Digital Communications and Networks 9 (2023) 677–687

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

Internet of things: Conceptual network structure, main challenges and future directions

Leonardo B. Furstenau [a,**], Yan Pablo Reckziegel Rodrigues [b], Michele Kremer Sott [c], Pedro Leivas [b], Michael S. Dohan [d], José Ricardo López-Robles [e], Manuel J. Cobo [f], Nicola Luigi Bragazzi [g], Kim-Kwang Raymond Choo [h,*]

[a] Department of Industrial Engineering, Federal University of Rio Grande do Sul, Porto Alegre 90035-190, Brazil
[b] University of Santa Cruz do Sul, Av. Independência, 2293, Santa Cruz do Sul, RS, Brazil
[c] Business School, Unisinos University, Av. Dr. Nilo Peçanha 1600, 91330-002, Porto Alegre, Brazil
[d] Lakehead University, Thunder Bay, ON, P7B 5E1, Canada
[e] Academic Unit of Accounting and Management, Autonomous University of Zacatecas, Calle Comercio y Administración S/N, Fracc. Progreso, C.P. 98066, Zacatecas, Zacatecas, Mexico
[f] Department of Computer Science and Artificial Intelligence, University of Granada, 18071 Granada, Spain
[g] York University, ON, M3J 1P3, Canada
[h] Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, TX, 78249, USA

ARTICLE INFO

Keywords:
Internet of things
Strategic intelligence
Industry 4.0
SciMAT
Bibliometric analysis
Science mapping

ABSTRACT

Internet of Things (IoT) is a key technology trend that supports our digitalized society in applications such as smart countries and smart cities. In this study, we investigate the existing strategic themes, thematic evolution structure, key challenges, and potential research opportunities associated with the IoT. For this study, we conduct a Bibliometric Performance and Network Analysis (BPNA), supplemented by an exhaustive Systematic Literature Review (SLR). Specifically, in BPNA, the software SciMAT is used to analyze 14,385 documents and 30,381 keywords in the Web of Science (WoS) database, which was released between 2002 and 2019. The results reveal that 31 clusters are classified according to their importance and development, and the conceptual structures of key clusters are presented, along with their performance analysis and the relationship with other subthemes. The thematic evolution structure describes the important cluster(s) over time. For the SLR, 23 documents are analyzed. The SLR reveals key challenges and limitations associated with the IoT. We expect the results will form the basis of future research and guide decision-making in the IoT and other supporting industries.

1. Introduction

Internet of Things (IoT) is one of the key technologies supporting the fourth Industrial Revolution and the concept of Industry 4.0 [1]. IoT devices and systems allow large amounts of data to be sensed, collected and stored for further processing using connected devices [2,3]. Generally, data is processed in cloud-based centralized servers [4] that are powered by the latest robust techniques to ensure high performance, e.g., cellular network edge [4], mobile cloud computing [5], mobile edge computing and energy harvesting [6]. The results can then be used for decision-making at different levels [7] and facilitate real-time interaction between different sectors and supply chain partners [8]. Financial estimations show that the economic impact of IoT will increase from $3.9 trillion to $11.1 trillion by 2025 [9,10]. The IoT can be used to improve industries such as healthcare [11], transportation [12], energy [13,14], supply chain [15], manufacturing [16], and other industries. Despite the potential benefits of IoT, several challenges and limitations remain to be addressed. Examples of such challenges and limitations include security and privacy [17–19], communication, hardware and software, IoT-related skillsets, regulation, legislation and culture [20].

To better understand IoT, researchers are working to understand its applications, challenges, barriers and trends, as evidenced by existing

* Corresponding author.
** Corresponding author.
E-mail addresses: leonardo.furstenau@ufrgs.br (L.B. Furstenau), yanrodrigues@mx2.unisc.br (Y.P.R. Rodrigues), sott.mk@gmail.com (M.K. Sott), pedrooliveiral@hotmail.com (P. Leivas), msdohan@lakeheadu.ca (M.S. Dohan), ricardolopezrobles@outlook.com (J.R. López-Robles), mjcobo@decsai.ugr.es (M.J. Cobo), robertobragazzi@gmail.com (N.L. Bragazzi), raymond.choo@fulbrightmail.org (K.-K.R. Choo).

https://doi.org/10.1016/j.dcan.2022.04.027
Received 31 March 2021; Received in revised form 26 April 2022; Accepted 28 April 2022
Available online 2 May 2022

literature reviews and surveys [7,21–42] and bibliometric analyses [43–47]. However, to the best of our knowledge, no study has conducted a complete analysis of the entire academic publication of the IoT (2002–2019) (see Table 1 in section 2). The bibliometric analysis supported by Systematic Literature Review (SLR) is an appropriate method to produce an overview of the research field and identify obstacles and challenges, and inform future researchers. Therefore, in this study, we conduct a Bibliometric Performance and Network Analysis (BPNA) and then an SLR to fully understand the literature of the IoT.

As part of the study, we will provide new insights to support the discovery of research opportunities and gaps in the literature. To this end, we depicted the strategic themes, thematic evolution structure, key challenges, and future research directions of IoT. As a result, 31 clusters were plotted in a strategic diagram and classified according to their centrality and density. According to findings in the literature, the most developed and important motor themes in these clusters were discussed. The thematic evolution structure presented the most significant cluster over time in terms of centrality and density and an in-depth discussion was made regarding the IoT history from 2002 to 2019. The SLR revealed IoT's main challenges and difficulties from 23 review articles, which were classified according to six factors specified by Uslu, Eren, Gür and Özcan [21]. We also presented the number of publications over time, the most productive and cited researchers, the universities and journals related to IoT.

2. Methodology and dataset

To achieve our goal, we execute a BPNA supported by an exhaustive SLR. For the BPNA, the software SciMAT was used to analyze all documents related to IoT. For the SLR, the PRISMA protocol was used to analyze documents whose objectives were to identify the challenges of IoT. The steps and criteria to perform the BPNA and SLR are described below. For this study, we propose three (3) research questions:

RQ1: What are the strategic themes of IoT?
RQ2: How is the scientific thematic structure of IoT evolved?
RQ3: What are the main challenges and limitations of IoT?

The existing bibliometric analysis of IoT in Web of Science (WoS) is shown in Table 1, presenting five (5) types of research. The coverage and focus show the differences between the bibliometric approaches, highlighting the novelty of this work in the last line.

2.1. Bibliometric performance and network analysis

Although there are Google Scholar and many databases (e.g., Scopus), studies have shown that the Web of Science (WoS) database generally indexes influential/higher quality academic journals [48]. Therefore, in this study, we used the WoS database. One of the search terms was "Internet of Things". A filter was used to find documents containing any of the search terms in the title, abstract and keywords. The document types sought were articles, articles in press and reviews. Data were extracted on December 16, 2019, using the SciMAT (Science Mapping Analysis Software Tool [49]).

Cobo, López-Herrera, Herrera-Viedma and Herrera [50] analyzed nine (9) existing bibliometric software applications, and revealed that there was no existing software in the literature that can analyze all the key elements of a science mapping. This problem forced the researchers to use other software simultaneously to perform a complete bibliometric analysis. Considering this research problem, the SciMAT was developed by the same authors [49], which enables researchers to perform a complete bibliometric process [51]. It uses procedures, algorithms and measurements at all stages of science mapping, from preprocessing to result visualization, and can also be downloaded for free [52–55]. Considering all benefits of SciMAT, a robust preprocessing module is the most important since data exported from databases requires a rigorous information preprocessing step to ensure quality data [56]. SciMAT can also create strategic diagrams (Fig. 1a) to visually identify the most important themes, the conceptual network structures (Fig. 1b) to understand the relationship between authors, keywords or references as well as the thematic evolution structure (Fig. 1c), which helps to understand how the field evolves over time [57]. The results of SciMAT can be used to enhance decision-making [58] and provide future trends, literature gaps and future directions in any research field [59–67]. Keywords were the analyzed items and the frequency of co-occurrence of the keywords was extracted. We applied the equivalence index to calculate similarity. The clustering algorithm used to identify themes was the Simple Center algorithm. In the data collection, 14,388 documents were exported and included in bibliometric analysis, including 33,489 keywords.

To discover the evolution of the research themes in the whole period, the thematic evolution structure was studied. To create this thematic evolution map, the inclusion index was used. Fig. 1c demonstrates a classic map. Lines 1 and 2 (solid lines) depict that linked clusters share the core themes, line 3 (dashed line) indicates the clusters share elements that are not the core themes, and the non-existence of a line implies discontinuity (new cluster). The thickness of the lines is proportional to the inclusion index, and the size of the clusters is proportional to the number of related documents [49]. The thematic evolution was divided into four subperiods: 2002–2006; 2007–2011; 2012–2016 and 2017–2019.

Table 1
Existing bibliometric analysis of IoT in literature.

Study	Coverage	Focus
[43]	2000–2015	Identification of the most critical studies, research themes and authors related to visions and applications of IoT
[44]	2006–2015	Applications of IoT and big data on the circular economy environment.
[45]	2011–2018	Exploration of the applications of IoT in food safety contexts.
[46]	2010–2017	Investigation of IoT field in the Arab countries.
[47]	2004–2017	Trends and innovations analysis of IoT patents.
This paper	2002–2019	Holistic understanding of the strategic themes, thematic evolution structure, main challenges and future directions.

2.2. Systematic literature review

The SLR of this work aims to identify the challenges and obstacles in the field of IoT. This method is based on the Preferred Reporting Items for Systematic Reviews and Meta-Analyzes (PRISMA) [68,69]. The PRISMA is divided into four phases: identification, screening, eligibility, and inclusion. Fig. 2 shows the flowchart. For this SLR, we used the same criteria used in BPNA in terms of database, period, and documents type. From the 14,388 documents exported from WoS, we excluded three (3) Duplicate Documents (DD) using Endnote. For the screening, documents with titles containing "challenges", "limits", "limitations", "difficulties", "obstacles", and "barriers" were searched (461). Articles without these words in the title were excluded (EX = 13,924). In the eligibility step, the documents selected (461) were read and those vaguely related (VR = 438) were excluded. Finally, 23 documents were included for qualitative analysis.

