Vol. 4, No. 2, 1-15. DOI: 10.47909/ijsmc.129

Pro-Metrics

ORIGINAL RESEARCH

Scientometric analysis of global cyber security research output based on Web of Science

Iranna M. Shettar[1], Gururaj S. Hadagali[2], Manjunath Kaddipujar[3], Shivanand D. Bulla[4], Kotrayya Agadi[5], Gireesh A. Ganjihal[6], Rudramuni Hiremath[7], Akshaykumar Dundannanavar[8], B. Ramesh Babu[9],

[1] Central Library, National Institute of Technology Warangal, India.
Email: imshettar@gmail.com. **ORCID:** https://orcid.org/0000-0002-6790-2530.
Autor correspondiente.
[2] Department of Library and Information Science (DLISC), Karnatak University, India.
[3] Raman Research Institute, India.
[4] Dr. A.V. Baliga College of Arts and Science, India.
[5] Central University of Gujarat, India.
[6] University of Horticultural Sciences, India.
[7] Department of Library and Information Centre, Shri Shankar Arts and Commerce College, India.
[8] Department of Library and Information Science (DLISC), Karnatak University, India.
[9] Department of Library and Information Science, University of Madras, India.
Faculty of Informatics, Mahasarakham University, Thailand

ABSTRACT

Objective. This study aims to analyze global cyber security research using various scientometric indicators for 25 years, from 1999 to 2023.

Design/Methodology/Approach. The study used the Web of Science international citation database to retrieve a total of 5,640 records. The records were extracted in the CSV file format and further analyzed using an MS-Excel spreadsheet, VosViewer, and Biblioshiny software..

Findings. The findings revealed that a 300% annual growth rate was recorded for the publications in 2002. The USA emerged as the top contributor (31.15%) among the countries. The authors affiliated with the State University System of Florida have more publications (107 contributions). Authors Lingfeng Wang of the University of Wisconsin-Milwaukee and Kim-Kwang Raymond Choo of the University of Texas at San Antonio have contributed the equal and highest number of (21) papers..

Originality/Value. Cyber security research helps to guardian the individual or nation's digital sovereignty, protecting it against sophisticated cyber threats and potential attacks. The discipline has become the subject of global research. This study helps cyber security experts, software or web developers, and researchers identify the primary research evidence and its impact on the research community and policymakers for evidence-based policymaking to combat invisible global threats.

Keywords: cyber security research; scientometrics; global publications; cyberspace; cybercrime; cyberattack.

Received: 15-08-2024. **Accepted:** 26-09-2024. **Published:** 01-10-2024.

How to cite: Shettar, I., Hadagali, G. S., Kaddipujar, M., Bulla, S. D., Agadi, K., Ganjihal, G. A., Hiremath, R., Dundannanavar, A., & Babu, B. R. (2024). Scientometric analysis of global cyber security research output based on Web of Science. *Iberoamerican Journal of Science Measurement and Communication; 4*(2), 1-15. DOI: 10.47909/ijsmc.129

1. INTRODUCTION

Cyberspace is one of the most important inventions of the 21st century that has influenced everyone's lives (Priyarani *et al.,* 2024). It has crossed all barriers and has changed how people talk, play games, work, shop, make friends, listen to music, watch movies, order food, pay bills, and so on. It has also made human life easier by making it comfortable. One must be very careful when dealing with the flexibility that the most incredible technology has brought. Technology is innovative, and so are fraudsters or cyber attackers. Many use this technology for cyberattacks. These cyberattacks often involve accessing, altering or destroying sensitive information, extorting money from users through ransomware, or disrupting normal business processes. Better connectivity through the World Wide Web promises large-scale progress, opening our digital societies to new vulnerabilities. Cybercrimes have no boundaries and evolve in tandem with emerging technologies.

Cybercrime is a global concern. According to the Encyclopedia of Britannica (2024), cybercrime is "the use of a computer as an instrument to further illegal ends such as committing fraud, trafficking in child pornography and intellectual property, stealing identities or violating privacy." Implementing effective cyber security measures is incredibly challenging because there are more devices than the population. Meanwhile, attackers are using emerging technologies and becoming more innovative. Cyber security needs to be more effective as many people have become victims of cyberattacks, many have lost their lives, and also many celebrities have faced challenges and become victims of deepfake videos. The National Institute of Standards and Technology (2024) defines cyberattack as "any kind of malicious activity that attempts to collect, disrupt, deny, degrade or destroy information system resources or the information itself." In their survey on cyber security, Jang-Jaccard and Nepal (2014) gave a comprehensive overview of existing security vulnerabilities. They have analyzed the new cyberattack patterns in emerging technologies and given potential future research directions in cyber security. Mahdavifar and Ghorbani (2019) conducted a survey on the application of deep learning in cyber security. Xu (2019) introduced a new concept, cyber security dynamics to achieve cyber security modeling, analysis, quantification, and management from a holistic perspective rather than a building-blocks perspective. Florackis *et al.* (2022) highlighted the cyber security risks in their study.

The objective of the study is to conduct a bibliometric analysis of cyber security global research output during 1999-2023 in relation to productivity patterns, collaboration, and their research impact.

2. RELATED WORKS

A review of relevant literature is one of the critical steps in every research. The primary goal of a literature review is to summarize the previous works in the field chosen by the researcher for analysis. As a platform for this study, some pertinent works conducted on cyber security and its related subjects are discussed here. Today, most information is shared through the Internet, and cyber security is a growing and sensitive issue. Various machine-learning techniques were used to deal with cyber security threats. Makawana and Jhaveri (2018) analyzed 149 research papers from January 2015 to December 2016 to enlighten researchers about the latest trends in this research field. They classified cited papers using implementation method, article type, publisher, and article efficiency. The study shows that the UK and Germany were the leading countries researching machine learning for cyber security. Rai *et al.* (2019) analyzed the trends in global cyber security research. The USA was the top contributing country, followed by the UK, People's Republic of China, and India. The study suggests that the Indian defense needs to focus on cyber security and plan strategically. Improving security can help eliminate significant problems in any domain. Supplementing to this view, Garg *et al.* (2019) felt that there is a need for research and development in security techniques, and they thought of stating the existing state of research through a bibliometric approach. A total of 15,591 publications related to cloud computing security were extracted from the Scopus database. The results reveal that People's Republic of China (29.84%) and India (23.86%) have earned significantly compared to Canada (15.81%), the USA, and Australia in terms of citations.

