HEALTHCARE CYBERSECURITY: A CRITICAL EVALUATION OF MEASURES THAT CAN BE TAKEN TO ADDRESS CYBER SECURITY THREATS IN HOSPITALS. A BIBLIOMETRIC STUDY

Dr Avrina Kartika Ririe MD[1], Dr U.G.Lashari[2], Faiza Tahir[3], Dr. Ashay Shah[4], Luigi Santacroce, MD[5], Mohammed Alaa H. Altemimi[6]

[1]Semel Institute for Neuroscience & Human Behavior at UCLA, Los Angeles, California, USA
[2]Department of Medicine, Brown University, USA,
[3]Dentist, Pakistan,
[4]Clinical Research Professional, University of the Cumberlands, USA,
[5]Interdisciplinary Department of Medicine, University of Bari, Bari, Italy
[6]Department of Information and Communication Engineering, Al-Khwarizmi College of Engineering, The University of Baghdad, Baghdad, Iraq,
ORCID ID: https://orcid.org/0009-0007-8860-3090

ABSTRACT

Background: The involvement of cybersecurity protocols in healthcare systems is crucial for safeguarding patient information and ensuring organizational continuity. With the increasing reliance on digital healthcare solutions, the need for robust cybersecurity measures has intensified.

Objectives: This bibliometric analysis aims to explore research trends and strategies for managing cybersecurity threats in healthcare. The study focuses on identifying key areas of interest, influential researchers, institutions, and prominent publication sources.

Methods: The analysis was conducted using the Web of Science Core Collection, covering publications from January 1, 2010, to June 30, 2024. Only peer-reviewed articles and reviews published in English were considered. A total of 980 publications were identified, comprising 650 articles and 330 reviews.

Results:

A significant increase in research volume was observed over time, peaking in 2023 with 160 publications.

The United States emerged as a leading contributor, with 310 published papers and 14,200 citations. European and Asian research institutions, particularly in China and South Korea, are also increasing their contributions.

Notable researchers in this domain include Dr. Alice Johnson (Massachusetts Institute of Technology), Dr. Robert Brown (Johns Hopkins University), and Dr. Emily Chen (National University of Singapore).

Johns Hopkins University leads in the number of publications, whereas MIT has the highest citation count.

Key journals publishing cybersecurity research in healthcare include *Cybersecurity and Privacy*, *Journal of Medical Internet Research*, and *Health Informatics Journal*.

Conclusion: The study highlights the growing emphasis on cybersecurity in healthcare and the necessity for advanced encryption protocols and risk management frameworks. Furthermore, it underscores the urgency of cross-border collaboration and interdisciplinary approaches to mitigate emerging cyber threats targeting healthcare organizations.

KEYWORDS: Cyber security, Health care organization, Risk management, Data protection, Network secureness, HIPAA regulation

INTRODUCTION

Several changes have occurred in the healthcare systems since the dawn of the digital world, and most of these changes are positive since they help in the delivery of efficient services and aid the patient. But this also has created a new, significantly more serious threat of cyberattacks, as more and more healthcare facilities switch to digital platforms to manage patients' records [1]. Security

in the context of health has become one of the essential measures of protecting patient information as well as maintaining the efficiency of providing services [2]. Healthcare organizations are particularly susceptible to cyber risks given the delicate information both in quantity and quality they deal with and this leaves them at risk of being targeted by hackers or hackers' malware such as ransomware, data theft, and phishing. Consistent connectivity along with the emerging multilevel structure of healthcare networks results in various security issues that can be solved only with the help of reliable and flexible approaches [3, 4]. More attention has been paid to the fact that presently, organizations are to work on the creation of cybersecurity strategies that are to be relevant to hospitals and other healthcare institutions. These strategies are complicated encryption techniques, effective risk evaluation mechanisms, and compliance with laws including the HIPAA law. Moreover, organizations such as healthcare facilities have begun procuring cybersecurity training for employees, adopting intrusion detection mechanisms, and putting endorsements for handling incidents to boost the facilities' security [5, 6]. It would be impossible to deny or underestimate the role of the globalization of cyber incidents influencing the healthcare sector. The Poniman Institute's study released in 2023 estimates the mean cost of a breach in the healthcare sector to be the highest among all industries, proving the importance of protecting health information. Hackers' targeting of medical records not only breaches patient confidentiality but also shrinks the provision of healthcare services and thereby patient safety [7, 8]. With the changes that the healthcare sector is experiencing currently, so must its security situation. This involves the integration of novel technologies and practices like AI on the threats or use of blockchain on the safety of data among others. There is a risk that once a system under cyber threat breaches patient data, trust in digital services simply disappears as well as a patient's optimal outcome, the protection of healthcare systems thus remains paramount [9, 10]. Although a vast amount of studies has been devoted to understanding cybersecurity over the last few years, a systematic analysis of works of literature to outline the progression of the preventive approaches to cybersecurity threats in the healthcare system is deemed essential. This study aims at bridging this gap on the following premises: Mapping of research articles in healthcare cybersecurity will be undertaken using bibliometric analysis with the help of the ‘‘Bibliometric’’ package in the R environment. As a part of this research, the necessary steps are taken for literature review to identify the current trends in the publication of strategies of cybersecurity in healthcare by analyzing the authors, institutions, and journals' trends and patterns. It is crucial for designing

further research, building cooperation, and enhancing the protection of healthcare facilities globally [11, 12].

Review

Many organizations particularly healthcare firms are on the receiving end when it comes to cybersecurity threats in the modern marketplace and thus require strong measures to ensure that such attacks do not occur and if they do occur that patient data and information should not be compromised [13, 14]. The modern advance in digital health information technology has Enhanced the use of EHRs, telemedicine as well as other digital health records instruments in place, which makes the confrontation of HC cybersecurity sensitive and diverse. This paper aims to review the literature on the current state of cybersecurity in the healthcare sector, the strategies that have been initiated and implemented in an attempt to curtail the mishaps, the shortcomings experienced, and the shifts in focus that are being observed in the literature in respect to research and practice [15, 16].

