Jestr

Journal of Engineering Science and Technology Review 16 (3) (2023) 181 - 190

Research Article

JOURNAL OF
Engineering Science and Technology Review

www.jestr.org

Security of Medical Internet of Things (MIoT)- A Bibliometric Analysis

Rachana Y. Patil[1,*], Yogesh H. Patil[2] and Aparna Bannore[3]

[1]Pimpri Chinchwad College of Engineering, Pune, Maharashtra, India
[2]Dr. D. Y. Patil College of Engineering, Pune, Maharashtra, India
[3]SIES Graduate School of Technology, Mumbai, India

Received 4 October 2022; Accepted 30 May 2023

Abstract

The integration of the Internet and communication technologies has improved our lives in numerous ways. To date, the Internet of Things has evolved the healthcare industry from healthcare 1.0 to 4.0 which is known as the MIoT. In Healthcare 4.0, data is shared among multiple stakeholders through the use of cloud computing, fog computing, and telehealth. MIoT devices and technology's interconnected, heterogeneous nature raises new concerns about access to confidential patient data, which is often done without patients' or medical staff's knowledge. This is because security and privacy concerns for MIoT devices and technology are frequently ignored or undermined by relevant stakeholders. Medical IoT security and privacy are becoming increasingly important as a result of the increasing number of security breaches targeting the MIoT in healthcare.To impartially reveal the research scenario of Security of MIoT biblioshiny and VOS viewer software are used to conduct a quantitative assessment of research papers belonging to this field for the period 2012–2021 in the Web of Science (WoS) and Scopus databases. From the results, it is seen that for the past 10 years, the sum of articles on Security of MIoT has increased. This research domain covers 35 territories. MIoT, Security, Privacy, authentication, access control are the most often used keywords in this field of research in recent years. The research flashpoints in the field primarily emphasize research directions such as the, the security and privacy concerns related to MIoT sensor data and how to get rid of them. The top five nations considering research volume are the China, India, Saudi Arabia, USA, and Korea, but a lack of collaborative work amongst these countries is seen. Finally, the paper provides future research directions on security of MIoT, such as Privacy of patient information , Lightweight Protocols for MIoT Devices, Trust management, patient data sharing and insecure networks.

Keywords: Medical Internet of Things (MIoT), Security, Bibliometric, Healthcare

1. Introduction

Technological evolvement and its integration is becoming essential part of our daily lives. The Internet of Things (IoT) plays an important role in providing smooth and seamless ubiquitous services for everyone, reducing the need for human labor, and assisting in all over the place linking everyone [1].

Along with healthcare and smart cities, it's also being used in agriculture and the armed forces [2-5]. As a result, the Internet of Things (IoT) has the potential to transform how individuals engage with the world. In 2020 the IoT market share was estimated around USD 761.4 billion and by 2026 it is expected to achieve USD 1386.06 billion; this indicates its global relevance as leading technology concept for increasing the welfare of millions of people.[6–10].

IoT in healthcare, or Medical IoT (MIoT), describes a broad variety of IoT devices that have a primary objective to serve and support in basic patient care system [11]. It is estimated that globally the IoT in the healthcare industry would rise to USD 446.52 billion in 2028, from USD 71.84 billion in 2020.

Patients' critical body parameters and pathological data can be monitored by wearable or implantable medical sensors [12–14]. Currently, healthcare industries are opting for more modern MIoT-based products and services for treating patients, diagnosing, and managing disease with better patient care at minimum cost. A real time patient monitoring is possible from a distance using MIoT devices, and the data collected can be analysed and sent to the cloud or medical record centers for further handling and storage prior it is made available to respective participants, like doctors, paramedical staff, and health insurance service providers [15].

Medical IoT devices with a variety of smart sensors are typically found in MIoT healthcare applications. Smart gadgets are also integrated into global information networks system for easy and immediate access. Physical objects in the MIoT system can be integrated and connected to the Internet, allowing for remote access to equipment that checks, analyses, forecast, and store crucial medical information. On the other side, due to the fast-developing IoT threat environment, the interloper can exploit and way into the MIoT network for excess abuse of the overall medical system and setup[16].

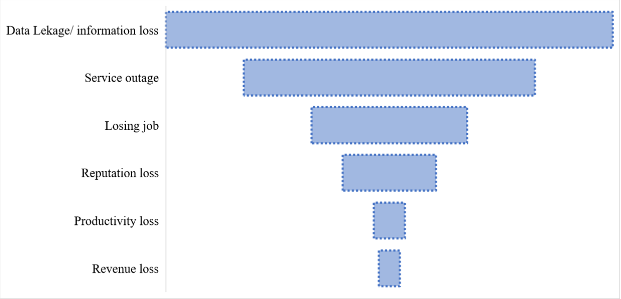


Fig. 1. Volume of damage due to cyber-attacks in the healthcare industry.

*E-mail address: rachana.patil@pccoepune.org

ISSN: 1791-2377 © 2023 School of Science, IHU. All rights reserved.
doi:10.25103/jestr.163.22

The rapid development of IoT based MIoT systems causes exposing the patient's personal information which is confidential and is accessible to unauthorized parties. It is possible for invaders to access the implanted or any life-supporting medical device remotely to change the critical body parameters, which is life-threatening to patients [17].

Furthermore, it's at high risk for patients if passive network operators could misuse patient's personal information from network traffic for marketing purposes. The lack of sufficient acquaintance regarding the security of MIoT devices and networks among end users and related stakeholders like patient, medical experts, leads to intensify vulnerabilities and in many cases, attackers can take the advantage of such situations pushing patients' lives at risk [18].

It's not limited to this, but in the event of cyber-attacks, the major concerns for the healthcare industry would be data theft and loss of critical information, ultimately resulting in compromising patients' data [19-22]. The recent statistics of cyber-attacks in the healthcare industry shows the volume of damage as shown in figure 1. The continuous expansion of IoT based healthcare market expects a total business turnover of 100 billion USD by 2025, this study also confirms our attempts to verify the present scenario of safety and security of MIoT.

Surprisingly the whole world experienced a shock in November 2019 by the outbreak of a lethal virus called COVID-19 that spread very quickly to nations all over the world putting worldwide pandemonium. It is estimated that the global population is reduced by around 4 million due to COVID -19 casualties till date and yet it's not clear about the outbreak of the next variants of COVID-19 viruses and their severity, diagnosis, and management. Possible measures like imposing complete or partial lockdown, night curfews and restrictions on public gatherings; social functions are implemented to control the spread of this fatal disease. MIoT played a crucial role during this COVID pandemic while working with government agencies, various NGOs, and healthcare institutes for monitoring the disease. The COVID virus being contagious, the life of the treating medical team is at risk, remote patient tracking, monitoring and management is essential and becomes possible due to MIoT technology. There is a huge surge in demand for MIoT based applications and devices during the COVID pandemic period and ultimately the incidences of cyber threats increased as per the literature [23-24] which encourages for the study in this domain.