Elango *et al.* (2020) considered delineating the keywords for the emerging area as essential to enlighten the emerging technology's research path. The authors have identified a set of keywords. Keyword delineation was carried out in a phased manner. Information security, for example, protects information of any kind. In contrast, computer security is related to preserving a standalone computing machine, and cyber security is the prevention of information in cyberspace, which is an individual and international concept. Dhawan *et al.* (2021) analyzed global cyber security literature and tried to find underlying trends and developments at the international, national, institutional, and individual levels. Cyber security research recorded a growth of 46.41%, with an average of 5.05 citations per paper, and external agencies funded more than 15% of the research. The study also found that the top 10 countries contributed 76.52%, with the USA (43.75%) leading, and the other countries' contribution was in the single digits. Regarding Indian contribution, India ranked fourth in terms of research productivity, with 4.34% of the global share. Cojocaru and Cojocaru (2022) explore the level of research in cyber security in the Republic of Moldova and compare it with Eastern European countries (EEC). The study was based on the data extracted from three databases: the Web of Science (WoS), Scopus, and National Bibliometric Instrument (IBN) from the Republic of Moldova. There were 68,000 records from scientific journals and conference proceedings. The findings reveal that in 10 EEC, 441 publications on cyber security were indexed in the Scopus, and 504 publications were indexed in the WoS database. However, the publications' productivity of EEC was listed more in WoS. The authors also compared the productivity of BRICS (Brazil, Russia, India, China, and South Africa) countries in terms of cyber security, and the results reveal that Scopus had 12.2% and WoS had 16.7% of the research output of BRICS countries. The top five most productive countries from both databases were the Russian Federation, Poland, Romania, Czech Republic, and Ukraine. Further, the authors also investigated the international collaboration of the EEC on cyber security. They found that the majority of the collaborative works of the EEC were with the UK, USA, Italy, France, and Germany.

Slagarp and Haggstorm (2022) gathered publication data from cyber security conferences, tried to identify unknown patterns and trends, and introduced a new index or metric that better captures the impact of authors than current standard indices. The study identified new and growing trends in cyber security research, for example, machine learning, blockchain, and differential privacy. The study revealed that the Computer and Communications Security (CCS) conference made the highest contributions to cyber security research compared to other notable meetings. The authors have also identified other flaws in using standard metrics in the cyber security research field. They have suggested adopting the pure R-index with normalized proportional counting as the score calculation method since it considers the authors' number and order and does not discriminate against authors with few publications with many citations. Cyber security is a focus of research around the world. Hence, Loan *et al.* (2022) conducted a scientific analysis to identify global research productivity. The author used the terms "cyber security," "cyber-security," "web security," "information security," "computer security," and so on, to retrieve the required data from the database. The study reveals that the research output in cyber security during 2011-2020 has shown an increasing trend, and the peak output in 2020 (1,581) is 715% more than in 2011 (221). Globally, the best number of countries (93) contribute to cyber security research, and the highest share of research publications was by the USA (23.55%).

Ravichandran and Siva (2022) analyzed cyber security publications from the Scopus database from 2001 to 2020. A total of 14,190 research publications were found on cyber security. A maximum of 2,718 (19.15%) research publications were published in 2019; the highest citations (14,849 [14.44%]) were in 2017. The relative growth rate observed was 2.94 in 2002 and 0.46 in 2020. At the same time, the doubling time was found to be 0.24 in 2002 and 1.52 in 2020. The USA contributed to a maximum of 5,195 (41.37%) research publications. The authors have also calculated that the time series analysis in cyber security research publications in 2025 will equal 1,920 and 2,525 in 2030. Sharma *et al.* (2023) presented an extensive bibliometric analysis on cyber security and cyber forensic research publications published in WoS during 2011-2021. The

findings of the study reveal that over 2,000 cyber security- and forensics-related publications occur annually in WoS, with a large percentage (51.19%) being research papers. Institute of Electrical and Electronics Engineers (IEEE) Access publishes the most articles on cyber security and forensics (490). Computer science was the most popular research field, with the highest number of cyber security publications (6,245).

3. MATERIALS AND METHODS

The study extracted the global research publication records on cyber security from the primary bibliographic and citation database WoS for a period of 25 years, covering the years from 1999 to 2023. The search string formulated to extract the bibliographic records: *((TI=(cybersecurity OR "cyber security")) OR AK=(cybersecurity OR "cyber security")) AND PY=(1999-2023),* which is formulated using the WoS's Advanced Search Query Builder. The search string was formulated to extract the bibliographic records with the terms "cybersecurity" OR "cyber security" used in the title or author keywords. The first publication indexed on cyber security in the WoS was published in the year 1999; the period of the study was restricted from 1999 to 2023. Additionally, the secondary search output enhanced the bibliographic data with "year-wise," "data-type," "author tag," "affiliation tag," "country tag," and "source title tag," and so on, to enhance the statistics on global publication output by author-wise, organization-wise, country-wise, journal-wise, and so on. The citation data for the extracted publications were collected on March 12, 2024. The following basic indicators and science mapping tools have been employed to process and visualize the results:

- Annual growth rate (AGR): This was calculated using the mathematical formula to find the increase in the value of publications over a period of time.
- Average citations per publication: This metric is determined by dividing the total number of citations received by the total number of publications, which provides the average citations per paper (ACPP). This is an essential indicator to assess the effect and influence of study by an individual, institution, country, or journal over a period of time.
- H-index: This is the most commonly used indicator, which measures the impact of research publications by a researcher, institutions, and so on. This is determined based on the number of publications and citations. The author has "n" number of publications, cited at least "n" numbers of times; "n" is treated as the h-index of an author.
- VOSviewer: This is a free-to-download software tool for constructing and visualizing bibliometric networks. This software allows researchers to create maps based on keyword co-occurrence, citation links, or co-authorship links, enabling them to identify patterns and relationships in scientific research output.
- Biblioshiny: This is the Shiny user interface that encapsulates the core functions of the bibliometrix R-package. This provides an interactive web interface to create network maps using bibliographic coupling, co-citation, collaboration, co-occurrence analyses, and so on.

4. RESULTS AND DISCUSSION

The data have been analyzed and presented under three primary bibliometric indicators: productivity, collaboration, and impact.