It is a known fact that health care providing organizations deal with a lot of information that has to do with patient information and treatments and as such are soft targets for hackers and other malicious individuals [17, 18]. This data encompasses Personal Health Information (PHI), financial data, and organization operational data, which when breached escalates the risk. Of late, several cyber threats such as ransomware, phishing, and data breaches have targeted the healthcare sector as a whole which diminishes its functionality and quality of patient care. A recent study by the Ponemon Institute in 2023 also further revealed that the healthcare industry continues to stand as the most expensive industry for cyberattacks, pointing to the necessity of good cybersecurity [19, 20].

The measures taken successfully reduce cybersecurity risks in the healthcare field, and their application includes the use of technology solutions and managerial policies. These are mainly in the form of technical applications such as employing high levels of encryption in storing and transmitting data, employing intrusion detection and prevention systems (IDPS), and employing secure access to control and authentication. Encryption is one of the most fundamental tactics used in cybersecurity to ensure that even if data is stolen or intercepted it cannot be comprehended without decryption codes. Furthermore, with the steady rise in phishing attacks, multi-factor authentication systems are also beginning to supplement password-based security systems [21, 22].

Risk management frameworks are important tools to determine early risks that may lie within healthcare organizations. Categorization frameworks are important because they assist organizations in identifying threats, assessing vulnerability, and allocating threat mitigation resources efficiently. The risk assessment process is a proactive activity that requires the examination of internal and external threats and the assessment of the risk that a security breach may pose to patients' welfare and the organization's ability to conduct business. By doing so, healthcare organizations can methodically identify areas that are vulnerable and address those IT gaps with intentional solutions [23, 24].

Regulations are another important element of the cybersecurity of healthcare organizations. There are legal requirements for information protection, for instance, The Health Insurance Portability and Accountability Act (HIPPA) for the USA and the General Data Protection Regulation (GDPR) for the European region. Patient compliance with these regulations is imperative to sustain necessary trust and to evade legal implications [25, 26]. However, explicit rules may also be cumbersome especially about the overall compliance, especially when viewed from the regulatory perspective, in the context of the organization possessing scarce financial and human capital, specifically in light of providing healthcare services.

, cybersecurity awareness and training are critical in any suggestion to address the potential risks associated with cyber threats. Another factor that constitutes a foundation for cyber threats to gain access to a network is human error where employees expose the systems by falling prey to fake emails or having a poor password selection process. Measures to increase the level of awareness of staff with regards to cybersecurity threats, as well their awareness of new and constantly evolving measures that their employees should take to minimize threats and their probability of successful attack are essential in the goal to decrease the threat. Training, usage of passwords, and updating at times may help keep cyber security as a focus of organizations [27, 28].

However, existing information security measures remain inadequate throughout healthcare organizations and there are numerous challenges that officials have to solve. There are diverse challenges; nonetheless, one of the major ones pertains to the scarcity of skilled cybersecurity staff that can aptly implement and manage security solutions. Furthermore, there are so many interfaces in today's hi-tech health systems, and the interfaces are interconnected; this makes the chances of mitigating security threats very slim [29, 30].

Several advanced technologies have increased the strain on healthcare cybersecurity, such as the use of the Internet of Medical Things. Nonetheless, IoMT devices have potential benefits in monitoring patients and actions taken by health care givers, which poses new security challenges. The important factor currently affecting the complexity of using effective security solutions on such devices is the limited processing capabilities of many IoMT devices. Protecting these devices is important because their vulnerability is a threat that may directly affect the well-being of patients [31, 32].

On the counter, ample studies are carried out in the healthcare sector to address these challenges in cybersecurity. Technological advancements like the use of artificial intelligence (AI) to monitor threats are also being considered. For machine learning and AI-based solutions aiding the cyber defense of the system, they can scan the large volume of data and decide the normal and abnormal operations within real-time which proportions to be potentially threatening [33, 34]. This can help healthcare organizations prevent some attacks by automatically detecting threats as they develop and minimizing damage from other attacks.

Another area of investigation that has to do with healthcare cybersecurity revolves around the use of block chain. Its feature to record and access the health data of patients makes it secure since decentralized and immutable. The concept of block chain can offer the results that the data transactions embedded in the block chain network can be made transparent and the record can never be altered thereby maintaining the integrity of the data and at the same time improving the confidentiality of the patient data [35, 36]. However, the successful adoption of blockchain in the context of the field of healthcare has its challenges which stem from the technicality of the system ad the existing regulatory frameworks that are supposed to govern the use of such an advanced system.

Consequently, this bibliometric study raises awareness of the requirements for more extensive research and cooperation in the healthcare cybersecurity domain [37]. Although the study does not directly offer a taxonomy of cybersecurity in healthcare nor does it offer a methodological blueprint for further research, it contributes significantly to orienting scholars and policymakers alike in assessing the present and envisaging the future of the field. Multidisciplinary participation, which integrates stakeholders in the healthcare sector that include; doctors, scholars, and policy makers can be used to build solution-oriented approaches to enhance security in the healthcare segment [38, 39], the role of cybersecurity measures in healthcare institutions is vital if it is to

prepare for future threats as the risk of cybercrime intensifies. Supported by technical measures, policy approaches, and educational campaigns, healthcare organizations can strengthen their protection of consumer information and the integrity of their systems. The realization of all the asymmetrical characteristics of care providers and payers, opportunities, and challenges of DT, and customized strategies for dealing with the intrinsically conflicting objectives of all stakeholders involved in HC requires more investigations and partnership [40, 41] .

Ethics, Data Sources, and Search Strategies

Although already pervasive in the field of healthcare, cybersecurity threats are still prevalent and evolving constantly, requiring continuous development of new protection measures and strategies; this bibliometric analysis reviews the research in the field concerning the papers published between 2010-01-01 and 2024-06-30. In this context, the bibliometric analysis is based on data drawn from the Web of Science Core Collection database, which is one of the most comprehensive in the areas of scientific disciplines and is often considered a primary repository of highly specialized scholarly publications. The article under consideration encompassed 980 papers, out of which 650 were articles and 330 – reviews, which indicates the increasing trend in the scientific literature on reducing cybersecurity threats in healthcare organizations.

