ISSN 2007-9737

Impact of 5G Technology on Cybersecurity: A Comprehensive Systematic and Bibliometric Review

Javier Gamboa-Cruzado[1,*], Luis Cuya-Chuica[2], Jefferson López-Goycochea[3], Angel Nuñez-Meza[4], Carlos Del-Valle-Jurado[5]

[1] Universidad Nacional Mayor de San Marcos,
Facultad de Ingeniería de Sistemas e Informática,
Peru

[2] Universidad Nacional Federico Villareal,
Facultad de Ingeniería Industrial y de Sistemas,
Peru

[3] Universidad de San Martín de Porres,
Facultad de Ingeniería y Arquitectura,
Peru

[4] Universidad Nacional Daniel Alcides Carrión,
Facultad de Ingeniería de Sistemas,
Peru

[5] Universidad Nacional Mayor de San Marcos,
Facultad de Ingeniería Geológica, Minera, Metalúrgica y Geográfica,
Peru

jgamboa65@hotmail.com, 2018006116@unfv.edu.pe, jlopezg@usmp.pe,
anunezm@undac.edu.pe, cdelvallej@unmsm.edu.pe

Abstract. The integration of 5G technology is progressively becoming standardized in everyday life, presenting notable benefits. However, it also remains largely uncharted territory, whether due to the diversity of applicable areas or its innovative nature. As such, there is a growing interest in delving into its various fields of application. In this context, the aim of the present research is to discern the state of the art of 5G technology and its impact on cybersecurity. To achieve this goal, a systematic review of studies published between 2016 and 2022 was conducted. The search strategy employed yielded a total of 13,235 papers from recognized sources such as Scopus, Web of Science, ARDI, ACM Digital Library, IEEE Xplore, and EBSCOhost. From this set, 68 papers were identified as relevant studies, after applying the established filters and exclusion criteria. Among the derived findings, there is a notable concentration of bibliometric flow by countries, the various areas of application, and the co-occurrence of organizations that previously researched this topic. The main implication of this research lies in identifying a tangible need to increase and improve studies regarding the application of 5G technology and its impact on cybersecurity.

Keywords. Technology, 5G, cybersecurity, systematic review, bibliometric review.

1 Introduction

At this stage of technological progress, as 5G technology has become an integral part of our daily lives, its application is evident in various areas such as: communication between devices on the mobile network [81], data transmission [82], and network slicing [83].

This fifth generation, by offering a broader array of services compared to its predecessors, allows for a wider application in areas like the interconnection of open systems [84]. However, concerns arise regarding security and privacy [85], given the emerging vulnerabilities.

Despite these advancements, a comprehensive understanding of the state of the art concerning this technology's impact on cybersecurity is still lacking, which, if explored, could pave the way for future developments in this domain. Recent studies indicate that the 5G generation is designed to offer faster speeds, lower latency, and a more robust connection compared to previous communication technologies.

However, a heightened security threat is anticipated due to the wide range of vectors through which adversaries can launch attacks. Consequently, cybersecurity becomes crucial, as it is associated with the protection of confidential data and user personal information [78], key elements to counteract such threats.

On the other hand, the impacts of 5G technology on cybersecurity [76] are promising, considering that any traditional system involves restricting cyber access to confidential data and components, which is expected to benefit the user. It is suggested to conduct a holistic assessment to understand the attack surface of a 5G-based system, with the aim of comprehending the potential cyber risk for such infrastructure and developing appropriate mechanisms for protection against these threats [73].

Furthermore, it is necessary to delve into the different definitions addressed in the review and conduct a classification of the various forms of existing information [75], to gain a clearer and structured understanding of the cybersecurity landscape in the 5G environment. It is evident that 5G technology applications can enhance cybersecurity and provide an overall better service; however, there is not yet specific research that analyzes the impact of this technology on cybersecurity.

This paper aims to determine the state of the art of 5G technology and its impact on cybersecurity. The structure of the document is organized as follows: Section II presents the theoretical framework; Section III describes the review method used; Section IV highlights the results and derived discussions; and finally, Section V provides the conclusions and suggests directions for future research in this field.

2 Background and Related Work

2.1 Research Problems and Objectives

To adequately understand 5G technology, which is already widely used today, it's essential to review some fundamental concepts.

2.1.1 First Generation (1G)

Mobile systems have evolved significantly since the emergence of the first generation in the 1980s. Back then, there were no robust security mechanisms [36].

2.1.2 Second Generation (2G)

The second generation of mobile phone services, known as 2G, was introduced in 1991, succeeding 1G. Mobile devices equipped with this technology offered voice and messaging services. However, 2G posed a series of security challenges. Within the realm of 2G networks, cyber attackers often used spam tactics as a means to distribute unsolicited information to users. This strategy facilitated the spread of malicious code among mobile device users. Attackers were using malicious code for harmful purposes [53].

2.1.3 Third Generation (3G)

The security system in 3G considered all the vulnerabilities detected in 2G and proceeded to rectify them. The security architecture implemented in 3G communications was articulated into five components: network access security, network domain security, user domain security, application security, and visibility and configurability security. Some of these vulnerabilities were related to unauthorized acquisition of users' confidential information, illicit interventions, and identity spoofing attacks [84].

2.1.4 Fourth Generation (4G)

The 4G security architecture was developed based on experiences and lessons drawn from the 2G and 3G networks. 4G introduced a revamped set of cryptographic algorithms and a significantly

different key structure compared to 2G and 3G. However, 4G also inherited certain security problems present in these earlier networks. With the adoption of 4G technology, mobile operators had the capability to offer novel services, including those at high speeds. It is important to note that cybercriminals demonstrated an organization and adaptability that surpassed expectations [85].

2.1.5 Fifth Generation (5G)

Currently, a vast amount of information is in multimedia formats, such as images and videos. Given the increasing demand for this data, multimedia exchange has positioned itself as one of the most sought-after Internet services. Concurrently, the emergence of fifth generation (5G) networks brings numerous benefits in terms of providing these multimedia sharing services.

It is imperative to note that, given the relevance of image exchange in the multimedia context [47], the 5G network demands the implementation of security mechanisms adapted to the new applications, network architectures, and air interface technologies [77].

2.1.6 Future of the Network (6G)

The 6G promises to incorporate various components, such as edge computing, cloud computing, and artificial intelligence. Among these elements, the communications infrastructure expects to have the largest market share, reaching figures of up to one billion US dollars [29].

2.2 Cybersecurity

Cybersecurity is recognized as an essential element in the implementation of 5G technology within the European Union (EU). It is projected that 5G networks will play a leading role in the Digital Single Market (DSM), significantly influencing areas such as energy, transportation, and health services.

Furthermore, with the emergence of 5G, we are heading towards an even more interconnected world. In this context, vulnerabilities detected in the 5G systems of a member state could impact the entire EU. Consequently, it is essential to promote collaboration and cooperation among nations to ensure a safe and coordinated implementation of 5G [50].

3 Review Method

To conduct the systematic review on the impact of 5G technology on cybersecurity, the principle proposed by Petersen [69] and Rimaki [70] was followed.

They suggest the formulation of research questions, the search in relevant sources to extract data, and answering these questions considering the identified limitations and conclusions.

For more details, refer to Figure 1. A keyword map was also used as suggested by Kitchenham [71], with the aim of showing the most predominant research trends and detecting the topics present within the analyzed field.

A word map facilitates visualization and a better understanding of the actual meaning of each concept developed on the topic, as explained by Linnenluecke [72].

3.1 Research Problems and Objectives

A general research question (RQG) is formulated, and additionally, several specific research questions (RQ) are proposed along with their respective objectives, as shown in Table 1 below.

3.2 Information Sources and Search Strategies

The sources selected for this systematic review include IEEE Xplore, ARDI, Web of Science, EBSCOhost, Scopus, and ACM Digital Library. To conduct the information search related to both dependent and independent variables, synonyms were sought, considering how authors refer to them in their papers, as shown in Table 2.

To track research papers based on search descriptors, equations were initially used in the selected sources. Boolean logic was also applied, tailoring it to the specifics of each source, as shown in Table 3.

3.3 Identified Studies

In this section, the number of results obtained per source for the research is presented, as shown in Figure 2.

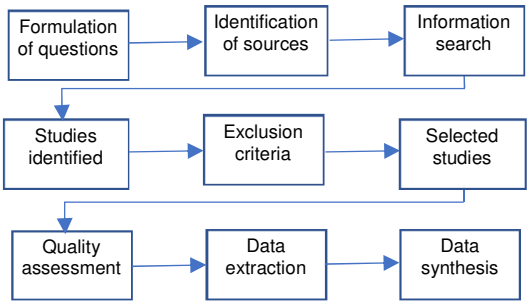

Fig. 1. RSL process

3.4 Exclusion Criteria

After obtaining the papers, the next step is to select them for evaluation to determine if they are suitable for the research. For this purpose, four filters with eight exclusion criteria (EC) were used, detailed as follows:

EC1: The papers are more than 7 years old.

EC2: The papers are not written in English.

EC3: The papers have not been published in conferences or journals.

EC4: The papers are systematic reviews.

EC5: The titles and keywords of the papers are not descriptive or relevant.

EC6: Full text of the papers is not available.

EC7: The papers are not unique.

EC8: The paper is less than 10 pages long.

3.5 Study Selection

Next, the selection of studies is presented using the PRISMA diagram, as shown in Figure 3.