4.1. Research productivity

4.1.1. Year-wise distribution of research output on cyber security

Table 1 presents the year-wise distribution according to publications and citations received on "cyber security" research. During the study period, 5,640 research papers were published between 1999 and 2023. These publications have received 93,128 citations at the rate of 16.51 ACPP and recorded 120 h-index. The highest papers were published in 2023 (21.15%), followed by 2022 (18.26%) and 2021 (16.68%), and the lowest was observed during 1999 (0.02%). Overall, 225.6 publications per year were recorded during the study period. The study also presents the AGR of the publications; the highest AGR was recorded for the publications in 2002 (300%), followed by 2007 (128.57%) and 2016 (112.05). Similarly, the lowest AGR was recorded in 2006 (–65.00%), followed by 2010 (–10.34%) and 2004 (–6.25%), indicating a decrease in the number of publications

in the respective years. The publications under study have received a total of 93,128 citations and the highest being 16,840 citations in 2020, followed by 2019 (15,510) and 2021 (12,849). However, publications in 2000 and 2001 have not received any citations. According to the ACPP, publications in 2013 achieved the highest ACPP (65.72), followed by 2012 (63.73) and 2011 (48.28). The highest h-index was recorded for the publications in 2020 (60), followed by 2019 (58) and 2018 (54). Table 1 shows a fluctuating trend in the yearly research publications on "cyber security." Figure 1 shows the chart for year-wise publications and citations received across the study period for infographic representation.

4.1.2. Distribution of research output by document types

A total of 5,640 publications on cyber security have been published in 12 different document types, presented in Table 2. The maximum number of researchers has preferred to publish their research literature on "cyber security" as "Articles" (82.48%), followed by Reviews (7.41%) and Editorials (6.3%). Similarly, research literature published as "Articles" has received the highest citations (78,616), followed by Reviews (11,864) and Editorials (1,766), and these document types have achieved the highest h-index, that is, 108, 55, and 18, respectively. However, the document type "Review" has achieved the highest ACPP (28.38), followed by Proceeding Papers (20.27) and Articles (16.90).

PY	TP	AGR (%)	TC	ACPP	h-index
1999	1	—	9	9.00	1
2000	2	100.00	0	0.00	0
2001	3	50.00	0	0.00	0
2002	12	300.00	3	0.25	1
2003	16	33.33	13	0.81	2
2004	15	−6.25	31	2.07	2
2005	20	33.33	60	3.00	4
2006	7	−65.00	67	9.57	3
2007	16	128.57	434	27.13	7
2008	21	31.25	501	23.86	6
2009	29	38.10	245	8.45	10
2010	26	−10.34	965	37.12	10
2011	29	11.54	1,400	48.28	14
2012	37	27.59	2,358	63.73	15
2013	58	56.76	3,812	65.72	24
2014	65	12.07	2,294	35.29	21
2015	83	27.69	2,315	27.89	26
2016	176	112.05	5,651	32.11	36
2017	215	22.16	7,438	34.60	47
2018	384	78.60	11,368	29.60	54
2019	531	38.28	15,510	29.21	58
2020	730	37.48	16,840	23.07	60
2021	941	28.90	12,849	13.65	49
2022	1,030	9.46	6,889	6.69	31
2023	1,193	15.83	2,076	1.74	15
Total	5,640	—	93,128	16.51	—

Table 1. Year-wise distribution of publications and citations. **Notes:** PY: publication years; TP: total publications; AGR: annual growth rate; TC: total citations; ACPP: average citations per paper.

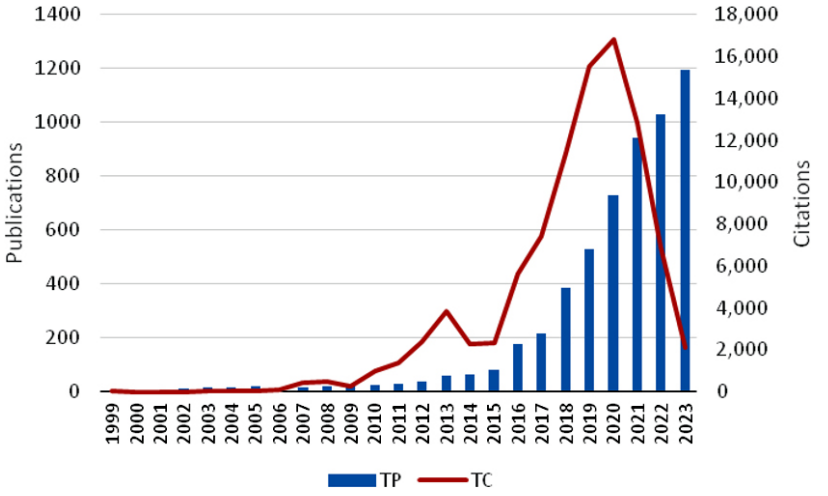

Figure 1. Year-wise distribution of research publications on cyber security and its impact. **Notes:** TP: total publications; TC: total citations.

Document types	TP	TC	ACPP	h-index
Articles	4,652	78,616	16.90	108
Reviews	418	11,864	28.38	55
Editorials	357	1,766	4.95	18
News Items	90	40	0.44	2
Proceedings Papers	37	750	20.27	16
Meeting Abstracts	22	2	0.09	1
Book Reviews	22	4	0.18	1
Letters	19	56	2.95	4
Corrections	12	0	0.00	0
Retracted Publications	8	16	2.00	2
Data Papers	2	3	1.50	1
Book Chapters	1	11	11.00	1

Table 2. Distribution of research output by document types.
Notes: TP: total publications; TC: total citations; ACPP: average citations per paper.

4.1.3. Most productive countries in the field of cyber security

Table 3 presents the list of top 10 most productive countries involved in publishing the research literature on "cyber security." It is evident from the study that 118 countries were involved in publishing the research papers under study. The USA was the top most productive country with the highest contributions (31.15%), followed by People's Republic of China (11.86%) and UK (9.01%), respectively. Similarly, the USA has received the highest number of citations (37,500), followed by People's Republic of China (14,224) and Australia (11,232). Australia has achieved the highest ACPP among the top 10 most productive countries (28.22), followed by the USA (21.34) and People's Republic of China (21.26). The USA has the highest h-index (86), followed by People's Republic of China (62) and Australia (54). Figure 2 shows a collaborative network map of countries involved in the research publications on "cyber security." Out of 118 countries, 116 have collaborations with one or more countries. These 116 collaborated countries were divided into 15 clusters with 1,152 links and 4,470 total link strengths.

Countries	TP	TC	ACPP	h-index
USA	1,757	37,500	21.34	86
People's Republic of China	669	14,224	21.26	62
UK	508	9,668	19.03	48
Saudi Arabia	411	4,248	10.34	34
Australia	398	11,232	28.22	54
India	339	5,343	15.76	37
Italy	255	4,964	19.47	33
Spain	253	3,427	13.55	30
South Korea	249	3,691	14.82	29
Canada	248	4,913	19.81	34

Table 3. Top 10 most productive countries.
Notes: TP: total publications; TC: total citations; ACPP: average citations per paper.