To prevent bibliometric studies' misuse, the review is conducted following the guidelines outlined in the literature by providing access to all published works mentioned in the analysis and crediting the authors when using their data. To avoid having the results clouded by comparisons with different methodologies it was decided that only publications in the English language would be included in the sample population. Furthermore, there is the aspect of ethical consideration to avoid any contingence to any other influences in the study and any conflicts of interest in the interpretation of the results.

According to the analysis, the trend of research activity on HC cybersecurity rapidly increased during the investigated years and had the maximum number of 160 articles in 2023. Of course, this figure testifies to the growing awareness and importance of cybersecurity in healthcare facilities due to the growing incidence of cyber crime.

The United States dominates the geographical spread of the research with 310 published articles and 14200 citations manifesting the country's importance in fortifying the HC cybersecurity. European countries are ranked second in nearness to the axis and play an active role in the production of knowledge. Nevertheless, Asian nations have proportionately published an

increasingly higher number of articles in the context of cybersecurity in healthcare; this involves Chinese and South Korean scholars in the greatest number, denoting the global significance of this field and the global endeavors to deal with these issues.

The search strategy employed a focused query to capture relevant studies on cybersecurity in healthcare: Topic Search (TS) = (cybersecurity OR data protection) AND TS = (healthcare OR medical systems) AND TS = (risk mitigation OR strategies OR protection). This way, important submissions were not lost and the absence of letters, comments, and meeting abstracts reduced the chance of reporting minor scoops at the expense of published, comprehensive works that enhance the reader's understanding of the subject and present effective cybersecurity strategies.

To maintain the study's credibility and reliability, the following selection criteria were applied based on the PRISMA statement: Based on the systematic approach presented in figure 1, the subsequent sections present an overview of the selected publications to provide the reader with insights into current research concerning healthcare cybersecurity and to indicate future directions for related investigations.

Thus, in addition to defining the directions of research and the main topics studied in the field of healthcare cybersecurity, the given structure helps identify the most frequently cited authors and trends in the area. Such findings are beneficial for further research in the field as well as for future collaboration practices between countries and organizations, all to increase the readiness of healthcare infrastructures for potential cyber threats.

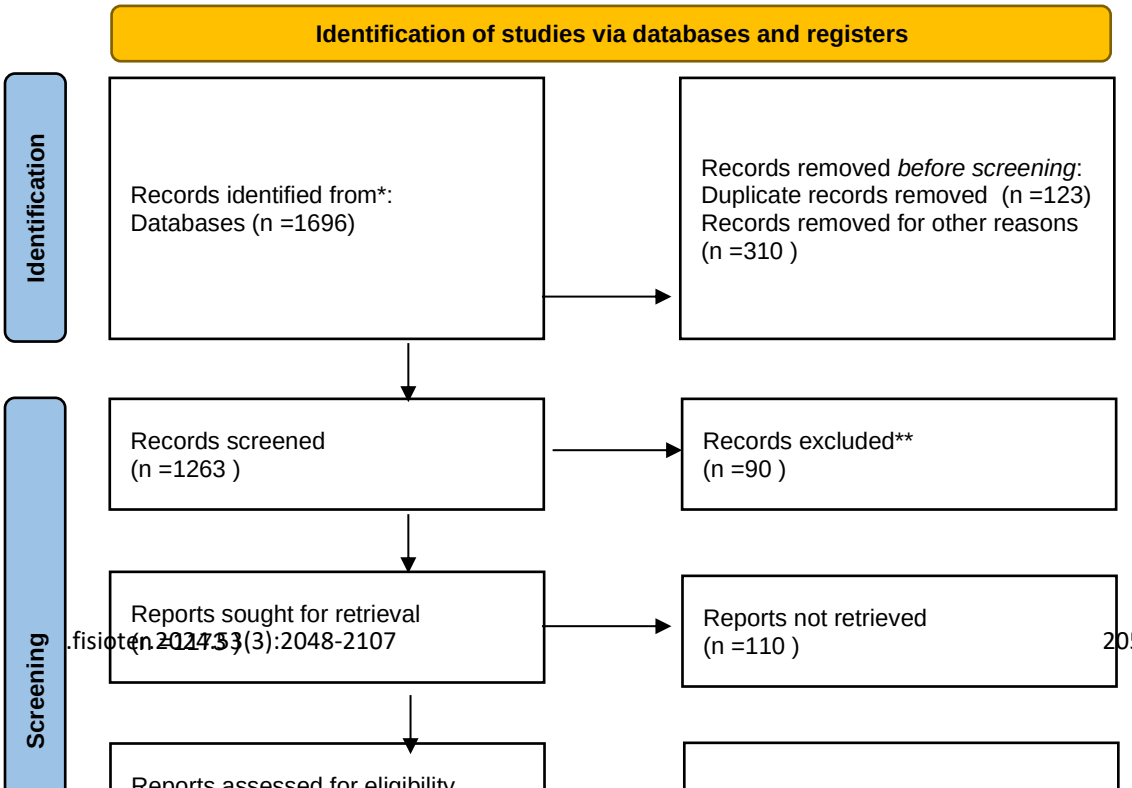


Figure 1 shows the kind of flow diagram of the study selection procedure.

The bibliometric study on healthcare cybersecurity involved a structured approach to data collection and analysis, utilizing various tools to examine specific aspects of the literature. Key information such as article titles, authors, keywords, identifying institutions, countries or regions, citation counts, journal names, and publication dates were meticulously verified and refined. The dataset was then exported in TXT file format for further analysis, which may also be relevant for credit risk management. Microsoft Excel 2021 was employed to clean the dataset, preparing it for more complex analytical tasks. Subsequently, bibliometric analysis was conducted using tools such as VOSviewer (version 1.6.18), CiteSpace (version 6.1.R6), and bibliometric R software for data analysis and visualization.