3.6 Quality Assessment

At this stage, the quality of the 68 selected papers was assessed after applying the exclusion criteria. To ensure the quality of the papers, 7 quality criteria (QA) were established for their evaluation, which are as follows:

QA1: Does the paper consider fundamental research?

QA2: Does the paper reference the instruments used for data collection?

QA3: Does the paper provide access to the full text of the research?

QA4: Does the paper present a clear and precise delimitation of the specific area it addresses in its research?

QA5: Does the paper provide a comprehensive explanation of the context in which the research was conducted?

QA6: Does the researcher have relevant academic training in the field of study of 5G Technology and Cybersecurity?

QA7: Does the researcher provide contact information or institutional affiliation for future inquiries?

The assessment of the QA questions is conducted using a rating scale that ranges from 1 to 3 (1- Not good, 2- Good, and 3- Very good). The minimum value for inclusion is 12 (60% of the maximum). 68 papers were chosen as they scored ≥ 12. Table 4 displays the results of the quality assessment.

3.7 Data Extraction Strategies

Now, the process began to extract the most relevant papers with the aim to precisely address the established research questions. The extracted information included: Reference number, paper title, URL, source, year, countries, ISSN, type of publication, name of the publication, authors, affiliations, quartile, H-Index, research methodology, number of citations, abstract, keywords, discussion, and conclusion. To categorize the papers, Mendeley Desktop tool was utilized, as shown in Figure 4.

3.8 Synthesis of Findings

The information extracted for the research questions (RQ) was tabulated and presented as quantitative data, which was used to conduct a statistical comparison between the different findings corresponding to each research question.

These data obtained facilitated the identification of certain research patterns that have manifested over the past seven years.

4 Results and Discussion

In this section, key findings derived from the systematic review of the analyzed papers are presented and discussed. We examine the most prominent application areas, the quality levels of the sources, the co-authorship networks of the most influential researchers, the geographical distribution of the research, and the clusters of papers with similarity in titles.

This section provides a comprehensive view of the results obtained, contributing to a deeper understanding of this field of study and its evolution in recent years.

4.1 General Description of the Studies

The general findings obtained in this review are presented below. Figure 5 illustrates the percentage of papers according to the types of publication. In this study, 68 papers were selected, setting the criteria to only include papers from journals and conferences. Figure 5 reveals that 97.1% are from journals, while only 2.9% are from conferences, out of the total types of papers considered.

In the research conducted by Farooqui, Arshad, and Khan [73], both types of papers—conferences and journals—were also considered, aligning with the criteria used in this paper. On the other hand, Raveendran and Tabet [74] also used 68 papers in their review.

Authors Lozano and Mateo [75] state that in their paper, they employed 62.42% from conferences, 30.96% from journals, and included books, which constituted 6.62% of the participation, thus differentiating their review in terms of the exclusion criteria of the type of paper used in the current research.

It is noted that, over the years, the authors of the reviews are considering approximately 70 papers for their research, in addition to prioritizing papers from journals and conferences in their exclusion criteria.

In the future, authors might consider papers from journals and conferences as primary information, given the preference for these types of publications in this research field, as reflected in the various reviews considered. Table 5 displays the number of papers by continent and year.

Table 1. Research questions and objectives

Research Question	Objectives
RQG: What is the state of the art in research regarding 5G Technology and its impact on Cybersecurity?	Determine the state of the art in research regarding 5G Technology and its impact on Cybersecurity.
RQ1: In which industrial sectors or fields of study is 5G Technology having a significant impact?	Determine the industrial sectors or fields of study where 5G Technology is influential.
RQ2: How are the publications on 5G Technology and its impact on Cybersecurity distributed among the different journal quartiles?	Identify the distribution of publications on 5G Technology and its impact on Cybersecurity among different journal quartiles.
RQ3: Who are the most prolific or influential authors in the field of 5G Technology and its impact on Cybersecurity, and what are their co-authorship networks?	Determine authors who frequently co-author papers on 5G Technology and its impact on Cybersecurity.
RQ4: Which countries lead in producing research on 5G Technology and its impact on Cybersecurity, and how are the bibliometric flows distributed among these countries?	Identify countries that often feature bibliometric flows in research on 5G Technology and its impact on Cybersecurity.
RQ5: How can papers be grouped based on the thematic similarity of their titles in the field of 5G Technology and its impact on Cybersecurity, and which topics dominate each cluster?	Identify clusters of papers whose titles show similarity in research about 5G Technology and its impact on Cybersecurity.

Table 2. Search descriptors and their synonyms

Descriptor	Description
5g technology/ 5g/ 5g network/ 5g mobile telephony/ fifth generation	Independent Variable
cybersecurity / online safety / security/cyber	Dependent Variable

Table 3. Information sources and search equation

Source	Search equation
Scopus	TITLE-ABS-KEY (("5g technology" OR 5g OR "5g network" OR "5g mobile telephony" OR "fifth generation") AND (cybersecurity OR "online safety" OR security OR cyber))
Web of Science	("5g technology" OR 5g OR "5g network" OR "5g mobile telephony" OR "fifth generation") AND (cybersecurity OR "online safety" OR security OR cyber) (Title) OR ("5g technology" OR 5g OR "5g network" OR "5g mobile telephony" OR "fifth generation") AND (cybersecurity OR "online safety" OR security OR cyber) (Abstract)
IEEE Xplore	(("Document Title":5g OR "Document Title":"5g technology" OR "Document Title":"5g network" OR "Document Title":"5g mobile telephony" OR "Document Title":"fifth generation") AND ("Document Title":cybersecurity OR "Document Title":"online safety" OR "Document Title":security OR "Document Title":cyber)) OR (("Abstract":5g OR "Abstract":"5g technology" OR "Abstract":"5g network" OR "Abstract":"5g mobile telephony" OR "Abstract":"fifth generation") AND ("Abstract":cybersecurity OR "Abstract":"online safety" OR "Abstract":security OR "Abstract":cyber))
ARDI	((Abstract:(\("5g technology" OR 5g OR "5g network" OR "5g mobile telephony" OR "fifth generation"\) AND \(cybersecurity OR "online safety" OR "security" OR "cyber"\))) OR (TitleCombined:(\("5g technology" OR 5g OR "5g network" OR "5g mobile telephony" OR "fifth generation"\) AND \(cybersecurity OR "online safety" OR "security" OR "cyber"\))))
EBSCO host	AND ("5g technology" OR 5g OR "5g network") AND (cybersecurity OR "online safety" OR security) Title OR ("5g technology" OR 5g OR "5g network") AND (cybersecurity OR "online safety" OR security) Abstract
ACM Digital Library	[[[Title: "5g technology"] OR [Title: 5g] OR [Title: "5g network"] OR [Title: "5g mobile telephony"] OR [Title: "fifth generation"]] AND [[Title: cybersecurity] OR [Title: "online safety"] OR [Title: security] OR [Title: cyber]]] OR [[[Abstract: "5g technology"] OR [Abstract: 5g] OR [Abstract: "5g network"] OR [Abstract: "5g mobile telephony"] OR [Abstract: "fifth generation"]] AND [[Abstract: cybersecurity] OR [Abstract: "online safety"] OR [Abstract: security] OR [Abstract: cyber]]]

The papers selected for this research cover the period from 2016 to 2022, with contributions from all continents. As shown, the year 2022 recorded the most contributions, while 2016 had the fewest contributions. In the study by Gamboa-Cruzado [89], a continuous increase in publications from 2016 to 2021 is observed, which coincides with the current research.

Figure 7 illustrates the number of papers contributed by each continent, classifying them into categories: good, average, and low. On the other hand, the previous figure reveals that the continents of Asia and Europe are classified as good, contributing more than 30 papers each, while Africa and Oceania are considered low, contributing fewer than 10 papers each.

In the study by Raveendran and Tabet [74], papers were considered over a broader time range, from 2000 to 2020, providing a more extended temporal window compared to the current paper. On the other hand, Lozano, and Mateo [75] align with the results presented in this paper in identifying Asia as the continent with the most publications, accounting for 39.65%, followed by Europe with 32.25%. In a study conducted by Zeb, Mahmood, Hassan, Piran, Guizani, and Gildlund [76], the chosen time range spanned from 2003 to 2021.

It can be concluded that, for potential future research on this topic, it would be prudent to prioritize the search for information on the Asian continent, given the trend observed in the results found, as well as in the research of other authors, suggests that this continent is the most productive in terms of contributions, followed by Europe.

Regarding temporality, it might be beneficial to broaden the range of years considered to gain a broader and possibly more representative view of the state of the art in the field of 5G technology and its impact on cybersecurity.

4.2 Answers to the Research Questions

Following are the conclusions and specific findings that address each of the research questions posed in the study.

Each research question is tackled individually, providing detailed analyses and answers based on the data gathered and assessed in the previous section. This part of the paper offers a clear structure for understanding how the results relate to the research objectives and provides valuable insights into the current state of the field in relation to the questions raised.

RQ1: In which industrial sectors or fields of study is 5G Technology having a significant impact?

The following presents Table 6, which illustrates the sectors where 5G technology finds greater application according to this review.

From the table, it is evident that the predominant areas of application for 5G technology in this study are physics at 58.8%, transport at 38.2%, and healthcare at 32.3%.