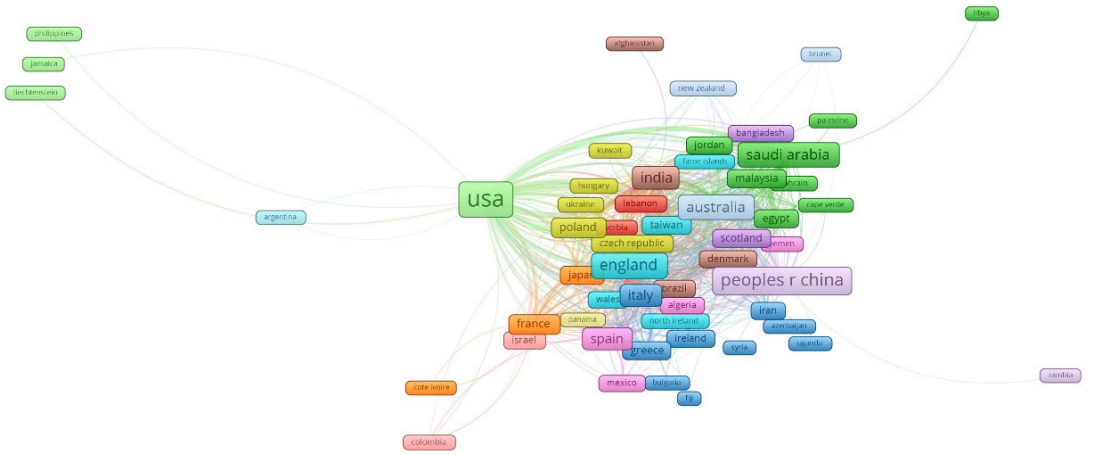

Figure 2. Co-authorship map of most productive countries in the field of cyber security.

4.1.4. Most productive organizations

A total of 4,285 organizations participated in the 5,640 research publications on "cyber security." Table 4 presents the top 10 most productive organizations involved. The authors affiliated with the State University System of Florida have published the highest research publications (107), followed by the Egyptian Knowledge Bank (EKB; 99) and the University of Texas System (93), respectively. Out of 4,285 organizations, 2,584 contributed one paper each, 1,111 contributed between two and five papers, 280 contributed between 6 and 10 papers, 206 contributed between 11 and 20 papers, 91 contributed between 21 and 50 papers, 12 contributed between 51 and 100 papers, and only one organization has contributed more than 100 papers. Among the top 10 productive organizations, the University of Texas System has received the highest citations (1,860), and the King Saud University has received the lowest citations (1,045). The Deakin University has achieved the highest ACPP (24.70), and the University of Texas System has achieved the highest h-index (22). Among the top 10 productive organizations, the EKB leads in international collaborated publications with 86 papers, followed by the University of Texas System and the King Abdulaziz University with 47 papers each. Figure 3 shows a collaborative network map of organizations involved in the research publications on "cyber security." Out of 4,285 organizations, 999 organizations with a minimum of three publications have collaborations with one or more organizations. These 999 collaborated organizations were divided into 29 clusters with 5,087 links and 6,714 total link strengths.

Affiliations	TP	TC	ACPP	h-index	ICP	TC-ICP
State University System of Florida	107	1,503	14.05	21	30	481
EKB	99	970	9.80	16	86	931
University of Texas System	93	1,860	20.00	22	47	1,157
United States Department of Energy	90	1,735	19.28	20	20	493
United States Department of Defense	80	1,370	17.13	20	10	301
Deakin University	69	1,704	24.70	21	40	891
King Abdulaziz University	68	1,045	15.37	16	47	964
King Saud University	62	687	11.08	16	46	614
University System of Georgia	60	1,455	24.25	22	21	869
University System of Ohio	60	1,275	21.25	20	13	221

Table 4. Top 10 most productive organizations.
Notes: TP: total publications; TC: total citations; ACPP: average citations per paper; ICP: international collaborative papers; TC-ICP: total citations for international collaborative papers.

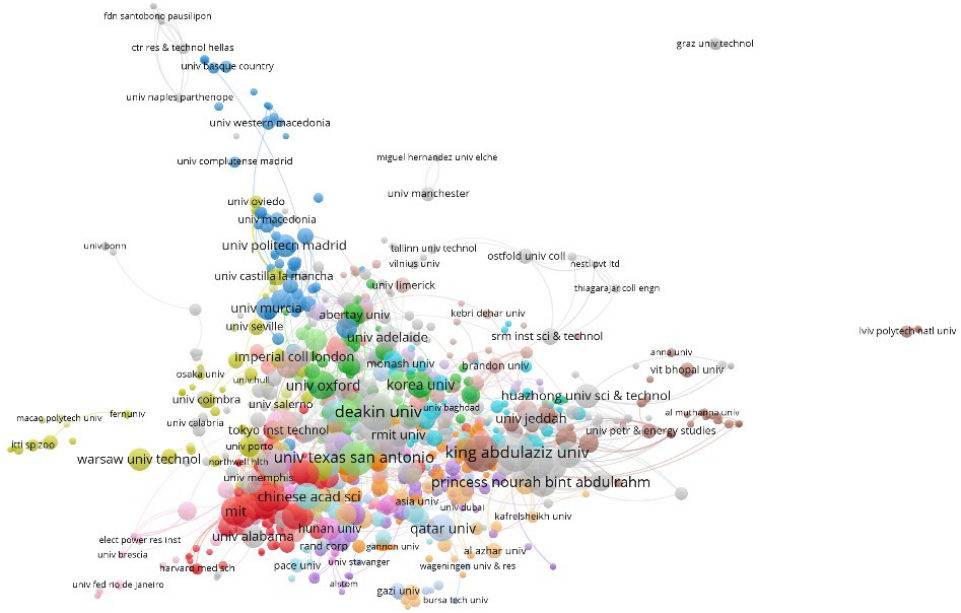

Figure 3. Co-authorship map of most productive organizations in the field of cyber security.

4.1.5. Most productive authors

A total of 13,651 authors have participated in the publications of 5,640 research papers, with an average of 2.42 authors per paper. Out of 13,651 authors, 10,472 authors have participated in a single paper, 1,822 authors in two papers, 637 authors in three papers, 308 authors in four papers, 158 authors in five papers, 207 authors in 6–10 papers, 44 authors in 11–20 papers, two authors in 21 papers, and 54 papers have published with no author, that is, Anonymous. Table 5 presents the top 10 most productive authors, where Lingfeng Wang of the University of Wisconsin-Milwaukee and Kim-Kwang Raymond Choo of the University of Texas at San Antonio (UTSA) have contributed the equal and highest number of papers (21). However, Mamoun Alazab of Charles Darwin University has received the highest citations (1,605), along with the highest ACPP (84.47). Lingfeng Wang and Mamoun Alazab have achieved the highest h-index (13). Among the top 10 most productive authors, Kim-Kwang Raymond Choo and Mamoun Alazab have the highest number of international collaborated papers (18). Of the 10 most productive authors, four are from the USA, two are from Australia, and one each from Poland, Saudi Arabia, Scotland, and Japan. Figure 4 shows a collaborative network map of authors who have contributed to the "cyber security" literature. Out of 13,651 authors, 1,137 authors with a minimum of three publications have collaborations with one or more authors. Five hundred ninety-five collaborated authors were divided into 28 clusters with 2,835 links and 4,194 total link strengths.