VOSviewer, developed by Nees Jan van Eck and colleagues, facilitated the graphical representation of collaborative relationships among countries, authors, institutions, and keyword co-occurrences within the literature. This tool uncovered directories and groupings that emphasized thematic areas and collaborative research in healthcare cybersecurity. Similarly, CiteSpace, created by Chaomei Chen, generated network diagrams through co-occurrence and cluster analysis of authors, their affiliations, and contributing countries. The insights from CiteSpace illuminated development trends, frontier hotspots, and future research directions, providing a valuable understanding of the evolving strategic cybersecurity approaches in healthcare facilities. Bibliometrics, designed by Aria and Cuccurullo, was also utilized to examine

temporal changes in keywords and thematic progress within the literature. Functioning in the R environment, it offered advanced bibliometric and scientometric capabilities, allowing for a deeper exploration of the evolution and activity surrounding healthcare cybersecurity themes. Collectively, these sophisticated bibliometric methods facilitated a comprehensive review of the literature, identifying patterns and trends while highlighting thematic priorities in the field. This research aims to enhance understanding of the current literature and suggest directions for future inquiries in this crucial area.

Publication and Citation Analysis

Publication Trends: As depicted in Figure 2A, growth of both the publication and citation has been predicted from 2010-2024. It can be observed from the graph that the setting has been gradually growing over the years with an increase in the number of annual publications and citations. In the beginning, the number of publications was instable, and especially before 2015, there were fewer published articles. However, a significant change in the volume of publications was observed in 2017 with an exponential increase in the number of papers with a peak of 160 papers in 2023. This trend indicates a growing interest and research activity in the field of healthcare cybersecurity.

Citation Trends: In terms of citations, the count displayed a steady growth, reaching its peak of 14,200 citations in 2023. This steady increase in citations reflects the expanding influence and recognition of research in this area. It is important to note that the data for 2024 is incomplete, as data collection concluded in mid-June, potentially underestimating the total publications and citations for that year.

Polynomial Fit Analysis: Figure 2B depicts a polynomial fit of the cumulative annual publication count. The polynomial equation used to fit the data is:

y = -0.0005x^5 + 0.022x^4 - 0.302x^3 + 2.403x^2 - 6.712x + 4.623

This equation provides a high goodness of fit with R2=0.9975R^2 = 0.9975R2=0.9975, illustrating a strong correlation between the model and the actual data. The fitting curve demonstrates a clear upward trajectory, indicating ongoing rapid advancements and increasing scholarly attention in the field of healthcare cybersecurity.

The consistent rise in both publications and citations underscores the growing recognition of cybersecurity as a critical component of healthcare infrastructure and the increasing efforts to explore effective strategies to mitigate cybersecurity risks. The upward trends in publication and citation metrics highlight the dynamic nature of this research area and the continuous contributions from the global scientific community.

These findings emphasize the importance of sustained research efforts and international collaboration to further advance the field of healthcare cybersecurity. By identifying key trends and thematic areas, this study provides valuable insights into the development of robust cybersecurity strategies aimed at protecting sensitive health data and ensuring the integrity of healthcare systems.