3. Bibliometric performance analysis of IoT

Fig. 3 shows the number of publications of IoT between 2002 and 2019. It can be observed that the first article was published in 2002 [70]. A number of studies were also carried out in the following years [71–74] and continued to increase thereafter. This is not suprising as IoT has been known to be one of the pillars of industry 4.0 [1]; for example, this phenomenon may be related to the "advanced manufacturing partnership" (AMP) plan launched by the US government in 2011 [75] and the

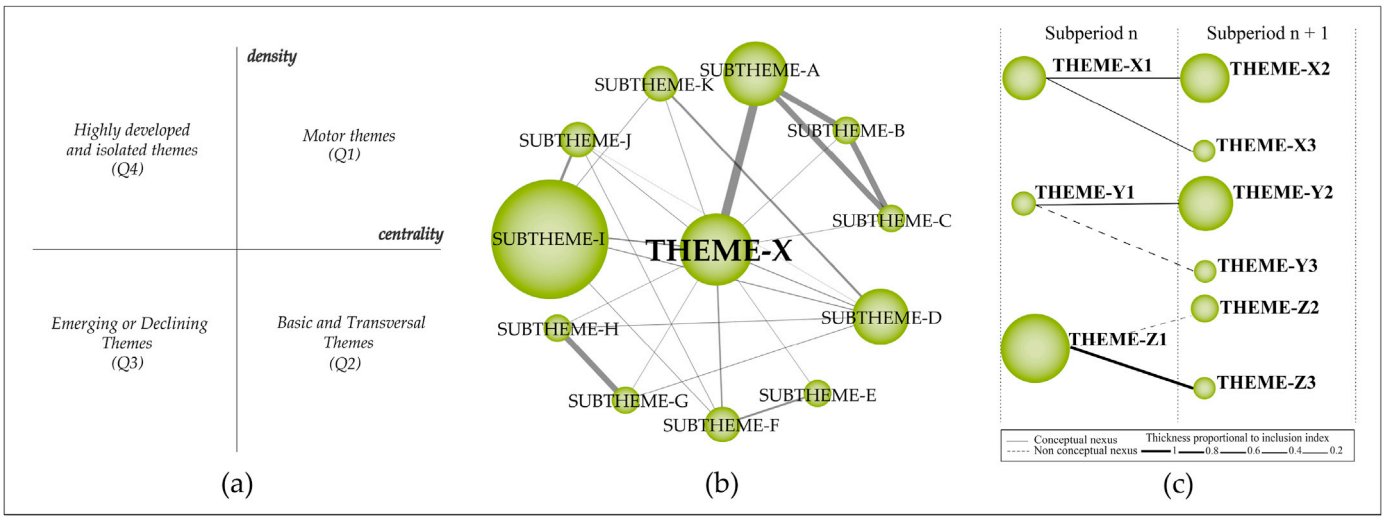


Fig. 1. Strategic diagram (a). Thematic network structure (b). Thematic evolution map (c).

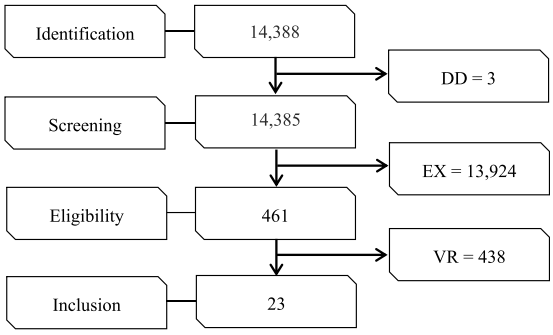


Fig. 2. The flow of information through the SLR.

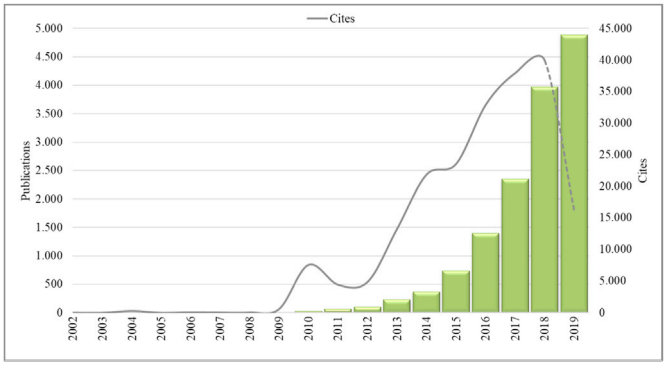


Fig. 3. The number of publications over time (2002–2019).

"High-Tech Strategy 2020" formulated by the German government in early of 2012 [1,76]. The citation performance shows an increasing trend, highlighting positive prospects in the IoT field.

Table 2 lists the most productive/cited authors from 2002 to 2019. JJPC Rodrigues is the most productive researcher in the field of IoT, with 66 publications, followed by KKR Choo and L.T. Yang. L. Atzori is the most cited writer with 6351 citations, followed by A. Iera and G. Morabito.

Table 3 lists the journals and universities that publish research related to IoT. IEEE Access ranks first, followed by IEEE Internet of Things Journal and Sensors. The most productive university is the Chinese Academy of Sciences, followed by the Beijing University of Posts Telecommunications.

Table 2
Most productive/cited authors from 2002 to 2019.

Most cited authors	Cit.	Most productive authors	Doc.
Atzori, L	6351	Rodrigues, JJPC	66
Iera, A	6113	Choo, KKR	54
Morabito, G	5888	Yang, LT	52
Xu, LD	5158	Guizani, M	51
Buyya, R	3791	Kumar, N	49
Palaniswami, M	3784	Zeadally, S	44
Vasilakos, A	2245	Park, JH	43
Guizani, M	2219	Sangaiah, AK	39
Li, S	2170	Wang, W	38
Zorzi, M	1999	Wang, ZL	37

Table 3
Journals and universities that publish studies on IoT.

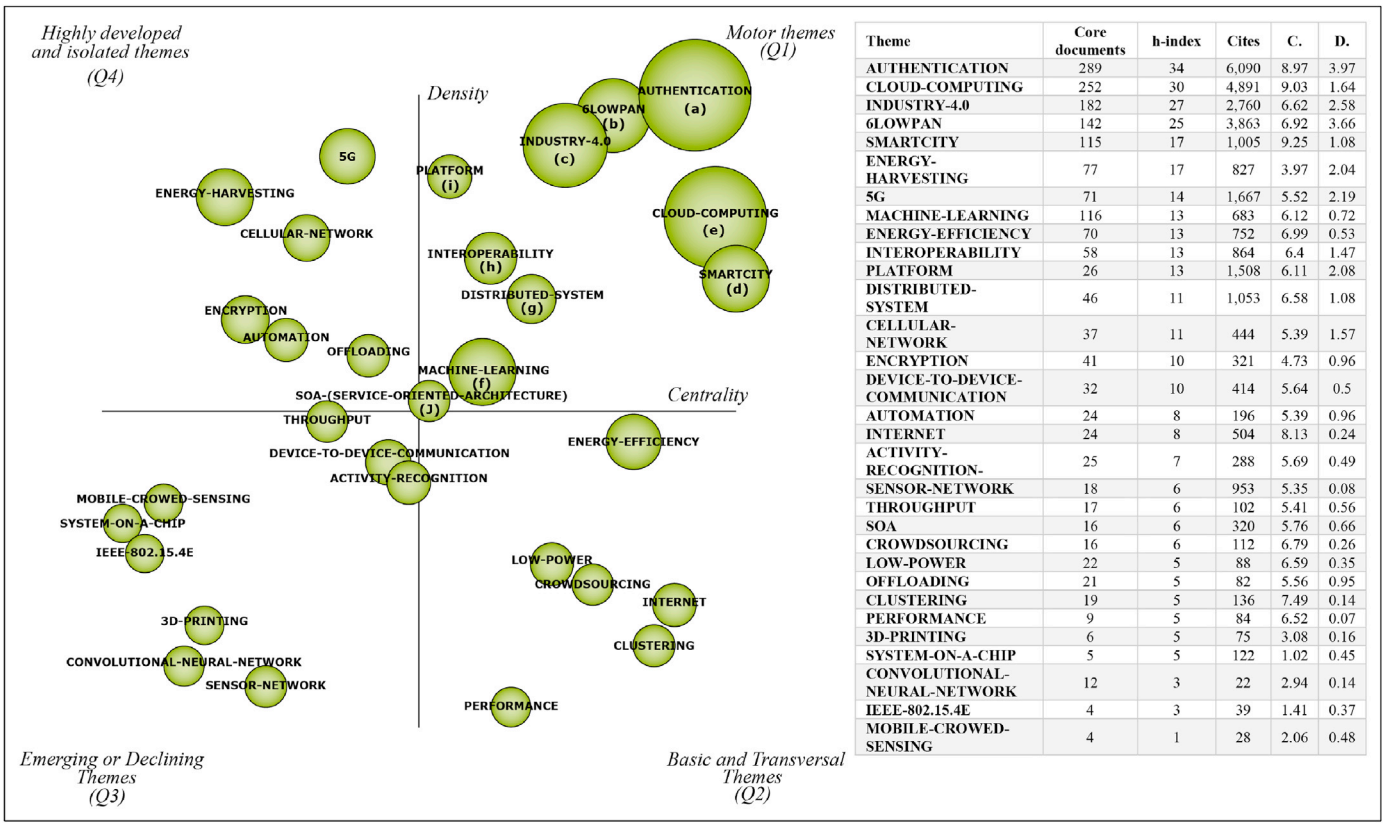
Journals	Doc.	Universities	Doc.
IEEE Access	1155	Chinese Ac. of Sciences	459
IEEE IoT Journal	1077	Beijing Univ. Posts Telecom.	282
Sensors	974	Univ. of California Syst.	222
Int. J. of E science	334	King Saud University	205
Int. J. of Dist. Sensor Net.	269	Univ. of Elect. Sci. Tech. of China	200
IEEE Tran. on Ind. Inf.	190	Univ. System of Georgia	194
IEEE Com. Magazine	178	CNRS	169
Wireless Personal Com.	174	Tsinghua University	169
Computer Networks	150	Xidian University	166
IEEE Sensors Journal	149	Indian Inst. of Technology	150

4. Bibliometric network analysis of IoT from 2002 to 2019

In this section, the bibliometric network analysis of IoT is depicted in the strategic diagram (4.1), the thematic network structure (4.2) and the thematic evolution structure (4.3). Section 2 describes each topic for better understanding.