4.1.6. Most preferred publication sources

In this study, 5,640 research publications were published across 1,034 publication titles. Of these, 487 journals have published one research paper each, 356 journals have published two to five papers each, 104 journals have published 6-10 papers each, 57 journals have published 11-25 papers each, 17 journals have published 26-50 papers each, seven journals have published 51-100 papers each, and six journals have published 101-409 papers each. Table 6 lists the top 10 most preferred journals by the researchers. Among the publication titles, *IEEE Access* has published the highest papers (409), followed by *Computers & Security* (284) and *Sensors* (206). Among the journals, *IEEE Access* has received the highest citations (7,603), followed by *Computers & Security* (6,079) and *IEEE Transactions on Smart Grid* (5,896). Of the top 10 most preferred journals, *IEEE Transactions on Smart Grid* has achieved the

Author	Affiliation	TP	TC	ACPP	h-index	ICP	TC-ICP
Lingfeng Wang	University of Wisconsin-Milwaukee, USA	21	931	44.33	13	2	110
Kim-Kwang Raymond Choo	UTSA, USA	21	626	29.81	10	18	470
Michal Choras	Bydgoszcz University of Science & Technology, Poland	20	233	11.65	9	7	142
S. M. Suhail Hussain	King Fahd University of Petroleum & Minerals, Saudi Arabia	19	383	20.16	12	17	65
Mamoun Alazab	Charles Darwin University, Australia	19	1,605	84.47	13	18	1,525
Shouhuai Xu	University of Colorado at Colorado Springs, USA	18	321	17.83	9	11	126
Karen V. Renaud	University of Strathclyde, Scotland	18	168	9.33	7	16	167
Adnan Anwar	Deakin University, Australia	17	520	30.59	10	11	237
Taha Selim Ustun	National Institute of Advanced Industrial Science and Technology (AIST), Japan	17	378	22.24	12	14	360
Ramesh Karri	New York University, USA	16	519	32.44	9	7	288

Table 5. Top 10 most productive authors.
Notes: TP: total publications; TC: total citations; ACPP: average citations per paper; ICP: international collaborative papers; TC-ICP: total citations for international collaborative papers.

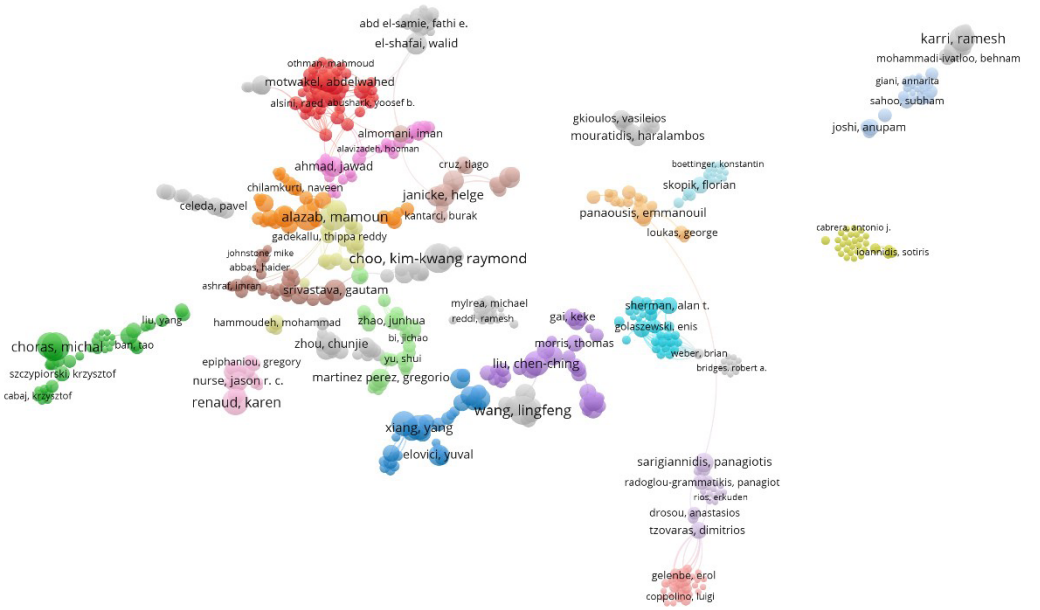

Figure 4. Co-authorship map of most productive authors in the field of cyber security.

highest ACPP (51.27), followed by *IEEE Transactions on Industrial Informatics* (31.82) and *Computers & Security* (21.40). However, *IEEE Security & Privacy* has achieved the highest h-index (51), followed by *IEEE Transactions on Smart Grid* (45) and *IEEE Access* (41). Among the top 10 most preferred publications listed, *IEEE Transactions on Industrial Informatics* has the highest impact factor (12.3). Multidisciplinary Digital Publishing Institute (MDPI) published five journals, and IEEE published four journals, whereas Elsevier has published one journal. Figure 5 presents an overlay visualization map of the publication titles of published literature on "cyber security," which shows developments over time and indicates the researchers' preference for journals across the study period.

Publication titles	IF-2023	Publisher	TP	TC	ACPP	h-index
IEEE Access	3.9	IEEE	409	7,603	18.59	41
Computers & Security	5.6	Elsevier	284	6,079	21.40	40
Sensors	3.9	MDPI	206	1,976	9.59	23
Applied Sciences—Basel	2.7	MDPI	174	1,535	8.82	19
Electronics	2.9	MDPI	145	1,514	10.44	22
IEEE Transactions on Smart Grid	9.6	IEEE	115	5,896	51.27	45
IEEE Security & Privacy	1.9	IEEE	98	751	7.66	51
Energies	3.2	MDPI	78	1,002	12.85	16
IEEE Transactions on Industrial Informatics	12.3	IEEE	62	1,973	31.82	24
Sustainability	3.9	MDPI	54	330	6.11	10

Table 6. Top 10 most preferred journals. **Notes:** IF-2023, impact factor of journal for the year 2023; TP: total publications; TC: total citations; ACPP: average citations per paper.