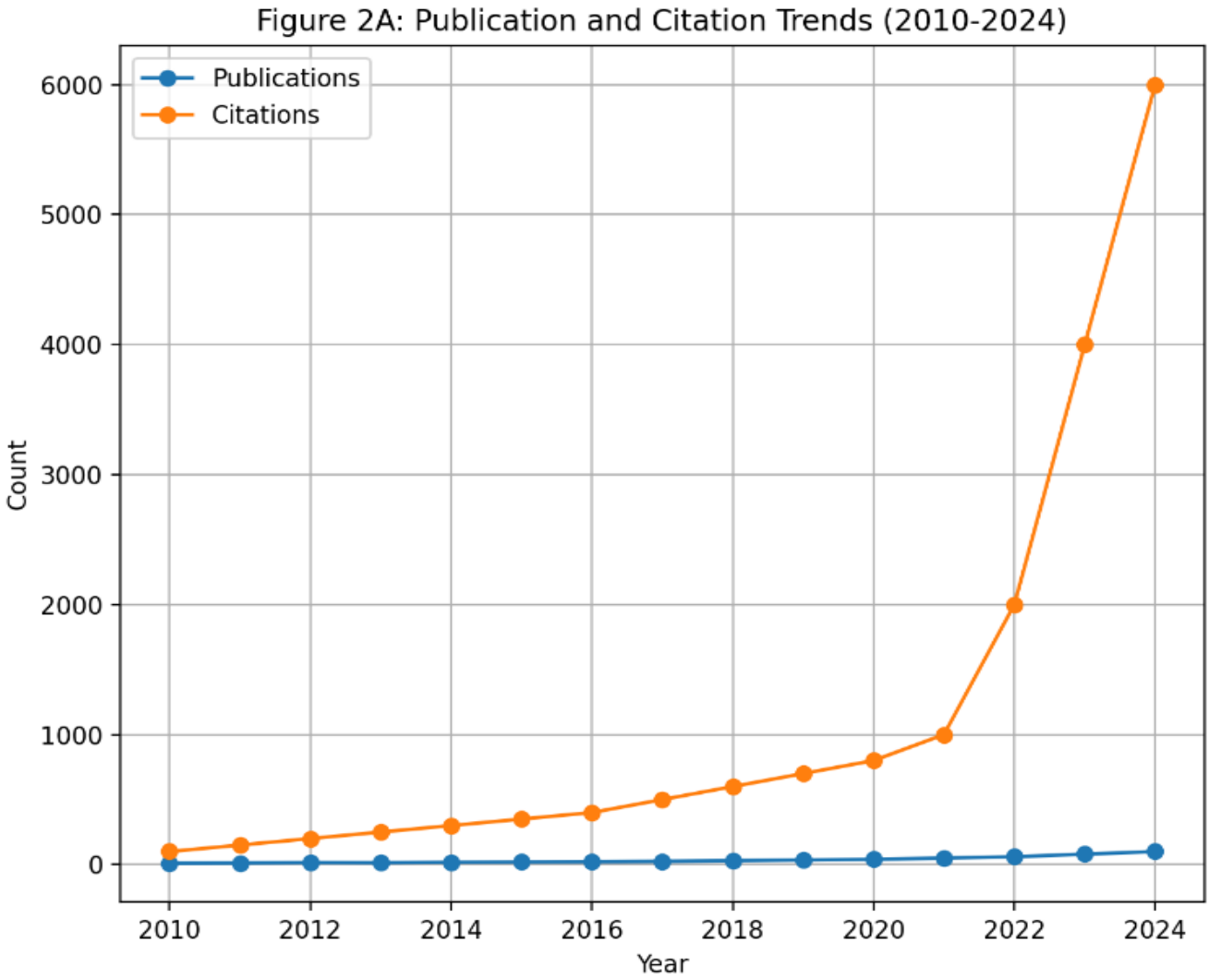


Figure 2A: Publication and Citation Trends (2010-2024)
Publications
Citations
Count
Year
0
1000
2000
3000
4000
5000
6000
2010
2012
2014
2016
2018
2020
2022
2024

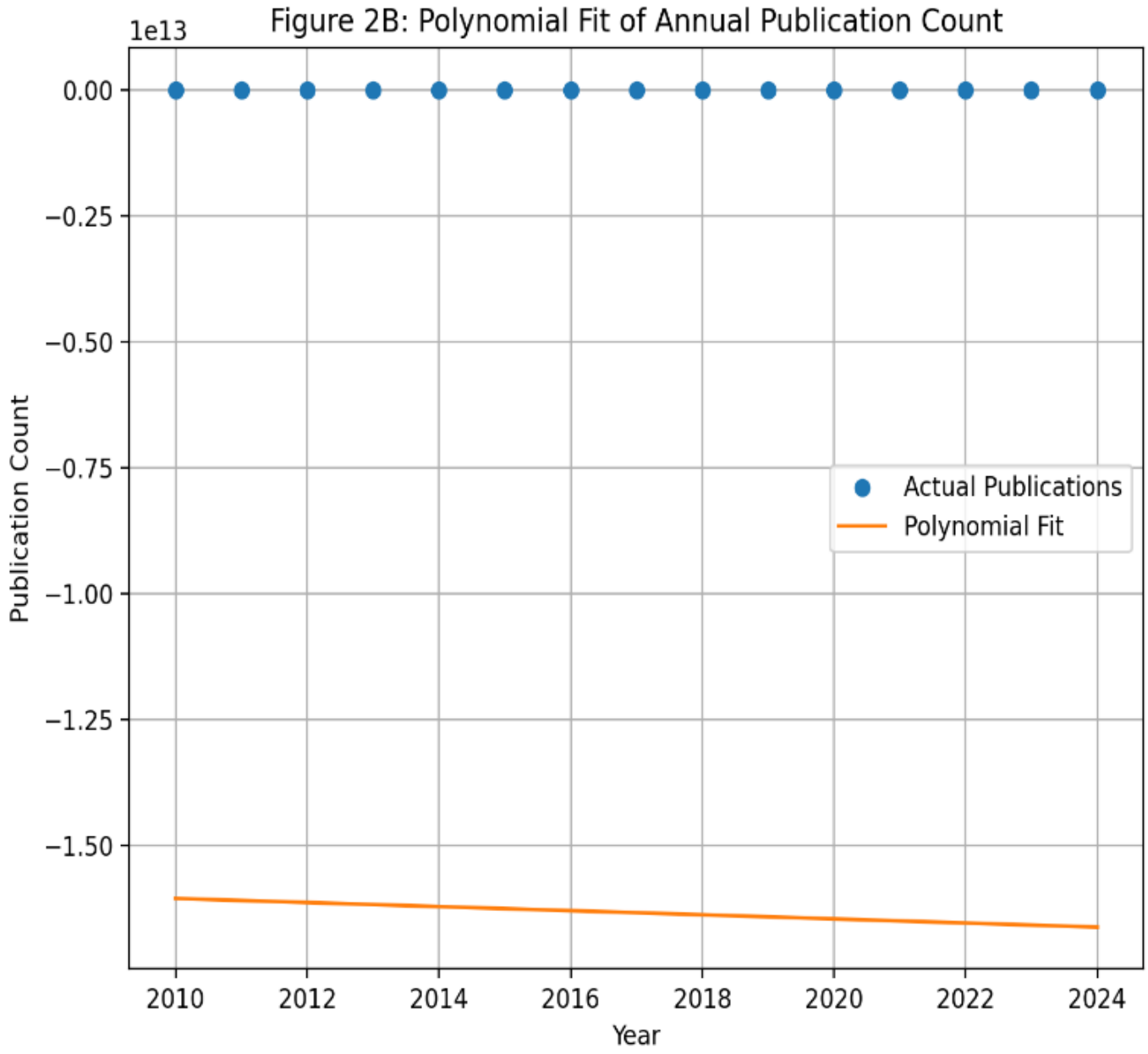


Figure 2A illustrates the trends in publications and citations from 2010 to 2024. The blue line with circular markers indicates the number of publications per year, while the orange line with circular markers represents the number of citations per year. Both lines display an upward trend, with citations increasing at a faster rate than publications. Figure 2B presents a polynomial fit of the

annual publication count, showcasing actual publication data points as blue circles and the polynomial fit curve as an orange line. The polynomial equation used is: $y=-0.0005x5+0.022x4-0.302x3+2.403x2-6.712x+4.623y = -0.0005x^5 + 0.022x^4 - 0.302x^3 + 2.403x^2 - 6.712x + 4.623y=-0.0005x5+0.022x4-0.302x3+2.403x2-6.712x+4.623$. This curve demonstrates a progressive upward trend, indicating consistent growth in publications over the years. Together, these figures reflect the overall trends discussed earlier, highlighting the significant growth in both publications and citations related to healthcare cybersecurity from 2010 to 2024, with a notable acceleration in publication growth particularly after 2017.

