A Bibliometric Approach to Quantitatively Assess Current Research Trends in 5G Security

Abstract

Cellular communication has seen remarkable growth since its inception and has now evolved into fifth generation (5G) networks. Promising services and use cases are envisioned leveraging the advancements within this technology including but not limited to the Internet of Things (IoT), massive MIMO, Device to Device communication (D2D), Vehicle to Everything (V2X) communication, and VR/AR applications. It integrates enabling technologies such as Edge computing, Network Function Virtualization (NFV), and Software Defined Networks (SDN) to support a broad range of use cases and application scenarios. Significant security and privacy challenges have arisen and are attracting interest from both academia and industry to develop bespoke solutions to address them. This study aims to examine research within security and privacy for 5G-based systems highlighting contributions made by the research community and identify research trends within different subdomains of 5G security where open issues still exist. The paper uses a bibliographic approach to review the state-of-the-art in the field of 5G security and is the pioneering effort to investigate 5G security research using this methodology. Specifically, the paper presents a quantitative description of the existing contributions in terms of authors, organizations, and countries. It then presents detailed keyword and co-citation analysis which shows the quantity and pattern of research work in different subfields. Finally, 5G security areas, having open challenges, are identified for future research work.

Keywords: Bibliometrics, 5G, Security and Privacy, Scientometric, Edge Computing, Cyber-physical Systems

1. Introduction

5G is the latest mobile network technology expected to deliver high bandwidth up to 10 Gbps, low latency in the range of 1 and 2 milliseconds, and increased reliability resulting in improved user experience (Agriwal et al. 2016). It is envisaged to introduce new and strengthen existing application scenarios and services such as massive IoT, connected vehicles, healthcare, smart grids, and multimedia communication. Enabling technologies such as edge computing, network function virtualization, software-defined network, and network slicing underpin 5G's ability to achieve better performance, reliability, and security. According to Qualcomm's 5G economy study (Qualcomm, 2020), the full impact of 5G on the global economy will be realized by 2035 and will be worth $13 trillion. It is therefore attracting significant interest from both research and commercial aspects. A Gartner study (Gartner, 2020) highlighted that the worldwide investment in 5G network infrastructure by the communication service providers (CSP) doubled from $4 billion in 2019 to $8 billion in 2020. It now represents 20% of the total investment in the wireless infrastructure and will exceed LTE/4G in 2022. Another Gartner study (Gupta, 2020) estimates the number of 5G mobile phones shipped in 2020 to be 11% of total mobile phones which is expected to double in number to 440 million.

Alongside the emergence of new use cases to leverage capabilities provided by 5G, the security and privacy challenges introduced as a result of 5G adoption are significant (Fang et al. 2017) and require bespoke solutions from both industry and academia. For instance, Internet of Things devices, which will underpin massive machine-type communications (mMTC) are typically resource-constrained with limited computation power and memory. It makes them an easy target for attackers to use in distributed denial of service attacks (Gupta et al., 2017). Similarly, connected vehicles are another prominent use case of developments within 5G. However, security and privacy are of fundamental significance to the correct operation especially for

autonomous connected vehicles where secure operation can affect the safety of the vehicular system. Further, the emerging applications of 5G also include critical national infrastructures such as smart grids which have been a victim of cyber-attacks in recent years (Liang et al., 2016). Consequently, security and privacy within 5G is a fundamental element to its widespread adoption and although 5G can leverage advancements made within 4G in this respect, new use-cases and capabilities introduced by 5G require further work in this area.

The use of edge computing has been proposed in 5G applications scenarios such as autonomous vehicles, healthcare, augmented and virtual reality, and video and speech analytics which require real-time operations. Edge computing is envisaged to play an important role in changing the way security of applications and network infrastructure works. Ultra-high bandwidth and faster connections available after 5G means attackers have improved connections as well. Edge computing delivers cloud services such as compute and store at the network edge and can apply security services, artificial intelligence, and machine learning to provide privacy and authentication to the network and applications. (Zhang et al., 2020) proposed privacy-preserving authentication framework based on edge computing for 5G-enabled vehicular networks. (Rasheed et al. 2020) presented edge computing-based privacy protocol for 5G vehicular network.

Bibliometrics is a quantitative approach to assess published articles (Garousi et al., 2016) in a specific field. Various bibliometric techniques are used to determine the most active authors and organizations in a specific research field (Ding, 2011). The term *bibliometrics* is closely related to "*scientometrics*" as mentioned in (Ellegaard and Wallin, 2015). A bibliometric analysis in the field of 5G Security will be helpful to determine the academic ranking and productivity of the countries and authors over a period, country-wise research collaboration network, amount of published scientific work by various organizations, and the shift in publication trends in 5G security domain. Furthermore, it will provide a detailed analysis to the researchers and help them make intelligent choices of institutions and organizations for professional or research affiliation. It will also help them review the direction or emerging subfields of 5G security, and to examine different aspects of scientific collaboration.

Comprehensive surveys have been conducted to present and analyze state-of-the-art research in secure 5G networks (Zhang et al. 2019), physical layer security (Wu et al., 2018), security and privacy of 5G technologies (Khan et al. 2019), and security and privacy challenges when 5G is used in IoT (Sicari et al. 2020). However, our research has revealed that currently there exist no bibliometric studies in this area, and therefore, to the best of our knowledge, this paper represents pioneering such effort for security within 5G. Specifically, this study includes a detailed bibliometric analysis of existing research work within 5G security identifying metrics such as most contributing countries, authors, and institutions, co-occurring keywords, most cited papers, and authors. Further, utilizing the analysis of existing research in the area, the paper identifies research gaps within the 5G security domain and discusses future research challenges. Whereas, most surveys lack identification of open challenges and future research directions which can help highlight research trends within 5G security. This study includes a separate section to discuss open issues and research challenges related to 5G security.

1.1 The motivation of the study

The purpose of this study is to achieve a comprehensive understanding of the state-of-the-art 5G security research. This work is aimed at identifying not only the active researchers, institutes, and countries in the field of 5G security but the collaboration between them as well. Another goal is to identify the emerging research areas within 5G security. To answer these queries, this bibliometric study performs the analysis of the relevant research publications in the Web of Science from 2014 to 2020.

1.2 Our Contribution

The major contributions of our paper are explained below:

- To the best of our knowledge, this is the first study that presents a systematic, quantitative and thorough approach for bibliometric analysis on 5G security. The study takes into account research concerning 5G and enabling paradigms such as Cyber-Physical Systems, Edge Computing, Fog Computing, and Internet of Things.
- This paper has presented a critical review of research trends within the edge computing-enabled 5G paradigm. Edge computing is a fundamental paradigm underpinning developments within 5G especially due to its significance in supporting cutting-edge applications of IoT.
- Scientifically gathering, characterizing, and investigating 5G security research papers that have been published between 2014 and 2020 and indexed by Web of Science. In total, 715 articles were shortlisted and have been analyzed for types of publications, most active authors, organizations, and countries as well as listing most cited papers in the said field.
- Keyword co-occurrence, co-citation, and co-authorship analysis based on countries and organizations are presented. Identifying active authors, organizations and countries help both researchers and industry to start collaboration and work together on different projects.
- Through the analysis conducted within this paper, we identify key areas of 5G security and highlight open challenges which require the focus of the future research directions in 5G security.

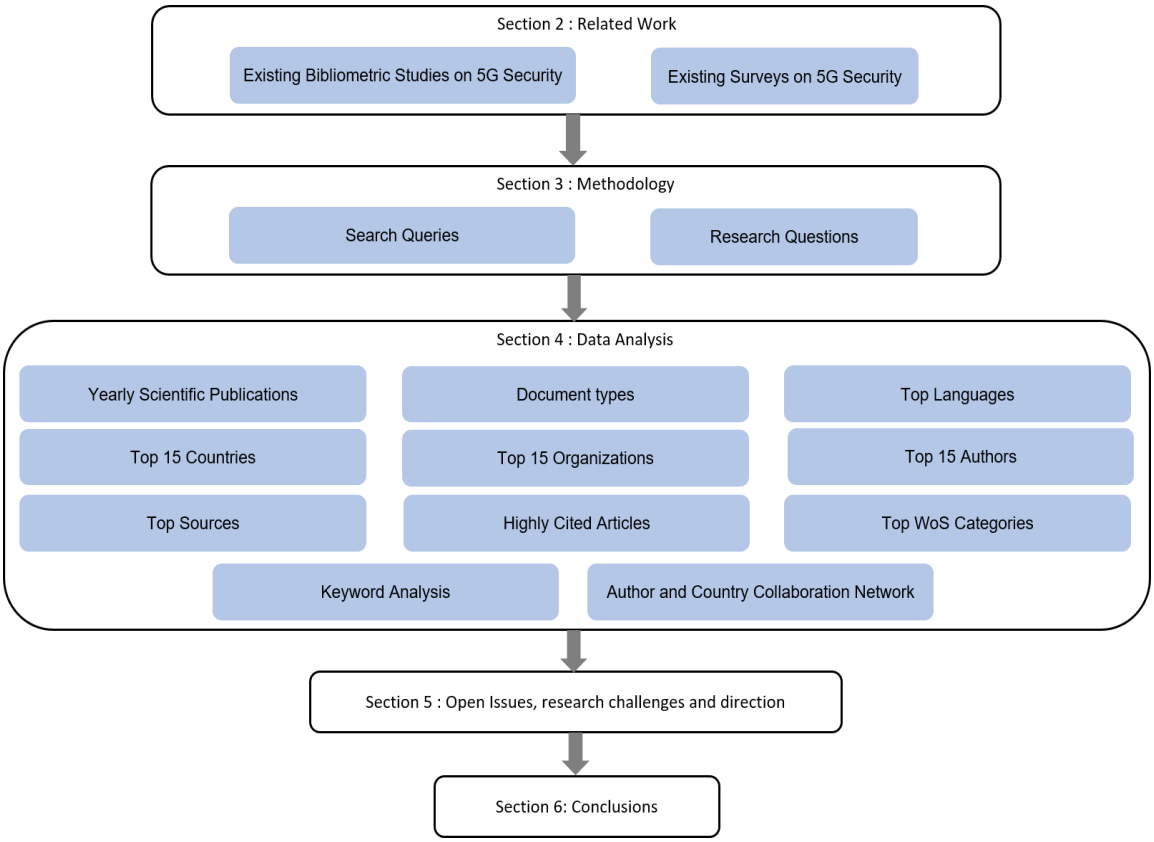


Figure 1: Paper structure

1.3 Paper Outline

An overview of paper structure is presented in Fig. 1 and elaborated as follows. Section 2 presents the literature review on the work done with respect to bibliometric analysis within 5G security domain followed by a detailed description of the method adopted for our research in Section 3. In Section 4, detailed data analysis is presented including, productivity, collaboration network, and keyword analysis. In Section 5, we review the open challenges and suggest future work in the field of 5G Security. The final section summarizes the bibliometric study.