Bibliometric is the statistical evaluation used to analyze bibliometric qualities and records like publications, citations, and research outputs. It permits researcher scholars to identify the composition, attributes, and forms of research behaviors [25-27]. The analysis technique creates the research actions into a reasonable course of a research area which includes literature surveys of scientific actions in distinct perspectives like publications, citations, authors, institutes, and nations. It is a process that states the thorough assessment of the development of research areas. The bibliography analysis is helpful in many ways as 1)The authors can prove the importance of their investigation and publication, 2) Institutions can measure publishing impact and performance, 3)investigators can expect scope of future research and important effects on any specific areas, and 4) researchers can assess the increment in subject data.

To explain the security issues associated to MIOT domain, this paper aims to investigate the domain by organizing a thorough evaluation of security issues of MIOT research methods published in the WoS from 2012 to 2021. The methodology comprises the publication trends, research areas, and assessment on MIOT security. To focus on this study, we prepared the research queries as: (a) Is there a pattern to the number of articles published on the topic of MIOT security, and if so, (b) how does this information point to the field's future course?

Using "MIOT security" as the primary keyword, we found more than 2000 articles and examined prior to be categorized into 622 from WoS, and 487 from the Scopus database. These all are brought from the WoS with few exclusions on certain journal data bases. The reason for excluding the few journal databases is to eliminate non-English articles and patents.

On selected papers, analysis is completed by building the correlation among the title, abstract, research area, publication, citation, geographical location, and the keywords used. Also, this paper revels the trends by recapping the significant research attempts and emphasizing probable upcoming trails for security issues of MIOT research.

2. Methodology and Databases

Numerous databases are use up to index journal articles like IEEE Explore, Scopus, Science Direct, WoS, Google Scholar, Springer and Association for Computing Machinery (ACM). Though, Elsevier's Scopus, WoS, and Google Scholar are the major bibliometrics data sources for exploring literature, for journal rankings, these data sources are typically utilized to measure the journal's productivity and the number of citations it receives to estimate its influence and reputation. Here, we opted to WoS and Scopus database due to the reasons as, First, it's the only means for bibliometrics analysis, and second, we eliminate Google Scholar to evade similarity between the databases. Due to low data quality which creates doubts about its appropriateness for research assessment, google scholar datasets are excluded. Moreover, IEEE Explore, Science Direct, Springer and ACM are restricted for indexing their individual publishers, while WoS unites the preferred and high-ranking publication from the aforesaid databases. Furthermore, we go for WoS and Scopus databases since it is renowned in the bibliometric analysis for envisioning the estimation of literature in research fields. The significance of WoS and Scopus database is that it comprises all article types, index institutes, bibliographic references, and authors for every single article [28].

The WoS and Scopus databases served as this paper's search engine. The data- base offers effective searching and surfing choices by allowing various options to sort and limit the findings. Along with searching, the WoS and scopus databases are also capable to separate the articles based on specific factors like publication dates, freshly updated publications, citation score, usage counts, applicability, and based on name of first author. Furthermore, improving the outcomes also allowed particular outcomes to be ignored by document types, organizations, authors, years, and nations. Additionally, its capability to deliver required information like citation score, quartile ranks and impact factors makes the study further encouraging [29-31].

Our main interest is to carry out bibliometric study on ''security in MIOT'', so the keywords utilized in the search query is as: "medical internet of things" OR "Internet of medical things" OR "Medical cyber physical system" AND "Security" Timespan: 2010–2021. We opted 2010 as the beginning year for this search since the security issues in MIOT emerged in late 2010's. Though, in 2012 the first publication came out which is indexed by Scopus and WoS both with the search query presented on 05th July 2022. The Indexes are as Social Science Citation Index (SSCI), Science Citation Index-Expanded (SCI-E), the, Emerging Social Science Citation Index (E-SCI) and Scopus which are the benchmark indexes considered in the field of computer engineering. The title, author, abstract, country, author affiliation, citation record is some of the labels which are recovered (from WoS and Scopus).

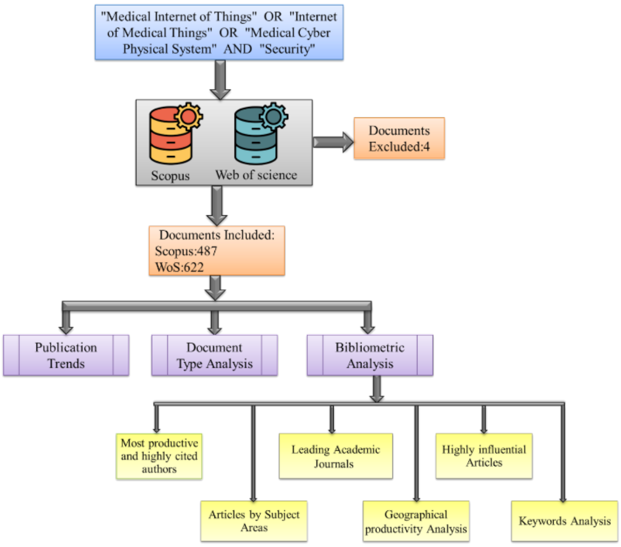

"Medical Internet of Things" OR "Internet of Medical Things" OR "Medical Cyber Physical System" AND "Security"
Scopus
Web of science
Documents Excluded:4
Documents Included:
Scopus:487
WoS:622
Publication Trends
Document Type Analysis
Bibliometric Analysis
Most productive and highly cited authors
Leading Academic Journals
Highly influential Articles
Articles by Subject Areas
Geographical productivity Analysis
Keywords Analysis

Fig. 2. The data collection and process flow diagram.

The data collection and process flow diagram is described in figure 2. A search for comparable papers in the Scopus and Web of Science data set is used to limit the extent of the study between 2012 and 2021 by using the query defined above. A total of 622 publications were found in WoS, and 487 publications were found in the Scopus database of several journals and volumes as well as patterns and subsections within those books. High Impact journals, highly cited publications, research topics, and productivity were all brought into consideration in the study. Keyword frequency was also taken into consideration, along with institutes and authors. Our last option for a visualization tool was the free VOSviewer [32] application and Biblioshiney [33], which have several capabilities that allow us to analyze the data.

3. Publication Trends / Distribution of Annual Documents

Security of MIoT has earned prominence in current years because of its enormous importance in a variety of disciplines, there has been significant progress in this field in recent years. Figure 3 depicts the progress of research in this research area since 2012, when the first publication was indexed in Scopus and Wos. According to Scopus, there were only six publications up until 2016. Scopus indexed 12 papers in 2012, with the number gradually increasing in subsequent years. The year 2021 is expected to have the most publications, with 179 papers.

Only six contributions were discovered in WoS until 2016. The number of publications then increased at an exponential rate. In 2018, 35 papers were received, with a 97.14 percent increase to 269 papers in 2019. Furthermore, 155 and 206 publications were published in the same year.

The majority of publications are in the year 2021 (TP=206), and we hopefully this development will continue in the upcoming years. Surprisingly, approximately 56 percent (350) of publications were published only in the last two years (2021-22). The number of citations per paper throughout the years as shown in figure 3 validates the noticeable progress in this domain.