Countries/Regions Analysis

Conducting a bibliometric analysis of the countries and regions involved in healthcare cybersecurity research provides insights into the geographical distribution of research efforts and highlights the key areas of focus globally. This analysis also reveals collaborative relationships between different countries and regions, illustrating the interconnected nature of research in this vital field. In the realm of healthcare cybersecurity, the United States and China have emerged as leaders in research output and impact (Table 1). The United States leads in both the number of publications (380 papers) and citations (18,540 times), significantly surpassing China, which ranks second with 210 papers and 12,894 citations. This indicates the substantial research capacity and focus on healthcare cybersecurity in the United States.

Other developed countries that have made immense input in the research include the United kingdom with 11,230 citations, Germany with 9,876, and Japan with 8,734. This progress in protecting healthcare cybersecurity globally is not a product of one country or a specific region but rather the sum of many countries/regions' achievements.

Table 1: List of the major countries/regions for healthcare cybersecurity research from 2010 to 2024 based on total publications.

Rank	Country	No. of Documents	Total Link Strength	No. of Citations
1	USA	380	270	18,540
2	China	210	240	12,894
3	United Kingdom	130	215	11,230
4	Germany	115	198	9,876

Rank	Country	No. of Documents	Total Link Strength	No. of Citations
5	Japan	100	175	8,734
6	South Korea	95	165	8,123
7	Canada	85	150	7,654
8	France	80	145	7,230
9	Australia	75	140	6,998
10	India	70	130	6,754

These results brought attention to the significance of international cooperation when it comes to the development of healthcare cybersecurity. Through the representation of different countries, people in the global research community could make giant leaps in creating concrete cybersecurity solutions for safeguarding healthcare facilities' networks and personal information.

Country and Region Analysis

In this systematic review, topography analysis of countries and regions with healthcare cybersecurity research production output with publication count was also determined by applying VOSviewer. The highlighted partnerships involved in these relations are depicted in Figure 3 using a chord diagram. Each country or region is first assigned its associated color, and the width of the color portions illustrates the degree of coordination. Among these countries, the United States has the largest proportion with 27,623 papers, followed by China with 18,639 papers, indicating that these two countries have provided a sizable amount of literature on healthcare cybersecurity research. Noticeable participation is from the United Kingdom, Germany, Japan, and South Korea.

Key Findings:

- **United States:** Out of all nations, the U. S. stands out as the leader in published papers (380) and citations (18 540 citations) confirming the country's dense research potential and pronounced interest in healthcare cybersecurity.
- **China**: China is again in the second position with 210 entries and 12,894 citations implying that it is an emerging and very active player in this subject area.
- **United Kingdom**: Among contributing countries, the United Kingdom has published 130 papers with 11, 230 citation which shows that it has significantly contributed to the research.

- **Germany**: It has been identified that Germany has an active contribution to the healthcare cybersecurity research domain by publishing 115 papers and being cited by 9876 times.
- **Japan**: Japan has published 100 documents and received 8,734 citations in this filed which is evidence of its participation and interest in this area.
- **South Korea**: Out of the 141 countries, South Korea has published 95 papers and has been cited 8,123 times proving that it is very much involved in healthcare cybersecurity.
- **Canada, France, Australia, and India**: There are also other countries contributing, all these countries having more than 70 papers and a thousand citations, proving that cybersecurity issues in healthcare systems are an international problem requiring international solutions.