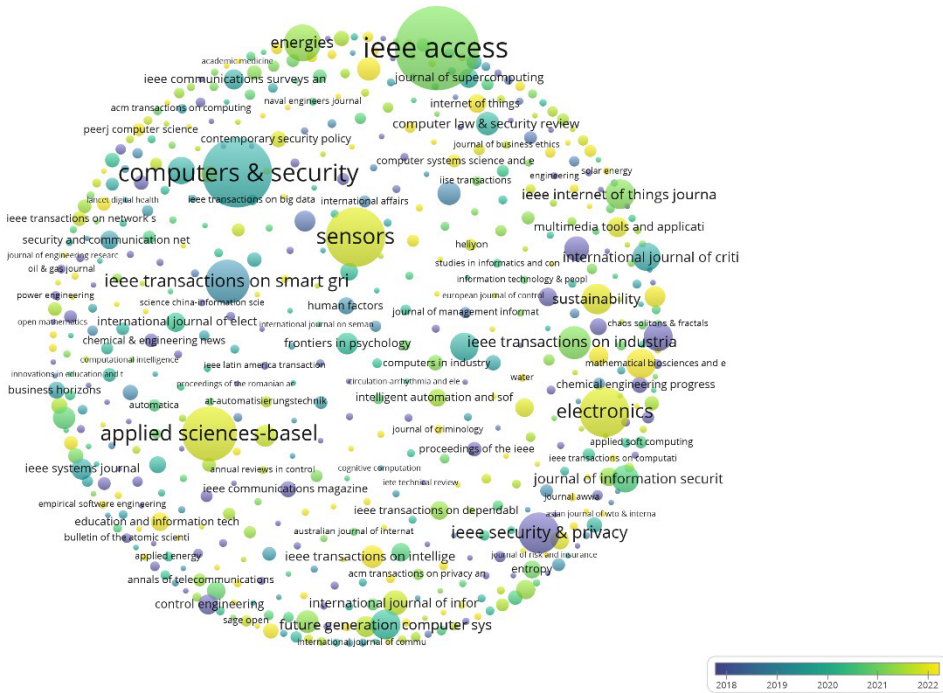

Figure 5. Overlay visualizations map of publication sources.

4.2. Research collaboration

4.2.1. Collaboration among the top 10 most productive countries

Table 7 presents the analysis of collaborative linkages among the top 10 most productive countries, and these countries have a high rate of collaborations, ranging from 1 to 149 research publications. Among the top 10 countries, the USA has the highest international collaborated publications (576), followed by People's Republic of China (364) and UK (300). However, Saudi Arabia has the highest share of publications (71.78%), followed by Australia (63.32%) and UK (59.06%). Australia has achieved the highest ACPP (28.62). Among the top 10 productive countries, the USA and People's Republic of China have the highest collaborated research publications (149), and the lowest collaboration was observed for Saudi Arabia and Spain, with only one publication.

Countries	TP	ICP	%ICP	TC-ICP	ACPP	CL	TCL
USA	1,757	576	32.78	15,094	26.20	2(149), 3(52), 4(48), 5(61), 6(43), 7(36), 8(12), 9(29), 10(54)	484
People's Republic of China	669	364	54.41	9,976	27.41	1(149), 3(49), 4(30), 5(65), 6(17), 7(10), 8(5), 9(23), 10(31)	379
UK	508	300	59.06	6,685	22.28	1(52), 2(49), 4(27), 5(26), 6(9), 7(33), 8(24), 9(15), 10(12)	247
Saudi Arabia	411	295	71.78	3,521	11.94	1(48), 2(30), 3(27), 5(35), 6(53), 7(2), 8(1), 9(18), 10(14)	228
Australia	398	252	63.32	7,211	28.62	1(61), 2(65), 3(26), 4(35), 6(22), 7(6), 8(3), 9(15), 10(14)	247
India	339	188	55.46	3,685	19.60	1(43), 2(17), 3(9), 4(53), 5(22), 7(5), 8(5), 9(13), 10(6)	173
Italy	255	138	54.12	3,088	22.38	1(36), 2(10), 3(33), 4(2), 5(6), 6(5), 8(19), 9(9), 10(6)	126
Spain	253	111	43.87	1,670	15.05	1(12), 2(5), 3(24), 4(1), 5(3), 6(5), 7(19), 9(4), 10(4)	77
South Korea	249	111	44.58	2,292	20.65	1(29), 2(23), 3(15), 4(18), 5(15), 6(13), 7(9), 8(4), 10(7)	133
Canada	248	146	58.87	3,353	22.97	1(54), 2(31), 3(12), 4(14), 5(14), 6(6), 7(6), 8(4), 9(7)	148

Table 7. Collaborative linkages among the top 10 most productive countries.
Notes: TP: total publications; ICP: international collaborative papers; %ICP: percentage of international collaborative papers; TC-ICP: total citations for international collaborative papers; ACPP: average citations per paper; CL: collaborative linkages; TCL: total collaborative linkages.

4.2.2. Collaboration among the most productive countries

The study found that a total of 118 countries were involved in publishing research papers on cyber security, and among them, 116 have collaborations with one or more countries. Only Costa Rica and Malta have no collaborated research publications with other countries. However, both countries have published only one research paper on cyber security. Figure 6 shows an international collaborative network map of countries involved in the research publications on "cyber security." All the 116 collaborated countries were divided into 15 clusters with 1,152 links and 4,470 total link strengths. The line between the country nodes indicates the collaboration between those countries, and thickness indicates the volume of collaborative research publications.

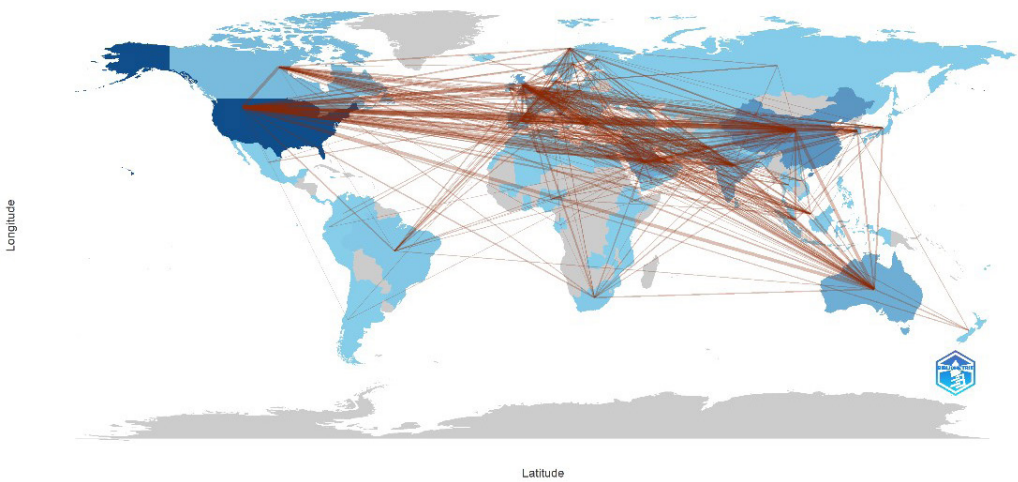

Figure 6. International collaboration map of countries in the field of cyber security.