Raveendran and Tabet [74] identify main themes as categories in their research, leading them to formulate five master themes related to higher-order concerns, namely: electromagnetic pollution, cybersecurity issues, data center overload, proliferation of submarine cables, and electronic waste.

On the other hand, Zeb, Mahmood, Hassan, Piran, Guizani, and Gildlund [76] primarily focus on the information of the industrial digital twin for control and management processes in industrial applications. Still, they also touch upon cloud computing, machine learning, artificial intelligence, 5G industrial services, industrial twin placement strategies, green communication, and automated optical inspection.

Goudarzi, Ghayoor, Waseem, Fahad, and Traore [86] place importance on the realm of the Internet of Things in next-generation IoT-enabled smart grids, with a higher number of contributions derived from parts of their papers included in their review. Authors Sodhro, Awad, Beek, and Nikolakopoulos [87] examine network layer approaches and other technologies in their review, with the areas of network and security having the most contributions recorded.

Ferrag, Maglaras, Argyriou, Kosmanos, and Janicke [88] point out that the research area receiving the most contributions in the papers they selected is security and privacy. The diversity in the criteria mentioned by various authors when addressing 5G technology reflects the breadth and complexity of this emerging technology.

Based on the focus of the review, areas of physics and electromagnetism, as well as security, are particularly emphasized, indicating that these are significant areas of interest in the current 5G literature.

Physics and electromagnetism are fundamental to understanding and advancing 5G technology, as they lie at the core of how wireless signals are transmitted and received.

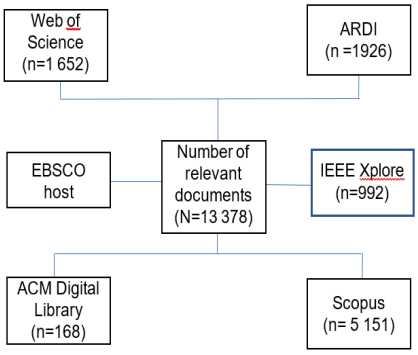

Fig. 2. Number of papers by source

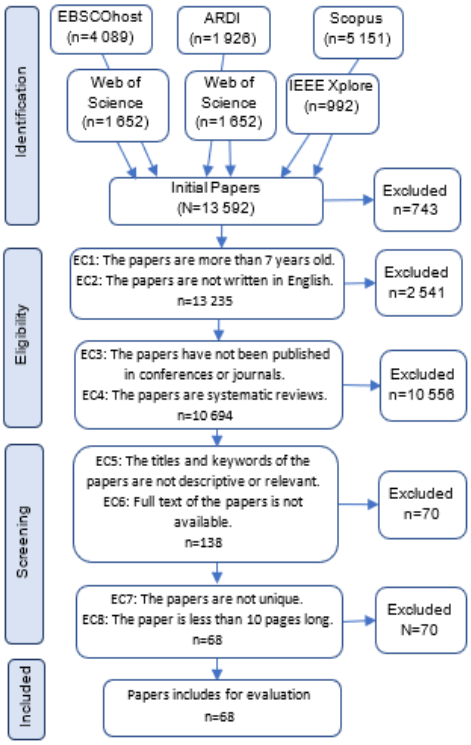

Fig. 3. PRISMA flow diagram

The implications of 5G technology in these fields are vast and could lead to new innovations or technical challenges that have not yet been fully explored. Future research in the field of 5G technology could greatly benefit from the findings and themes highlighted in the current review.

However, it is crucial for future researchers to also follow their own criteria and personal focus,

Table 4. Quality assessment of the papers

Ref.	QA1	QA2	QA3	QA4	QA5	QA6	QA7	Score
[1]	2	3	3	3	2	3	1	17
[2]	2	1	3	3	1	2	3	15
[3]	2	1	3	3	1	2	3	15
[4]	3	1	3	3	1	2	3	16
[5]	3	3	0	3	3	2	3	17
[6]	3	3	3	0	3	3	0	15
[7]	3	3	3	3	3	0	3	18
[8]	3	3	2	3	3	3	3	20
[9]	3	3	2	3	3	3	3	20
[10]	3	3	2	3	3	3	3	20
[11]	3	0	2	3	3	3	0	14
[12]	3	3	0	3	3	3	3	18
[13]	3	3	3	3	3	3	3	21
[14]	3	3	3	0	3	3	3	18
[15]	3	3	3	3	3	3	3	21
[16]	0	3	0	3	3	3	1	13
[17]	3	3	3	3	3	3	3	21
[18]	3	3	3	1	3	3	3	19
[19]	3	3	3	3	3	3	3	21
[20]	3	0	3	3	3	3	3	18
[21]	3	3	3	3	3	3	0	18
[22]	3	3	3	0	3	3	3	18
[23]	3	3	3	3	3	3	3	21
[24]	0	3	3	3	1	3	3	16
[25]	3	3	3	3	3	3	3	21
[26]	3	3	3	3	3	3	0	18
[27]	2	3	3	3	3	3	3	20
[28]	3	3	0	3	3	3	3	18
[29]	3	3	3	3	3	3	3	21
[30]	3	3	3	3	3	3	3	21
[31]	3	3	3	3	0	3	3	18
[32]	3	3	3	3	3	3	3	21
[33]	1	3	3	3	2	3	3	18
[34]	3	3	3	3	3	3	3	21
[35]	3	0	3	3	3	3	2	17
[36]	3	3	3	3	3	3	3	21
[37]	3	3	3	3	3	2	3	20
[38]	0	3	3	3	3	3	3	18
[39]	3	3	3	3	3	3	3	21
[40]	3	3	3	2	3	3	3	20
[41]	3	0	3	3	3	3	3	18
[42]	3	3	3	3	0	3	3	18
[43]	2	3	3	3	3	0	3	17
[44]	3	1	3	3	3	3	3	19
[45]	3	2	3	0	3	3	3	17
[46]	3	0	3	3	3	3	3	18
[47]	3	3	3	3	3	3	3	21
[48]	3	3	3	3	3	0	1	16
[49]	3	3	1	3	3	3	3	19
[50]	3	3	3	3	3	3	3	21
[51]	3	0	3	3	3	3	3	18
[52]	3	3	3	0	3	3	3	18
[53]	2	3	3	3	3	0	3	17
[54]	3	3	3	3	3	3	3	21
[55]	3	3	2	3	3	3	3	20
[56]	3	3	3	3	3	2	3	20
[57]	3	3	3	3	3	3	3	21
[58]	3	3	3	0	3	1	3	16
[59]	3	0	3	1	3	3	3	16
[60]	2	3	3	3	3	3	3	20
[61]	3	3	3	3	3	3	3	21
[62]	3	3	3	3	3	3	3	21
[63]	2	3	3	2	3	3	0	16
[64]	3	0	3	3	0	3	3	15
[65]	2	3	3	3	3	3	3	20
[66]	3	3	3	3	3	3	3	21
[67]	2	3	3	0	3	3	3	17
[68]	3	3	3	3	3	3	3	21

and perhaps explore other relevant areas or topics that might not have been extensively covered in current studies. The advice to adhere to the author's criteria suggests that each researcher should also bring their unique perspective and focus to the field, which could lead to new ideas and advancements not yet considered.

This is especially relevant in a rapidly moving and evolving technological field like 5G, where innovation and continuous exploration are essential for advancing knowledge and the practical application of the technology.

RQ2: What is the distribution of publications on 5G Technology and its impact on Cybersecurity among the different quartiles of journals?

Figure 6 displays the quartile levels broken down by year. The Figure 8 presented below

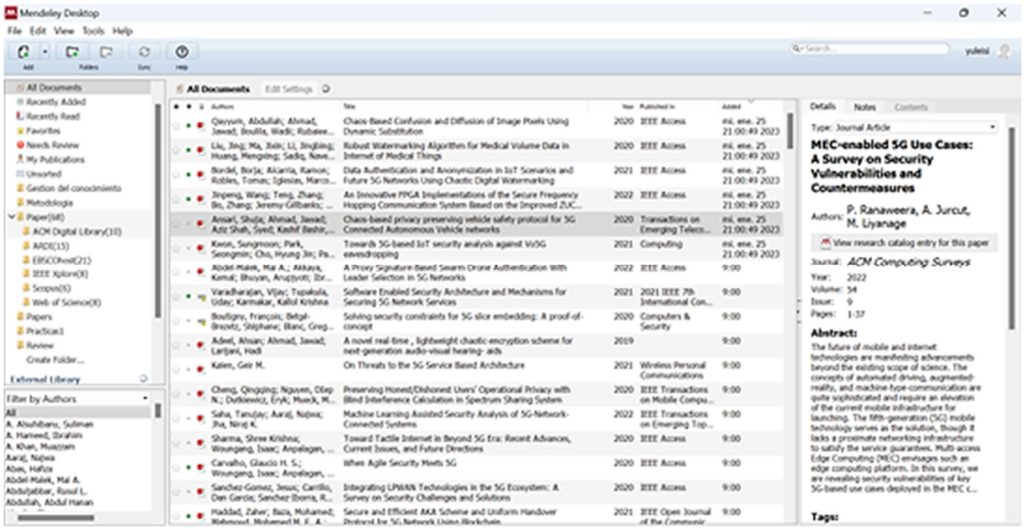

Fig. 4. Reporting of papers using Mendeley desktop

illustrates the relationship between the quartiles and the sources used in the review through a Sankey diagram. This type of diagram allows for a clear and effective visualization of how the different quartiles are distributed among the various reviewed sources, facilitating the understanding of the correlation between these two elements.