4.1. Bibliometric performance and network analysis

Fig. 4 shows 31 clusters, ten (10) of which are classified as motor themes, six (6) as basic and transversal themes, nine (9) as emerging or declining themes, and six (6) as highly developed and isolated themes. The size of each cluster is proportional to the number of core documents associated with the theme, followed by the total of citations (in brackets).



Theme	Core documents	h-index	Cites	C.	D.
AUTHENTICATION	289	34	6,090	8.97	3.97
CLOUD-COMPUTING	252	30	4,891	9.03	1.64
INDUSTRY-4.0	182	27	2,760	6.62	2.58
6LOWPAN	142	25	3,863	6.92	3.66
SMARTCITY	115	17	1,005	9.25	1.08
ENERGY-HARVESTING	77	17	827	3.97	2.04
5G	71	14	1,667	5.52	2.19
MACHINE-LEARNING	116	13	683	6.12	0.72
ENERGY-EFFICIENCY	70	13	752	6.99	0.53
INTEROPERABILITY	58	13	864	6.4	1.47
PLATFORM	26	13	1,508	6.11	2.08
DISTRIBUTED-SYSTEM	46	11	1,053	6.58	1.08
CELLULAR-NETWORK	37	11	444	5.39	1.57
ENCRYPTION	41	10	321	4.73	0.96
DEVICE-TO-DEVICE-COMMUNICATION	32	10	414	5.64	0.5
AUTOMATION	24	8	196	5.39	0.96
INTERNET	24	8	504	8.13	0.24
ACTIVITY-RECOGNITION-	25	7	288	5.69	0.49
SENSOR-NETWORK	18	6	953	5.35	0.08
THROUGHPUT	17	6	102	5.41	0.56
SOA	16	6	320	5.76	0.66
CROWDSOURCING	16	6	112	6.79	0.26
LOW-POWER	22	5	88	6.59	0.35
OFFLOADING	21	5	82	5.56	0.95
CLUSTERING	19	5	136	7.49	0.14
PERFORMANCE	9	5	84	6.52	0.07
3D-PRINTING	6	5	75	3.08	0.16
SYSTEM-ON-A-CHIP	5	5	122	1.02	0.45
CONVOLUTIONAL-NEURAL-NETWORK	12	3	22	2.94	0.14
IEEE-802.15.4E	4	3	39	1.41	0.37
MOBILE-CROWED-SENSING	4	1	28	2.06	0.48

Fig. 4. Strategic diagram of IoT (2002–2019).

Table 4
Journals and universities that publish studies on IoT.

Theme	Core documents	h-index	Sum Citation
AUTHENTICATION	289	34	6090
CLOUD-COMPUTING	252	30	4891
INDUSTRY-4.0	182	27	2760
6LOWPAN	142	25	3863
SMARTCITY	115	17	1005
MACHINE-LEARNING	116	13	683
PLATFORM	26	13	1508
INTEROPERABILITY	58	13	864
DISTRIBUTED-SYSTEM	46	11	1053
SOA	16	6	320

Table 4 shows the performance analysis of the research themes and their respective core documents, sum citation and h-index.

Motor themes are regarded as the ten (10) motor themes that emerged from this analysis were “AUTHENTICATION”, “6LOWPAN”, “INDUSTRY-4.0”, “SMART-CITY”, “CLOUD-COMPUTING”, “MACHINE-LEARNING”, “DISTRIBUTED-SYSTEM”, “INTEROPERABILITY”, “PLATFORMS”, and “SOA-(SERVICE-ORIENTED-ARCHITECTURE”. A total of 1258 core documents on these motor theme have been cited 23,357 times.

4.2. Thematic network structure of IoT

Fig. 5 shows the thematic network structure of the motor themes of IoT presented in Table 4. The co-occurrence among keywords was deeply analyzed and depicted in order to present hidden patterns.

4.2.1. Authentication (a)

The cluster “AUTHENTICATION” (Fig. 5a) is the most important cluster in the strategic diagram due to its performance in terms of core documents, h-index, sum citation, and that it is identified as a motor theme. Authentication methods

can be seen as a series of adopted procedures to confirm an entity's identity in a network [77,78]. In the IoT environment, security and privacy are the primary concerns. Since the equipment does not have many resources to protect, data leakage is hindered, which makes it very difficult to implement robust security systems. With this in mind, we can explain the emergence of the most cited subthemes, “SECURITY” [79] and “PRIVACY” [80]. Furthermore, “RADIO--FREQUENCY-IDENTIFICATION” [81] has attracted a lot of attention because RFID is one of the leading IoT technologies that help create efficient and reliable systems. However, there are challenges surrounding the development of low-cost encryption methods.

4.2.2. Cloud computing (e)

The cluster “CLOUD-COMPUTING” (Fig. 5e) uses internet protocols as a model for consumption and delivery of technology resources. This technology is characterized by on-demand accessibility of systems, large data storage and high computer capacity [82]. The most relevant subthemes within this research theme are “FOG-COMPUTING” [83], “EDGE-COMPUTING” [84] and “QUALITY–OF–SERVICE-(QOS)” [85]. Edge Computing refers to an approach in which storage and other resources are physically closer to data producers. This method does not replace cloud computing, but rather complements it by providing communication efficiency and additional scalability [86]. The co-occurrence of this concept with “FOG-COMPUTING” might be explained by the fact that fog computing can be considered the highest evolution of the principle of edge computing. Fog computing provides distributed computing, storage control and networking capabilities closer to the user. Furthermore, “QUALITY–OF–SERVICE-(QOS)” and “HEALTHCARE” present a significant co-occurrence since QoS is an essential factor in healthcare systems, especially in cloud computing in

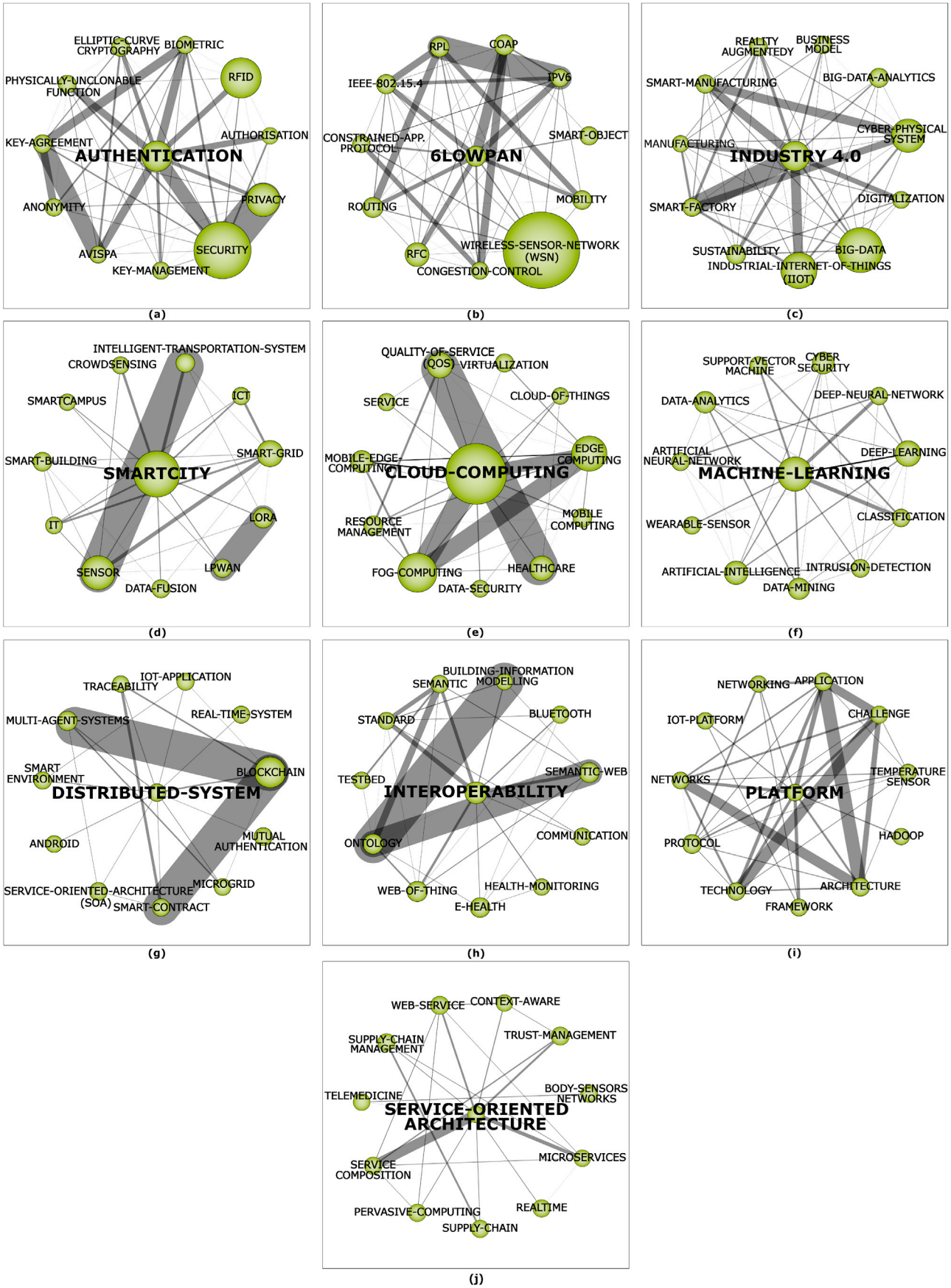


Fig. 5. Thematic network structure of IoT (2002–2019).

the IoT environment [87]. The application of QoS with cloud computing improves IoT in healthcare through data exchange between devices, security and privacy, data storage, data management, and ubiquitous access.