2. Related Work

Bibliometric studies are focused on helping researchers understand the characteristics, structure, and patterns of research activities. Also, the statistical analysis conducted as part of a bibliometric study helps identify trends within a research domain. This involves literature studies of scientific activities in different contexts such as publications, authors, institutions, citations, and countries. Moreover, this method reports on the comprehensive evaluation of the expansion of research fields.

Bibliometric studies have been performed in diverse research domains. For instance, (Ab Razak et al. 2016) have conducted research practices published in the Web of Science in Malware practices domain between the years 2005 and 2015. However, through our research, we have identified that no such studies have been published in the field of 5G security in general and edge-enabled 5G in particular. However, we identified considerable literature available on the privacy and security issues in 5G communication networks, the latest emerging paradigms and use cases as well as some efforts to present a survey of existing work in this area. Table 1 presents a list of surveys and studies published on various 5G security issues.

References	Field	Year
Panwar et al., 2016	A survey on 5G: The Next Generation of Mobile Networks	2016
Wu et al., 2018	5G Physical Layer Security	2018
Ahmed et al., 2018	Overview of 5G Security Challenges and solutions	2018
Ahmed et al., 2019	Security for 5G and Beyond	2019
De Ree et al., 2019	Key Management for 5G	2019
Behrad et al., 2019	Network Authentication and Access Control in 5G	2019
Zhang et al., 2019	Securing 5G Networks	2019
Cao et al., 2019	3GPP 5G Network Security	2019
Sánchez et al., 2020	5G Physical layer Security	2020
Khan et al., 2019	Security and Privacy of 5G technologies	2019
Sicari et al., 2020	Security and Privacy in 5G IoT	2020

Table 1: List of surveys published in 5G security

(Wu et al., 2018) presented a detailed overview of the state-of-the-art in research on 5G physical layer security. These technologies include massive MIMO, mmWave communication, and physical layer security coding. The advantage of physical layer security over traditional cryptographic measures is that it does not depend on computational complexity. As a result, secure communication is still possible even if the attacker has powerful devices. It is extremely beneficial since most of the 5G use cases need to connect devices with different power and computational capabilities. With respect to the physical layer security coding, the paper reviews three security codes, including low-density parity-check (LDPC) code, parity code, and lattice code. The authors also discuss exploiting extra spatial resources in massive MIMO to protect against eavesdropping attacks as well as highlighting the integration of physical layer security and traditional cryptographic techniques to provide confidentiality and privacy in 5G communications.

(De Ree et al., 2019) presented a survey of the state-of-the-art key management schemes for small mobile 5G cells-based network architecture including mobile ad hoc networks and ad hoc D2D networks. These approaches include certificate chaining-based, mobility-based, self-certification-based, pre-distribution-based, partially distributed trusted third party (TTP) based, and fully distributed TTP-based. The authors have presented a comparative analysis of all these techniques and have also discussed the open challenges and future directions.

Study in (Zhang et al. 2019), identified security and privacy issues in 4G and presented state-of-the-art in the 5G security especially focusing on how 5G can leverage advancements made within 4G security. The authors first discuss the lessons learned from the 4G networks especially with respect to limitations of architecture, user privacy leakage, weak home network control, and risk of radio interference. 5G threats and security solutions are discussed regarding the new scenarios and business models including IoT in which both devices and networks can be subjected to threats and attacks such as device trigger, signaling attack, and privacy leakage. The use of enabling technologies such as network function virtualization (NFV), software-defined networks (SDN), edge computing, and network slicing in 5G use cases and application scenarios will improve performance, flexibility, and reliability but can introduce new security challenges. For instance, D2D communication can face attacks such as impersonation, eavesdropping, privacy sniffing, jamming, free-riding, and location spoofing. A secure 5G framework, therefore, can be divided into several domains such as Network access security, network domain security, user domain security, application domain security, and SBA domain security.

The authors in (Khan et al., 2019) presented a comprehensive study on IoT threats, 5G security model, and 5G network threat analysis and identified various security challenges related to 5G security and key 5G technologies such as network slicing, software-defined networks, network function virtualization, multi-access edge computing, and cloud computing. The authors also discussed the 5G physical layer security and privacy from users' perspective as well as the work done by the standardization bodies in this regard. The authors highlight specific ongoing efforts with respect to different sub-domains within 5G security as well as highlighting future research directions.

Authors in (Sicari et al. 2020), analyzed the latest trends in 5G security and privacy solutions. The study focuses on the 5G network aspects such as millimeter wave, non-orthogonal multiple access, backhaul, multi-access edge computing, user association mechanisms, energy-efficient techniques, and cooperative localization. Security requirements such as privacy, trust, authentication, confidentiality, integrity, non-repudiation, intrusion detection, and key management are discussed in detail. The authors also highlighted the role of evolving paradigms such as blockchain, fog computing, and IoT in addressing security challenges within 5G paradigm.

Authors	Study Type	Year	Focus/Research Focus	IoT	SDN	NFV	MEC	Slicing
Wu et al.	Survey	2018	5G physical Layer Security	X	X	X	X	X
Ijaz et al.	Survey	2019	Security for 5G and Beyond	X	X	✓	✓	✓
De Ree et al.	Survey	2019	Key Management for 5G	X	X	X	X	X
Behrard et al.	Survey	2019	Access Control in 5G	✓	X	✓	X	✓
Zhang et al.	Survey	2019	Securing 5G Networks	✓	✓	✓	✓	✓
Khan et al.	Survey	2019	Security and Privacy of 5G Technologies	✓	✓	✓	✓	✓
Sabrina	Survey	2020	Security and Privacy in 5G IoT	✓	X	X	✓	✓

Table 2: Analysis of existing studies within 5G security

From our research (summarized in Table 2), we conclude that authors in (Khan et al. 2019) presented an exhaustive survey of current challenges within 5G security and efforts being made to address these challenges. Most of the survey papers are limited to the discussion of the security of enabling technologies in 5G such as SDN, NFV, and MEC but do not cover the security architecture of 5G networks. Furthermore, the majority of surveys lack identification of open challenges and future research directions which can help highlight research trends within 5G security in general and edge computing-enabled 5G security in particular. This study attempts to bridge this gap by adopting a bibliometric approach to scout existing efforts and identify research trends to help the research community.

As shown in Table 2, there have been several surveys published on 5G security which cover different aspects such as physical layer security, key agreement protocols, 5G in the Internet of Things, access control, and privacy of 5G technologies; still, not a single bibliometric study has been published on this topic. Our study highlights the state-of-the-art in the field of 5G security whilst presenting a detailed bibliometric analysis of the existing research within 5G security, identifying the gap in the literature, and discusses future research challenges.

3. Methodology

The methodology of this study is presented in Fig 2 and comprises five distinct phases: 1) Pre-planning, 2) Data collection, 3) Data refinement, 4) Data analysis and 5) Documentation. In the pre-planning phase, search queries were selected, and appropriate research questions were formulated. In the data collection phase, ISI Web of Science and Scopus databases were searched using the selected keywords and the results were downloaded for data analysis. In the data refinement phase, publications were refined based on criteria such as the language of the publication. In the fourth phase, data analysis and visualization were performed on the refined results based on the following criteria: a) Annual scientific production, b) Document type, c) Productivity with respect to countries, organizations, and authors d) Research Areas, e) Web of Science categories and sources, f) Highly cited research publications g) Keyword analysis and h) Country

collaboration network. Further details of individual phases of our method are explained in dedicated subsections below.

We used the ISI Web of Science (WoS) database during the search process for the articles published during (2014 – 2020) in 5G Security. The ISI Web of Science is one of the most renowned electronically available databases originally provided by Thomson Scientific's Institute for Scientific Information in terms of research publications. Currently, it is maintained by Clarivate Analytics. It was launched in 1997 and covers multi-disciplinary research publications from 1900 to date. It has around 90 million records. Citation reports and data in WoS are prepared after careful investigation, thus WoS provides citation service at the highest level and we can say that WoS indexes high-quality journals, proceedings papers, reviews, editorial materials, and books.

3.1 Data Collection and Refinement

Our data collection process involved defining the criteria based on appropriate search terms to collect relevant data required for performing a comprehensive bibliometric assessment. To achieve this objective, we adopted a methodical approach to filter search results as summarized in Fig 2 and Table 3. Applying different stages of filtering (elaborated below), we analyzed 715 articles relevant to 5G security extracted via ISI Web of Science Core Collection (WoS). Refinement and analysis of multiple criteria are discussed below.

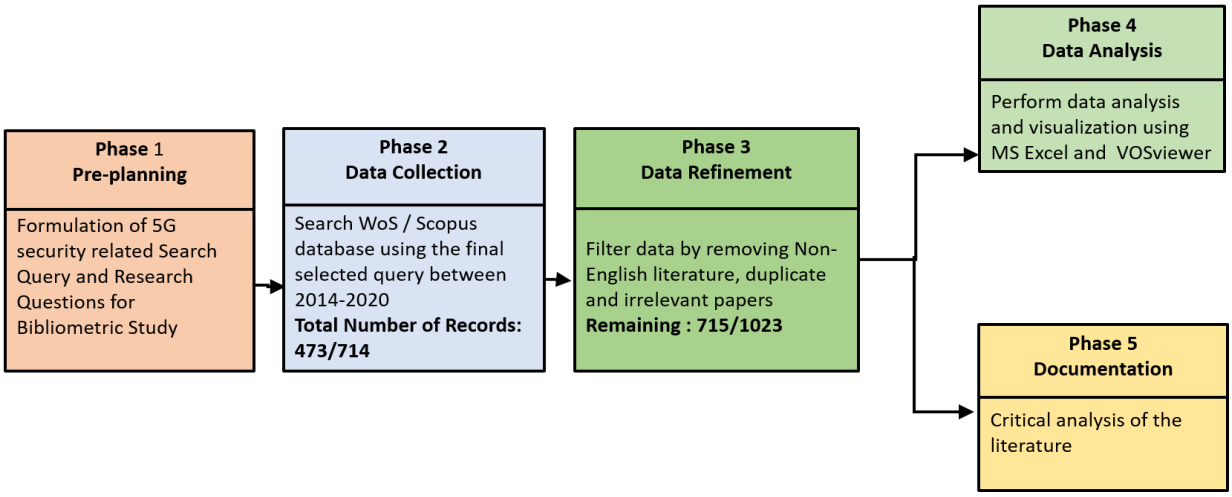


Figure 2: Methodology used in the bibliometric study

S. No.	Queries	No. of Results (WoS)	No. of Results (Scopus)
1	5G	31279	35497
2	5G AND Security	1444	2280
3	5G AND (Security OR Privacy)	1532	2280
4	5G AND Security AND (Edge OR Fog OR CPS OR IoT)	525	800
5	5G AND security AND ("Edge Computing" OR "Fog computing" OR IoT)	473	714
6	5G AND (Security OR Privacy) AND (Edge OR "Edge Computing" OR Fog OR "Fog Computing" OR "Internet of Things" OR IoT OR "Cyber-Physical-Systems" OR CPS OR	715	1023

	"Network Function Virtualization" OR NFV OR "Software Defined Networks" OR SDN)		

Table 3: Different search queries and results in WoS and Scopus

3.2 Description and Refinement of Appropriate Search Terms

Search Query 1: We initially completed our investigation on ISI WoS Core Collection by the term "5G" to assess the amount of research work carried out in the field. The query returned 31279 results. However, these results included a significant number of irrelevant research papers belonging to other domains such as medicines and molecular biology which utilize 5G for innovative applications. Furthermore, our primary goal was to study the work done in 5G security related to different edge computing paradigms. We, therefore, enhanced our search criterion by using the search string based on Query 2.