Through graphical flows, the Sankey diagram displays how the quartiles are associated with each source, providing an intuitive visual representation that can be greatly helpful in understanding the distribution and trend of the quartiles in relation to the sources consulted in the systematic review process.

The Figure underscores that papers in this research are categorized into quartile levels Q1, Q2, Q3, and Q4, with Q1 being the most prevalent. Moreover, it is observed that the year 2022 contributed the highest number of papers.

On the other hand, the correlation between quartiles and the sources from which the papers originated is illustrated, revealing that all papers categorized in the Q1 quartile come from all consulted sources, with the exception of EBSCOhost.

This analysis reflects not only the distribution of papers across different quartiles and their yearly evolution but also the relationship between the perceived quality of the papers, represented by the quartiles, and the sources from which they were drawn, providing an in-depth perspective on the provenance and quality of the papers reviewed in this research.

The authors Ogbodo, Abu-Mahfouz, and Kurien [77] also agree with the findings of this research, including the same quartiles in their paper, with the exception of Q2. This reflects a similarity in the distribution of the quality of papers across different studies, although with some differences regarding the Q2 quartile.

This might indicate variations in the selection or evaluation of papers among different studies. This overlap, with the mentioned exception, could suggest a trend or pattern in the distribution of papers based on their quality and provides a basis for comparing and contrasting results among different studies in the realm of 5G Technology and its impact on cybersecurity.

It is observed that the considered papers span all quartile levels, though there is a notable decrease in the Q2 category. This could be a point of consideration for future researchers looking to evaluate the quality of this type of research.

The variability in the quartile distribution, particularly the drop in Q2, may offer insights regarding the quality and relevance of existing studies in the realm of 5G Technology and its impact on cybersecurity.

Furthermore, this pattern could serve as a guide for future research, suggesting a more

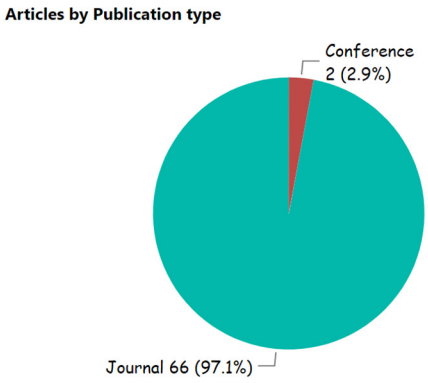

Fig. 5. Percentage of papers by journal and conference

Table 5. Number of papers by continent and year

Years / Continent	2016	2017	2018	2019	2020	2021
Asia	1	1	4	1	11	16
Europe	1	4	5	7	13	4
America	0	0	1	1	6	1
Oceania	0	0	0	0	2	1
Africa	0	0	0	0	1	
Total	2	5	10	9	33	22

thorough review of evaluation criteria and paper selection, especially concerning Q2.

This could contribute to a broader and more accurate understanding of the existing literature, and possibly influence the direction and focus of future research efforts in this field.

RQ3: Who are the most prolific or influential authors in the field of 5G Technology and its impact on Cybersecurity, and what are their co-authorship networks?

With respect to co-occurrence, there are semantic distributional models based on count vectors that represent by means of a matrix the frequency of occurrence of words (authors, in this case) in a document. The similarity between two words vectors can be obtained through the angle they form, specifically by the cosine of the angle.

It is considered that the smaller the angle, and consequently the cosine of the angle, the greater the similarity between them. With the following equation, we obtain the cosine measure between the documents d_i and d_j where d_{ik} is the weight of the semantic feature k in the document d_i:

$$\sin(d_i, d_j) = \cos(a) = \frac{\sum_{k=1}^{m}(d_{ik} * d_{jk})}{\sqrt{(\sum_{k=1}^{m} d_{ik}^2) * (\sum_{k=1}^{m} d_{jk}^2)}}. \quad (1)$$

Figure 9 illustrates the bibliometric network that highlights the frequency with which certain authors collaborate as co-authors in the studies considered in this review.

This visualization can provide a clear representation of the connections and collaborations among researchers within the study field of 5G Technology and its impact on cybersecurity. Through this network, it is possible to identify clusters of authors who frequently work together, which may indicate research groups or institutions that are actively contributing to this area.

Figure 9 displays the bibliometric network of co-authors in this review, highlighting four authors who show a recurring co-authorship frequency: Zhu Han, Latif U. Khan, Choong Seon Hong, and Ibrar Yacoob, who each contribute to three research papers respectively with other researchers.

This visualization can be significant in understanding existing collaborations and the network of professional relationships in the field of 5G Technology and its impact on cybersecurity. Identifying these recurring authors may point to individuals or research groups that have a notable influence or specialization in the area.

Lozano and Mateo [75] highlight two papers as the most cited in their research: "Performance evaluation of the IEEE 802.11p WAVE communication standard" and "Delay and broadcast reception rates of highway safety applications in vehicular ad hoc networks," both authored by Eichler.

These papers focus on the performance evaluation of vehicular communication standards and highway safety applications, respectively. On the other hand, Ly, and Yao [78] identify the publication "Deep learning in mobile and wireless networking: A survey" as the most recurring in their review, written by Zhang, Patras, and Haddadi.

This work encompasses a comprehensive review of deep learning applied to mobile and wireless networks, reflecting an interest in the

intersection between machine learning technologies and communication networks.

Based on the obtained results, it is evident that there are various prominent authors in the findings, which vary depending on the focus of the review. This suggests that in future research related to this topic, it might be beneficial to define one or several key benchmarks that could guide or inform the study in question.

Identifying these benchmarks can not only provide a solid foundation for the analysis but could also help situate the work within the broader context of the existing literature in this field. RQ4: What are the leading countries in the production of research on 5G Technology and its impact on Cybersecurity, and how are the bibliometric flows distributed among these countries?

The bibliometric flow between two countries can be calculated using the co-authorship matrix (A) as follows. A flow matrix (F) is created where $F_{(i,j)}$ represents the bibliometric flow from country i to country j. The total collaborations of a country are calculated, which can be defined as $C_{(i)}$ for country i. This can be determined by summing the values of the corresponding row in the co-authorship matrix A.

Then, the bibliometric flow from country i to country j is calculated by dividing the number of collaborations between these two countries $(A_{(i,j)})$ by the total collaborations of country i $(C_{(i)})$:

$$F_{(i.j)} = A_{(i,j)}/C_{(i)}. \quad (2)$$

The result is a flow matrix that displays the relative collaboration flow among all country pairs. This metric allows for the identification of which countries collaborate more closely in scientific production and how that collaboration is distributed globally.

Figure 10 illustrates the bibliometric flow coming from different countries. This visualization provides a graphic representation of the contribution and participation of various countries in the literature related to the researched topic.

This information is essential to understand the geographical distribution of the research and can help identify the leading regions on the subject, as well as potential international collaborations. It can also offer insight into how regional policies or trends might influence the evolution and

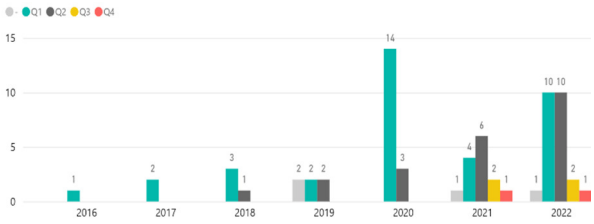

Fig. 6. Quartile levels by year

Table 6. Sectors where 5G technology is most applied

Sector	Reference	Qty (%)
Telecommunications	[7] [8] [14] [17] [33] [40] [48] [52]	8 (11,7)
Health	[6] [8] [9] [10] [12] [15] [17] [18] [28] [29] [30] [33] [36] [37] [47] [48] [50] [51] [52] [59] [60] [62]	22 (32,3)
Transport	[2] [3] [6] [7] [8] [13] [15] [16] [17] [22] [23] [28] [30] [35] [36] [38] [39] [40] [44] [48] [50] [51] [52] [53] [55] [58]	26 (38,2)
Logistics	[2] [7] [13] [25] [32] [46] [57]	7 (10,2)
Agriculture	[6] [13] [15] [17] [28] [30] [50]	7 (10,2)
Education	[48] [51] [59]	3 (4,4)
Physical	[1] [2] [4] [5] [6] [8] [9] [10] [12] [13] [14] [15] [17] [18] [19] [21] [22] [24] [27] [28] [29] [30] [33] [35] [37] [39] [42] [45] [48] [49] [51] [52] [53] [54] [55] [56] [59] [60] [65] [68]	40 (58,8)
Economy	[21] [59]	2 (2,9)
Programming	[4] [5] [9] [26] [35] [41] [60]	7 (10,2)

application of 5G technology and its impact on cybersecurity.

Figure 11 displays the list of countries with the highest bibliometric flows. The Figure above shows the bibliometric flow of countries, which allows us to appreciate the number of co-occurrences between them. This representation showcases international collaborations in the field of research.

Specifically, it details that the United Kingdom tops the list with six instances of international collaborations, positioning itself as the country with

the highest frequency in this respect, followed by China and France.

This analysis highlights the global interconnection in research on 5G technology and its impact on cybersecurity and may suggest a trend towards international collaboration on these critical and emerging topics. Additionally, it provides insight into how different regions are contributing and collaborating to advance knowledge in this specific field.