4.2.3. Industry 4.0 (c)

The cluster "INDUSTRY-4.0" (Fig. 5c) is a proposal developed by the German government (High-Tech Strategy 2020) to build a new economy based on high-tech technologies [1]. This concept accelerated the fourth industrial revolution and is based on technologies such as cyber-physical systems, IoT [88], big data and analytics [53], cloud computing [89], sensors, machine learning, computer simulation, 3D printing, artificial intelligence, augmented reality, real-time monitoring and decision-making, cybersecurity, robotics, among others [1,52]. The most important subthemes within this research theme are: "INDUSTRIAL-INTERNET–OF–THINGS-(IIOT)" [90], "CYBER-PHYSICAL SYSTEMS-(CPS)" [91], and "BIG-DATA" [92]. This co-occurrence may be trivial since big data, CPS and IoT represent the leading technologies that constitute the industry 4.0 concept. However, IIoT highlights a more significant research effort in the industrial sector, where higher robustness of technology is demanded in terms of complexity, legal regulations, hardware and infrastructure aspects, device compatibility, more significant investments, data network and security, among others.

4.2.4. 6LoWPAN (b)

The cluster "6LOWPAN" (Fig. 5b) is a Low-Power Personal Area Network, which refers to devices with low energy consumption, computer power consumption and memory. They communicate using low-power wireless standards, such as IEEE 802.15.4 for IPv6 [93,94]. The most important subtheme within this research theme is "WIRELESS-SENSOR-NETWORK-(WSN)" [95]. Co-occurrences among clusters, such as "6LOWPAN", "IEEE 802.15.4", "IPV6", can be explained because science has been using IEEE 802.15.4 standard and 6LoWPAN in the WSN context. WSN provides low power connectivity to the internet by wireless for IoT. In addition, the IEEE 802.15.4 standard provides lower power consumption for these systems. 6LoWPAN gives an IPv6 for each device, which can be connected through the Internet. "COAP" aims to replace HTTP for lightweight and low-resource devices. It is a stateless protocol, and combines 6LoWPAN and COAP to provide a web-oriented protocol basis for embedded systems. The subthemes "RPL" and "SMART-OBJECT" have a strong co-occurrence with 6LoWPAN as well. In this perspective, 6LoWPAN helps connect these smart devices with an adaption layer to the Internet and RPL, a distant vector protocol designed for IPV6 on IEEE 802.15.4 standard. RPL manages data routing for devices with lower resources and ensures bidirectional connectivity, robustness, reliability, flexibility, and scalability [96].

4.2.5. Smart city (c)

The cluster "SMART-CITY" (Fig. 5d) concept emerged in 2012 [97] and can be seen as using the IoT and other emerging technologies to improve the functions of cities. IoT can be applied in heterogeneous environments and is the best way to improve smart cities [98]. The most important subthemes within this research theme are "SENSOR" [99] and "SMART-GRID" [100]. A large number of studies using these technologies focus on building smart grid systems using wireless sensors to automatically collect and take action on the available information on the behavior of suppliers and consumers. The same situation occurs with "INTELLIGENT-TRANSPORTATION-SYSTEM", in which applications mainly focuses on vehicle safety, network communication and traffic management.

4.2.6. Machine learning (f)

The cluster "MACHINE-LEARNING" (Fig. 5f) can be seen as the most representative algorithm of artificial intelligence [101]. This algorithm is used to learn from data, make sense of data, and discover patterns that can be used to predict what will happen in future situations [102]. Recently, the interest in using machine learning to improve IoT security is increasing [103], which justifies the emergence of subthemes such as "CYBER-SECURITY" and "INTRUSION DETECTION". Other important subthemes within this theme are "DEEP-LEARNING" [104], "DEEP--NEURAL-NETWORK", "ARTIFICIAL-INTELLIGENCE" etc. [105]. A logical explanation for this co-occurrence pattern might be associated with the large number of studies conducted to benchmark machine learning algorithms using other techniques to evaluate performance in IoT environments (e.g., resource utilization, efficiency, accuracy, scalability).

4.2.7. Platforms (i)

The cluster "PLATFORMS" (Fig. 5i) facilitates exchanges, reduces transactions cost, facilitates transactions between companies and provide products and services [106]. IoT platforms integrate tasks into information and provides services for IoT devices through cooperation with other platforms [107]. The most important subthemes within this research theme are: "NETWORK" [108], "ARCHITECTURE", "CHALLANGE", "TECHNOLOGY" and "APPLICATION" [109]. Here, several applications of IoT platforms rely on interconnected wireless sensor networks. It is vital to have a robust IoT architecture for a proper connection between these sensors. In this sense, the central purpose of an IoT architecture in a system is to provide users with necessary real-time information. In order for these data communications to be accurate and useful, anyone requesting the platform's application must be properly authorized in advance. In addition, IoT platforms are becoming more and more complex, which puts forward higher technical requirements for organizations to deploy these platforms.

4.2.8. Interoperability (h)

The cluster "INTEROPERABILITY" (Fig. 5h) is a property of a system that shares data and communicates with other systems [110,111]. The most important subthemes within this research theme are "SEMANTIC-WEB" [112], "BUILDING-INFORMATION-MODELLING" and "ONTOLOGY". Academia have developed semantic web models using ontologies. Ontologies are used for semantic reasoning to provide interoperability in several aspects. The semantic web allows bidirectional transfer between cloud modes, promoting users to switch between different clouds and controlling the authorization to share manufacturing resources. In addition, it allows organizations to integrate three service models after a Return on Investment (ROI) analysis to consider factors such as manufacturing capabilities, business strategy and security issues. Therefore, it is crucial to consider the use of the semantic web in interoperability schemes.

4.2.9. Distributed system (g)

The cluster "DISTRIBUTED-SYSTEM" (Fig. 5g) is a group of autonomous computers presented to its users as a single integrated system [113]. Important roles of the distributed systems are storage, collaborative computing and security. These systems have become the basis for research in areas such as blockchain [114], multi-agents [115], smart home [116], fog computing and cloud computing [117]. The most important subthemes within this research theme are "BLOCK-CHAIN" [114], "SMART-CONTRACT" and "MULTI-AGENT-SYSTEM" [115]'. When "BLOCK-CHAIN" was created, specifically for Bitcoin, academic interest began to increase due to its strong security structure. Researchers then started to implement the technology in different fields. The above co-occurrence was highly developed by researchers since "SMART--CONTRACT" is a self-execution script that exists on the blockchain, allowing for a chain with general computational purposes. The same is true of "MULTI-AGENT-SYSTEM," which makes it possible to enhance autonomy, flexibility and higher integration of IoT systems. Unfortunately, security vulnerabilities become a challenge, yet blockchain seems to have been developed through multi-agent systems to enhance security.

4.2.10. Service oriented architecture (g)

The cluster "SOA-(SERVICE-ORIENTED-ARCHITECTURE)" (Fig. 5j) is a software architecture that allows the connection of resources to get or give data on demand. It enables interoperability between various IoT devices (SOA-based IoT systems) [118,119]. The most important subthemes within this research theme are "SERVICE-COMPOSITION" [118] and "MICROSERVICES" [120]. These describe virtual entities that process, exchange, or store information. Composite services are being used in supply chain, virtual enterprise, accounting, finances, and e-science. They are a merging of services that can be found in IoT applications. That happens because users need more complex functions that only services cannot perform. In this sense, microservices are a new way of creating services. It makes an application be a collection of services. Also, SOA provides guidelines for heterogeneous web services, which can be integrated.

4.3. Thematic evolution structure of IoT

Fig. 6 shows the overlapping map and the thematic evolution structure of IoT. In the first subperiod (2002–2006), three (3) keywords were used by authors; five (5) articles were published and the most significant cluster is "ANT-COLONY-ALGORITHM". This algorithm was used to establish self-coordination as the dominant paradigm of operation for ubiquitous computing [121]. However, this algorithm has the advantages of local improvements, overall performance search, parallel computing and can be used in combination with other optimization approaches [122]. The concept started to gain momentum in the IoT environment years later when researchers used the algorithm to find intelligent logistic paths in cyber-physical systems [123]; select the shortest path to obtain the global importance of nodes and the optimal path for sensors [124]; improve efficiency and picking distance in a fishbone layout warehouse [125]; reduce the energy consumption [126]; or as a task scheduling strategy to maximize the benefit of workers [74].

In the second subperiod (2007–2011), 333 new keywords were used and three (3) were lost. In this subperiod, 108 articles were published. The cluster "INTERNET" and "FUTURE-INTERNET" highlights the discussion of the role of the internet in upcoming years and how IoT could use the internet and emerging technologies to turn daily objects into smart objects with the ability to recognize and act in response to the environment [127]. The concept of the future internet was founded by the European Commission [128] and was slowly evolved into IoT [129].

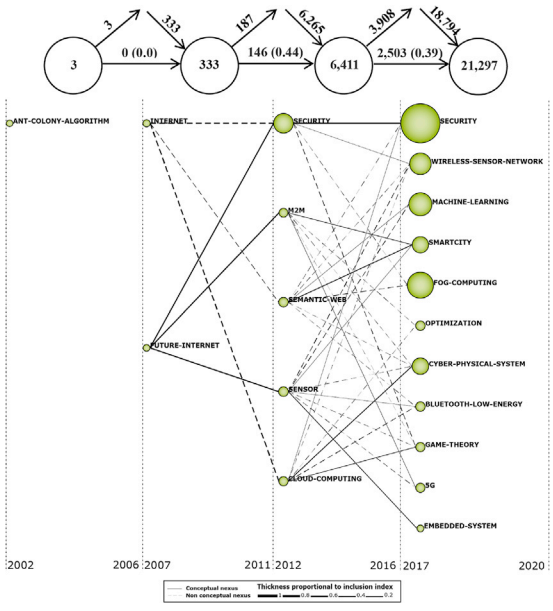


Fig. 6. Thematic evolution structure of IoT (2002–2019).

In this sense, technical and non-technical challenges have attracted attention, prompting the scientific community to put forward new architecture suggestions to support topics such as security, mobility, performance reliability and social content [130]. At the end of this subperiod, IoT became one of the pillars of industry 4.0 [1], partly due to the German government's strategic plan "High-Tech Strategy 2020" [1].