Search Query 2: After recording the outcome of search Query 1, we then used "5G AND Security" as a search term. Compared to query 1, the results returned by this search were significantly narrowed down to 1444 research publications mainly related to security issues in the 5G network with respect to IoT and edge computing. We, therefore, decided to perform a broad-spectrum analysis on the field of 5G by including several related keywords in multiple search queries.

Search Query 3: In this query, we used the related terms security and privacy, to assess the existing literature. In this case, the number of results increased to 1358 which included work related to the security of 5G applications such as IoT, cyber-physical systems, connected vehicles, and edge computing paradigms. It was therefore tempting to include these applications of 5G in the search query and analyze work done concerning their security issues.

Search Query 4: In this query, we refined our search query even further by introducing related terms such as Edge, Fog, or IoT with 5G and searched for 5G AND Security AND (Edge OR Fog OR CPS OR IoT). In this case, the number of results was 525 which included work related to the security of 5G applications such as IoT, cyber-physical systems, connected vehicles, and edge computing paradigms.

Search Query 5: Query 4 used a short form of enabling technologies within 5G and to address this, we formulate a query will the full form of these enabling technologies. Therein, the query used was "5G AND security AND ("Edge Computing" OR "Fog Computing" OR IoT) which resulted in 473 research publications.

Search Query 6: Analyzing the results from Query 4 and 5 we realized that there remained literature that was not captured through these queries. Therefore, we decided to improve our search query to include both short and full forms of the 5G enabling technologies. In this respect, the query which was used to gather the relevant dataset was 5G AND (Security OR Privacy) AND (Edge OR "Edge Computing" OR Fog OR "Fog Computing" OR "Internet of Things" OR IoT OR "Cyber-Physical-Systems" OR CPS OR "Network Function Virtualization" OR NFV OR "Software Defined Networks" OR SDN) which returned 715 research publications.

3.3 Research questions

Another very important step in conducting a bibliometric study is the selection of appropriate research questions. The quality of study fully depends on the research questions so they must be carefully selected. Table 4 lists the 9 research questions we have formulated to investigate through our study.

Research question	Issues covered	Paper section
RQ1: How much is the research publication contribution in different languages?	What is the number of research publications in different languages including English?	Section 4
RQ2: Which type of documents are analyzed in the study?	How many papers are published in journals and conferences?	Section 4.1
RQ3: What is the annual scientific output in 5G Security?	▪ Quantity of research studies published in 5G Security. ▪ The yearly trend in 5G security research. ▪ The trend in annual scientific studies	Section 4.2
RQ4: What are the most active countries in 5G security research?	▪ What are the top 15 countries according to the publication frequency and also the h-index values and the average number of citations/item for each of the top 15 countries? ▪ Country-wise co-authorship analysis is done to show the collaboration between the countries.	Section 4.3.1
RQ5: What is the yearly contribution of different organizations?	▪ What are the top 15 organizations according to the publication frequency and also the h-index values and the average number of citations/item for each of the top 15 institutes?	Section 4.3.2
RQ6: Who are the most active authors in the field of 5G Security?	▪ Who are the top 15 active authors according to publication count? ▪ What is the impact of each author in terms of h-index and the average citations per publication?	Section 4.3.3
RQ7: What are the most highly cited research papers in the field of 5G security?	▪ Which research work has been most highly cited in the 5G security? ▪ It Helps identifies the notable contributions which have been recognized by fellow researchers.	Section 4.6
RQ8: How are the documents related in terms of keywords?	▪ Co-keyword analysis is used to demonstrate the relationship amongst studies based on the occurrence of keywords in research publications.	Section 4.7
RQ9: Which countries have strong collaborative research networks?	Country-wise co-authorship analysis is done to show the collaboration between the countries.	Section 4.8

Table 4: Research questions for the bibliometric study

4. Data Analysis

The bibliometric study involves various steps to appropriately record, assess, and interpret data. It enables investigators to present the outcomes of empirical studies based on co-word analysis, co-citation analysis, and bibliographic couplings. VOSviewer is a comprehensive software visualization tool for analyzing

bibliometric maps (Van Eck et al., 2010). To support our study, we used VOSviewer to perform co-word analysis and research collaboration network analysis with respect to countries. (Small, 1973; and Liu et al, 2018) previously performed co-citation analysis on the literature to show the relationship between documents. Further, we have used MS Excel for the graphical analysis of the results.

Time Frames	Top Languages	Research Titles
2014 - 2020	English	714
-	German	1

Table 5: Language used in literature

Table 5 shows the number of papers published in different languages. All but one paper is written in the English language which clearly shows that almost all the journals/conferences in which 5G security-related research is published are in the English language. Furthermore, Table 6 presents different scientific domains where 5G security research has been published.

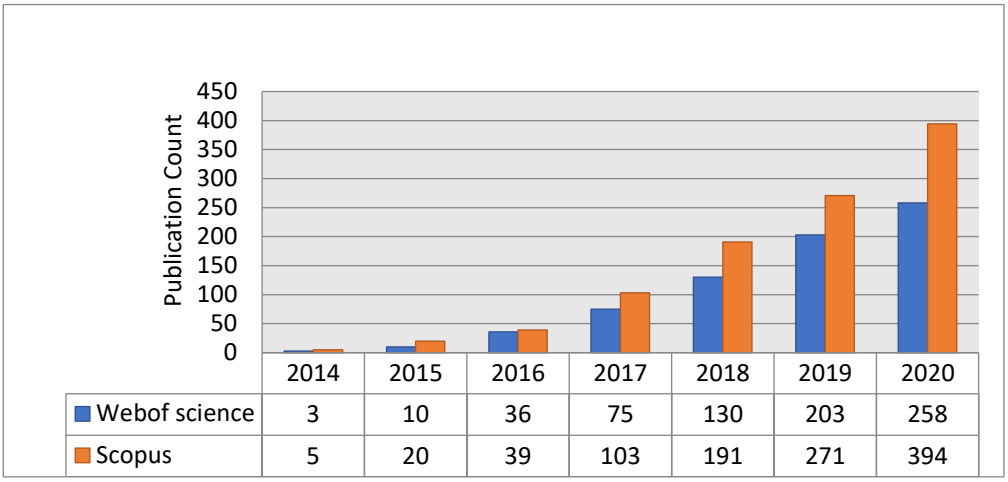
Multi-disciplinary Research Areas					
Computer Science	Engineering	Telecommunications	Chemistry	Instruments Instrumentation	Automation Control Systems
Transportation	Physics	Optics	Materials Science	Science Technology Other Topics	Energy Fuels
Operations Research Management Science	Robotics	Education Educational Research	Imaging Science Photographic Technology	Medical Informatics	Remote Sensing

Table 6: Multi-disciplinary research areas for 5G security research

4.1 Annual Scientific Production

In our paper, the ISI Web of Science database is used to extract the pool of published studies for the period (2014 – 2020) as per query 6 presented in Table 3. In this respect, year-wise publications presented in Fig 3 highlight the publication trend in the 5G security field within the aforementioned time frame. Annual scientific production presents a means to observe variation in scientific contributions over a specified time duration. The analysis represents the fact that the global publication trend in Security analysis concerning 5G and Edge computing touched its peak during the years 2018 – 2020. The frequency of scientific publications in 5G security depicts the intensity of research in this field in the last 7 years.

Annual scientific production presents a means to observe variation in scientific contributions over a specified time duration and enables investigators to identify trends among the research community. As evident from Fig 3, the global publication trend in security analysis with respect to 5G attracted the most attention during the years 2018 – 2020 with 2020 being the most productive year (258 publications). Therein, the frequency of scientific publications depicts the intensity of research within the 5G security domain in the last 7 years.

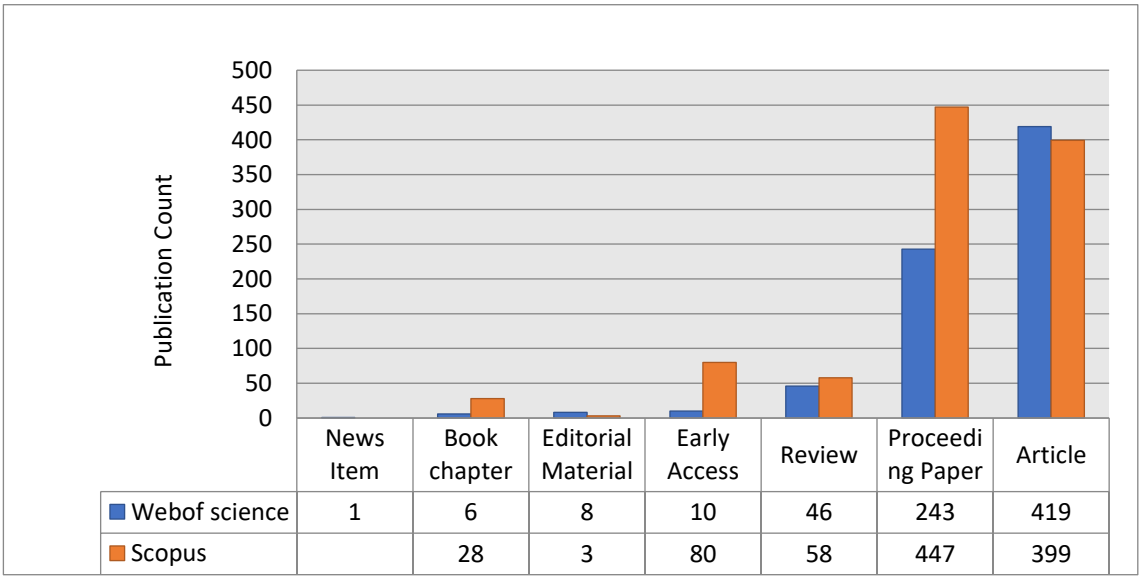


	2014	2015	2016	2017	2018	2019	2020
Webof science	3	10	36	75	130	203	258
Scopus	5	20	39	103	191	271	394

Figure 3: Yearly publications within 5G security

4.2 *Document Type*

Through our analysis, we identified that journal and conference papers represent the most significant types of documents. This analysis is presented in Fig 4 which shows that 419 articles were published in journals whereas just over 243 papers were presented in the conferences. Furthermore, there were 46 review papers, 11 Editorial materials, 6 book chapters, 3 early access, and 1 news item. This analysis confirms the trend among the research community to publish findings within conferences and journals. However, the analysis also shows the research community's preference to publish in good quality Journals compared to conferences as 55 percent of work is published in Journals and only 33 percent are presented in conferences. Among the 46 review materials, we could not find any bibliometric study on the selected topic which makes our work novel and is expected to help researchers perform good quality work.