4.2.3. Collaboration among the top 10 most productive organizations

Table 8 presents the collaboration among the top 10 productive organizations. Among the top 10 most productive organizations, the State University System of Florida has collaborations with the seven organizations listed, followed by the University of Texas System and the University System of Georgia, which have collaborations with six organizations listed as the top 10 productive organizations. However, the EKB has the highest number of total collaborated linkages (21), followed by the State University System of Florida (20) and the University of Texas System (16). The maximum number of collaborations was observed between the EKB and the King Abdulaziz University with 11 publications, followed by collaborations between the EKB and the King Saud University with eight publications together. Of these top 10 productive organizations, six organizations are in the USA, followed by Saudi Arabia (two), and one each in Australia and Egypt. Figure 7 shows a collaborative network map of the top 10 most productive organizations involved in the research publications on "cyber security." Out of 10 organizations, collaboration between each other varies from two to seven organizations. These top 10 most productive organizations were divided into three clusters with 21 links and 64 total link strengths.

Affiliations	City	TP	CL	TCL
State University System of Florida	Florida, USA	107	2(1), 3(3), 4(3), 5(5), 6(1), 9(4), 10(3)	20
Egyptian Knowledge Bank	Cairo, Egypt	99	1(1), 7(11), 8(8), 9(1)	21
University of Texas System	Austin, USA	93	1(3), 4(3), 5(2), 6(3), 8(1), 9(4)	16
United States Department of Energy Doe	Washington, USA	90	1(3), 3(3), 9(4), 10(3)	13
United States Department of Defense	Washington, USA	80	1(5), 3(2),	7
Deakin University	Victoria, Australia	69	1(1), 3(3), 8(2), 9(1)	7
King Abdulaziz University	Jeddah, Saudi Arabia	68	2(11), 8(1)	12
King Saud University	Riyadh, Saudi Arabia	62	2(8), 3(1), 6(2), 7(1)	12
University System of Georgia	Georgia, USA	60	1(4), 2(1), 3(4), 4(4), 6(1), 10(1)	15
University System of Ohio	Athens, USA	60	1(3), 4(3), 9(1)	7

Table 8. Collaboration among the top 10 productive organizations.
Notes: TP: total publications; CL: collaborative linkages; TCL: total collaborative linkages.

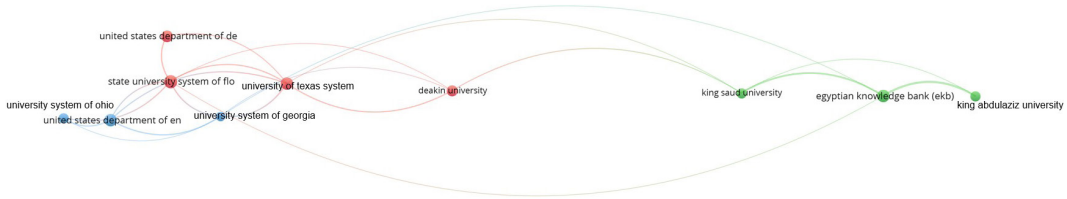

Figure 7. Co-authorship map within the top 10 most productive organizations.

4.3. Research impact

4.3.1. Most impactful organizations

The organizations with at least 10 publications were analyzed on their research impact (citations per paper), and the top 10 among them were presented in Table 9. Only three organizations ranked among the top 10 productive organizations made their place in the list of top 10 impactful organizations, such as the Deakin University, the University System of Georgia, and the University System of Ohio. Among the top 10 impactful organizations, the Pennsylvania Commonwealth System of Higher Education (PCSHE) has achieved the highest ACPP (45.52), followed by the Massachusetts Institute of Technology (MIT; 34.07)

and the University of New South Wales Sydney (34.02). The University System of Georgia has achieved the highest h-index (22), followed by the Deakin University (21) and the University System of Ohio (20). Among these top 10 impactful organizations, the Deakin University has the highest international collaborated paper (40), followed by the UTSA (34) and the University of New South Wales Sydney (26).

Affiliation	TP	TC	ACPP	h-index	ICP	TC-ICP
PCSHE	46	2,094	45.52	15	17	479
MIT	41	1,397	34.07	16	17	879
University of New South Wales Sydney	46	1,565	34.02	17	26	834
Carnegie Mellon University	41	1,295	31.59	13	12	111
Chinese Academy of Sciences	41	1,092	26.63	17	21	839
Deakin University	69	1,704	24.70	21	40	891
University System of Georgia	60	1,455	24.25	22	21	869
UTSA	57	1,299	22.79	18	34	796
University System of Maryland	40	865	21.63	13	5	402
University System of Ohio	60	1,275	21.25	20	13	221

Table 9. Top 10 most impactful organizations.
Notes: TP: total publications; TC: total citations; ACPP: average citations per paper; ICP: international collaborative papers; TC-ICP: total citations for international collaborative papers.

4.3.2. Most impactful authors

The authors have analyzed the ACPP of authors having 10 or more publications. Table 10 presents the top 10 impactful authors based on the ACPP. Only two authors who were listed as the most productive authors have found a place in the list of most impactful authors, that is, Mamoun Alazab and Lingfeng Wang. Among the top 10 impactful authors, Chen-Ching Liu of the Virginia Polytechnic Institute & the State University has achieved the highest ACPP (110.25), followed by Chee-Wooi Ten (104.00) and Mamoun Alazab (84.47), and these authors have published 12, 10, and 19 papers, respectively. The author, Mamoun Alazab has received the highest citations (1,605) among the most impactful authors, followed by Chen-Ching Liu (1,323) and Chee-Wooi Ten (1,040).

Author	Affiliation	TP	TC	ACPP	h-index	ICP	TC-ICP
Chen-Ching Liu	Virginia Polytechnic Institute & State University, USA	12	1,323	110.25	11	9	897
Chee-Wooi Ten	Michigan Technological University, USA	10	1,040	104.00	9	4	431
Mamoun Alazab	Charles Darwin University, Australia	19	1,605	84.47	13	18	1,525
Vinayakumar Ravi	Prince Mohammad Bin Fahd University, Saudi Arabia	12	878	73.17	7	11	878
Mohamed Amine Ferrag	University of Guelma, Algeria	10	725	72.50	8	10	725
Leandros Maglaras	De Montfort University, UK	13	819	63.00	9	9	745
Helge Janicke	Edith Cowan University, Australia	13	813	62.54	9	8	692
Hideaki Ishii	Tokyo Institute of Technology, Japan	13	800	61.54	10	6	307
Yang Xiang	Swinburne University of Technology, Australia	10	482	48.20	7	2	225
Lingfeng Wang	University of Wisconsin-Milwaukee, USA	21	931	44.33	13	2	110

Table 10. Top 10 most impactful authors.
Notes: TP: total publications; TC: total citations; ACPP: average citations per paper; ICP: international collaborative papers; TC-ICP: total citations for international collaborative papers.