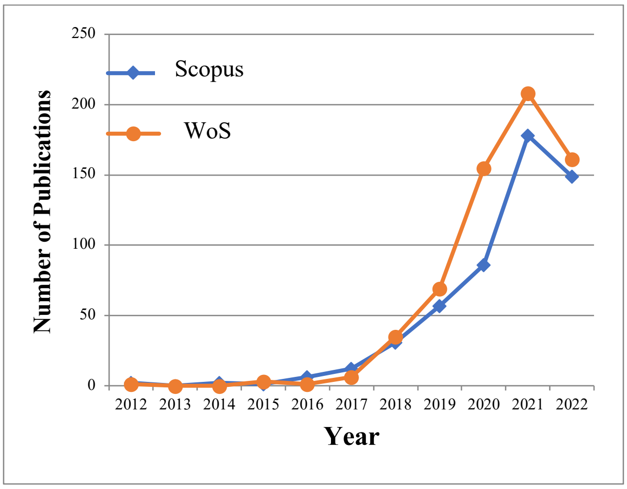


Fig. 3. Publication trends over the years 2011 to 2021 (WoS and Scopus accessed on 22-07-2022).

There are a variety of reasons for the recent increase in papers about MIoT security in the medical field. The broad implementation of IoT tools in medical facilities is a major contributor. Connecting medical devices to the internet has many benefits, including better patient care, remote monitoring, and data collection. Yet, this also creates new security threats and challenges [34-36].

Concern and attention to MIoT security has grown in response to the sensitive nature of medical data and the possible harm that could follow from a security compromise in a medical device. The need for secure MIoT solutions is further driven by the regulatory landscape, which imposes stringent regulations for the security of EHR, such as HIPAA in the United States.

The increased incidence of cyber threats like ransomware attacks against healthcare [37-40] businesses has also increased the importance of taking strong MIoT security measures.

The growing number of papers that address the MIoT security indicates that this is an area where researchers are actively engaged. Due to the novelty and rapid development of the topic, there is a significant need for continued research into the security of MIoT.

There is a strong need for MIoT security measures because of the rising number of vulnerable devices in healthcare [41,42] settings and the potential damage that could arise from a security breach. Evidenced by an increase in publications, the field is actively attempting to address these challenges by investigating novel approaches to secure medical equipment and data.

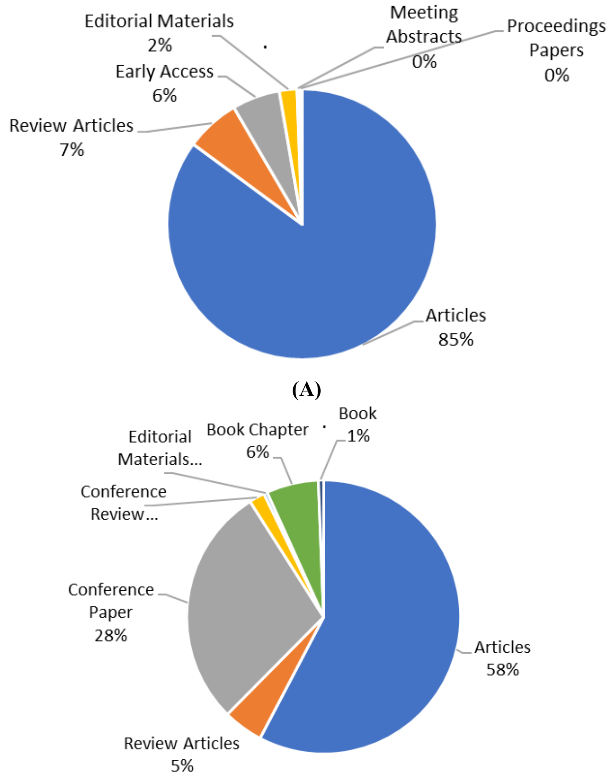
4. Analysis of Document Types

In WoS, a total of 622 research articles were segregated with six distinct types of documents, including 565 articles, 43 review articles, 38 early access articles, 14 proceeding papers, and 2 meeting abstracts.

Scopus categorizes documents into seven types: articles (281), reviews (23), conference papers (139), conference reviews (9), book chapters (30), books (3), and editorial materials (2). Table 1 lists all the document types. In this case, 'percent' signifies the percentage of contribution for a specific type of document. The document analysis is shown in table 1 and the visual representation is shown in fig. 4.

Table 1. Documents type analysis (WoS and Scopus accessed on 22-07-2022).

Document Types	WoS		Scopus	
	Total Number	%	Total Number	%
Articles	565	90.545	281	57.70
Review Articles	43	6.891	23	4.72
Conference Paper	-	-	139	28.54
Early Access	38	6.09	-	-
Conference Review	-	-	9	1.84
Editorial Materials	14	2.244	2	0.41
Meeting Abstracts	2	0.321	-	-
Proceedings Papers	2	0.321	-	-
Book Chapter	-	-	30	6.16
Book	-	-	3	0.61



(A)

(B)

Fig. 4. Visual representation of Documents type analysis ((A):WoS and (B):Scopus accessed on 22-07-2022).

5. Bibliometric Analysis

This segment is allotted into several sub-sections, with the most creative and principally cited authors, the uppermost subject areas, the most frequently referenced sources, country-by-country analysis, institute-by-institute analysis, and the most important papers in the field of "MIOT Security."

5.1 Most Creative and Very Well Referred Authors

For the bibliometric analysis, the obtained data are examined using the different performance evaluating tools available in the literature. Total Papers (TP) is defined as the total number of articles published by the source, Total Citations (TC) is the total number of citations received by the article, and Citations Per Paper (CPP) is defined as the ratio of total number of citations received and total articles published. The popular parameter for evaluating quality of the journals is termed as Impact Factor (IF) and is calculated as the average number of citations for the articles published in the journal for the period of past two or five years.

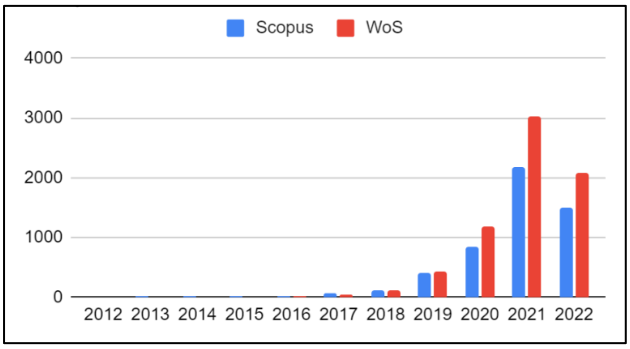


Fig. 5. The number of citations per paper in Scopus and WoS.

The number of citations per paper in fig. 5 validates the increase in publication in WoS and Scopus over the years. WoS had no significant citation count prior to 2015. The number of citations on Scopus is increasing. It received a total of 2188 citations in 2021. Scopus currently shows a total citation out of 5216 in MIOT Security domain.

In the case of WoS, the year 2016 saw a rise in the total count of citation, which had been merely 5 in the preceding four years, as actual publications (TP=5, TC=21) began in the same year. More than 61.19 percent of citations (a total of 4216 citations) got in the two years, mirroring the growth pattern in total publications (2020-21). Based on the total number of papers, the list of the most creative authors is compiled and ranked from both indexing databases. Table 2 shows the top ten most productive authors, as well as a comparison of both databases.

Table 2. Top 10 most productive authors.