Raveendran and Tabet [74] place the United States as the country that contributes most to their research, followed by India. Lozano and Mateo [75] indicate that the United States is the country with the most international collaborations in their research, differing from the results of this review, but still considering the UK and France as the top contributors.

Based on the pre-existing findings and those obtained in this study, it is observed that the UK and the US are the countries that most frequently contribute to other countries, closely followed by France and India.

Therefore, it is suggested to consider these countries as primary reference points in future research in the field of 5G Technology and its impact on cybersecurity.

These nations, it seems, maintain a prominent position in the development and international collaboration on these critical topics, which might be of relevance for researchers looking to understand global trends and establish fruitful collaborations in this rapidly advancing field.

RQ5: How can papers be grouped based on the thematic similarity of their titles in the field of 5G Technology and its impact on Cybersecurity, and which themes predominate in each cluster? Similarity Metrics: Cosine similarity is examined and used to find the similarity of the papers based on term vectors.

Cosine Similarity: Cosine similarity allows determining the angle between two vectors; they will be similar if they are quite close in terms of direction and magnitude.

Cosine similarity helps measure the cosine of the angles between two vectors. The value of cosine similarity lies in the range of -1 to 1. A value of 1 indicates that the vectors are perfectly similar, and a value of -1 indicates that the vectors are exactly opposite to each other. Two papers are

Fig. 7. Heatmap of the number of papers by continent

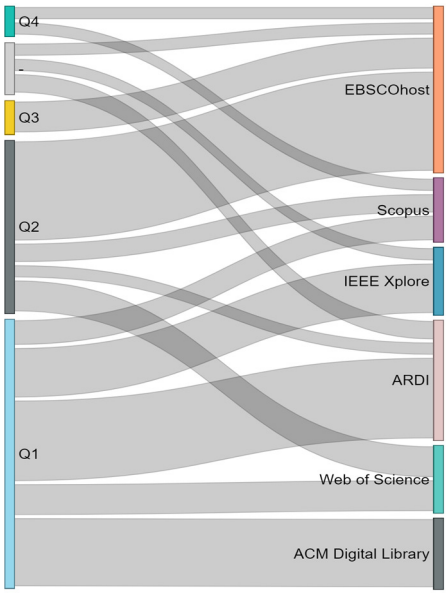

Fig. 8. Sankey diagram of quartile level by source

similar if their cosine similarity values are close to 1.

Moreover, these similarity measures are always between pairs of papers. Cosine similarity can only be calculated for vectors of similar sizes. The formula for cosine similarity for two vectors A and B is as follows:

$$\cos(\theta) = \frac{A.B}{\|A\|\|B\|}. \quad (3)$$

Here, A.B is the dot product between the two vectors, and $||A||$ and $\|B\|$ represent the magnitude of these two vectors respectively. The above formula can also be represented as follows:

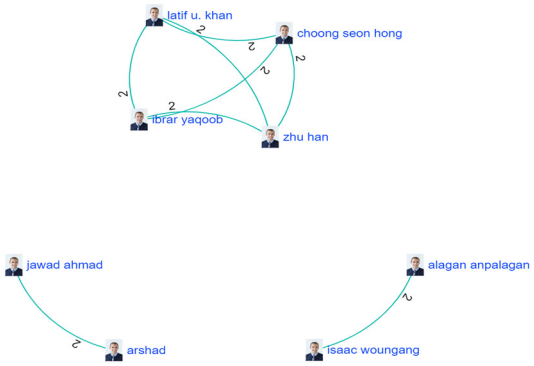

Fig. 9. Bibliometric network of co-authors

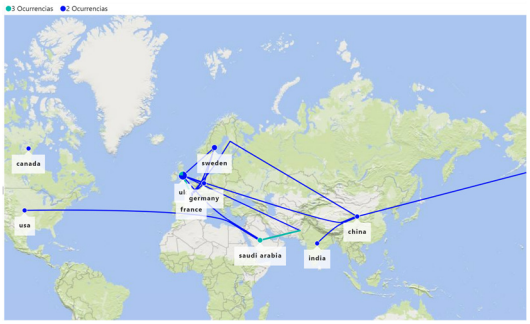

Fig. 10. Bibliometric flow of countries

$$\cos(\theta) = \frac{A.B}{\sqrt{\sum_{i=1}^{i=N} \omega_{iA}^2}\sqrt{\sum_{i=1}^{i=N} \omega_{iB}^2}}. \quad (4)$$

Here, ω_A and ω_B represent the weight or magnitude of vectors A and B along the i-th dimension, respectively, in an n-dimensional space. To find the similarity of all papers with each other, there is a shortcut model to compute all the numbers with a single command (Albrecht, Ramachandran, & Winkler, 2020, p. 127). Generalizing the formula from the previous section, we find that the similarity between paper i and paper j is as follows:

$$S_{ij} = d_i . d_j. \quad (5)$$

If one wants to use a term-document matrix, the dot product can be expressed as a summation:

$$S_{ij} = \Sigma_K D_{ik} D_{jk} = \Sigma K D_{ik} D T_{kj} = (D.D^T)_{ij}. \quad (6)$$

Therefore, this is the matrix product of the term-document matrix with its own transpose. Clustering is a machine learning task, and the techniques used in clustering can also be applied to text.

Clustering is the task of grouping data points into the same cluster, where points within the same cluster are more similar to each other than to points in different clusters. These data points can be considered as either documents or, in some cases, words.

TF-IDF is a method that assigns higher weight to rarer words, setting each element of the term-document matrix equal to the value w of multiplying the term frequency (TF) by the inverse document frequency (IDF) of each token (Kamath, Liu, & Whitaker, 2019, p. 96):

$$W = tfxidf = (1 + \log(TF_t))xlog\left(\frac{N}{n_i}\right). \quad (7)$$

Term frequency (TF) is the number of times a word appears in a document. The IDF helps to understand the importance of a word within a document.

By calculating the inverse fraction (scaled logarithmically) of the documents over the number of documents containing the term, and then taking the logarithm of that quotient, one can get a measure of how common or rare a word is across all documents. Currently, TF-IDF is the most popular weighting method, as over 80% of today's digital libraries use it.

Figure 12 illustrates four groupings of papers based on the similarity of their titles in this study. These groupings, or clusters, can help identify common themes or focuses in the existing literature on 5G Technology and its impact on cybersecurity.

By analyzing the similarity in titles, patterns or trends in the research can be uncovered, which in turn can provide valuable insight into the predominant focus areas in this field. This graphical representation aids in understanding how different works cluster together and can serve as a helpful guide to explore specific areas of interest.

The Figure groups the papers into four clusters based on the similarity of their titles. This grouping allows for the identification and categorization of works based on common themes or terminologies, thereby facilitating a clearer understanding of the main focus areas within the research on 5G Technology and its impact on cybersecurity.

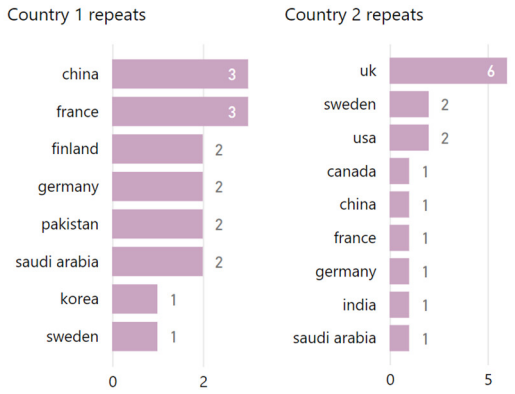

Fig. 11. Countries with the highest bibliometric flow

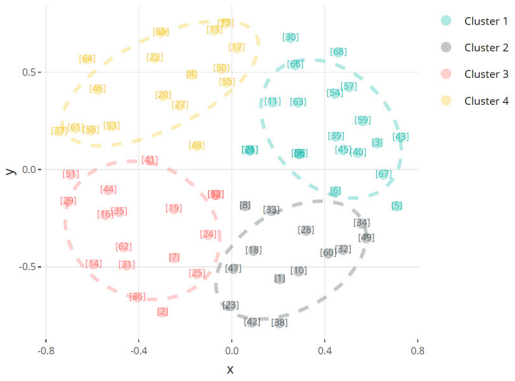

Fig. 12. Clusters of papers with title similarity

Through these clusters, an organized and structured view of the existing literature can be obtained, which could be beneficial for identifying trends, comparing approaches, and discovering potential areas that still require deeper exploration.

In their review, Raveendran and Tabet [74] opted for a more detailed classification and categorized the literature into 11 thematic clusters, focusing on aspects such as direct impacts on the environment, unrecognized rebound effects, and direct impacts on humans.

This more granular categorization allowed for a deep and specific exploration of various aspects and consequences associated with 5G technology. In contrast, the organization into 4 clusters, as shown in Figure 11, might provide a more general view but less detailed insight into the prevailing themes in the literature on 5G Technology and cybersecurity.

Both approaches have their advantages and disadvantages, and the choice between them will depend on the specific goals of the review and the level of detail researchers wish to achieve in their analysis of the existing literature.

Indeed, the organization of papers into clusters is a strategy that allows for grouping information in a way that facilitates analysis and interpretation of data.

This clustering can be done based on various criteria, such as similarity in titles, themes, methodologies, authors, among others. The way one decides to organize the clusters will depend on the focus of the research and the objectives they wish to achieve.