From the second subperiod to the third subperiod (shown in Fig. 6 below), 146 (44%) keywords were repeated, 187 were lost and 6.265 new keywords were used, totalizing 6411. Besides, 2832 articles were published in the scientific literature. This subperiod is represented by five (5) such as "SECURITY", "CLOUD-COMPUTING", "SENSOR", "M2M" and "SEMANTIC-WEB". This subperiod highlights the use of IoT with other industry 4.0 technologies and concepts. In this sense, industry 4.0 initiated the significant growth of IoT by attracting the scientific community to develop smart environments through Machine-to-Machine Communication (M2M), a data transference among systems and sensors in the cloud. When data transfer and management increase, the need for security protocols becomes a challenge. In this sense, the most representative cluster is "SECURITY". If security is ignored, the development of IoT will be restricted, and personal and strategic information may be leaked [131,132]. Therefore, to ensure a secure IoT network, properties such as availability, authenticity, confidentiality, integrity and non-repudiation became attractive to researchers [133].

From the third subperiod to the fourth subperiod (shown in Fig. 6 above), 2503 (39%) keywords were repeated, 3908 were lost and 18,794 new keywords were used, totalizing 21,297. Besides, 11,440 articles were published in the scientific literature. Eleven (11) clusters represent this subperiod. These clusters will be used to provide an overview of trends and propose future directions of IoT. The cluster "SECURITY" continues to prevail, presenting more associated documents. We found that documents of this cluster are most related to smart home, cloud computing, blockchain and authentication. The second most discussed cluster is "FOG-COMPUTING". Studies on this theme are related mainly to concepts, such as the industrial internet of things and edge computing. The cluster "MACHINE-LEARNING" is related to big data and analytics, artificial intelligence, deep learning and cybersecurity. The cluster "WIRELESS-SENSOR-NETWORK" is mainly related to energy efficiency, energy harvesting and consumption. The cluster "SMART-CITY" is related to smart grid, sensors, sustainability, interoperability, and intelligent transportation systems. The cluster "CYBER-PHYSICAL-SYSTEM" is mainly related to the industry 4.0 context.

5. Main challenges, limitations and difficulties of IoT

In this section, an exhaustive SLR of the main challenges and difficulties faced by IoT is presented. Twenty-three (23) articles were selected for analysis. Table 5 presents the findings regarding the challenges and difficulties classified according to 6 factors mentioned by Uslu, Eren, Gür and Özcan [21]: communication, technology, privacy and security, job, legal regulations, culture, and 26 related topics according to each factor.

Uslu, Eren, Gür and Özcan [21] investigated companies' IoT difficulties using multi-criteria decision-making methods. The results showed that challenges related to technologies (e.g., architecture, design, hardware) are the main difficulties faced by experts. The second most crucial difficulty was privacy and security using multi, followed by communication, job, legal regulations and culture.

Hameed, Khan, and Hameed [22] provided an updated overview of IoT challenges in terms of security and privacy. The authors classified five (5) security requirements: confidentiality, privacy, safe routing, robust and resilient management and damage detection. They also provided future directions for each challenge.

Pereira and Pereira [23] explored the trends and challenges of IoT. The main challenges were 6LoWPANs (20), data storage, software, cloud computing infrastructure, and big data (volume, velocity, variety and veracity).

Čolaković and Hadžialić [24] conducted an exhaustive review to

Table 5
Main challenges, limitations and difficulties of IoT.

Factor	Topics related	Authors	Sum
Priv. and Sec.	Data Privacy Network Security IoT Device Security Software Security Conflict of Interest	[7,21,22,24–26,28–38,40–42]	20
Tech.	Architecture and Design Heterogeneity of Devices Hardware Structure Fault Tolerance	[7,21,23–25,28,30,33–36,38,41,42]	19
Com.	Addressing Data Management Infrastructure Software	[7,21,23–34,36,37,39–41]	19
Job	Business Model Investing in Internet Develop. of Objects Economic Development Opportunities and Problems Customer Expect. And Service Quality	[7,21,24,26,29–31,33,35,36,38,42]	12
Legal Reg.	Data Usage Rate Ownership Standardization Global Cooperation of the Company Obligation	[21,24,30,31,33,34,36,39,40]	9
Cult.	Ethics of Education and Teaching Ethics Confidence Vandalism	[21,24,34]	3

identify the challenges of IoT. The results show 13 research areas: standardization, system architecture, interoperability and integration, availability and reliability, data storage and processing, scalability, management and self-configuration, performance and QoS, identification and unique.

identity, power and energy consumption, security and privacy, environmental issues.

Raja, Rajkumar, and Raj [25] reviewed the challenges and issues of IoT in literature. The main challenges highlighted the need to build smart platforms, middleware to integrate devices, fog computing, data storage, privacy and security.

Lee and Lee [26] explored the role of IoT, investments, challenges and difficulties for companies. The results show five (5) main challenges: data management, data mining, privacy, security and chaos challenge.

Tsai, Lai and Vasilakos [27] explored the future IoT, its main challenges and issues. The research describes five (5) main challenges: cloud computing, social network, infrastructure, data management and computational intelligence.

Miorandi, Sicari, De Pellegrini and Chlamtac [28] introduced applications, technologies and main challenges of IoT. The results highlighted five (5) main challenges: computing, communication and identification technologies, distributed intelligence, security and privacy.

Bujari, Furini, Mandreoli, Martoglia, Montangero and Ronzani [29] explored the limitations of using IoT and highlighted possible solutions. The authors pointed out four (4) main challenges: interoperability, lack of a visible business model, privacy and security.

Hammoudi, Aliouat and Harous [30] highlighted the main challenges of IoT and possible solutions to overcome these difficulties. This research identified 12 main challenges: architecture, security, privacy, standardization, the quantity of data, high energy consumption, storage, availability, reliability, management, interoperability and need for high technology.

Silva, Khan and Han [7] reviewed the challenges, architectures, emerging technologies in the IoT environment and possible solutions. The results show seven (7) main challenges: availability, performance, security, reliability, scalability, interoperability, and mobility.

Miloslavskaya and Tolstoy [31] investigated the challenges and solutions of information security in the IoT environment. The results highlighted six (6) major challenges: a large number of Internet-oriented IoT devices, the demand for high technology, lack of standardization, data management, privacy and security.

[32] investigated trends and challenges of management architecture for IoT. The authors highlighted eight (8) challenges: Security, load balancing, energy consumption, QoS, the quantity of data, data management, mobility management and energy management.

Balaji, Nathani and Santhakumar [33] explored the role of IoT in healthcare, smart city, industrial, agriculture, and the main challenges and future directions related to IoT frameworks. This research highlighted eight (8) major challenges: the vast number of devices, cost, maintenance, energy consumption, internet connections, interoperability, security, and privacy.

Harlamova, Kirikova and Sandkuhl [34] investigated the challenges of semantic web in IoT environment. The authors highlighted six (6) major challenges: scalability, standardization, data processing, privacy, data quality and data interpretation.

Xue, Li, Nazarian and Bogdan [35] developed a mathematical modeling structure to identify IoT characteristics from a macro approach. The authors highlighted six (6) major challenges: efficient sensing, cost, robustness, energy efficiency and security and decentralized computation.

Ryan and Watson [36] investigated the role of Operational Research (OR) and how OR can support overcoming IoT challenges. This research described 13 major challenges: business model, performance, cloud computing, data management, availability, reliability, energy efficiency, scalability, interoperability, architecture, mobility, security and privacy.

Ma, Liu, Zhou and Zhao [37] explored the main problems of IoT from the perspective of networks. The challenges highlighted include: internet, sensor networks, mobile support, network security, and network imbalance.

Chen, Xu, Liu, Hu and Wang [38] investigated the role and status of IoT in China. The main challenges are architecture, complex technologies, cost, energy consumption, standardization, privacy and security.

Ma [39] reviewed the role of IoT technologies and scientific challenges. The authors highlighted three (3) major challenges: data exchange, integration and service adaptation.

Bandyopadhyay and Sen [40] explored the state-of-the-art of the IoT, key technologies, possible applications, future research and challenges. This research points out nine (9) challenges: mobility, availability, manageability, scalability, security, privacy, management and a large number of devices and applications.

Hussein [41] explored the IoT technologies development, proposed future directions and pointed out challenges. The results show seven (7) major challenges: monitoring, processing, analyzing and managing data, interoperability, privacy, and security.

Yao, Wang, Sheng, Dustdar and Zhang [42] proposed directions, challenges, and recommendations for the IoT field. The author pointed out five major challenges: dynamic context awareness, the requirement of multiple types of IoT resources, security, privacy and interface.

6. Prospect of future research in IoT

The growing number of connected machines and devices requires new levels of security and privacy, network routing and interconnection between equipment and management systems [134]. This multiplicity of authentications and data traffic transcends the levels of data management usually used by organizations. This reinforces the importance of ongoing research to support the development of management tools and methods that can manage the diversity of devices and data in real time. Technologies, such as cloud computing, distributed systems and machine learning, are also trend themes (Fig. 4) that can be used to address several IoT-related challenges. However, such technologies also present their implementation, integration and management challenges and limitations. Examples of recent cloud limitations are related to delay due to

physical distances. Then, in order to enhance data processing in cloud-based centralized servers [4], it is necessary to use more robust techniques to ensure high performance, e.g., cellular network edge [4], mobile cloud computing [5], mobile edge computing and energy harvesting [6].

Future works should pursue such issues in order to provide in-depth investigations using BPNA and exhaustive SLRs. Although "AUTHENTICATION" is a highly central and dense motor theme, discussions related to the user and device authentication techniques are still a significant challenge for smart organizations, especially regarding data security and privacy (Fig. 6 and Table 5). The authentication challenge is closely related to the cluster "SECURITY" (Fig. 5a), which is one of the key themes in the fourth subperiod (Fig. 6). Besides, the most discussed themes in recent years (subperiod 2017–2019) show that even though many technologies, such as machine learning, fog computing, cyber-physical systems and embedded systems, seem to be of great significance to the technological transformation in organizations, the concern is similarly critical when it comes to security and optimization. These themes highlight the need for future research on IoT technologies and their integration. From this perspective, new frameworks will be required to optimize organizational processes and technological implementation, as well as security techniques.

Hence, we recommend that future research be related to security and authentication themes, as well as related to the clusters in the fourth subperiod, because these themes are the most representative in today's research field. The conceptual network structures (Fig. 5) can also be extended in future research because they the interrelationships of the main clusters related to IoT. More research on IoT applications can be carried out in different scenarios and sectors, such as smart cities, healthcare, industry, supply chain, public security, agriculture, and education. In addition, the use of such technologies should focus on developing approaches to reach perspectives beyond productivity efficiency. Such efforts must be able to act for the interests of sustainable development and the satisfaction of enterprise stakeholders.