WoS				Scopus			
Author	NP	TC	CPP	Author	NP	TC	CPP
Mohanty SP	12	238	19.83	Chen F.	10	79	7.9
Choo KKR	8	276	34.5	Lakhan A.	8	48	6
Guo JH	8	126	15.75	Mohanty S.P.	8	106	13.25
Liu Z	8	91	11.38	Huang C.	7	56	8
Almogren A	7	139	19.86	Zhang Z.	7	26	3.71
Din IU	7	124	17.71	Cheng X.	6	68	11.33
Guizani M	7	111	15.86	Choo K.-K.R.	6	361	60.17
Guo Y	7	177	25.29	Guizani M.	6	82	13.67

Hassan MM	7	116	16.57	Vijayakumar P.	6	32	5.33
Khan MA	6	46	7.67	Wang H.	6	31	5.17

As the WoS shows, Mohanty SP has written the most in the topic of "MIOT security," with a total of 12 publications. Next in line are Choo, Guo, and Liu Z, all of whom have 8 books to their names. Five other authors, Almogren, Din, Guizani, Guo, and Hassan, all have TPs of 7.

Chen F. has more articles (10 total) than any other author in Scopus. Next in line are (TP=7) holders Lakhan A. and Mohanty S.P. The minimal number of publications required for inclusion in the top ten list of Scopus is 6, according to data from both the Scopus and the WoS databases.

When looking at the top 10 most creative authors in WoS, Choo K.K.R. has the greatest total citations with 276 (TP=8), followed by Mohanty SP with 238 (TP=12). Guo Y (TC=177), Almogren A (TC=139), Guo JH (TC=126), Din IU (TC=124), Hassan MM (TC=116), and Guizani (TC=111) are among the other authors with over 100 citations. Although Mohanty SP has written more books, Choo K.K.R. has the highest citation rate (34.5/paper).Table 3 shows the top ten most prominent authors, as well as a comparison of both databases.

Table 3. Top 10 most prominent authors.

WoS				Scopus			
Author	**TC**	**NP**	**CPP**	**Author**	**TC**	**NP**	**CPP**
CHOO KKR	276	8	34.5	CHOO K.-K.R.	361	6	60.17
MOHANTY SP	238	12	19.83	LEE I.	284	5	56.8
PIRBHULAL S	219	7	31.29	SOKOLSKY O.	249	2	124.5
GUO Y	177	7	25.29	KIM B.	240	2	120
KOUGIANOS E	177	7	25.29	GADEKALLU T.R.	165	3	55
ALMOGREN A	139	7	19.86	LI Y.	163	4	40.75
GUPTA D	138	6	23	ABUHUSSEIN A.	150	5	30
SODHRO AH	136	7	19.43	ALSUBAEI F.	150	5	30
GUO JH	126	8	15.75	SHIVA S.	150	5	30
DIN IU	124	7	17.71	SUN W.	148	2	74

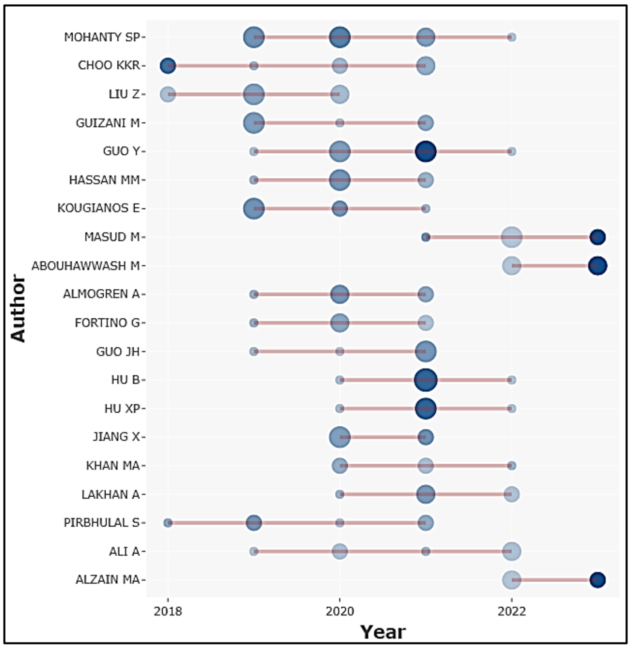


Fig. 6. Visualization of the top 20 significant contributing authors (Source: Biblioshiny R-package.)

Interestingly, none of the top 10 most prolific authors including Liu Z, Guizani M, Hassan MM, and Khan MA emerge in the top 10 list of most eminent authors. Scopus ranks Choo K.-K.R. first since his or her 6 papers have been cited 361 times.

Sokolsky O. once again has the highest CPP, at 124.5. Kim B. (CPP=120), SUN W. (CPP=74),and Choo follow him. (CPP=60.16). Since this sector is more active and demanding, we anticipate that this ranking of the writers may vary dramatically, during the following 5 years.

Fig 6. depicts a visualization of the top 20 significant contributing authors. Only 13 of the scholarly articles in this field were written by a single author, even though 2053 authors contributed to them. The average productivity is reduced because 80.22 percent of the authors have only one paper.

5.2. Scientific Analysis of Articles by Subject Areas

The WoS and Scopus repositories assign subject groups/areas to the papers they index. Table 4 shows the top ten disciplines with MIOT security applications that we extracted.

WoS and Scopus are the top two database and in that Computer Science and Engineering are the two most popular research areas. Out of the total publications, in computer science WoS has 411, Scopus has 328 while in Engineering, Scopus has 442 and 258 publications. One thing to keep in mind here is that the paper could be assigned to more than one category. As a result, it is entirely possible that the total percentage will be greater than 100 percent. According to WoS, the MIOT Security is most profitable field as knowledge retrieval is concerned, researchers from Mathematical Computational Biology and Medical Informatics also have started publications with 40 and 22 papers, respectively. Scopus also indexes a wide range of research fields, including Medicine (TP=45), Physics and Astronomy (TP=43).

Table 4. Top 10 subject areas in the WoS and Scopus.

WoS				Scopus			
Sr. No	**Subject area**	**TP**	**%**	**Sr. No**	**Subject area**	**TP**	**%**
1	Computer Science	411	65.6	1	Computer Science	442	38.8
2	Engineering	328	52.3	2	Engineering	258	22.6
3	Telecommunications	250	39.9	3	Mathematics	73	6.4

4	Chemistry	55	8.7	4	Decision Sciences	51	4.5
5	Instruments Instrumentation	52	8.3	5	Materials Science	51	4.5
6	Mathematical Computational Biology	40	6.3	6	Medicine	45	3.9
7	Physics	30	4.7	7	Biochemistry, Genetics and Molecular Biology	44	3.9
8	Materials Science	28	4.4	8	Physics and Astronomy	43	3.8
9	Health Care Sciences Services	22	3.5	9	Social Sciences	26	2.3
10	Medical Informatics	22	3.5	10	Health Professions	25	2.2

5.2.1. Leading Academic Journals

Figure 7 depicts the progress of the best five sources from 2012 to 2022. Up until 2017, IEEE Access, IEEE Internet of Things Journal, Sensors, Future Generation Computer Systems-The International Journal of EScience, and Computer Communications were consistent. IEEE Internet of Things Journal alone has published more than 35 articles between 2012 and 2022 which is significantly high.