5. SUMMARY OF FINDINGS AND IMPLICATIONS FOR FURTHER RESEARCH

Cyber security has become a crucial element for the sustainable development across the globe and collaborative compendium among countries. Cyber security research is a fast-growing research area, which includes different prospects of cyber security, such as computer security, network security, information security, IoT security, phishing, and data breaches. Cyber security research helps to guardian the individual or nation's digital sovereignty, protecting it against sophisticated cyber threats and potential attacks. Hence, cyber security research becomes a subject of global interest. However, 90% of the research publications were published by the top 10 most productive countries. Among the top 10 countries, the USA is dominant in the research productivity on "cyber security" with 31.15% of world shares, followed by People's Republic of China (11.86%), and the other's individual world shares are in the single digits only. According to IMF's *World Economic Outlook Database* (2024), of these top 10 most productive countries, six countries were listed among the top 10 countries with the highest gross domestic product (GDP), nine were among the top 15 countries with the highest GDP, and all are listed in the top 20 countries with the highest GDP. According to the World Cybercrime Index by Bruce *et al.* (2024), "Cybercrime is a major challenge facing the world with estimated costs ranging from the hundreds of millions to the trillions. Despite the threat it poses, cybercrime is somewhat an invisible phenomenon," and out of the top 10 most productive countries involved in the "cyber security" research, eight were listed in the top 50 countries by World Cybercrime Index score. Hence, this study helps cyber security experts, software or web developers, and researchers identify the primary research evidence and its impact on the research community and also helps the policymakers for evidence-based policymaking to combat invisible global threats.

Conflict of interests

The authors declare that there are no conflicts of interest.

Contribution statement

Iranna M. Shettar: Conceptualization, resources, formal analysis, investigation, software, visualization, writing – original draft

Gururaj S. Hadagali: Conceptualization, writing – review & editing, project administration

Manjunath Kaddipujar: Resources, data curation, methodology, writing – original draft

Shivanand D. Bulla: Project administration

Kotrayya Agadi and Gireesh A. Ganjihal: Validation

Rudramuni Hiremath and Akshaykumar Dundannanavar: Methodology

B. Ramesh Babu: Writing – review & editing

Statement of data consent

The data generated during the development of this study has been included in the manuscript.

REFERENCES

Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLOS ONE, 19*(4), Article e0297312. https://doi.org/10.1371/journal.pone.0297312

Cojocaru, I., & Cojocaru, I. (2022). A bibliomeric analysis of cybersecurity research papers in Eastern Europe: Case study from the Republic of Moldova. *Central and Eastern European eDem and eGov Days, 335,* 151-162. https://doi.org/10.24989/ocg.v335.12

Dhawan, S. M., Gupta, B. M., & Elango, B. (2021). Global cyber security research output (1998-2019): A scientometric analysis. *Science & Technology Libraries, 40*(2), 172-189. https://doi.org/10.1080/0194262X.2020.1840487

Elango, B., Matilda, S., & Jeyasankari, J. (2020, June 2020). Redefining search terms for cybersecurity: A bibliometric perspective. In: *Proceedings of the international conference on recent advances in computational techniques (IC-RACT) 2020.* https://dx.doi.org/10.2139/ssrn.3688394

Encyclopedia of Britannica. (2024). *Cybercrime*. https://www.britannica.com/topic/cybercrime

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2022). Cybersecurity risk. *The Review of Financial Studies, 36*(1), 351-407. https://doi.org/10.1093/rfs/hhac024

Garg, D., Sidhu, J., & Rani, S. (2019). Emerging trends in cloud computing security: A bibliometric analyses. *IET Software, 13*(3), 223-231. https://doi.org/10.1049/iet-sen.2018.5222

Loan, F. A., Bisma, B., & Nahida, N. (2022). Global research productivity in cybersecurity: A scientometric study. Global Knowledge, *Memory and Communication, 71*(4/5), 342-354. https://doi.org/10.1108/GKMC-09-2020-0148

Mahdavifar, S., & Ghorbani, A. A. (2019). Application of deep learning to cybersecurity: A survey. *Neurocomputing, 347,* 149-176. https://doi.org/10.1016/j.neucom.2019.02.056

Makawana, P. R., & Jhaveri, R. H. (2018). A bibliometric analysis of recent research on machine learning for cyber security. In Y.-C. Hu, S. Tiwari, K. K. Mishra, & M. C. Trivedi (Eds.), *Intelligent communication and computational technologies* (Vol. 19, pp. 213-226). Springer Singapore. https://doi.org/10.1007/978-981-10-5523-2_20

National Institute of Standards and Technology. (2024). *Cyber attack*. https://www.nist.gov/cybersecurity

Priyarani, A. G., Priyanka, R., Priyanka, V. K., Rachana, N., & Naik, C. (2024). Operational security, safe quantum, space communications and data privacy cyber security. *International Journal of Networks and Systems, 13*(2), 66-71. https://doi.org/10.30534/ijns/2024/011322024

Rai, S., Singh, K., & Varma, A. K. (2019). Global research trend on cyber security: A scientometric analysis. *Library Philosophy and Practice (e-Journal),* 3769. https://digitalcommons.unl.edu/libphilprac/3769

Ravichandran, S., & Siva, N. (2022). Scientometric analysis of cybersecurity in global research from Scopus database during the periods 2001-2020. *International Journal of Development Research, 12*(3), Article 54328. https://doi.org/10.37118/ijdr.23978.03.2022

Sharma, D., Mittal, R., Sekhar, R., Shah, P., & Renz, M. (2023). A bibliometric analysis of cyber security and cyber forensics research. *Results in Control and Optimization, 10,* Article 100204. https://doi.org/10.1016/j.rico.2023.100204

Slagarp, J., & Haggstorm, E. (2022). *Trends and scientometrics in cyber security research*. KTH Royal Institute of Technology.

Xu, S. (2019). Cybersecurity dynamics: A foundation for the science of cybersecurity. In C. Wang & Z. Lu (Eds.), *Proactive and dynamic network defense* (Vol. 74, pp. 1-31). Springer International Publishing. https://doi.org/10.1007/978-3-030-10597-6_1