This research allowed us to find hidden patterns in a large amount of data to propose future works in the IoT field using SciMAT and PRISMA protocols. For instance, the strategic diagram in Fig. 4 helps understand in which topics are the IoT scientific community putting the most effort and which topics are the most important to advance the IoT field of research. In this sense, future research related to motor themes (authentication, 6LoWPANs, industry 4.0, smart cities, cloud computing, among others) is particularly urgent and crucial. However, we also suggest future research work on emerging or declining themes, such as 3D printing, M2M communication, etc., to support new subjects to gain momentum and mitigate the decline of promising themes.

The thematic evolution structure in Fig. 6 showed how themes are evolved over time and how the number of keywords is increases. As for future research, we propose to carry out research related to the last themes (fourth subperiod), such as cyber-physical systems, fog computing, machine learning, etc. However, old themes such as ant colony (first subperiod) seem to gain momentum since the research emphasizes the better applicability of the algorithm due to advances in IoT technologies.

Table 5 highlighted that privacy and security are the main challenges and difficulties of IoT as noted by researchers, followed by technology, communication, job, legal regulations and cultural aspects. These results reinforce the main challenges faced by Uslu, Eren, Gür and Özcan [21]. In order to promote IoT security and privacy, we recommend future work related to patterns found in Fig. 5a, which shows that researchers have been committed to methods such as "ELLIPTIC-CURVE CRYPTOGRAPHY", "AVISPA" and "PHYSICALLY-UNCLONABLE-FUNCTION". The development of authentication based on Elliptical Curve Cryptography (ECC) is expanding since this is a low-cost method with smaller key size and less memory footprint. ECC is also used as the basis of the digital signature algorithm elliptic curve that provides entity and data-origin authentication, non-repudiation services and integrity protection. The automated validation of internet security protocols and applications (AVISPA) is a simulation tool that can simulate attacks to test the authenticated protocols. Physically Unclonable Functions (PUFs) map an entry to a unique exit and this kind of system offers a low cost and addresses challenges like privacy and security.

The results presented here make evident future work needs to address the most frequently mentioned challenges (technology, communication and security). In order to move forward exploiting the full potential of IoT's benefits, efforts must focus on developing cultural challenges, especially appropriate education and training on IoT methods and concepts because of the high complexity of using IoT properly, which requires the efforts from universities, governments and companies.

Our findings reveal several patterns related to security and privacy issues, data management, interoperability, energy efficiency and consumption, QoS, IoT technologies, and infrastructure. Therefore, is reasonable to suggest that more research related to these topics be carried out to support research in the IoT field of research. We also suggest more empirical studies to understand the challenges and difficulties in practice since only 1 document [21] of SLR presented reports from IoT practitioners.

7. Conclusion

This research aimed to conduct a BPNA supported by an SLR into the IoT field to investigate the strategic themes and its conceptual network structure, thematic evolution structure, and the main challenges and difficulties. Our findings presented many publications over time, especially after the emergence of the industry 4.0 concept. The most productive and cited researchers and the universities and journals related to IoT were also presented. Thirty-one (31) main clusters were plotted in a strategic diagram and classified according to their centrality and density. The most developed and important of these are related to security and privacy, industry 4.0 technologies, development of smart cities and software systems properties. The thematic evolution structure presented the significant cluster over time in terms of centrality and density. The SLR revealed the main challenges and difficulties of IoT.

The limitations of this research also must be noted. Only the major themes and associated subthemes were examined. The analysis was limited to papers and reviews in English, using only the WoS database. Hence, a potential research agenda is to extend this research to include publications in other languages and use other databases.

This research does not provide possible solutions to these challenges and difficulties, nor does it discuss the performance of proposed solutions. Future work may provide a cooperative network among researchers, countries, and universities, which may help improve decision-making in IoT research. We used only SciMAT to perform this science mapping. Therefore, future studies can be carried out using other bibliometric software, such as VOSviewer, CiteSpace, Sci2tool, etc., in order to find hidden patterns in databases and give contrast with our results.

Lastly, future research may further explore the subthemes of the motor themes, as well as other themes (basic and transversal, emerging or declining and highly developed and isolated themes), their challenges and limitations, so as to support future research in the context of the IoT.

Acknowledgment

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brazil (CAPES) - Finance Code 001 and the Spanish Ministry of Science and Innovation under grants PID2019-105381 GA-100 (iScience). The authors thank to the Consejo Nacional de Ciencia y Tecnología (CONACYT) and Dirección General de Relaciones Exteriores (DGRI), Mexico, for the support provided to carry out this study. K.-K. R. Choo was supported only by the Cloud Technology Endowed Professorship.

References

[1] L.M. Kipper, L.B. Furstenau, D. Hoppe, R. Frozza, S. Iepsen, Scopus scientific mapping production in industry 4.0 (2011–2018): a bibliometric analysis, Int. J. Prod. Res. 58 (6) (2020) 1605–1627.

[2] D. Gil, A. Ferrández, H. Mora-Mora, J. Peral, Internet of things: a review of surveys based on context aware intelligent services, Sensors 16 (7) (2016) 1069.

[3] C.J. D'Orazio, K.-K.R. Choo, L.T. Yang, Data exfiltration from Internet of Things devices: iOS devices as case studies, IEEE Internet Things J. 4 (2) (2016) 524–535.

[4] Z. Chen, W. Liao, K. Hua, C. Lu, W. Yu, Towards asynchronous federated learning for heterogeneous edge-powered internet of things, Digital Commun. Network 7 (3) (2021) 317–326.

[5] Y. Li, S. Xia, B. Cao, Q. Liu, Lyapunov optimization based trade-off policy for mobile cloud offloading in heterogeneous wireless networks, IEEE Trans. Cloud Comput. 10 (1) (2022) 491–505.

[6] S. Xia, Z. Yao, Y. Li, S. Mao, Online distributed offloading and computing resource management with energy harvesting for heterogeneous MEC-enabled IoT, IEEE Trans. Wireless Commun. 20 (10) (2021) 6743–6757.

[7] B.N. Silva, M. Khan, K. Han, Internet of things: a comprehensive review of enabling technologies, architecture, and challenges, IETE Tech. Rev. 35 (2) (2018) 205–220.

[8] R.Y. Zhong, X. Xu, L. Wang, IoT-enabled smart factory visibility and traceability using laser-scanners, Procedia Manuf. 10 (2017) 1–14.

[9] J. Manyika, et al., Unlocking the Potential of the Internet of Things, McKinsey Global Institute, 2015.

[10] P. Fraga-Lamas, T.M. Fernández-Caramés, M. Suárez-Albela, L. Castedo, M. González-López, A review on internet of things for defense and public safety, Sensors 16 (10) (2016) 1644.

[11] A.M. Rahmani, et al., Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: a fog computing approach, Future Generat. Comput. Syst. 78 (2018) 641–658.

[12] M. Babar, F. Arif, Real-time data processing scheme using big data analytics in internet of things based smart transportation environment, J. Ambient Intell. Hum. Comput. 10 (10) (2019) 4167–4177.

[13] A. Perles, et al., An energy-efficient internet of things (IoT) architecture for preventive conservation of cultural heritage, Future Generat. Comput. Syst. 81 (2018) 566–581.

[14] J. Iqbal, et al., A generic Internet of Things architecture for controlling electrical energy consumption in smart homes, Sustain. Cities Soc. 43 (2018) 443–450.

[15] M. Ben-Daya, E. Hassini, Z. Bahroun, Internet of things and supply chain management: a literature review, Int. J. Prod. Res. 57 (15–16) (2019) 4719–4742.

[16] Y. Lu, J. Cecil, An Internet of Things (IoT)-based collaborative framework for advanced manufacturing, Int. J. Adv. Manuf. Technol. 84 (5–8) (2016) 1141–1152.

[17] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Network. 57 (10) (2013) 2266–2279.

[18] M.A. Khan, K. Salah, IoT security: review, blockchain solutions, and open challenges, Future Generat. Comput. Syst. 82 (2018) 395–411.

[19] S. Banerjee, et al., A provably secure and lightweight Anonymous user authenticated session key exchange scheme for internet of things deployment, IEEE Internet Things J. 6 (5) (2019) 8739–8752.

[20] M. Abdel-Basset, N.A. Nabeeh, H.A. El-Ghareeb, A. Aboelfetouh, Utilising neutrosophic theory to solve transition difficulties of IoT-based enterprises, Enterprise Inf. Syst. (2019) 1–21.

[21] B. Uslu, T. Eren, Ş. Gür, E. Özcan, Evaluation of the difficulties in the internet of things (IoT) with multi-criteria decision-making, Processes 7 (3) (2019) 164.

[22] S. Hameed, F.I. Khan, B. Hameed, Understanding security requirements and challenges in Internet of Things (IoT): a review, J. Computer. Network. Commun 11 (2019) 1–14.

[23] R. Pereira, E.G. Pereira, Future internet: trends and challenges, Int. J. Space-Based Situated Comput. 5 (3) (2015) 159–167.

[24] A. Čolaković, M. Hadžialić, Internet of Things (IoT): a review of enabling technologies, challenges, and open research issues, Comput. Network. 144 (2018) 17–39.

[25] S. Raja, T.D. Rajkumar, V.P. Raj, Internet of things: challenges, issues and applications, J. Circ. Syst. Comput. 27 (12) (2018) 1830007.

[26] I. Lee, K. Lee, The internet of things (IoT): applications, investments, and challenges for enterprises, Bus. Horiz. 58 (4) (2015) 431–440.

[27] C.-W. Tsai, C.-F. Lai, A.V. Vasilakos, Future Internet of Things: open issues and challenges, Wireless Network 20 (8) (2014) 2201–2217.

[28] D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac, Internet of things: vision, applications and research challenges, Ad Hoc Netw. 10 (7) (2012) 1497–1516.

[29] A. Bujari, M. Furini, F. Mandreoli, R. Martoglia, M. Montangero, D. Ronzani, Standards, security and business models: key challenges for the IoT scenario, Mobile Network. Appl. 23 (1) (2018) 147–154.