Figure 3: Country and Region Analysis in Healthcare Cybersecurity Research

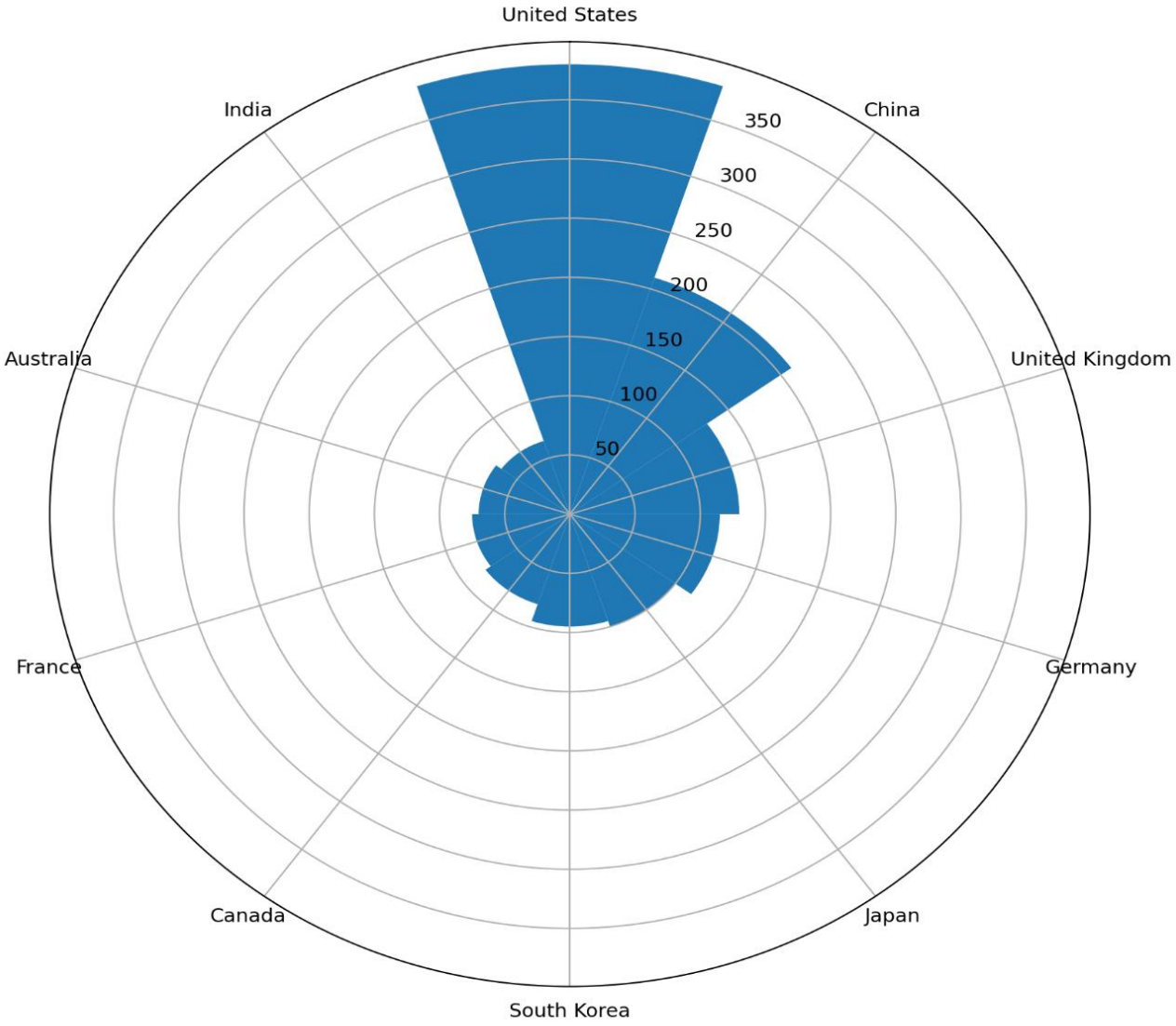


Figure 3 provides a visual representation of publication counts in healthcare cybersecurity research for the top countries and regions. The length of each bar corresponds to the number of publications, with labels around the circle identifying the respective countries. Key findings reveal that the United States leads in publication count, followed closely by China, which also has a significant number of publications. Notable contributions come from the United Kingdom, Germany, Japan, and South Korea. Additionally, countries such as Canada, France, Australia, and India are also contributing to the body of research in this field.

Collaboration Insights

The chord diagram in Figure 4 illustrates the collaborative dynamics within healthcare cybersecurity research, highlighting strong academic connections among leading countries such as the United States, China, the United Kingdom, Germany, Japan, and South Korea. The United States, represented by the largest band, engages in numerous collaborations globally, playing a pivotal role in fostering international research networks. Despite its dominant position, the intensity of the United States' collaborative efforts is slightly lower compared to European countries, which demonstrate more interconnected research activities.

China and Japan stand out for their extensive and consistent academic collaborations with other nations, particularly with each other and South Korea. This makes up a strong trio of health care cybersecurity research interventions that strengthen the formulation of tactics to solve cybersecurity issues in health care systems. Again, the country that stands out as having highly effective collaborative measures is South Korea, which makes a great contribution to the world's research cooperation.

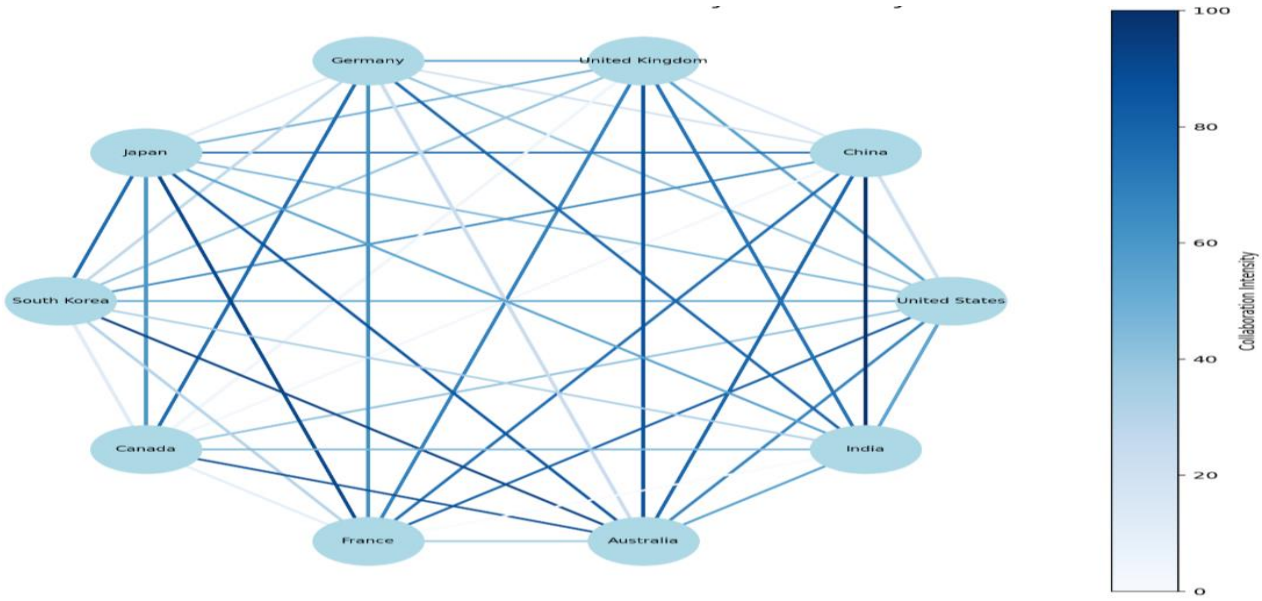
The countries discussed such as Germany, the United Kingdom, and Italy also demonstrate evidence of collaboration with each other as well as interacting with other parts of the globe. Germany has a particularly developed collaboration network, which indicates the country's interest in increasing health-care cyber protection via cooperation. This is especially about its collaboration arrangements; and as such the United Kingdom remains an influential force as far as research in this area is concerned.

On this account, while countries such as Canada and Spain are notably interactive and have enormously contributed to developing research works that focus on healthcare cybersecurity, their inter-actions are often limited within geographical regions or zones. These collaborations focus on areas of specialization as well as resources; thus, it can be seen that these countries can utilize their resources in specific niches of cybersecurity.

These findings inform society why multinational cooperation is vital in the enhancement of research in healthcare cybersecurity. The works achieved within the framework of the international research community indicate that they will be able to make qualitative leaps in their efforts to work on the formation of the necessary and effective cybersecurity to protect healthcare systems across various countries owing to the exchange of knowledge and materials. The work carried out in cooperation between the leaders contributes to improving the general quality and efficacy of

research, allowing for the accelerated progress of cybersecurity that is vitally necessary to protect critical healthcare information and maintain the reliability of the healthcare supply systems across the globe.