	News Item	Book chapter	Editorial Material	Early Access	Review	Proceeding Paper	Article
Webof science	1	6	8	10	46	243	419
Scopus		28	3	80	58	447	399

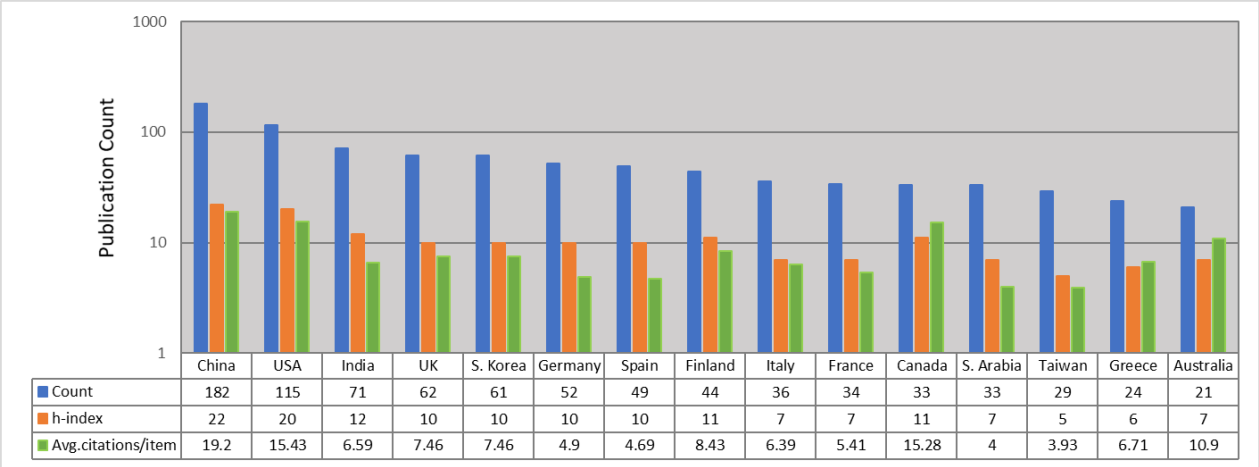
Figure 4: Document type within 5G security literature 2014-2020

4.3 Productivity

In terms of productivity analysis, we aim to highlight top scientific contributors within the 5G security domain. These contributors are classified as countries, organizations, and authors, and their respective analysis has been presented in the following sections.

4.3.1 Countries

Fig 5 shows the scientific contribution of the top 15 countries in 5G security research. It includes the research studies count, h-index, and average citations/item for each country. Our analysis revealed that China has the highest number of research publications, h-index as well as the average citations/item in the field of 5G security with 182, 22, and 19.2 respectively. The USA is the second country in terms of both the number of publications and h-index with 115 and 20. India with 71 publications and 12 h-index, the UK with 62 publications and 10 h-index, and South Korea with 61 publications and 10 h-index make the top 5 countries respectively.

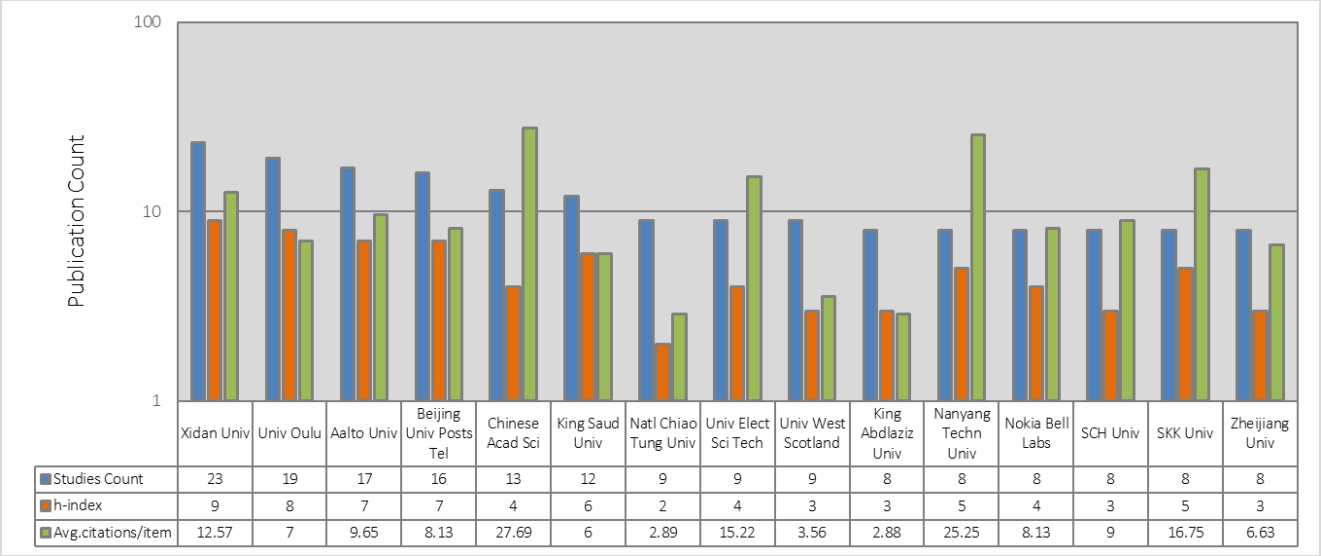


	China	USA	India	UK	S. Korea	Germany	Spain	Finland	Italy	France	Canada	S. Arabia	Taiwan	Greece	Australia
Count	182	115	71	62	61	52	49	44	36	34	33	33	29	24	21
h-index	22	20	12	10	10	10	10	11	7	7	11	7	5	6	7
Avg.citations/item	19.2	15.43	6.59	7.46	7.46	4.9	4.69	8.43	6.39	5.41	15.28	4	3.93	6.71	10.9

Figure 5: – Top 15 contributing countries

4.3.2 Organizations

Fig 6 present the top 15 contributing organizations towards 5G security research. These include the research studies count, h-index, and avg. citations/item for each organization. Xidian University from China has the highest number of research publications as well as the h-index in the field of 5G security while the University of Oulu Finland is in the second spot in terms of the number of publications and h-index. However, the Chinese Academy of Sciences has the highest average number of citations per research publication. Aalto Univ Finland, Beijing Univ Posts Telecom, and the Chinese Academy of Sciences make into the top 5 organizations in terms of scientific contribution.

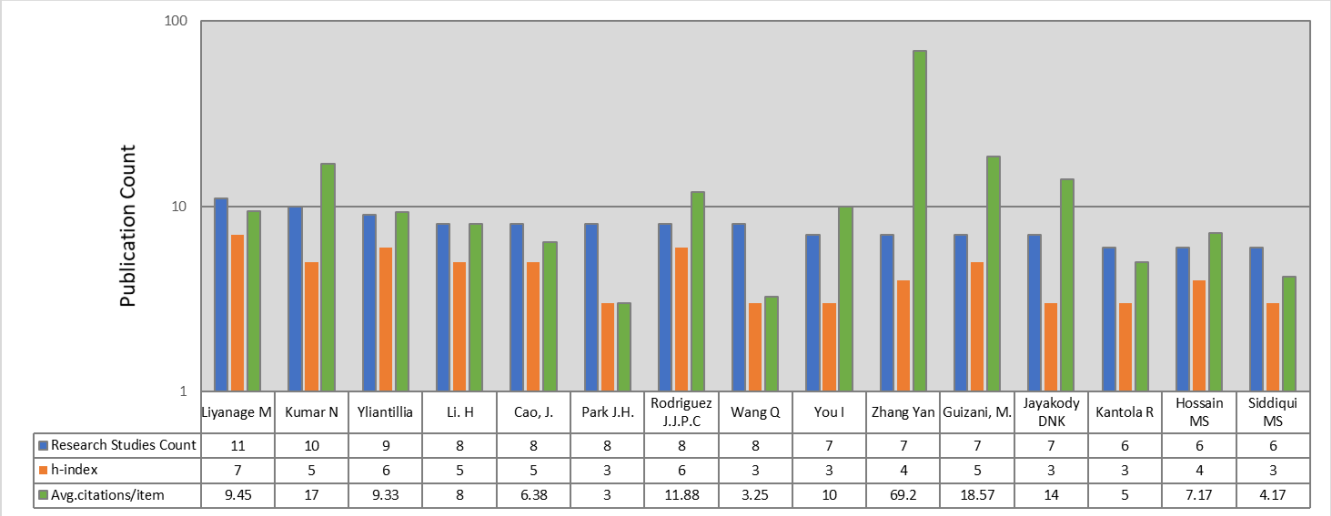


	Xidan Univ	Univ Oulu	Aalto Univ	Beijing Univ Posts Tel	Chinese Acad Sci	King Saud Univ	Natl Chiao Tung Univ	Univ Elect Sci Tech	Univ West Scotland	King Abdlaziz Univ	Nanyang Techn Univ	Nokia Bell Labs	SCH Univ	SKK Univ	Zhejiang Univ
Studies Count	23	19	17	16	13	12	9	9	9	8	8	8	8	8	8
h-index	9	8	7	7	4	6	2	4	3	3	5	4	3	5	3
Avg.citations/item	12.57	7	9.65	8.13	27.69	6	2.89	15.22	3.56	2.88	25.25	8.13	9	16.75	6.63

Figure 6: Top 15 contributing organizations to 5G security research

4.3.3 Authors

This section highlights the most active researchers in the field of 5G security with respect to the number of publications in this area. Therein, Fig 7 shows the 15 most published authors with the corresponding h-index and average citations per item. As is evident from this figure, Madhusanka Liyanage from University College Dublin has the most publications (11) followed by Kumar N. from Thapar Institute of Engineering and Technology, Patiala and Ylianttila, M. from the University of Oulu with 10 and 9 publications respectively. However, in terms of the influence of the research, Zhang Yan has the highest average citations per publication (69.2) which signifies that the authors publishing the most number of publications may not be top-cited as well.