[30] S. Hammoudi, Z. Aliouat, S. Harous, Challenges and research directions for internet of things, Telecommun. Syst. 67 (2) (2018) 367–385.

[31] N. Miloslavskaya, A. Tolstoy, Internet of Things: information security challenges and solutions, Cluster Comput. 22 (1) (2019) 103–119.

[32] F. Kiani, A survey on management frameworks and open challenges in IoT, Wireless Commun. Mobile Comput. 6 (4) (2018) 156–189.

[33] S. Balaji, K. Nathani, R. Santhakumar, IoT technology, applications and challenges: a contemporary survey, Wireless Pers. Commun. 108 (1) (2019) 363–388.

[34] M. Harlamova, M. Kirikova, K. Sandkuhl, A survey on challenges of semantics application in the internet of things domain, Appl. Comput. Syst. 21 (1) (2017) 13–21.

[35] Y. Xue, J. Li, S. Nazarian, P. Bogdan, Fundamental challenges toward making the iot a reachable reality: a model-centric investigation, ACM Trans. Des. Autom. Electron. Syst. 22 (3) (2017) 1–25.

[36] P.J. Ryan, R.B. Watson, Research challenges for the Internet of Things: what role can OR play? Systems 5 (1) (2017) 24.

[37] H. Ma, L. Liu, A. Zhou, D. Zhao, On networking of internet of things: explorations and challenges, IEEE Internet Things J. 3 (4) (2015) 441–452.

[38] S. Chen, H. Xu, D. Liu, B. Hu, H. Wang, A vision of IoT: applications, challenges, and opportunities with China perspective, IEEE Internet Things J. 1 (4) (2014) 349–359.

[39] H.-D. Ma, Internet of things: objectives and scientific challenges, J. Comput. Sci. Technol. 26 (6) (2011) 919–924.

[40] D. Bandyopadhyay, J. Sen, Internet of things: applications and challenges in technology and standardization, Wireless Pers. Commun. 58 (1) (2011) 49–69.

[41] A. Hussein, Internet of things (IOT): research challenges and future applications, Int. J. Adv. Comput. Sci. Appl. 10 (6) (2019) 77–82.

[42] L. Yao, X. Wang, Q.Z. Sheng, S. Dustdar, S. Zhang, Recommendations on the internet of things: requirements, challenges, and directions, IEEE Interent Comput 23 (3) (2019) 46–54.

[43] D. Mishra, A. Gunasekaran, S.J. Childe, T. Papadopoulos, R. Dubey, S. Wamba, Vision, applications and future challenges of Internet of Things, Ind. Manag. Data Syst. 116 (7) (2016) 1331–1355.

[44] G.C. Nobre, E. Tavares, Scientific literature analysis on big data and internet of things applications on circular economy: a bibliometric study, Scientometrics 111 (1) (2017) 463–492.

[45] Y. Bouzembrak, M. Klüche, A. Gavai, H.J. Marvin, Internet of Things in food safety: literature review and a bibliometric analysis, Trends Food Sci. Technol. 94 (2019) 54–64.

[46] A. Kaba, C.K. Ramaiah, Bibliometric analysis of research output on the internet of things in the arab world, DESIDOC J. Library. Info. Tech. 39 (5) (2019) 207–214.

[47] X. Li, C. Pak, K. Bi, Analysis of the development trends and innovation characteristics of Internet of Things technology–based on patentometrics and bibliometrics, Technol. Anal. Strat. Manag. 32 (1) (2020) 104–118.

[48] A. Aghaei Chadegani, et al., A comparison between two main academic literature collections: web of Science and Scopus databases, Asian Soc. Sci. 9 (5) (2013) 18–26.

[49] M.J. Cobo, A.G. López-Herrera, E. Herrera-Viedma, F. Herrera, SciMAT: a new science mapping analysis software tool, J. Am. Soc. Inf. Sci. Technol. 63 (8) (2012) 1609–1630.

[50] M.J. Cobo, A.G. López-Herrera, E. Herrera-Viedma, F. Herrera, Science mapping software tools: review, analysis, and cooperative study among tools, J. Am. Soc. Inf. Sci. Technol. 62 (7) (2011) 1382–1402.

[51] M.L. Kolling, et al., Data mining in healthcare: applying strategic intelligence techniques to depict 25 Years of research development, Int. J. Environ. Res. Publ. Health 18 (6) (2021) 3099.

[52] L.B. Furstenau, et al., 20 years of scientific evolution of cyber security: a science mapping, 2020, pp. 10–12.

[53] J.-R. López-Robles, J.R. Otegi-Olaso, I.P. Gomez, N.-K. Gamboa-Rosales, H. Gamboa-Rosales, H. Robles-Berumen, Bibliometric network analysis to identify the intellectual structure and evolution of the big data research field, in: International Conference on Intelligent Data Engineering and Automated Learning, Springer, 2018, pp. 113–120.

[54] J.-R. López-Robles, J.-R. Otegi-Olaso, I.P. Gómez, M.-J. Cobo, 30 years of intelligence models in management and business: a bibliometric review, Int. J. Inf. Manag. 48 (2019) 22–38.

[55] J.-R. López-Robles, J. Guallar, J.-R. Otegi-Olaso, N.-K. Gamboa-Rosales, El profesional de la información (EPI): bibliometric and thematic analysis (2006-2017), El Prof. Inf. 28 (4) (2019) e280417.

[56] M.K. Sott, et al., Agriculture 4.0 and Smart Sensors. The Scientific Evolution of Digital Agriculture: Challenges and Opportunities, 2021.

[57] P.P. Severo, L.B. Furstenau, M.K. Sott, D. Cossul, M.S. Bender, N.L. Bragazzi, Thirty years of human rights study in the web of science database (1990–2020), Int. J. Environ. Res. Publ. Health 18 (4) (2021) 2131.

[58] M.K. Sott, et al., Process modeling for smart factories: using science mapping to understand the strategic themes, main challenges and future trends, Bus. Process Manag. J. 27 (5) (2021) 1391–1417.

[59] J. López-Robles, et al., The relationship between Project Management and Industry 4.0: bibliometric analysis of main research areas through Scopus, Res. Eduation. Project Manage (2020) 56. Bilbao.

[60] L.M. Kipper, et al., Scientific mapping to identify competencies required by industry 4.0, Technol. Soc. 64 (2021), 101454.

[61] L.B. Furstenau, L.M. Kipper, R. Frozza, D. Hoppe, Proposta de aplicação do software Quality Function Deployment em ambiente computacional, Revista Jovens Pesquisadores 9 (2) (2019) 57–76.

[62] A.L.E. Silva, J.A.R. Moraes, L.B. Benitez, E.A. Kaufmann, L.B. Furstenau, Mapeamento da produção científica acerca do uso de biocompósitos nos processos de impressões 3D, Revista Ibero-Americana de Ciências Ambientais 11 (1) (2020) 236–250.

[63] L.B. Furstenau, et al., Link between sustainability and industry 4.0: trends, challenges and new perspectives, IEEE Access 8 (2020) 140079–140096.

[64] M.K. Sott, et al., Precision techniques and agriculture 4.0 technologies to promote sustainability in the coffee sector: state of the art, challenges and future trends, IEEE Access 8 (2020) 149854–149867.

[65] M.K. Sott, M.S. Bender, L.B. Furstenau, L.M. Machado, M.J. Cobo, N.L. Bragazzi, 100 years of scientific evolution of work and organizational psychology: a bibliometric network analysis from 1919 to 2019, Front. Psychol. 11 (2020).