The graph shows the Loess regression result in which independent factors such as journal quantity and publication date are provided. This implies that the approach allows the function to assume negative values if the data is very close to zero. In this way, it contributes to the visual impression and highlights the time difference between the two publications.

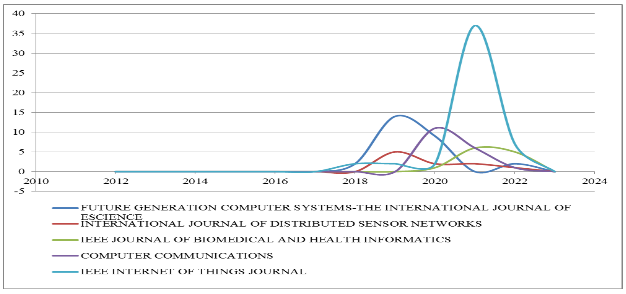


Fig. 7. Source Growth Analysis of top 5 Sources.

5.2.2. Top 10 Productive Journals Publishing Works MIOT Security

Academic journals are peer-reviewed publications that aim to advance the field(s) they cover on a regular basis (monthly, annually, etc.). In Table 5 we list the top 10 journals that regularly publish research on MIOT security. To facilitate your search, we have arranged these journals by total number of articles published.

WoS's best 10 list is topped by IEEE's two flagship journals: IEEE Access (TP=34) and IEEE Internet of Things Journal (TP=74), with Sensors Journal (TP=13) in third place. IEEE Access has an impressive 1133 total citations, putting it ahead of all other journals in the field. Future Generation Computer Systems: An International Journal of Escience (TC=626, TP=27), and the IEEE Internet of Things Journal (TC=664) follow in terms of citations per paper.

Remarkably, not a single Scopus source has a citation total that comes close to the greatest Scopus source count in WoS. Since researcher's value high-quality journals so highly, their work is more likely to be cited if it appears in one.

Table 5. Top 10 Academic Journals Sources.

WoS			Scopus		
Source	**TC**	**NP**	**Source**	**TC**	**NP**
IEEE Access	1133	74	IEEE Access	847	37
IEEE Internet of Things Journal	664	50	IEEE Internet of Things Journal	601	34
Sensors	209	34	IEEE Journal of Biomedical and Health Informatics	70	15
Future Generation Computer Systems-The International Journal Of Escience	626	27	Sensors	47	12
Computer Communications	357	18	Computer Communications	289	11
CMC-Computers Materials & Continua	21	15	IEEE Transactions on Industrial Informatics	40	11
Electronics	104	15	Lecture Notes in Computer Science (Including Lecture Notes In Bioinformatics)	16	10
IEEE Journal of Biomedical and Health Informatics	81	12	Electronics (Switzerland)	59	9
Journal of Healthcare Engineering	36	11	Communications in Computer and Information Science	15	8
Computational Intelligence and Neuroscience	6	10	Future Generation Computer Systems	221	8

Table 6. Top 10 influential journals.

WoS			Scopus		
Source	**TC**	**NP**	**Source**	**TC**	**NP**
IEEE Access	1133	74	IEEE Access	847	37
IEEE Internet Of Things Journal	664	50	IEEE Internet of Things Journal	601	34
Future Generation Computer Systems-the International Journal of Escience	626	27	Computer Communications	289	11
Computer Communications	357	18	Digital Communications and Networks	266	1
Sensors	209	34	Proceedings of the IEEE	241	1
Digital Communications and Networks	169	1	Future Generation Computer Systems	221	8

IEEE Transactions on Consumer Electronics	151	9	Security and Communication Networks	179	7
Neural Computing & Applications	136	7	Health Information Science and Systems	137	2
IEEE Transactions on Industrial Informatics	119	10	Journal of Medical Systems	133	3
Security And Communication Networks	115	7	Journal of Diabetes Science and Technology	120	2

In terms of impact (as measured by citations), Table 6 lists the topmost ten journals in WoS and Scopus. Based on data from Scopus, IEEE Access has 847 citations for only 37 articles. IEEE's Internet of Things Journal came in at No. 2 with 601 citations, just ahead of Computer Communications (289 citations). On the other hand, Digital Communications and Networks has 266 citations. These four journals are the only ones having over 250 citations. Scopus ranks high-quality journals among the most influential journals, outside of international conferences, which is not the case for the most prolific sources.

5.3. Geographical Productivity Analysis

Our findings are based on how the workload is distributed across many countries. Table 7 displays the related work on MIOT security from several nations. Based on the number of publications produced, the top 10 countries are listed and rated. WoS reports that China is alone responsible for 37.99 percent of all publications, with a total percentage (TP) of 182. After China, the next most visited countries are India (TP=83), Saudi Arabia (TP=47), the United States (TP=44), and South Korea (TP=36). The United States ranks fourth, but its AAC of 23.98 is far higher than that of Saudi Arabia's (10.96).

If we examine the trend retrieved from Scopus, the top three nations are identical to those of WoS, apart from India and the United States. In addition, they differ in terms of the number of citations and publications. While India has 142 publications, the United States and China have 98 and 94 publications, respectively. Here, Australia has the highest AAC of 21.23 followed by the United States(19.17) and South Korea (17.65).

Table 7. Countries and their Collaborative Index.

WoS							Scopus						
Country	**TP**	**TC**	**SCP**	**MCP**	**MCP_Ratio**	**AAC**	**Country**	**TP**	**TC**	**SCP**	**MCP**	**MCP_Ratio**	**AAC**
China	182	1704	103	79	0.434	9.36	India	142	1458	85	57	0.4	10.27
India	83	870	46	37	0.446	10.48	United States	98	1879	63	35	0.36	19.17
Saudi Arabia	47	515	13	34	0.723	10.96	China	94	980	56	38	0.4	10.43
Usa	44	1055	28	16	0.364	23.98	Saudi Arabia	85	969	24	61	0.72	11.4
Korea	36	312	12	24	0.667	8.67	Pakistan	46	415	12	34	0.74	9.02
Pakistan	26	221	7	19	0.731	8.5	United Kingdom	41	433	7	34	0.83	10.56
Egypt	19	211	2	17	0.895	11.11	Malaysia	26	167	6	20	0.77	6.42
Italy	17	181	11	6	0.353	10.65	South Korea	26	459	8	18	0.69	17.65
Malaysia	14	116	2	12	0.857	8.29	Australia	22	467	5	17	0.77	21.23
Japan	11	78	5	6	0.545	7.09	Egypt	20	258	2	18	0.9	12.9

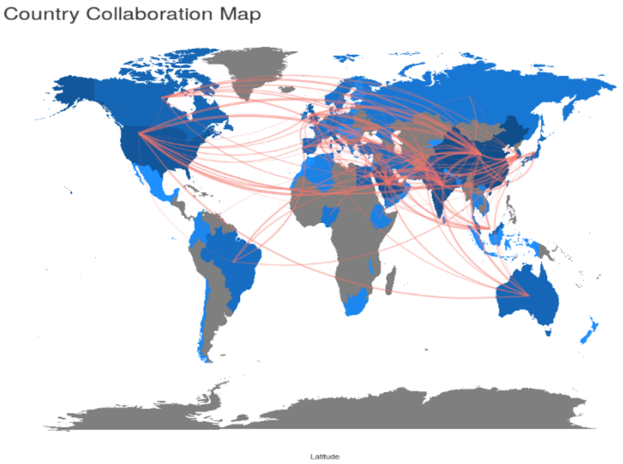


Fig. 8. Visualization of Country-wise Scientific Production and collaboration map on MIOT security literature (Image from Biblioshiny).