	Liyanage M	Kumar N	Ylianttilia	Li. H	Cao, J.	Park J.H.	Rodriguez J.J.P.C	Wang Q	You I	Zhang Yan	Guizani, M.	Jayakody DNK	Kantola R	Hossain MS	Siddiqui MS
Research Studies Count	11	10	9	8	8	8	8	8	7	7	7	7	6	6	6
h-index	7	5	6	5	5	3	6	3	3	4	5	3	3	4	3
Avg.citations/item	9.45	17	9.33	8	6.38	3	11.88	3.25	10	69.2	18.57	14	5	7.17	4.17

Figure 7: – Top 15 contributing authors to 5G security research 2014-2020

4.4 Research Areas

5G has been adopted across diverse application domains and therefore it is expected that scientific literature with respect to 5G can span across multiple research areas. In this context, Fig 8 illustrates the result of our analysis identifying subject areas attributed to within current 5G security research. As expected, the subject area that received the most attention from researchers was Computer Science, which marked 474 publications in 5G security research. Additionally, Engineering and Telecommunication are the other two subject areas where publications have been mapped to. Specifically, these subject areas have been mapped by 425 and 404 publications respectively.

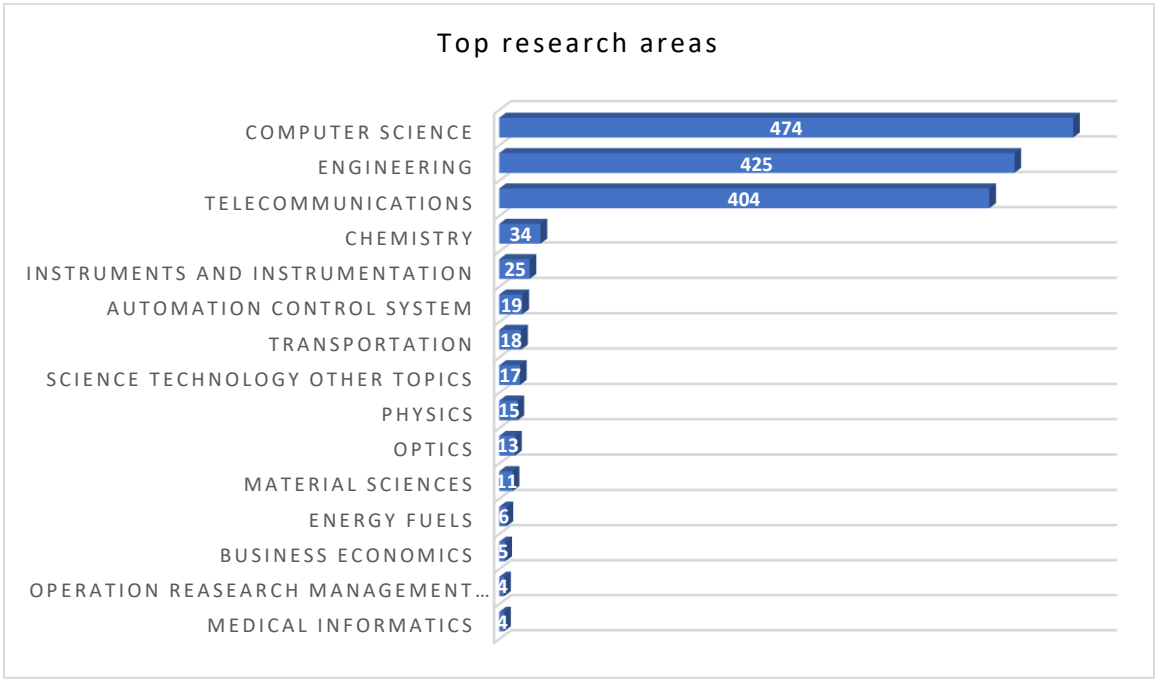


Figure 8: Top research areas within 5G security between 2014 – 2020

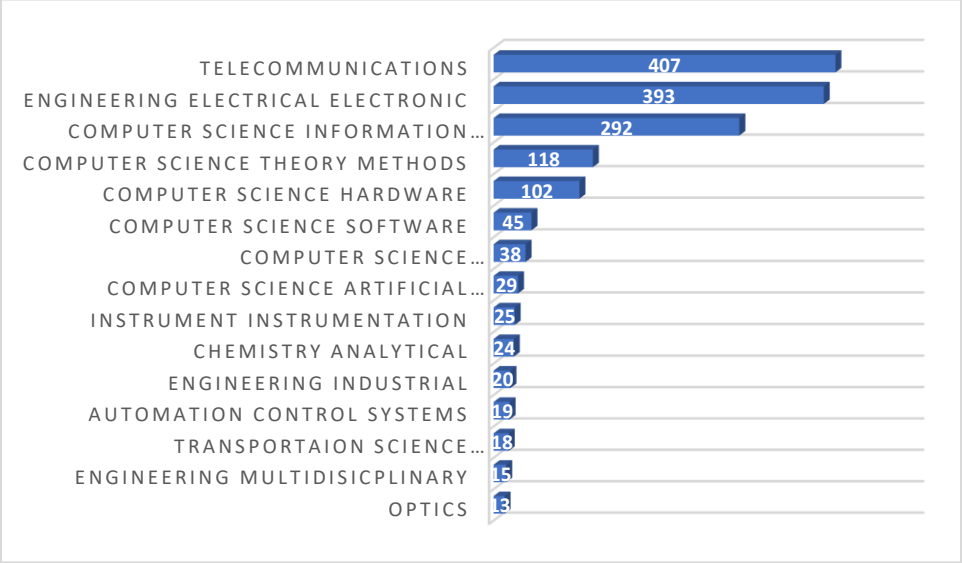


Figure 9: Top 10 WoS categories of research within 5G security

4.5 Web of Science Categories & Sources

Similar to section 4.4, Engineering, Telecommunication, and Computer Science dominate the WoS categories mapped against current 5G security literature. Fig 9 shows a detailed analysis of the relevant publications with respect to their mapping with WoS categories. Telecommunications is the most frequently used WoS category for 5G security literature with 407 publications followed by Engineering Electrical Electronic (393 publications) and Computer Science Information (292 publications).

To achieve further insight into the subject areas mapped with current 5G security research, we analyzed the venues publishing this research. Therein, Fig 10 shows the top 15 sources with respect to the number of publications related to 5G research. In this respect, IEEE Access represents the most popular publishing venue with 87 articles published with Sensors (24 publications) and IEEE Internet of Things Journal (23 publications) being the second and third most popular choices. We assume the popularity of IEEE Access is primarily due to its broad scope (general computer science), short publication time, and open access policy. These factors allow authors to publish their results within a short time whilst also ensuring broader readership due to the absence of a paywall. Furthermore, IEEE IoTJ and Sensors are focused on literature related to the Internet of Things and smartX systems which represent one of the most popular application domains of 5G and beyond.

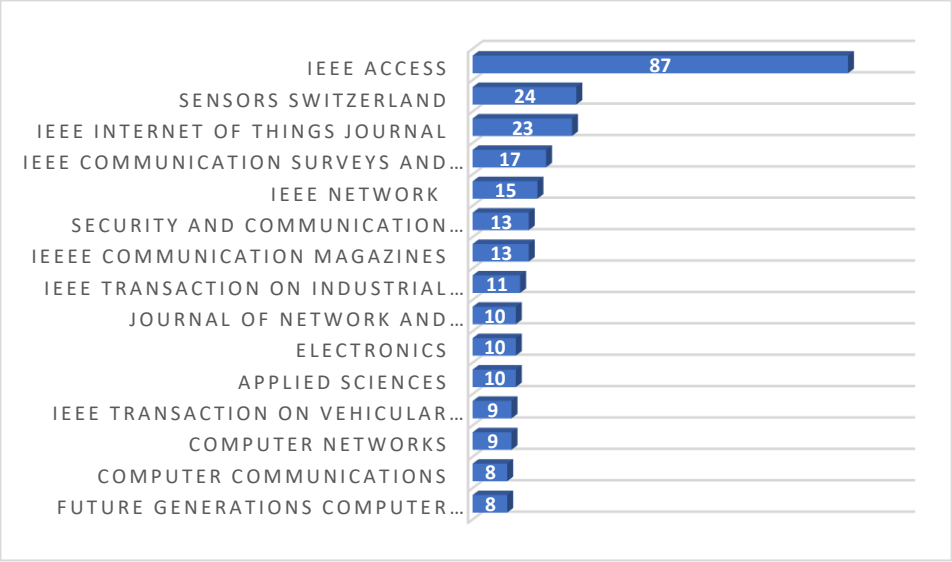


Figure 10: Top 15 source titles (publication venues) for 5G security research

4.6 Highly Cited research publications

Table 9 lists the top 15 highly cited research articles within 5G security between the years 2014 and 2020. Mao et al. (2017) titled “A survey on Mobile Edge Computing” and published in “IEEE Communications Surveys and Tutorial” is at the top with 900 citations. Abbas et al. (2017) having the title “Mobile Edge Computing: A survey” published in “IEEE Internet of Things Journal” was the second most highly cited paper with 456 citations. Akpakwu et al. (2017), li et al. (2018) and Yu et al. (2017) complete the top 5 with 322, 314, and 237 citations respectively.