[66] L.B. Furstenau, et al., An Overview of 42 Years of Lean Production: Applying Bibliometric Analysis to Investigate Strategic Themes and Scientific Evolution Structure, Technology Analysis & Strategic Management, 2021, pp. 1–20.
[67] L.B. Furstenau, et al., A bibliometric network analysis of coronavirus during the first eight months of COVID-19 in 2020, Int. J. Environ. Res. Publ. Health 18 (3) (2021) 952.
[68] A. Liberati, et al., The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: explanation and elaboration, Ann. Intern. Med. 151 (4) (2009). W-65-W-94.
[69] D. Moher, A. Liberati, J. Tetzlaff, D.G. Altman, Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement, Ann. Intern. Med. 151 (4) (2009) 264–269.
[70] C.R. Schoenberger, B. Upbin, The internet of things, Forbes Magazine 169 (6) (2002) 155–160.
[71] M. Tuters, K. Varnelis, Beyond locative media: giving shape to the internet of things, Leonardo 39 (4) (2006) 357–363.
[72] J. Cooper, A. James, Challenges for database management in the internet of things, IETE Tech. Rev. 26 (5) (2009) 320–329.
[73] E. Welbourne, et al., Building the internet of things using RFID: the RFID ecosystem experience, IEEE Internet computing 13 (3) (2009) 48–55.
[74] M. Zorzi, A. Gluhak, S. Lange, A. Bassi, From today's intranet of things to a future internet of things: a wireless-and mobility-related view, IEEE Wireless Commun. 17 (6) (2010) 44–51.
[75] R. Rafael, A. Shirley, A. Liveris, Report to the President Accelerating US Advanced Manufacturing. Report, US, Report, Washington DC, 2014.
[76] H. Kagermann, J. Helbig, A. Hellinger, W. Wahlster, Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0: Securing the Future of German Manufacturing Industry; Final Report of the Industrie 4.0 Working Group, Forschungsunion, 2013.
[77] X. Li, J. Niu, S. Kumari, F. Wu, A.K. Sangaiah, K.-K.R. Choo, A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments, J. Netw. Comput. Appl. 103 (2018) 194–204.
[78] X. Li, J. Peng, J. Niu, F. Wu, J. Liao, K.-K.R. Choo, A robust and energy efficient authentication protocol for industrial internet of things, IEEE Internet Things J. 5 (3) (2017) 1606–1615.
[79] E.L. Macedo, et al., On the security aspects of Internet of Things: a systematic literature review, J. Commun. Network. 21 (5) (2019) 444–457.
[80] F. Zhu, W. Wu, Y. Zhang, X. Chen, Privacy-preserving authentication for general directed graphs in industrial IoT, Inf. Sci. 502 (2019) 218–228.
[81] R. Baashirah, A. Abuzneid, Survey on prominent RFID authentication protocols for passive tags, Sensors 18 (10) (2018) 3584.
[82] Z. Maamar, T. Baker, M. Sellami, M. Asim, E. Ugljanin, N. Faci, Cloud vs edge: who serves the internet-of-things better? Internet Tech. Lett. 1 (5) (2018) e66.
[83] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, O. Rana, Fog computing for the internet of things: a Survey, ACM Trans. Internet Technol. 19 (2) (2019) 1–41.
[84] W.Z. Khan, E. Ahmed, S. Hakak, I. Yaqoob, A. Ahmed, Edge computing: a survey, Future Generat. Comput. Syst. 97 (2019) 219–235.
[85] S. Heidari, R. Buyya, Quality of Service (QoS)-driven resource provisioning for large-scale graph processing in cloud computing environments: graph Processing-as-a-Service (GPaaS), Future Generat. Comput. Syst. 96 (2019) 490–501.
[86] Y. Li, H. Ma, L. Wang, S. Mao, G. Wang, Optimized content caching and user association for edge computing in densely deployed heterogeneous networks, IEEE Trans. Mobile Comput. (,In press).
[87] R. Khamisy-Farah, L.B. Furstenau, J.D. Kong, J. Wu, N.L. Bragazzi, Gynecology meets big data in the disruptive innovation medical era: state-of-art and future prospects, Int. J. Environ. Res. Publ. Health 18 (10) (2021) 5058.
[88] V. Roblek, M. Meško, A. Krapež, A complex view of industry 4.0, Sage Open 6 (2) (2016) 1–11.
[89] J.H. Park, J.H. Park, Blockchain security in cloud computing: use cases, challenges, and solutions, Symmetry 9 (8) (2017) 164.
[90] H. Boyes, B. Hallaq, J. Cunningham, T. Watson, The industrial internet of things (IIoT): an analysis framework, Comput. Ind. 101 (2018) 1–12.
[91] Y. Lu, Cyber physical system (CPS)-based industry 4.0: a survey, J. Industrial Integration. Manage. 2 (3) (2017), 1750014.
[92] S. Gierej, Big data in the industry-overview of selected issues, Manag. Syst. Prod. Eng. 25 (4) (2017) 251–254.
[93] A. Le, J. Loo, A. Lasebae, M. Aiash, Y. Luo, 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach, Int. J. Commun. Syst. 25 (9) (2012) 1189–1212.
[94] C. Hennebert, J. Dos Santos, Security protocols and privacy issues into 6LoWPAN stack: a synthesis, IEEE Internet Things J. 1 (5) (2014) 384–398.
[95] J. Granjal, E. Monteiro, J.S. Silva, Security in the integration of low-power wireless sensor networks with the internet: a survey, Ad Hoc Netw. 24 (2015) 264–287.
[96] P.O. Kamgueu, E. Nataf, T.D. Ndie, Survey on RPL enhancements: a focus on topology, security and mobility, Comput. Commun. 120 (2018) 10–21.
[97] M. Batty, et al., Smart cities of the future, Eur. Phys. J. Spec. Top. 214 (1) (2012) 481–518.
[98] B. Hammi, R. Khatoun, S. Zeadally, A. Fayad, L. Khoukhi, IoT technologies for smart cities, IET Netw. 7 (1) (2017) 1–13.
[99] B.P.L. Lau, N. Wijerathne, B.K.K. Ng, C. Yuen, Sensor fusion for public space utilization monitoring in a smart city, IEEE Internet Things J. 5 (2) (2017) 473–481.
[100] N.K. Suryadevara, G.R. Biswal, Smart plugs: paradigms and applications in the smart city-and-smart grid, Energies 12 (10) (2019), 1957.
[101] L. Cui, S. Yang, F. Chen, Z. Ming, N. Lu, J. Qin, A survey on application of machine learning for Internet of Things, Int. J. Mahine. Learn Cybernet. 9 (8) (2018) 1399–1417.
[102] H. Assem, L. Xu, T.S. Buda, D. O'Sullivan, Machine learning as a service for enabling internet of things and people, Personal Ubiquitous Comput. 20 (6) (2016) 899–914.
[103] S. Zeadally, M. Tsikerdekis, Securing internet of things (IoT) with machine learning, Int. J. Commun. Syst. 33 (1) (2020) e4169.
[104] J. Chen, X. Ran, Deep learning with edge computing: a review, Proc. IEEE 107 (8) (2019) 1655–1674.
[105] L. Zhang, Y.-C. Liang, D. Niyato, 6G Visions: mobile ultra-broadband, super internet-of-things, and artificial intelligence, China Communications 16 (8) (2019) 1–14.
[106] F. Fraile, R. Sanchis, R. Poler, A. Ortiz, Reference models for digital manufacturing platforms, Appl. Sci. 9 (20) (2019) 4433.
[107] M. Kim, N.Y. Lee, J.H. Park, A security generic service interface of internet of things (IoT) platforms, Symmetry 9 (9) (2017) 171.
[108] J.D.C. Silva, J.J.P. Rodrigues, K. Saleem, S.A. Kozlov, R.A. Rabêlo, M4DN. IoT-A networks and devices management platform for internet of things, IEEE Access 7 (2019) 53305–53313.
[109] G. Marques, R. Pitarma, N. M Garcia, N. Pombo, Internet of things architectures, technologies, applications, challenges, and future directions for enhanced living environments and healthcare systems: a review, Electronics 8 (10) (2019) 1081.
[110] R.C. Motta, K.M. de Oliveira, G.H. Travassos, A conceptual perspective on interoperability in context-aware software systems, Inf. Software Technol. 114 (2019) 231–257.
[111] M. Noura, M. Atiquzzaman, M. Gaedke, Interoperability in internet of things: taxonomies and open challenges, Mobile Network. Appl. 24 (3) (2019) 796–809.
[112] A.J. Jara, A.C. Olivieri, Y. Bocchi, M. Jung, W. Kastner, A.F. Skarmeta, Semantic web of things: an analysis of the application semantics for the iot moving towards the iot convergence, Int. J. Web Grid Serv. 10 (2–3) (2014) 244–272.
[113] A.S. Tanenbaum, M. Van Steen, Distributed Systems: Principles and Paradigms, Prentice-Hall, 2007.
[114] W. Viriyasitavat, L. Da Xu, Z. Bi, A. Sapsomboon, New blockchain-based architecture for service interoperations in internet of things, IEEE Trans. Comput. Social. Syst. 6 (4) (2019) 739–748.
[115] L. Feng, H. Zhang, Y. Chen, L. Lou, Scalable dynamic multi-agent practical byzantine fault-tolerant consensus in permissioned blockchain, Appl. Sci. 8 (10) (2018) 1919.
[116] S. Hu, C. Tang, F. Liu, X. Wang, A distributed and efficient system architecture for smart home, Int. J. Sens. Netw. 20 (2) (2016) 119–130.
[117] V.B. Souza, et al., Towards a proper service placement in combined Fog-to-Cloud (F2C) architectures, Future Generat. Comput. Syst. 87 (2018) 1–15.
[118] R. Chen, J. Guo, F. Bao, Trust management for SOA-based IoT and its application to service composition, IEEE Trans. Service. Compute 9 (3) (2014) 482–495.
[119] F. Wang, L. Hu, J. Zhou, K. Zhao, A data processing middleware based on SOA for the internet of things, J. Sens. 5 (4) (2015) 123–145.
[120] T. Cerny, Aspect-oriented challenges in system integration with microservices, SOA and IoT, Enterprise Inf. Syst. 13 (4) (2019) 467–489.
[121] F.J. Rammig, Towards self-coordinating ubiquitous computing environments, in: International Conference on Embedded and Ubiquitous Computing, Springer, 2006, pp. 2–13.
[122] Y. Zhang, Y. Yu, S. Zhang, Y. Luo, L. Zhang, Ant colony optimization for Cuckoo Search algorithm for permutation flow shop scheduling problem, Syst. Sci. Control. Eng. 7 (1) (2019) 20–27.
[123] N. Zhang, Smart logistics path for cyber-physical systems with internet of things, IEEE Access 6 (2018) 70808–70819.
[124] T. Qiu, B. Li, W. Qu, E. Ahmed, X. Wang, TOSG: a topology optimization scheme with global small world for industrial heterogeneous Internet of Things, IEEE Trans. Ind. Inf. 15 (6) (2018) 3174–3184.
[125] L. Zhou, Z. Li, N. Shi, S. Liu, K. Xiong, Performance analysis of three intelligent algorithms on route selection of fishbone layout, Sustainability 11 (4) (2019) 1148.
[126] J. Xu, Z. Hao, R. Zhang, X. Sun, A method based on the combination of laxity and ant colony system for cloud-fog task scheduling, IEEE Access 7 (2019) 116218–116226.
[127] G. Kortuem, F. Kawsar, V. Sundramoorthy, D. Fitton, Smart objects as building blocks for the internet of things, IEEE Interent Comput 14 (1) (2009) 44–51.
[128] H. Ning, Z. Wang, Future internet of things architecture: like mankind neural system or social organization framework? IEEE Commun. Lett. 15 (4) (2011) 461–463.
[129] Q.Z. Sheng, S. Zeadally, Z. Luo, J.-Y. Chung, Z. Maamar, Ubiquitous RFID: where are we? Inf. Syst. Front 12 (5) (2010) 485–490.
[130] J. Pan, S. Paul, R. Jain, A survey of the research on future internet architectures, IEEE Commun. Mag. 49 (7) (2011) 26–36.
[131] Q. Jing, A.V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the internet of things: perspectives and challenges, Wireless Network 20 (8) (2014) 2481–2501.
[132] N. Moustafa, B. Turnbull, K.-K.R. Choo, An ensemble intrusion detection technique based on proposed statistical flow features for protecting network traffic of internet of things, IEEE Internet Things J. 6 (3) (2018) 4815–4830.
[133] D. Airehrour, J. Gutierrez, S.K. Ray, Secure routing for internet of things: a survey, J. Netw. Comput. Appl. 66 (2016) 198–213.
[134] K. Gai, K.-K.R. Choo, M. Qiu, L. Zhu, Privacy-preserving content-oriented wireless communication in internet-of-things, IEEE Internet Things J. 5 (4) (2018) 3059–3067.