Therefore, in future studies, it is recommended that authors clearly define the criteria they will use to group the papers into clusters, so that this organization allows them to gain a better understanding of the state of the art and key findings in the area of study they are exploring.

It is also crucial that the selected criteria for clustering align with the research questions posed, ensuring that the organization of the data effectively contributes to answering these questions and achieving the research objectives.

5 Conclusions and Future Research

This paper presents a meticulous bibliometric and systematic review on the deployment of 5G Technology in the field of Cybersecurity, adopting the methodology proposed by Petersen. For this purpose, renowned sources such as Scopus, Web of Science, ARDI, ACM Digital Library, IEEE Xplore, and EBSCOhost were selected.

Through the application of specific equations, 13,235 studies were identified, to which meticulously designed exclusion criteria were applied. Using the Prisma diagram, the selection of 68 papers published between 2016 and 2022 was outlined. Subsequently, the selected studies were evaluated and organized using the Mendeley software.

Regarding the findings of this investigation, it stands out that the areas of greatest focus in the application of 5G technology are health, transport, and physics. The paper titled "6G Wireless Communication Systems:

Applications, Requirements, Technologies, Challenges, and Research Directions" is notably highlighted for its significant contribution to research.

Geographically, the United Kingdom emerges as the country with the highest bibliometric flow in this area of study, underscoring its prominent position in research on the intersection of 5G Technology and Cybersecurity.

This review presents two limitations that could be addressed in future research. Firstly, it was confined to six information sources, which may have narrowed the breadth of the findings.

A more expansive exploration incorporating a wider variety of databases and information sources could provide a more holistic and representative view of the current state of knowledge at the intersection of 5G Technology and Cybersecurity.

Secondly, the considered time frame, from 2016 to 2022, while pertinent to capture the most recent developments, may have excluded pioneering or foundational research conducted before this period.

Extending the temporal scope to include studies published in earlier years could unravel a deeper and contextualized understanding of the evolution of 5G Technology and its impact on Cybersecurity, thus allowing for a richer appreciation of the trends, challenges, and opportunities that characterize this dynamic and rapidly evolving field.

References

1. **Abdel-Malek, M. A., Akkaya, K., Bhuyan, A., Ibrahim, A. S. (2022).** A proxy signature-based swarm drone authentication with leader selection in 5G networks. IEEE Access, Vol. 10, pp. 57485–57498. DOI: 10.1109/ACCESS.2022.3178121.
2. **Adeel, A., Ahmad, J., Larijani, H., Hussain, A. (2020).** A novel real-time, lightweight chaotic-encryption scheme for next-generation audio-visual hearing aids. Cognitive Computation, Vol. 12, No. 3, pp. 589–601. DOI: 10.1007/s12559-019-09653-z.
3. **Afzal, R., Murugesan, R. K. (2022).** Rule-based anomaly detection model with stateful correlation enhancing mobile network security. Intelligent Automation & Soft Computing, Vol. 31, No. 3, pp. 1825–1841. DOI: 10.32604/iasc.2022.020598.
4. **Al-Heety, O. S., Zakaria, Z., Ismail, M., Shakir, M. M., Alani, S., Alsariera, H. (2020).** A comprehensive survey: Benefits, services, recent works, challenges, security, and use cases for SDN-VANET. IEEE Access, Vol. 8, pp. 91028–91047. DOI: 10.1109/ACCESS.2020.2992580.
5. **Alanazi, F., Jambi, K., Eassa, F., Khemakhem, M., Basuhail, A., Alsubhi, K. (2022).** Ensemble deep learning models for mitigating DDoS attack in software-defined network. Intelligent Automation & Soft Computing, Vol. 33, No. 2, pp. 923–938. DOI: 10.32604/iasc.2022.024668.
6. **Anagnostopoulos, N. A., Ahmad, S., Arul, T., Steinmetzer, D., Hollick, M., Katzenbeisser, S. (2020).** Low-cost security for next-generation IoT networks. ACM Transactions on Internet Technology (TOIT), Vol. 20, No. 3, pp. 1–31. DOI: 10.1145/3406280.
7. **Ansari, S., Ahmad, J., Aziz-Shah, S., Kashif-Bashir, A., Boutaleb, T., Sinanovic, S. (2020).** Chaos-based privacy preserving vehicle safety protocol for 5G connected autonomous vehicle networks. Transactions on Emerging Telecommunications Technologies, Vol. 31, No. 5, pp. e3966. DOI: 10.1002/ett.3966.
8. **Arfaoui, G., Bisson, P., Blom, R., Borgaonkar, R., Englund, H., Félix, E., Klaedtke, F., Nakarmi, P., Näslund, M., O'Hanlon, P., Papay, J., Suomalainen, J., Surridge, M., Wary, J. P., Zahariev, A. (2018).** A security architecture for 5G networks. IEEE Access, Vol. 6, pp. 22466–22479. DOI:10.1109/ACCES.218.28 27419.
9. **Basir, R., Chughtai, N. A., Ali, M., Qaisar, S., Hashmi, A. (2022).** Mode selection, caching and physical layer security for fog networks. Bulletin of the Polish Academy of Sciences Technical Sciences, Vol. 70, No. 5, pp. 1–11. DOI: 10.24425/bpast.2022.142652.
10. **Bordel, B., Alcarria, R., Robles, T., Iglesias, M. S. (2021).** Data authentication and anonymization in IoT scenarios and future 5G

networks using chaotic digital watermarking. IEEE Access, Vol. 9, pp. 22378–22398. DOI: 10.1109/ACCESS.2021.3055771.

11. **Cao, L., Lu, X., Gao, Z., Han, M., Du, X. (2020).** Multilevel security network communication model based on multidimensional control. Mathematical Problems in Engineering, Vol. 2020, pp. 1–18. DOI: 10.1155/2020/3528439.
12. **Carvalho, G. H. S., Woungang, I., Anpalagan, A., Traore, I. (2020).** When agile security meets 5G. IEEE Access, Vol. 8, pp. 166212–166225. DOI: 10.1109/ACCESS.2020.3022741.
13. **Chen, Y., Sambo, Y. A., Onireti, O., Imran, M. A. (2022).** A survey on LPWAN-5G integration: Main challenges and potential solutions. IEEE Access, Vol. 10, pp. 32132–32149. DOI: 10.1109/ACCESS.2022.3160193.
14. **Cheng, Q., Nguyen, D. N., Dutkiewicz, E., Mueck, M. (2019).** Preserving honest/dishonest users' operational privacy with blind interference calculation in spectrum sharing system. IEEE Transactions on Mobile Computing, Vol. 19, No. 12, pp. 2874–2890. DOI: 10.1109/TMC.2019.2936377.
15. **Chowdhury, M. Z., Shahjalal, M., Ahmed, S., Jang, Y. M. (2020).** 6G wireless communication systems: Applications, requirements, technologies, challenges, and research directions. IEEE Open Journal of the Communications Society, Vol. 1, pp. 957–975. DOI: 10.1109/OJCOMS.2020.3010270.
16. **Condoluci, M., Gallo, L., Mussot, L., Kousaridas, A., Spapis, P., Mahlouji, M., Mahmoodi, T. (2019).** 5G V2X system-level architecture of 5GCAR project. Future Internet, Vol. 11, No. 10, p. 217. DOI: 10.3390/fi11100217.
17. **El-Mettiti, A., Oumsis, M. (2022).** A survey on 6G networks: Vision, requirements, architecture, technologies and challenges. Ingénierie Des Systèmes D'Information, Vol. 27, No. 1. DOI: 10.18280/isi.270101.
18. **Haddad, Z., Baza, M., Mahmoud, M. M. E. A., Alasmary, W., Alsolami, F. (2021).** Secure and efficient AKA scheme and uniform handover protocol for 5G network using Blockchain. IEEE Open Journal of the Communications Society, Vol. 2, No. pp. 2616–2627. DOI: 10.1109/OJCOMS.2021.3131552.
19. **Hamamreh, J. M., Ankarali, Z. E., Arslan, H. (2018).** CP-Less OFDM with alignment signals for enhancing spectral efficiency, reducing latency, and improving PHY security of 5G services. IEEE Access, Vol. 6, pp. 63649–63663. DOI: 10.1109/ACCESS.2018.2877321.
20. **Hao, Y., Yan, X., Wu, J., Wang, H., Yuan, L. (2021).** Multimedia communication security in 5G/6G: coverless steganography based on image text semantic association. Security and Communication Networks, pp. 1–12. DOI: 10.1155/2021/6628034.
21. **Hatzivasilis, G., Soultatos, O., Ioannidis, S., Spanoudakis, G., Katos, V., Demetriou, G. (2020).** MobileTrust. ACM Transactions on Cyber-Physical Systems, Vol. 4, No. 3, pp. 1–25. DOI: 10.1145/3364181.
22. **He, Y., Huang, D., Chen, L., Ni, Y., Ma, X. (2022).** A survey on zero trust architecture: challenges and future trends. Wireless Communications and Mobile Computing, Vol. 2022, pp. 1–13. DOI: 10.1155/2022/6476274.
23. **Huang, X., Yoshizawa, T., Baskaran, S. B. M. (2021).** Authentication mechanisms in the 5g system. Journal of ICT Standarization, Vol. 9, No. 2, pp. 61–78. DOI: 10.13052/jicts2245-800X.921.
24. **Hussain, S. R., Echeverria, M., Karim, I., Chowdhury, O., Bertino, E. (2019).** 5GReasoner. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 669–684. DOI: 10.1145/3319535.3354263.
25. **Kamran, M. I., Khan, M. A., Alsuhibany, S. A., Ghadi, Y. Y., Arshad, A., Arif, J., Ahmad, J. (2022).** A highly secured image encryption scheme using quantum walk and chaos. Computers, Materials and Continua, Vol. 73, No. 1, pp. 657–672. DOI: 10.32604/cmc.2022.028876.
26. **Jin, X., Duan, Y., Zhang, Y., Huang, Y., Li, M., Mao, M., Li, Y. (2021).** Fast search of

lightweight block cipher primitives via swarm-like metaheuristics for cyber security. ACM Transactions on Internet Technology, Vol. 21, No. 4, pp. 1–15. DOI: 10.1145/3417296.