Figure 8 shows the Visualization of Country-wise Scientific Production and collaboration map on MIOT security literature. Saudi Arabia emerged as the top collaborator with Pakistan (41 publications), followed by Saudi Arabia and India 31 publication, and India with the USA (27 publications). There were 26 collaborations between India and China. The least active among the 393 collaborators were Bangladesh and Australia with only 1 publication.

5.4. Highly Influential Articles

The table 8 and 9 showing the top ten articles with the greatest number of citations from both WoS and Scopus. These tables also contain the authors details and the date of the book's release. To be considered influential, the citation count of a paper must be increasing over time. There are six papers that are the same in both tables (Banerjee et al., 2018 [43]; Nguyen et al., 2019 [46]; Gatouillat et al., 2018 [47]; Elhoseny et al., 2020 [48]; Sun et al., 2018 [49];Swarna Priya et al., 2020) [44]. The most cited paper in both databases is Banerjee et al., 2018 [43]. (168 in WoS and 259 in Scopus) and rightly meets the criteria and attempted the survey of articles presenting IoT security solutions published in English since January 2016.

Swarna Priya et al. (2020) takes second place in WoS with a citation count of 115 (TC=115). The MIoT environment has been discussed in this paper, and an effective and efficient

IDS has been developed to classify and predict unforeseen cyberattacks. There are 112 citations to Mitchell and Chen's (2015) [45] paper, followed by Nguyen (2019) [54], Gatouillat et al. (2018) [47], and Elhoseny M (2020) [48], which each have 109, 108, and 107 citations. There were five papers published in 2018 that made the top 10.

Now, corresponding to Scopus, only four articles that are not listed in WoS top 10 articles. The article by Lee et al. (2012) [54] received 240 citations and SUN et al. (2018) [49] got 147 citations. The two other articles of Scopus are by Jagadeeswari et al.(2018) [55] and Azar and Dey et al., (2018) [56] having citation counts of 125 and 85, respectively.

Table 8. Top ten articles with the greatest number of citations from WoS.

Document	DOI	Year	TC
BANERJEE M, 2018, DIGIT COMMUN NETW [43]	10.1016/J.DCAN.2017.10.006	2018	168
SWARNA PRIYA MS, 2020, COMPUT COMMUN [44]	10.1016/J.COMCOM.2020.05.048	2020	115
MITCHELL R, 2015, IEEE T DEPEND SECURE [45]	10.1109/TDSC.2014.2312327	2015	112
NGUYEN DC, 2019, IEEE ACCESS [46]	10.1109/ACCESS.2019.2917555	2019	109
GATOUILLAT A, 2018, IEEE INTERNET THINGS [47]	10.1109/JIOT.2018.2849014	2018	108
ELHOSENY M, 2020, NEURAL COMPUT APPL [48]	10.1007/S00521-018-3801-X	2020	107
SUN WC, 2018, SECUR COMMUN NETW [49]	10.1155/2018/5978636	2018	96
KHEZR S, 2019, APPL SCI-BASEL [50]	10.3390/APP9091736	2019	92
JALAL AH, 2018, ACS SENSORS [51]	10.1021/ACSSENSORS.8B00400	2018	84
MASOOD A, 2018, J BIOMED INFORM [52]	10.1016/J.JBI.2018.01.005	2018	83
YANG SH, 2022, IEEE T ANTENN PROPAG [53]	10.1109/TAP.2021.3098589	2022	78

Table 9. Top ten articles with the greatest number of citations from Scopus.

Document	DOI	Year	TC
BANERJEE M. (2018), DIGITAL COMMUNICATIONS AND NETWORKS [43]	10.1016/j.dcan.2017.10.006	2018	259
LEE I. (2012), PROCEEDINGS OF THE IEEE [54]	10.1109/JPROC.2011.2165270	2012	240
NGUYEN D.C. (2019), IEEE ACCESS [46]	10.1109/ACCESS.2019.2917555	2019	158
SUN W. (2018), SECURITY AND COMMUNICATION NETWORKS [49]	10.1155/2018/5978636	2018	147
GATOUILLAT A. (2018), IEEE INTERNET OF THINGS JOURNAL [47]	10.1109/JIOT.2018.2849014	2018	144
SWARNA PRIYA R.M. (2020), COMPUTER COMMUNICATIONS [44]	10.1016/j.comcom.2020.05.048	2020	140
JAGADEESWARI V. (2018), HEALTH INFORMATION SCIENCE AND SYSTEMS [55]	10.1007/s13755-018-0049-x	2018	125
ELHOSENY M. (2020), NEURAL COMPUTING AND APPLICATIONS [48]	10.1007/s00521-018-3801-x	2020	100
DEY N. (2018), JOURNAL OF MEDICAL SYSTEMS [56]	10.1007/s10916-018-0921-x	2018	85
GRECO L. (2020), PATTERN RECOGNITION LETTERS [57]	10.1016/j.patrec.2020.05.016	2020	82

5.5. Keywords Frequency

In this sub section, a discussion on some of the keywords that most of the researchers used frequently is presented. Research journal articles can be found in both current and previous editions. Using keywords and a summary of an article's topic, the Web of Science began providing this information in 1990. Using these keywords and titles, you can look for research gaps and trends.

Data Provided Also show that the Security and Internet of Medical Things are regularly preferred in the literature by the authors, For Example, the article having titles "Medical Cyber Physical System Security-Mitigating Attacks Using Trust Model" and "Secure Identity Authentication of Community Medical Internet of Things" has the term "Security" and "MIoT".

As shown in the figure 9 the word map is represented based on the analysis of the articles content, and it is clear that word map is split up into 4 groups. The groups in fig.8 determines the enhancement in the progressive research that is connected to "MIoT". It demonstrates two main groups, which are MIoT(red) and security(green).The types of MIoT are marked by keywords that are associated to MIoT, especially, "healthcare," ''challenges'', ''management'', ''framework'', ''internet'', ''network'', ''architecture'', while security comprises terms such as ''access control'', ''protocol'', ''authentication'', ''security'', ''privacy'', ''scheme'', "authentication"). In Addition, ''iot'', "system model", and "big data" were noted as words that link up the research areas from the types of MIoT and security groups. The green cluster shown in fig. 8 is primarily aimed on research areas of security algorithms such as "classification", "prediction", "algorithm", "neural network", and "recognition".

