Research Part E-Logistics and Transportation Review, 135, 23.

Xu, L.D., He, W., & Li, S. (2014). Internet of Things in Industries: A Survey. IEEE Transactions on Industrial Informatics, 10(4), 2233-2243.

Yan, L., & Wang, K. (2010). Trust control in heterogeneous networks for Internet of Things. International Conference on Computer Application & System Modeling. IEEE, 1,12-22.

Yan, Z., Zhang, P., & Vasilakos, A.V. (2014). A survey on trust management for Internet of Things. Journal of Network and Computer Applications, 42, 120-134.

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for Smart Cities. Ieee Internet of Things Journal, 1(1), 22-32.

Zhang, N., Yang, Y., Su, J.F., & Zheng, Y.J. (2019). Modelling and analysis of complex products design based on supernetwork. Kybernetes, 48(5), 861-887.

Zhang, N., Yang, Y., Wang, J.X., Li, B.D., & Su, J.F. (2018). Identifying Core Parts in Complex Mechanical Product for Change Management and Sustainable Design. Sustainability, 10(12), 15.

Zhang, N., Yang, Y., Zheng, Y.J., & Su, J.F. (2019). Module partition of complex mechanical products based on weighted complex networks. Journal of Intelligent Manufacturing, 30(4), 1973-1998.

Zhang, Y., & Wen, J.T. (2017). The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications, 10(4), 983-994.

Zhang, Y. ,& Zhao, W.J. (2019). Dalian Institute of Chemical Physics, Chinese Academy of Sciences. National Science Review, 6(4), 843-843.