27. **Jinpeng, W., Teng, Z., Bo, Z., Jeremy-Gillbanks, Xin, Z. (2022).** An innovative FPGA implementations of the secure frequency hopping communication system based on the improved ZUC algorithm. IEEE Access, Vol. 10, pp. 54634–54648. DOI: 10.1109/ACCESS.2022.3176609.
28. **Kaur, M., Khan, M. Z., Gupta, S., Alsaeedi, A. (2022).** Adoption of blockchain with 5g networks for industrial IoT: recent advances, challenges, and potential solutions. IEEE Access, Vol. 10, pp. 981–997. DOI: 10.1109/ ACCESS.2021.3138754.
29. **Khan, L. U., Yaqoob, I., Imran, M., Han, Z., Hong, C. S. (2020).** 6G wireless systems: a vision, architectural elements, and future directions. IEEE Access, Vol. 8, pp. 147029–147044. DOI: 10.1109/ACCESS.2020. 3015289.
30. **Khan, L. U., Yaqoob, I., Tran, N. H., Han, Z., Hong, C. S. (2020).** Network slicing: recent advances, taxonomy, requirements, and open research challenges. IEEE Access, Vol. 8, pp. 36009–36028. DOI: 10.1109/ACCESS.2020. 2975072.
31. **Khan, M., Ginzboorg, P., Niemi, V. (2019).** Privacy preserving AKMA in 5G. Proceedings of the 5th ACM Workshop on Security Standardisation Research Workshop-SSR'19, PP. 45–56. DOI: 10.1145/3338500. 3360337.
32. **Kim, Y. E., Kim, M. G., Kim, H. (2022).** Detecting IoT botnet in 5G core network using machine learning. Computers, Materials & Continua, Vol. 72, No. 3, pp. 4467–4488. DOI: 10.32604/cmc.2022.026581.
33. **Krishnan, P., Jain, K., Jose, P. G., Achuthan, K., Buyya, R. (2021).** SDN enabled QOE and security framework for multimedia applications in 5G networks. ACM Transactions on Multimedia Computing, Communications, and Applications, Vol. 17, No. 2, pp. 1–29. DOI: 10.1145/3377390.
34. **Kwon, S., Park, S., Cho, H. J., Park, Y., Kim, D., Yim, K. (2021).** Towards 5G-based IoT security analysis against Vo5G eavesdropping. Computing, Vol. 103, No. 3, pp. 425–447. DOI: 10.1007/s00607-020-00855-0.
35. **Køien, G. M. (2021).** On threats to the 5G service based architecture. Wireless Personal Communications, Vol. 119, No. 1, pp. 97–116. DOI: 10.1007/s11277-021-08200-0.
36. **Le, T. V., Hsu, C. L. (2021).** An anonymous key distribution scheme for group healthcare services in 5G-enabled multi-server environments. IEEE Access, Vol. 9, 53408–53422. DOI: 10.1109/ACCESS.2021. 3070641.
37. **Liu, J., Ma, J., Li, J., Huang, M., Sadiq, N., Ai, Y. (2020).** Robust watermarking algorithm for medical volume data in internet of medical things. IEEE Access, Vol. 8, pp. 93939–93961. DOI: 10.1109/ ACCESS.2020. 2995015.
38. **Liu, P., Liu, B., Sun, Y., Zhao, B., You, I. (2018).** Mitigating DoS attacks against pseudonymous authentication through puzzle-based co-authentication in 5G-VANET. IEEE Access, Vol. 6, pp. 20795–20806. DOI: 10.1109/ACCESS.2018. 2826518.
39. **Liyanage, M., Ahmed, I., Okwuibe, J., Ylianttila, M., Kabir, H., Santos, J. L., Kantola, R., Perez, O. L., Itzazelaia, M. U., De-Oca, E. M. (2017).** Enhancing security of software defined mobile networks. IEEE Access, Vol. 5, pp. 9422–9438. DOI: 10.1109/ ACCESS.2017.2701416.
40. **Zaki, R. M., Wahab, H. B. A. (2021).** 4G network security algorithms: overview. International Journal of Interactive Mobile Technologies, Vol. 15, No. 16, pp.127. DOI: 10. 3991/ijim.v15i16.24175.
41. **Kim, T. W., Pan, Y., Park, J. H. (2022).** OTP-based software-defined cloud architecture for secure dynamic routing. Computers, Materials & Continua, Vol. 71, No. 1, pp. 1035–1049. DOI: 10.32604/cmc.2022. 015546.

42. **Manikandan, S., Rahaman, M., Song, Y. L. (2022).** Active authentication protocol for IoV environment with distributed servers. Computers, Materials & Continua, Vol. 73, No. 3, pp. 5789–5808. DOI: 10.32604/cmc.2022.031490.
43. **Ming, Z., Li, X., Sun, C., Fan, Q., Wang, X., Leung, V. C. M. (2022).** Sleeping cell detection for resiliency enhancements in 5G/B5G mobile edge-cloud computing networks. ACM Transactions on Sensor Networks, Vol. 18, No. 3, pp. 1–30. DOI: 10.1145/3512893.
44. **Mohammadkhan, A., Ramakrishnan, K. K., Jain, V. A. (2020).** Cleang—improving the architecture and protocols for future cellular networks with NFV. IEEE/ACM Transactions on Networking, Vol. 28, No. 6, pp. 2559–2572. DOI: 10.1109/TNET.2020.3015946.
45. **Pedone, I., Lioy, A., Valenza, F. (2019).** Towards an efficient management and orchestration framework for virtual network security functions. Security and Communication Networks, Vol. 2019, pp. 1–11. DOI: 10.1155/2019/2425983.
46. **Qayyum, A., Ahmad, J., Boulila, W., Rubaiee, S., Arshad, Masood, F., Khan, F., Buchanan, W. J. (2020).** Chaos-based confusion and diffusion of image pixels using dynamic substitution. IEEE Access, Vol. 8, pp. 140876–140895. DOI: 10.1109/ACCESS.2020.3012912.
47. **Qin, S., Tan, Z., Zhou, F., Xu, J., Zhang, Z. (2021).** A verifiable steganography-based secret image sharing scheme in 5G networks. Security and Communication Networks, Vol. 2021, pp. 1–14. DOI: 10.1155/2021/6629726.
48. **Ranaweera, P., Jurcut, A., Liyanage, M. (2022).** MEC-enabled 5G use cases: A survey on security vulnerabilities and countermeasures. ACM Computing Surveys, Vol. 54, No. 9, pp. 1–37. DOI: 10.1145/3474552.
49. **Saha, T., Aaraj, N., Jha, N. K. (2022).** Machine learning assisted security analysis of 5G-network-connected systems. IEEE Transactions on Emerging Topics in Computing, Vol. 10, No. 4, pp. 2006–2024. DOI: 10.1109/TETC.2022.3147192.
50. **Sanchez-Gomez, J., Carrillo, D. G., Sanchez-Iborra, R., Hernández-Ramos, J. L., Granjal, J., Marin-Perez, R., Zamora-Izquierdo, M. A. (2020).** Integrating LPWAN technologies in the 5G ecosystem: A survey on security challenges and solutions. IEEE Access, Vol. 8, pp. 216437–216460. DOI: 10.1109/ACCESS.2020.3041057.
51. **Sharma, S. K., Woungang, I., Anpalagan, A., Chatzinotas, S. (2020).** Toward tactile internet in beyond 5G Era: recent advances, current issues, and future directions. IEEE Access, Vol. 8, pp. 56948–56991. DOI: 10.1109/ACCESS.2020.2980369.
52. **Shokoor, F., Shafik, W., Matinkhah, S. M.** Overview of 5G & beyond security. EAI Endorsed Transactions on Internet of Things, Vol. 8, No. 30. DOI: 10.4108/eetiot.v8i30.1624.
53. **Sun, Q., Lin, K., Si, C., Xu, Y., Li, S., Gope, P. (2022).** A Secure and anonymous communicate scheme over the internet of things. ACM Transactions on Sensor Networks, Vol. 18, No. 3, pp. 1–21. DOI: 10.1145/3508392.
54. **Tang, Z., Wang, J., Li, H., Zhang, J., Wang, J. (2021).** Cognitive covert traffic synthesis method based on generative adversarial network. Wireless Communications and Mobile Computing, Vol. 2021, pp. 1–14. DOI: 10.1155/2021/9982351.
55. **Tian, F., Zhang, P., Yan, Z. (2017).** A survey on C-RAN security. IEEE Access, Vol. 5, pp. 13372–13386. DOI: 10.1109/ACCESS.2017.2717852.
56. **Wang, Y., Miao, Z., Jiao, L. (2016).** Safeguarding the ultra-dense networks with the aid of physical layer security: A review and a case study. IEEE Access, Vol. 4, pp. 9082–9092. DOI: 10.1109/ACCESS.2016.2635698.
57. **Wu, Y., Wei, D., Feng, J. (2020).** Network attacks detection methods based on deep learning techniques: A survey. Security and Communication Networks, Vol. 2020, pp. 1–17. DOI: 10.1155/2020/8872923.
58. **Xie, L., Ding, Y., Yang, H., Wang, X. (2019).** Blockchain-based secure and trustworthy internet of things in SDN-Enabled 5G-

VANETs. IEEE Access, Vol. 7, pp, 56656–56666. DOI. 10.1109/ACCESS.2019.2913682.