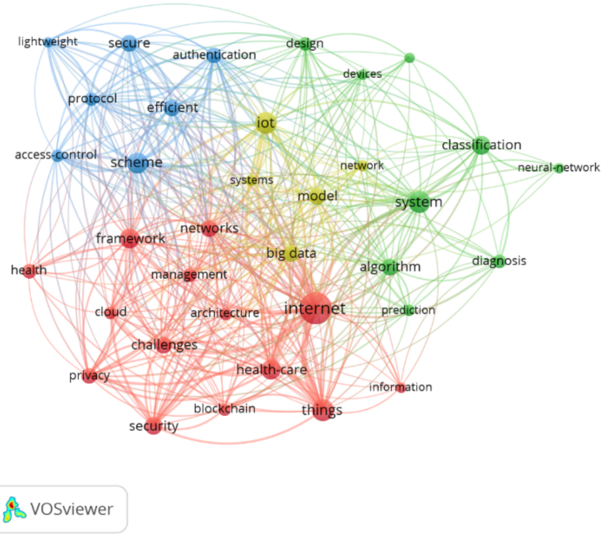


Fig. 9. Word map of author keywords.

6. Conclusion

Based on the Scopus, and WoS datasets, literature on the Security of MIoT from 2012–2021 were retrieved and analyzed with the help of biblioshiny and VOS viewer software. Security of MIoT research continue the following attributes and subject: First, from the point of view of publication patterns, the document number in the field of MIoT Security continues to grow, and the focus on security issues in healthcare domain research and the number of scholars taking part in the same study are rising over the time. Second, developed nations such as the China, India, Saudi Arabia, USA, and Korea are more critical as research power is considered, revealing less awareness of these security in countries like Egypt and Japan. The analysis of articles reveals that international collaboration is uncommon, while papers based on independent research are more common. This trend, however, is counterproductive to the ongoing globalization of scientific study. Third, the most often keywords used in the field of MIoT security are MIoT, Security, Privacy, authentication and access control. Conclusively, from the pooled analysis of most common keywords in the field of research that the need to maintain an individual organization's position and avoid any negative security events in the future, healthcare organizations will invest rapidly in advancing the organization's information security policy. Embedded security will take precedence over end-to-end security in the design of MIoT devices and components. More international collaborations, if promoted, may result in worldwide guidelines in security of healthcare data generated by MIoT devices -related practices and policies.

References

1. Thilakarathne NN, Kagita MK, Gadekallu TR, “The role of the internet of things in health care: a systematic and comprehensive study”. *International Journal of Engineering and Management Research*, 10(4), 2020, pp.145-159.
2. Thilakarathne NN. “Security and privacy issues in iot environment”. *International Journal of Engineering and Management Research,* 10(1), 2020, pp.26-29.
3. Alsubaei F, Abuhussein A, Shiva S. “Security and privacy in the internet of medical things: taxonomy and risk assessment”. *In Proceedings of the 42nd conference on local computer networks workshops (LCN workshops),* IEEE, 2017, pp. 112-120.
4. Darwish S, Nouretdinov I, Wolthusen SD. “Towards composable threat assessment for medical IoT (MIoT)”. *Procedia computer science.* 2017, pp. 27-32.
5. Tarouco LM, Bertholdo LM, Granville LZ, Arbiza LM, Carbone F, Marotta M, De Santanna JJ. “Internet of Things in healthcare: Interoperatibility and security issues”. *In Proceedings of the international conference on communications (ICC), IEEE,* 2012 , pp. 6121-6125.
6. Alsubaei F, Abuhussein A, Shandilya V, Shiva S. “IoMT-SAF: Internet of medical things security assessment framework”. *Internet of Things*, 8, 2019, pp. 100-123.
7. Hossain M, Islam SR, Ali F, Kwak KS, Hasan R. “An Internet of Things-based health prescription assistant and its security system design”. *Future generation computer systems*. 82, 2018, pp. 422-39.
8. Pattewar G, Mahamuni N, Nikam H, Loka O, Patil R. “Management of IoT devices security using blockchain—a review”. *In Proceedings of the Sentimental Analysis and Deep Learning, Springer, Singapore.* 2022, pp.735-43.
9. Gaikwad SR, Patil RY, Borse DG. “Advanced security in 2LQR code generation and document authentication”. *In Proceedings of the international conference on nascent technologies in engineering (ICNTE).* IEEE 2019, pp. 1-4.
10. Mahamuni N, Pattewar G, Nikam H, Loka O, Patil R. “A Blockchain and Proxy Re-Encryption Based Approach for IoT Data Security: A Review”. *In Proceedings of the International Conference on Emerging Technologies and Intelligent Systems, Springer, Singapore.* 2022, pp. 587-595.
11. Pirbhulal S, Samuel OW, Wu W, Sangaiah AK, Li G. “A joint resource-aware and medical data security framework for wearable healthcare systems”. *Future Generation Computer Systems*. 95, 2019, pp.382-91.
12. Kang J, Adibi S. “A review of security protocols in mHealth wireless body area networks (WBAN)”. *In Proceedings of the 1st International Conference on Future Network Systems and Security FNSS,* 2015, pp. 61-83.
13. El-Hajj M, Fadlallah A, Chamoun M, Serhrouchni A. “A survey of internet of things (IoT) authentication schemes”. *Sensors.* 19, 1141, 2019, pp.1-43.
14. Bhole D, Mote A, Patil R. “A new security protocol using hybrid cryptography algorithms”. *International Journal of Computer Sciences and Engineering*. 4(2), 2016, pp.8-22.
15. Almotiri SH, Khan MA, Alghamdi MA. “Mobile health (m-health) system in the context of IoT”. *In Proceedings of the 4th international conference on future internet of things and cloud workshops (FiCloudW),* IEEE 2016, pp. 39-42.
16. Yogesh PR, Devane SR. “Primordial fingerprinting techniques from the perspective of digital forensic requirements”. *In Proceedings of the 9th international conference on computing, communication and networking technologies (ICCCNT)*, IEEE 2018. pp. 1-6.
17. Patil RY, Devane SR. “Network forensic investigation protocol to identify true origin of cyber crime”. *International Journal of King Saud University-Computer and Information Sciences,* 34(5), 2019, pp. 2031-2044.
18. Sangpetch O, Sangpetch A. “Security context framework for distributed healthcare IoT platform”. *In Proceedings of the 3rd international conference on Internet of Things Technologies for HealthCare, HealthyIoT,* Springer International Publishing, 2016, pp. 71-76).
19. Patil RY, Karati A, Patil Y, Bannore A. “Reliable data sharing in medical cyber physical system using fog computing”. *In Intelligent Edge Computing for Cyber Physical Applications,* 2023, pp. 67-83.
20. Bannore, A., Patil, R.Y. and Devane, S.R. “An efficient proxy signature–based authority delegation scheme for medical cyber physical systems”. *In Cyber Security Threats and Challenges Facing Human Life.* 2022, pp. 13-23.
21. Sarode A, Karkhile K, Raskar S, Patil RY. “Secure Data Sharing in Medical Cyber-Physical system—a Review”. In *Proceedings of the 4th international conference on Futuristic Trends in Networks and Computing Technologies.* Springer Nature Singapore, 2022, pp. 993-1005.
22. Patil RY, Patil YH. “Identity-based signcryption scheme for medical cyber physical system in standard model”. *International Journal of Information Technology.* 14(5), 2022, pp.75-83.
23. Dimitrov DV. “Medical internet of things and big data in healthcare”. *Healthcare informatics research.* 22(3), 2016, pp.156-63.
24. Li C, Hu X, Zhang L. “The IoT-based heart disease monitoring system for pervasive healthcare service”. *Procedia computer science.* 2017, pp.28-34.
25. Laplante PA, Laplante N. “The internet of things in healthcare: Potential applications and challenges”. *It Professional.* 18(3), 2016, pp. 2-4.