Title	Authors	Citations	Journal	Year
A Survey on Mobile Edge Computing	Mao et al. 2017	900	IEEE Communication Surveys and Tutorial	2017
Mobile Edge Computing: A survey	Abbas et al. 2017	456	IEEE Internet of Things Journal	2017
A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges	Akpakwu et al. 2017	322	IEEE Access	2017
5G Internet of Things: A survey	Li et al. 2018	314	Journal of Industrial Information Integration	2018
A Survey on the Edge Computing for the Internet of Things	Yu et al., 2017	237	IEEE Access	2017
Authentication Handover and Privacy Protection in 5G HetNets Using Software-Defined Networking	Xiaoyu et al. 2015	116	IEEE Communication Magazine	2015
Application of Deep Reinforcement Learning in Communications and Networking: A survey	Nguyen et al. 2019	101	IEEE Communications Surveys and Tutorials	2019
Security Enhancement for IoT Communications Exposed to Eavesdroppers with Uncertain Locations	Xu et al. 2016	99	IEEE Access	2016
A comprehensive survey of Network Function Virtualization	Bo et al. 2018	96	Computer Networks	2018
Joint Optimization of Resource Utilization and Load Balancing with Privacy for Edge Services in 5G Networks	Xiaolong et al. 2020	89	Mobile Networks & Applications	2020
Blockchain for Internet of Things: A survey	Hong-Ning et al. 2019	85	IEEE Internet of Things Journal	2019
Cognitive Internet of Vehicles	Chen et al. 2018	83	Computer Communications	2018
Classifications and Applications of Physical Layer Security Techniques for Confidentiality: A Comprehensive Survey	Hamamreh et al. 2018	82	IEEE Communications Surveys and Tutorials	2018
Software defined Mobile Network Security	Chen et al. 2016	77	Mobile Networks and Applications	2016
Efficient and Secure Service-Oriented Authentication Supporting Network Slicing for 5G enabled IoT	Ni et al. 2018	70	IEEE Journal on Selected Areas in Communications	2018

Table 9: List of top 15 highly cited articles within 5G security research 2014 - 2020

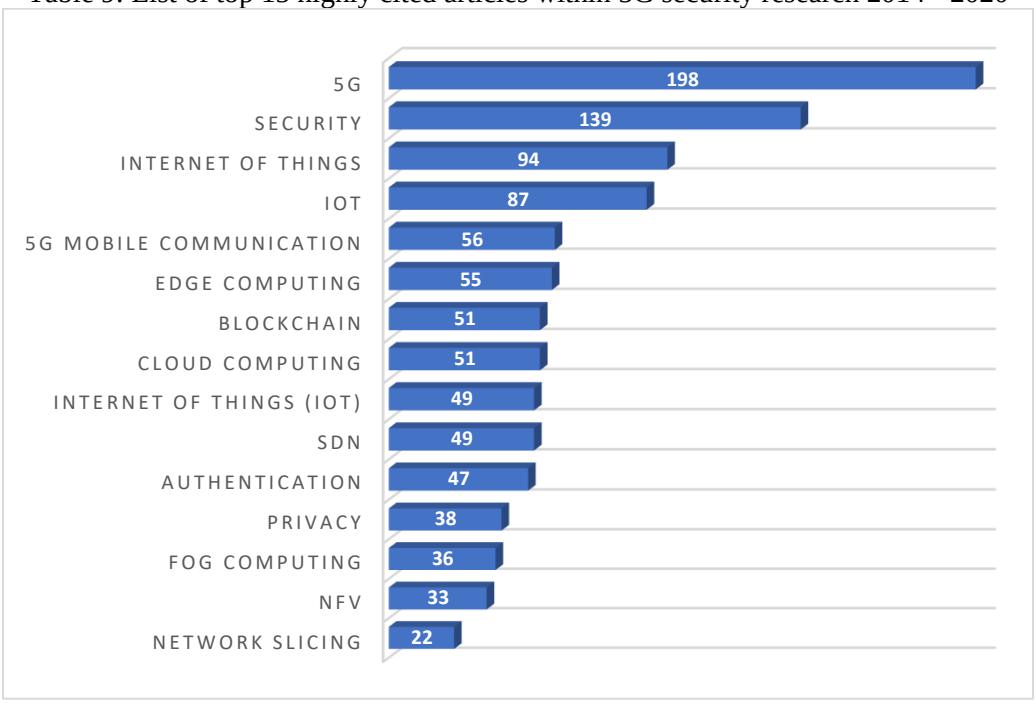


Figure 11: Top 15 keywords within 5G security research

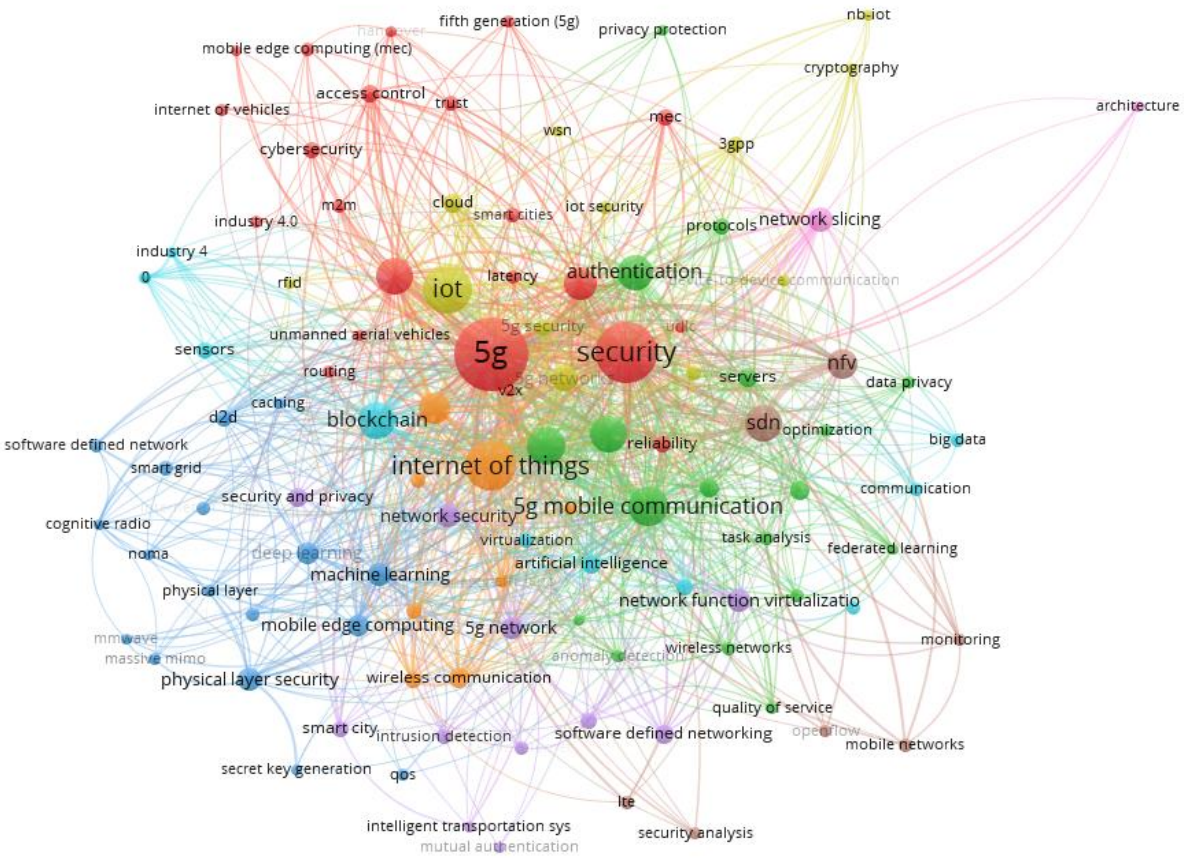


Figure 12: Keyword co-occurrences network

4.7 Keyword Analysis

The keywords of an article represent its primary research area, and the frequency of occurrences and co-occurrences can reflect themes focused on a specific field. This analysis can lead to the identification of sub-areas receiving the most attention from the research community and therefore the most significant challenges in the domain. In this section, we use keyword analysis and keyword co-occurrences to analyze the research trends within 5G security with the aim to highlights research gaps in the literature and identify potential future research directions. Fig 11 presents the top 15 keywords with the most occurrences in the field of 5G (198) followed by 5G Security (139). Analyzing this data with that of top publication venues in Fig 10 presents a strong correlation between 5G security and IoT as these represent the most frequently used keywords as well as the most frequently mapped subject areas in current literature. This highlights the focus of the research community on challenges introduced due to the application of 5G within IoT, especially concerning security.

In addition to the author keyword analysis, we also conducted a study of the co-occurrences among the 107 keywords using VOSviewer. (Ravikumar et al., 2015; Cambrosio et al, 1993; and Courtial 1994) presented co-word analysis in different fields of scientometrics. The outcome of our study and its analysis is presented in Fig 12 where the size of a node in the network shows the highest number of occurrences. For instance, 5G is represented as the largest node which confirms its use as the most frequent keyword. Also, the width of edges connecting nodes shows the frequency of keywords being used together in the research literature. In this context, It can be identified that *5G*, *Security*, and *Internet of things* have the highest frequency and 5G and security have the most co-occurrences in literature.

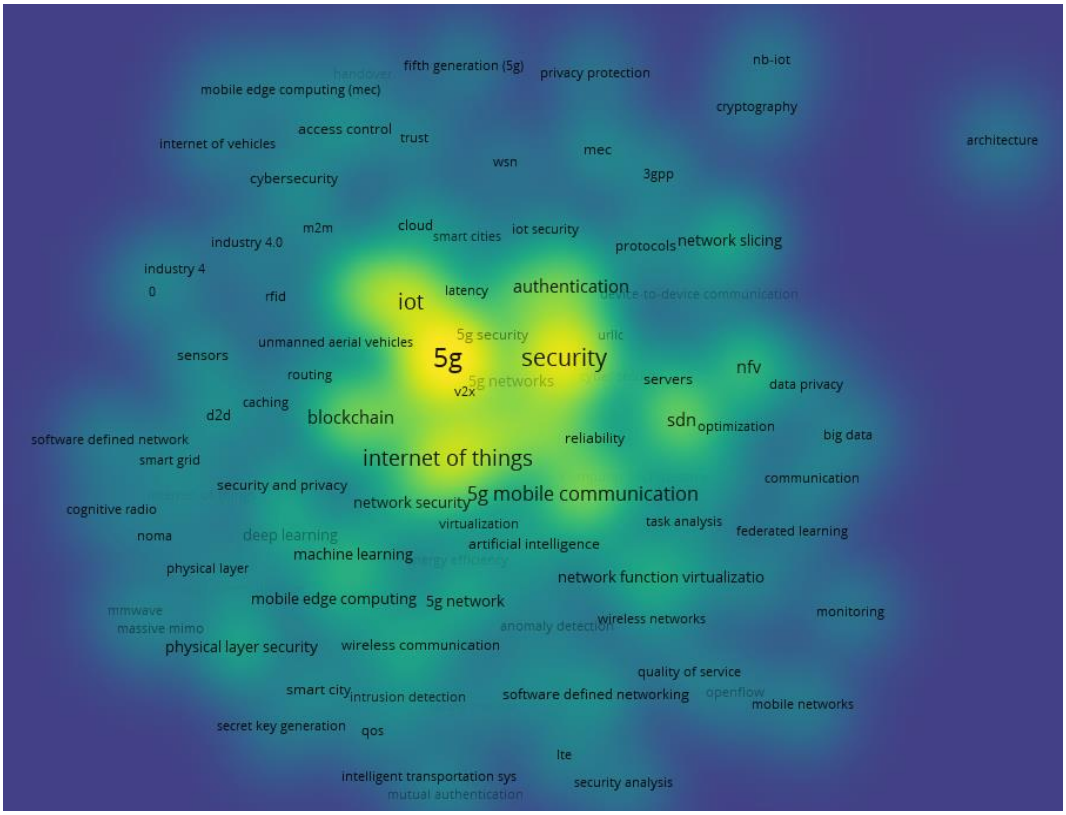


Figure 13: Keyword co-occurrence density

To enhance the analysis related to author keywords and their co-occurrences, we used a density visualization graph as presented in Fig 13. In the item density visualization, items are indicated by their label in a similar way as in the network visualization. Each point in a map has a color that depends on the density of items at that point. By default, this color is somewhere in between blue and green. Through this analysis, the same color nodes make a cluster which shows the research theme of that cluster as represented by their respective keywords. Further, the association between two nodes is dependent on two forces i.e. attractive, and repulsive. The higher the association between two nodes stronger the attractive force will be between two nodes. Nodes with high association strength are pulled together while nodes with a low association strength are pushed away from each other achieving distinct clustering among keywords. Moreover, the number of clusters depends on the resolution parameter (Van Eck et al., 2010) i.e. the larger the value of the resolution parameter, the larger the number of clusters that are obtained.