59. **Xu, Y., Liu, S., Chen, Y. (2022).** On the problems and countermeasures of college students' mental health and safe work under network environment. Journal of Environmental and Public Health, Vol. 2022, pp. 1–11. DOI: 10.1155/2022/2993982.
60. **Yadav, N., Pande, S., Khamparia, A., Gupta, D. (2022).** Intrusion detection system on IoT with 5G network using deep learning. Wireless Communications and Mobile Computing, Vol. 2022, pp. 1–13. DOI: 10.1155/2022/9304689.
61. **Yan, J., Du, Z., Li, J., Yang, S., Li, J., Li, J. (2022).** A threat intelligence analysis method based on feature weighting and BERT-BiGRU for industrial internet of things. Security and Communication Networks, Vol. 2022, pp. 1–11. DOI: 10.1155/2022/7729456.
62. **Yan, Z., Qian, X., Liu, S., Deng, R. (2022).** Privacy protection in 5G positioning and location-based services based on SGX. ACM Transactions on Sensor Networks, Vol. 18, No. 3, pp. 1–19. DOI: 10.1145/3512892.
63. **Yu, Z., Liu, S., Wang, W. (2022).** Dynamic threat weight of network security communication based on multisource data analysis. Wireless Communications and Mobile Computing, Vol. 2022, pp. 1–11. DOI: 10.1155/2022/6729827.
64. **Zeng, S., Chen, Y. (2018).** Concurrently deniable group key agreement and its application to privacy-preserving VANETs. Wireless Communications and Mobile Computing, Vol. 2018, pp. 1–9. DOI: 10.1155/2018/6870742.
65. **Chirieleison, C., Montrone, A., Scrucca, L. (2020).** Event sustainability and sustainable transportation: a positive reciprocal influence. Journal of Sustainable Tourism, Vol. 28, No. 2, pp. 240–262. DOI: 10.1080/09669582.2019.1607361.
66. **Zhang, X., Zhu, X., Wang, J., Bao, W., Yang, L. T. (2022).** DANCE: distributed generative adversarial networks with communication compression. ACM Transactions on Sensor Networks, Vol. 22, No. 2, pp. 1–32. DOI: 10.1145/3458929.
67. **Zhu, J., Huo, L., Ansari, M. D., Ikbal, M. A. (2021).** Research on data security detection algorithm in Iot based on K-means. Scalable Computing: Practice and Experience, Vol. 22, No. 2, pp. 149–159. DOI: 10.12694:/scpe.v22i2.1880.
68. **Zhu, Y., Du, Z. (2021).** Research on the key technologies of network security-oriented situation prediction. Scientific Programming, Vol. 2021, pp. 1–10. DOI: 10.1155/2021/5527746.
69. **Petersen, K., Vakkalanka, S., Kuzniarz, L. (2015).** Guidelines for conducting systematic mapping studies in software engineering: An update. Information and Software Technology, Vol. 64, pp. 1–18. DOI: 10.1016/j.infsof.2015.03.007.
70. **Ramaki, A. A., Rasoolzadegan, A., Bafghi, A. G. (2018).** A systematic mapping study on intrusion alert analysis in intrusion detection systems. ACM computing surveys, Vol. 51, No. 3. DOI: 10.1145/3184898.
71. **Kitchenham, B., Brereton, P. (2013).** A systematic review of systematic review process research in software engineering. Information and software technology, Vol. 55, No. 12, pp. 2049–2075. DOI: 10.1016/j.infsof.2013.07.010.
72. **Linnenluecke, M. K., Marrone, M., Singh, A. K. (2020).** Conducting systematic literature reviews and bibliometric analyses. Australian Journal of Management, Vol. 45, No. 2, pp. 175–194. DOI: 10.1177/0312896219877678.
73. **Farooqui, M. N. I., Arshad, J., Khan, M. M. (2022).** A Layered approach to threat modeling for 5G-based systems. Electronics, Vol. 11, No. 12, pp. 1–17. DOI: 10.3390/electronics11121819.
74. **Raveendran, R., Tabet-Aoul, K. A. (2021).** A meta-integrative qualitative study on the hidden threats of smart buildings/cities and their associated impacts on humans and the environment. Buildings, Vol. 11, No. 6. DOI: 10.3390/buildings11060251.
75. **Lozano, M., Sanguino, M. (2019).** Their applications: A comprehensive analysis over

time. Sensors. https://www.mdpi.com/1424-8220/19/12/2756.

76. **Zeb, S., Mahmood, A., Hassan, S. A., Piran, M. J., Gidlund, M., Guizani, M. (2022).** Industrial digital twins at the nexus of NextG wireless networks and computational intelligence: A survey. Journal of Network and Computer Applications, Vol. 200, pp. 103309. DOI: 10.1016/j.jnca.2021.103309.
77. **Ogbodo, E. U., Abu-Mahfouz, A. M., Kurien, A. M. (2022).** A Survey on 5G and LPWAN-IoT for improved smart cities and remote area applications: From the aspect of architecture and security. Sensors, Vol. 22, No. 16. DOI: 10.3390/s22166313.
78. **Ly, A., Yao, Y. D. (2021).** A review of deep learning in 5G research: Channel coding, massive MIMO, multiple access, resource allocation, and network security. IEEE Open Journal of the Communications Society, Vol. 2, pp. 396–408. DOI: 10.1109/OJCOMS.2021.3058353.
79. **Dangi, R., Jadhav, A., Choudhary, G., Dragoni, N., Mishra, M. K., Lalwani, P. (2022).** ML-Based 5G network slicing security: A comprehensive survey. Future Internet, Vol. 14, No. 4, pp. 1–28. DOI: 10.3390/fi14040116.
80. **Ben-Henda, N. (2019).** Overview on the security in 5G phase 2. Journal of ICT, Vol. 8, No. 1, pp. 1–14. DOI: 10.13052/jicts2245-800X.811.
81. **Celik, A., Tetzner, J., Sinha, K., Matta, J. (2019).** 5G device-to-device communication security and multipath routing solutions. Applied Network Science, Vol. 4, No. 1. DOI: 10.1007/s41109-019-0220-6.
82. **Segura, D., Munilla, J., Khatib, E. J., Barco, R. (2022).** 5G early data transmission (Rel-16): Security review and open issues. IEEE Access, Vol. 10, pp. 93289–93308. DOI: 10.1109/ACCESS.2022.3203722.
83. **Olimid, R. F., Nencioni, G. (2020).** 5G network slicing: A security overview. IEEE Access, Vol. 8, pp. 99999–100009. DOI: 10.1109/ACCESS.2020.2997702.
84. **Sullivan, S., Brighente, A., Kumar, S. A. P., Conti, M. (2021).** 5G security challenges and solutions: A review by OSI layers. IEEE Access, Vol. 9, pp. 116294–116314. DOI: 10.1109/ACCESS.2021.3105396.
85. **Khan, R., Kumar, P., Jayakody, D. N. K., Liyanage, M. (2020).** A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. EEE Communications Surveys & Tutorials, Vol. 22, No. 1, pp. 196–248. DOI: 10.1109/COMST.2019.2933899.
86. **Goudarzi, A., Ghayoor, F., Waseem, M., Fahad, S., Traore, I. (2022).** A Survey on IoT-enabled smart grids: emerging, applications, challenges, and outlook. Energies, Vol. 15, No. 19. DOI: 10.3390/en15196984.
87. **Sodhro, A. H., Awad, A. I., van-de-Beek, J., Nikolakopoulos, G. (2022).** Intelligent authentication of 5G healthcare devices: A survey. Internet of Things (Netherlands), Vol. 20, pp. 100610. DOI: 10.1016/j.iot.2022.100610.
88. **Ferrag, M. A., Maglaras, L., Argyriou, A., Kosmanos, D., Janicke, H. (2018).** Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes. Journal of Network and Computer Applications, Vol. 101, pp. 55–82. DOI: 10.1016/j.jnca.2017.10.017.
89. **Gamboa-Cruzado, J., Crisóstomo-Castro, R., Vila-Buleje, J., López-Goycochea, J. (2024).** Heart attack prediction using machine learning: a comprehensive systematic review and bibliometric analysis. Journal of Theoretical and Applied Information Technology, Vol. 102, pp. 1930–1944.

Article received on 01/11/2023; accepted on 17/03/2024.
**Corresponding author is Javier Gamboa-Cruzado.*