26. Koskinen J, Isohanni M, Paajala H, Jääskeläinen E, Nieminen P, Koponen H, Tienari P, Miettunen J. “How to use bibliometric methods in evaluation of scientific research? An example from Finnish schizophrenia research”. *Nordic journal of psychiatry*. 62(2), 2008, pp. 136-43.
27. Donthu N, Kumar S, Mukherjee D, Pandey N, Lim WM. “How to conduct a bibliometric analysis: An overview and guidelines”. *Journal of business research.* 133(1), 2021, pp.285-96.
28. Ellegaard O, Wallin JA. “The bibliometric analysis of scholarly production: How great is the impact?”. *Scientometrics.* 105, 2015, pp.1809-31.
29. Leydesdorff L, Bornmann L. “The operationalization of “fields” as WoS subject categories (WC s) in evaluative bibliometrics: The cases of “library and information science” and “science & technology studies”. *Journal of the Association for Information Science and Technology.* 67(3), 2016, pp.707-714.
30. Olczyk M. “A systematic retrieval of international competitiveness literature: a bibliometric study”. *Eurasian Economic Review.* 6, 2016, pp.429-57.
31. Chadegani AA, Salehi H, Yunus MM, Farhadi H, Fooladi M, Farhadi M, Ebrahim NA. A comparison between two main academic literature collections: Web of Science and Scopus databases. *Asian Social Science.* 9(5), 2013, pp.18-26.
32. Van Eck N, Waltman L. “Software survey: VOSviewer, a computer program for bibliometric mapping”. *scientometrics.* 84(2), 2010 pp.523-38.
33. Aria M, Cuccurullo C. “bibliometrix: An R-tool for comprehensive science mapping analysis”. *Journal of informetrics*. 11(4), 2017, pp.959-75.
34. Elhoseny M, Thilakarathne NN, Alghamdi MI, Mahendran RK, Gardezi AA, Weerasinghe H, Welhenge A. “Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions”. *Sustainability.* 13(21), 2021, pp.1-31.
35. Jackson Jr GW, Rahman S. “Exploring challenges and opportunities in cybersecurity risk and threat communications related to the medical Internet of Things (MIoT*)”. International Journal of Network Security & Its Applications (IJNSA).* 11(4), 2019, pp.75-86.
36. Mcgowan A, Sittig S, Andel T. “Medical internet of things: a survey of the current threat and vulnerability landscape”. *In the Proceedings of the 54th Hawaii International Conference on System Sciences ,* 2021, pp. 3850-3858.
37. Thamer N, Alubady R. “A survey of ransomware attacks for healthcare systems: Risks, challenges, solutions and opportunity of research”. *In the Proceedings of the 1st Babylon International Conference on Information Technology and Science (BICITS).* IEEE. 2021, pp. 210-216.
38. Spence N, Niharika Bhardwaj MB, Paul III DP. “Ransomware in healthcare facilities: a harbinger of the future?”. *Perspectives in Health Information Management.* 2018, pp.1-22.
39. Paul III DP, Spence N, Bhardwa N, PH CD. “Healthcare facilities: another target for ransomware attacks”. *In the Proceedings of the 54th Annual MBAA Conference*, Chicago, IL. 2018.
40. Gopinath S, Olmsted A. “Mitigating the effects of ransomware attacks on healthcare systems”. *In the Proceedings of the World Congress on Internet Security (WorldCIS-2021).* 2022.
41. Indrakumari R, Poongodi T, Suresh P, Balamurugan B. “The growing role of Internet of Things in healthcare wearables”. *In Emergence of Pharmaceutical Industry Growth with Industrial IoT Approach*. 2020, pp. 163-194.
42. Farahani B, Firouzi F, Chang V, Badaroglu M, Constant N, Mankodiya K. “Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare”. *Future generation computer systems*. 78(2), 2018, pp.659-676.
43. Banerjee M, Lee J, Choo KK. “A blockchain future for internet of things security: a position paper”. *Digital Communications and Networks.* 4(3), 2018, pp.149-60.
44. RM SP, Maddikunta PK, Parimala M, Koppu S, Gadekallu TR, Chowdhary CL, Alazab M. “An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture”. *Computer Communications*. 160, 2020, pp.139-49.
45. Mitchell R, Chen R. “Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems”. *IEEE Transactions on Reliability.* 65(1), 2015, pp.350-358.
46. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. “Blockchain for secure ehrs sharing of mobile cloud based e-health systems*”. IEEE access.* 7, 2019, pp.792-806.
47. Gatouillat A, Badr Y, Massot B, Sejdić E. “Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine”. *IEEE internet of things journal.* 5(5), 2018, pp.3810-22.
48. Elhoseny M, Shankar K, Lakshmanaprabu SK, Maseleno A, Arunkumar N. “Hybrid optimization with cryptography encryption for medical image security in Internet of Things”. *Neural computing and applications*. 32, 2020, pp.10979-93.
49. Sun W, Cai Z, Li Y, Liu F, Fang S, Wang G. “Security and privacy in the medical internet of things: a review”. *Security and Communication Networks*. 2018, pp.1-9.
50. Khezr S, Moniruzzaman M, Yassine A, Benlamri R. “Blockchain technology in healthcare: A comprehensive review and directions for future research”. *Applied sciences.* 9(9), 2019, pp.17-36.
51. Jalal AH, Alam F, Roychoudhury S, Umasankar Y, Pala N, Bhansali S. “Prospects and challenges of volatile organic compound sensors in human healthcare”. *Acs Sensors.* 3(7), 2018, pp.1246-63.
52. Masood A, Sheng B, Li P, Hou X, Wei X, Qin J, Feng D. “Computer-assisted decision support system in pulmonary cancer detection and stage classification on CT images”. *Journal of biomedical informatics*. 79, 2018, pp.117-28.
53. Yang S, Zhang L, Wang W, Zheng Y. “Flexible tri-band dual-polarized MIMO belt strap antenna toward wearable applications in intelligent internet of medical things”. *IEEE Transactions on Antennas and Propagation.* 70(1), 2021, pp.197-208.
54. Lee I, Sokolsky O, Chen S, Hatcliff J, Jee E, Kim B, King A, Mullen-Fortino M, Park S, Roederer A, Venkatasubramanian KK. “Challenges and research directions in medical cyber–physical systems”. *Proceedings of the IEEE*. 100(1), 2011, pp.75-90.
55. Jagadeeswari V, Subramaniyaswamy V, Logesh R, Vijayakumar V. “A study on medical Internet of Things and Big Data in personalized healthcare system”. *Health information science and systems*. 6, 2018, pp.1-20.
56. Dey N, Ashour AS, Shi F, Fong SJ, Tavares JM. “Medical cyber-physical systems: A survey”. *Journal of medical systems.* 42, 2018 pp.1-3.
57. Greco L, Percannella G, Ritrovato P, Tortorella F, Vento M. “Trends in IoT based solutions for health care: Moving AI to the edge”. *Pattern recognition letters*. 135, 2020, pp.346-53