Cluster #	Color	# of Keywords	Cluster Keywords
1	Red	22	5G, Access control, Cybersecurity, Fifth Generation (5g), Handover, Industry 4.0, Internet of things (IoT), Internet of Vehicles, Latency, M2M, MEC, Mobile Edge Computing (MEC), Privacy, Reliability, Routing, Security, Smart cities, Software-defined networking (SDN), Trust, Unmanned Aerial Vehicles, uRLLC, v2x
2	Green	18	5G mobile communication, Anomaly detection, Authentication, Cloud Computing, Computer Architecture, Data models, Data Privacy, Edge Computing, Federated Learning, Industrial Internet of Things, Optimization, Privacy Protection, Protocols, Quality of Service, Resource Management, Servers, Task analysis, Wireless Networks
3	Blue	17	Caching, Cognitive Radio, D2D, D2D Communication, Deep learning, Internet of Things, Machine Learning, Massive MIMO, mmWave, Mobile Edge Computing, NOMA, Physical Layer, Physical Layer Security, QoS, Secret Key Generation, Smart Grid, Software Defined Network
4	Yellow	12	3GPP, 5G Networks, 5G Security, Cloud, Cryptography, Cyber Security, Device-to-device communication, IoT, IoT Security, NB-IoT, RFID, WSN
5	Purple	11	5G Network, Intelligent Transportation System, Intrusion detection, Mutual authentication, Network Function Virtualization, Network Security, Security and Privacy, Smarty city, Software Defined Networking, software-defined networking, tactile internet
6	Berylline	10	6G, Artificial Intelligence, Big data, Blockchain, communication, Industry 4.0, Sensors, Software Defined Networks, Virtualization
7	Orange	8	Communication system, Energy Efficiency, Fog Computing, Game Theory, Internet of Things, Trust Management, Wireless communication, Wireless Sensor Networks,
8	Brown	7	LTE, Mobile Networks, Monitoring, NFV, OpenFlow, SDN, Security Analysis
9	Pink	2	Architecture, Network Slicing

Table 10: Keyword clusters

Table 10 lists the 9 clusters in which VOSviewer divides the keywords because of their cooccurrences in the 5G security literature. Cluster 1 is the biggest with 22 keywords and is shown by red color in Figure 12. The second and Third clusters have 18 and 17 keywords respectively and are shown by green and blue colors in Figure 12. Cluster 1 keywords suggest that researchers have discussed both privacy and access control in 5G in the same research publications most of the time. Cluster 2 represents the work done in the field of authentication, anomaly detection, and quality of service in Cloudy computing and mobile edge computing. Cluster 3 shows the research work done related to device-to-device communication, massive MIMO, and mmWave mostly in the same research publications. An area where future research may be directed is the provision of new services using fog and edge computing, network functions virtualization, software-defined networks, and Network Slicing.

4.8 Country Collaboration Network

Collaborative research is fundamental to the progress made by research communities within diverse disciplines. Within individual outputs of research, collaboration at the international level is determined by having at least one author belonging to a different country (Jung, J., 2012; Sarwar, R., & Hassan, S. U., 2015). To conduct this analysis, we used VOSviewer to identify how the authors from different organizations and countries are collaborating within 5G security research. In VOSviewer, units of analysis are represented as nodes/ items and links represent that two items have worked together on at least one scientific study. Distance between two nodes determines the strength of the link and the relation between two items (Van Eck et al., 2013). The weight of a node/item is reflected by the size of the corresponding node/item i.e. higher weights are reflected by larger sizes of circles (Van Eck, et al., 2013). Furthermore, different color schemes represent clusters to which an item belongs. Therefore, countries that have frequently co-authored research publications belong to the same cluster.

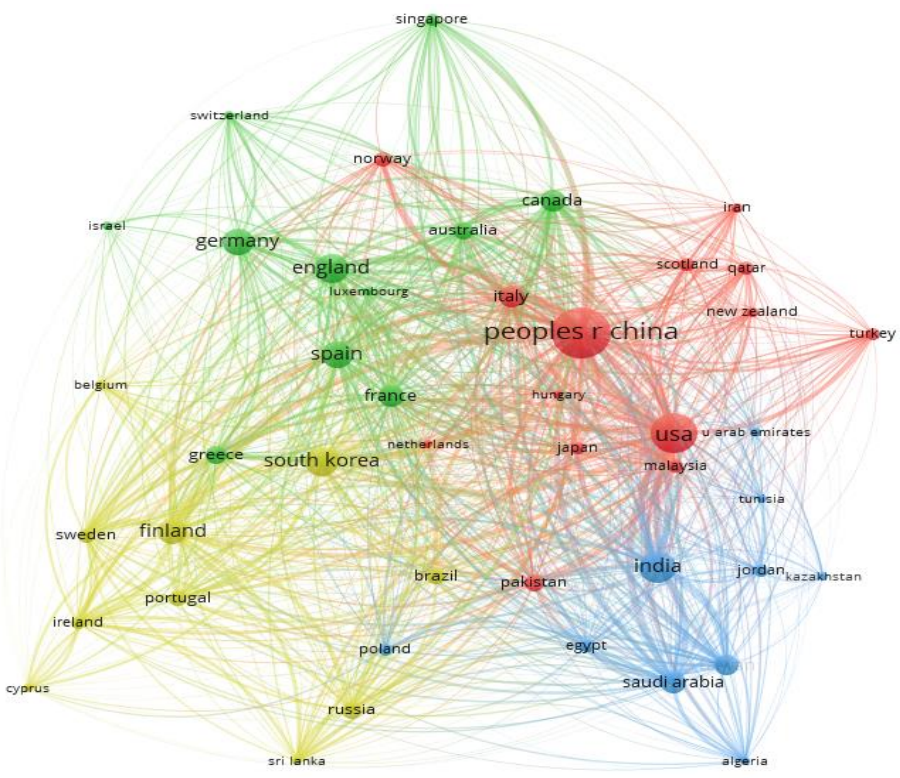


Figure 14: Most frequently collaborating countries within 5G security research

The country collaboration network presented in Fig 14 shows that China and the USA are the two countries with the highest collaboration. The top five collaborating country pairs are China-USA, China-South Korea, China-England, China-India, and England-Germany. Furthermore, the top 5 collaborating countries with the USA are China, South Korea, India, England, and Pakistan.

5. Open issues, research challenges, and directions

As highlighted earlier in this paper, 5G security is an area of great interest among the research community with several efforts being made to address specific challenges. In this section, we present the most significant open challenges within this domain along with their significance for 5G-based applications.

5.1 Privacy

Privacy is one of the most important security requirements in network communication. Numerous privacy-related threats and attacks have been identified in the literature which is possible in 5G networks which include man-in-the-middle, phishing, hijacking, and session replay. Several researchers (Khan et al. 2019; Ahmed et al. 2019; Sicari et al. 2020; Duan et al. 2015; and Ahmed et al. 2018) have identified open issues and suggested the need of defining a general architecture for privacy within 5G network which may include Privacy-by-Design. Location privacy also needs to be addressed in MEC-enabled applications such as IoT, healthcare, and autonomous vehicles. The use of AI/ML and Osmotic computing is suggested as a future research direction for MEC-based applications. Sticky policy implementation is also disused as a future research direction in which security and privacy policies are attached to owners' data and provide access control decisions and policy enforcement. The role of blockchain in the sticky policy-based mechanism may be another research direction in this regard.

5.2 Trust Management

In order to have secure communication within 5G networks, both device and network should be able to trust each other. Trust refers to the belief which an entity has about another entity. (Ahmed et al. 2019), (Sicari et al. 2020 and Ahmed et al., 2018) have identified trust management between the MEC nodes and 5G core as an open research direction worth exploring. (Ren et al. 2020) have proposed a blockchain-based trust establishment mechanism for the Internet of multimedia things.

5.3 Authentication and Key management

5G is envisioned to support several new use cases including autonomous vehicles, the Internet of Things, and AR/VR applications. Authenticating the connected devices, controlling access, and exchanging security credentials play a vital role in the security of the network. Distribution and protection of credentials and encryption keys is another challenge and several research directions have been identified in (Khan et al. 2019; Ahmed et al. 2019; and Ahmed et al. 2018). The use of Quantum cryptography is discussed as a future direction regarding Key Management and Secure Communication. ECC-based solutions are also suggested instead of RSA/AES-based SSL/TLS solutions for IoT devices with low processing and storage capabilities. (Behrad et al. 2019) proposed a scalable authentication and access control mechanism for 5G-based IoT. A lightweight authentication scheme for 5G based on the dynamic key approach was presented in (Pothumarti et al. 2021).

5.4 Secure Network Slicing

Network slicing enables end-to-end connectivity by creating multiple logical networks over shared physical resources/infrastructure. Slice-specific authentication, inter-slice communication isolation are some of the highlighted open issues within 5G Network Slicing. (Cao et al. 2019) and (Olimid and Nencioni 2020) identified several security challenges which include security protection between Network

Slice Management Function (NSMF) and the Communication Service Management Function (CSMF). The slice management interface should be protected so that only authorized parties may be able to create, delete or modify network slice instances. In the case of mutually exclusive access to two network slices, an access control mechanism is required. Slice-specific authentication and authorization also need the attention of researchers as it involves not only security challenges but also guaranteed QoS for a specific slice. (Behrad et al. 2019) have presented a slice-specific Authentication and Access control mechanism. Another open issue that is presented is the designing of group authentication and group security management because of mMTC. (Ksentini et al. 2020) have identified issues arising while extending network slicing to the edge and provided solutions for these issues. Providing secure slice mobility is also an open challenge suggested in the paper, which requires security protection mechanisms between AMF and 5GC. Open challenges in the network slice life cycle are also discussed in the literature. These include Slice-specific authentication, end-to-end security, proper isolation between network slices and network functions, traffic analysis, and anomaly detection. Research on the evaluation of overall trust and its technical mechanisms may be another area of interest.

6. Conclusion

5G is the 5th generation mobile network that promises to provide global connectivity and support ultra-high data speeds, ultra-low latency, high network capacity, and reliability. These inherent properties of the technology encourage the introduction of innovative use cases and application scenarios with the help of enabling technologies.

Security challenges in the 5G network and applications have attracted significant interest from both academia and industry. Although several systematic reviews and surveys exist on 5G security, this paper is the first bibliometric study in the field. In this paper, we have presented a comprehensive analysis of existing research within 5G security which includes the most significant work published in the field from 2014 to 2020. Based on data available from the ISI Web of Science and Scopus databases, the study analyzed 715 articles out of which 419 articles have been published in academic journals and 243 articles have been published in conferences proceedings.

Our study shows that China leads the world in terms of published research in the field of 5G security with 182 publications in the specified period while the USA and India ranked second and third with 115 and 71 publications respectively. Aligned with this trend, the Xidian University, China is the highest-ranked organization in terms of the number of publications with 23 articles, while University Oulu and Aalto University Finland are at second and third with 19 and 17 publications respectively. Beijing University and the Chinese Academy of Sciences complete the top 5 organization list.

Among the most active authors, Liyanage M. from University College Dublin has published 11 articles and is followed by Kumar N. from Thapar Institute of Engineering and Technology, Patiala and Ylianttila, M. from the University of Oulu with 10 and 9 publications respectively. It is also identified that Zhang Yan has the highest average citations per publication which imply that the authors with the highest number of publications may not always have the most read and cited articles.

IEEE Access, Sensors, and IEEE Internet of Things Journal are the top 3 sources where authors have preferred to publish the research work in the field of 5G security with 87, 24, and 23 publications respectively. Computer Science, Engineering, and Telecommunications are the top three research areas in the field of 5G security.

We performed keyword and co-occurrence analysis to identify the most significant areas in which 5G security research has been carried out. This analysis indicates that Internet of Things, Blockchain, Data Privacy, Authentication, and Network Slicing have attracted the most attention from researchers.

VOSviewer visualizations have identified nine keyword clusters that suggest how different technologies and subfields are interrelated. Using analysis for productivity, research areas, and keywords, this paper has identified research trends in 5G security among the scientific community as well as highlighting specific challenges which require further efforts. These trends include privacy, trust management, authentication, key management, and network slicing.

7. Data availability statement

The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request

References

Abbas, N., Zhang, Y., Taherkordi, A. and Skeie, T., 2017. Mobile edge computing: A survey. IEEE Internet of Things Journal, 5(1), pp.450-465.

Ab Razak, M.F., Anuar, N.B., Salleh, R. and Firdaus, A., 2016. The rise of "malware": Bibliometric analysis of malware study. Journal of Network and Computer Applications, 75, pp.58-76.

Agiwal, M., Roy, A. and Saxena, N., 2016. Next generation 5G wireless networks: A comprehensive survey. IEEE Communications Surveys & Tutorials, 18(3), pp.1617-1655.

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M. and Gurtov, A., 2018. Overview of 5G security challenges and solutions. IEEE Communications Standards Magazine, 2(1), pp.36-43.

Ahmad, I., Shahabuddin, S., Kumar, T., Okwuibe, J., Gurtov, A. and Ylianttila, M., 2019. Security for 5G and beyond. IEEE Communications Surveys & Tutorials, 21(4), pp.3682-3722.

Akpakwu, G.A., Silva, B.J., Hancke, G.P. and Abu-Mahfouz, A.M., 2017. A survey on 5G networks for the Internet of Things: Communication technologies and challenges. IEEE access, 6, pp.3619-3647.

Behrad, S., Bertin, E., & Crespi, N. (2019). A survey on authentication and access control for mobile networks: from 4G to 5G. *Annals of Telecommunications*, *74*(9), 593-603.

Behrad, S., Bertin, E., Tuffin, S., & Crespi, N. (2019, June). 5G-SSAAC: Slice-specific Authentication and Access Control in 5G. In *2019 IEEE Conference on Network Softwarization (NetSoft)* (pp. 281-285). IEEE.

Cambrosio, A., Limoges, C., Courtial, J., & Laville, F. (1993). Historical scientometrics? Mapping over 70 years of biological safety research with coword analysis. Scientometrics, 27(2), 119-143.

Cao, J., Ma, M., Li, H., Ma, R., Sun, Y., Yu, P. and Xiong, L., 2019. A survey on security aspects for 3GPP 5G networks. IEEE communications surveys & tutorials, 22(1), pp.170-195.

Chen, M., Tian, Y., Fortino, G., Zhang, J. and Humar, I., 2018. Cognitive internet of vehicles. Computer Communications, 120, pp.58-70.

Chen, M., Qian, Y., Mao, S., Tang, W. and Yang, X., 2016. Software-defined mobile networks security. Mobile Networks and Applications, 21(5), pp.729-743.

Courtial, J. (1994). A coword analysis of scientometrics. Scientometrics, 31(3), 251-260.

De Ree, M., Mantas, G., Radwan, A., Mumtaz, S., Rodriguez, J. and Otung, I.E., 2019. Key management for beyond 5G mobile small cells: A survey. IEEE Access, 7, pp.59200-59236.

Ding, Y. (2011). Scientific collaboration and endorsement: Network analysis of coauthorship and citation networks. Journal of informetrics, 5(1), 187-203.

Duan, X. and Wang, X., 2015. Authentication handover and privacy protection in 5G hetnets using software-defined networking. IEEE Communications Magazine, 53(4), pp.28-35.

Ellegaard, O., & Wallin, J. A. (2015). The bibliometric analysis of scholarly production: How great is the impact? Scientometrics, 105(3), 1809-1831.

Fang, D., Qian, Y. and Hu, R.Q., 2017. Security for 5G mobile wireless networks. IEEE Access, 6, pp.4850-4874.

Gartner, 2020. Newsroom press release (2020) Available at https://www.gartner.com/en/newsroom/press-releases/gartner-says-worldwide-5g-network-infrastructure-spending-to-almost-double-in-2020 (Accessed 22 December 2020)

Garousi, V. and Mäntylä, M.V., 2016. A systematic literature review of literature reviews in software testing. Information and Software Technology, 80, pp.195-216.

Gupta (2020) Market share Mobile phone worldwide Available at https://www.gartner.com/en/documents/3991988 (Accessed 24 December 2020)

Gupta, A., Jha, R.K., Gandotra, P. and Jain, S., 2017. Bandwidth spoofing and intrusion detection system for multistage 5G wireless communication network. IEEE Transactions on Vehicular Technology, 67(1), pp.618-632.

Hamamreh, J.M., Furqan, H.M. and Arslan, H., 2018. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey. IEEE Communications Surveys & Tutorials, 21(2), pp.1773-1828.

Khan, R., Kumar, P., Jayakody, D.N.K. and Liyanage, M., 2019. A Survey on Security and Privacy of 5G Technologies: Potential Solutions, Recent Advancements, and Future Directions. IEEE Communications Surveys & Tutorials, 22(1), pp.196-248.

Ksentini, A. and Frangoudis, P.A., 2020. Toward Slicing-Enabled Multi-Access Edge Computing in 5G. IEEE Network, 34(2), pp.99-105.

Liu, S., & Chen, C. (2012). The proximity of co-citation. Scientometrics, 91(2), 495-511.

Li, S., Da Xu, L. and Zhao, S., 2018. 5G Internet of Things: A survey. Journal of Industrial Information Integration, 10, pp.1-9.

Liang, G., Weller, S.R., Zhao, J., Luo, F. and Dong, Z.Y., 2016. The 2015 ukraine blackout: Implications for false data injection attacks. IEEE Transactions on Power Systems, 32(4), pp.3317-3318.

Mao, Y., You, C., Zhang, J., Huang, K. and Letaief, K.B., 2017. A survey on mobile edge computing: The communication perspective. IEEE Communications Surveys & Tutorials, 19(4), pp.2322-2358.

Ni, J., Lin, X. and Shen, X.S., 2018. Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT. IEEE Journal on Selected Areas in Communications, 36(3), pp.644-657.

Olimid, R.F. and Nencioni, G., 2020. 5G network slicing: a security overview. IEEE Access, 8, pp.99999-100009.

Panwar, N., Sharma, S. and Singh, A.K., 2016. A survey on 5G: The next generation of mobile communication. Physical Communication, 18, pp.64-84.

Pothumarti, R., Jain, K. and Krishnan, P., 2021. A lightweight authentication scheme for 5G mobile communications: a dynamic key approach. Journal of Ambient Intelligence and Humanized Computing, pp.1-19.

Qualcomm (2020) The 5G Economy, Available at https://www.qualcomm.com/5g/the-5g-economy (Accessed 22 December 2020)

Rasheed, I., Zhang, L. and Hu, F., 2020. A privacy preserving scheme for vehicle-to-everything communications using 5G mobile edge computing. Computer Networks, 176, p.107283.

Ravikumar, S., Agrahari, A., & Singh, S. N. (2015). Mapping the intellectual structure of scientometrics: A co-word analysis of the journal Scientometrics (2005–2010). Scientometrics, 102(1), 929-955.

Ren, Y., Zhu, F., Zhu, K., Sharma, P.K. and Wang, J., 2020. Blockchain-based trust establishment mechanism in the internet of multimedia things. Multimedia Tools and Applications, pp.1-24.

Sánchez, J.D.V., Urquiza-Aguiar, L., Paredes, M.C.P. and Osorio, D.P.M., 2020. Survey on physical layer security for 5G wireless networks. Annals of Telecommunications, pp.1-20.

Sicari, S., Rizzardi, A. and Coen-Porisini, A., 2020. 5G in the Internet of Things era: an overview on security and privacy challenges. Computer Networks, p.107345.

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

Van Eck, N., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. scientometrics, 84(2), 523-538.

Van Eck, N. J., & Waltman, L. (2013). VOSviewer manual. Leiden: Univeristeit Leiden, 1(1), 1-53.

Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K.K. and Gao, X., 2018. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. IEEE Journal on Selected Areas in Communications, 36(4), pp.679-695.

Xu, Q., Ren, P., Song, H. and Du, Q., 2016. Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. IEEE Access, 4, pp.2840-2853.

Yi, B., Wang, X., Li, K. and Huang, M., 2018. A comprehensive survey of network function virtualization. Computer Networks, 133, pp.212-262.

Yu, W., Liang, F., He, X., Hatcher, W.G., Lu, C., Lin, J., and Yang, X., 2017. A survey on edge computing for the Internet of Things. IEEE Access, 6, pp.6900-6919.

Zhang, S., Wang, Y. and Zhou, W., 2019. Towards secure 5G networks: A Survey. Computer Networks, 162, p.106871.

Zhang, J., Zhong, H., Cui, J., Tian, M., Xu, Y., and Liu, L., 2020. Edge computing-based privacy-preserving authentication framework and protocol for 5G-enabled vehicular networks. IEEE Transactions on Vehicular Technology, 69(7), pp.7940-7954.