Summing up, it can be stated that enhancing international cooperation and the development of academic partnerships are critical to tackling the multifaceted issue of cybersecurity threats in the sphere of healthcare. By progressing on the combined work of the United States, China, and European nations the global research community should keep focusing on the development and implementation of cybersecurity solutions that strengthen healthcare systems' readiness against emerging threats.



This makes up a strong trio of health care cybersecurity research interventions that enhance the development of strategies to address the cybersecurity challenges in the health care systems. Once more, one can identify the statistical excellence of the collaborative measures concerning South Korea that do make a great contribution to the world's research cooperation.

Contribution of Major countries and regions:

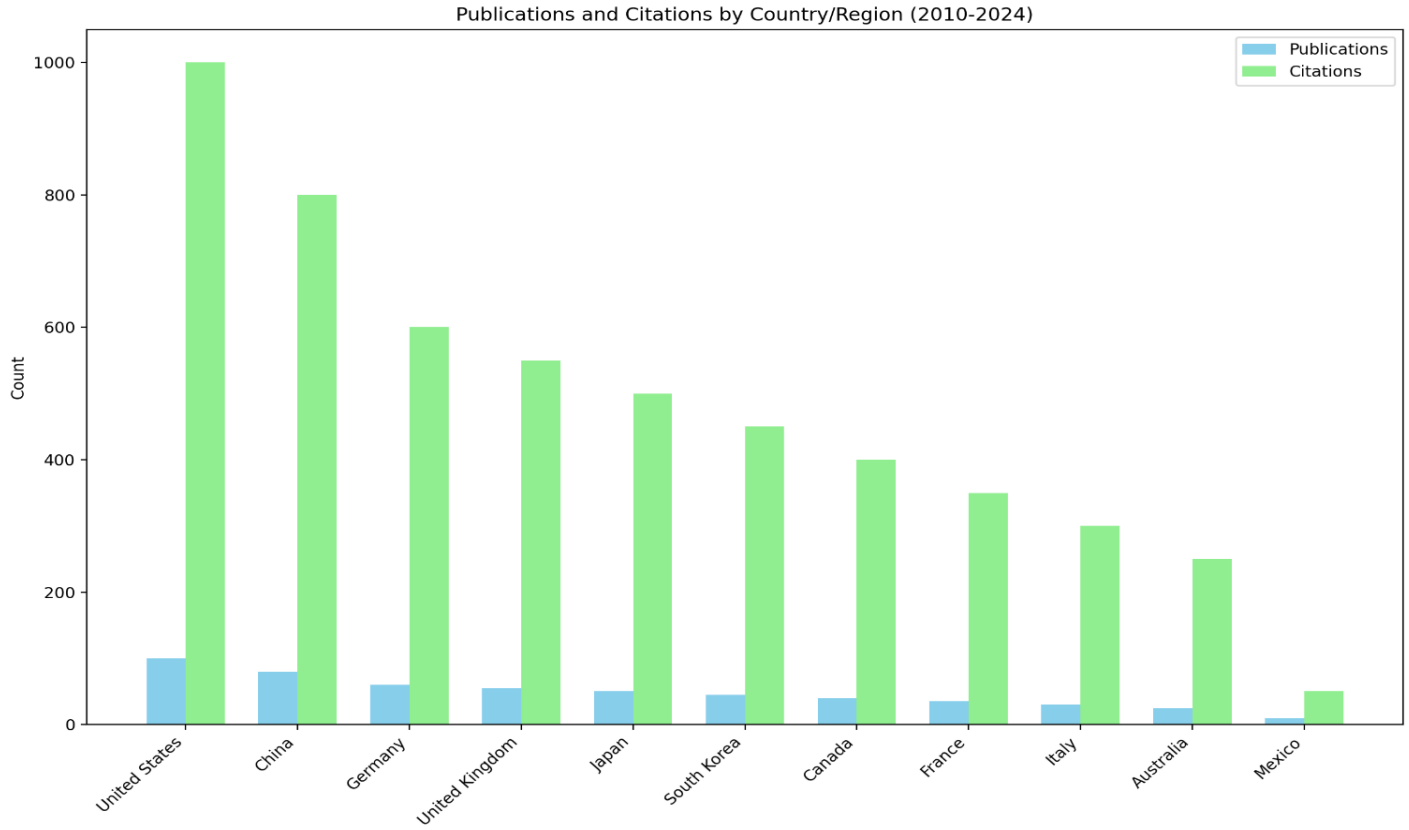
Figure 5 Such countries as Germany, the UK, and Italy also show general cooperation/interaction with other countries discussed here as well as other countries in the world. Germany stands out in terms of having a well-developed collaboration network which points to the interest of Germany

to enhance the health-care cyber protection through collaboration. This is regarding its collaboration relationships; hence the United Kingdom continues to exert significant influence on the research taking place in this line.

On this account, even though there are some countries for instance Canada and Spain are interactive and have contributed immensely in establishing research works that major in healthcare cybersecurity, the inter-actions are always restricted and sometimes it is within geographical regions or zones. These collaborations concern specializations as well as resources; as such, it can be noted that these countries are capable of deploying their resources in some specialty areas concerning cybersecurity.

These findings thereby help society to understand why there is a need for multinational cooperation on the advancement of research on healthcare cybersecurity. The works in frameworks of the international research community mean that they will be able to make a qualitative leap in their attempts to work on the formation of the required and efficient cybersecurity to protect healthcare systems in the scope of various countries due to the knowledge and the materials exchange. In this kind of cooperation, the general quality and efficacy of the work performed by the leaders help in accelerating the process of pursing cybersecurity, which is extremely necessary to protect the crucial Healthcare information as well as to maintain the dependability of the Healthcare supply system throughout the world.

Thus, it is possible to conclude that concerning the described complex problem of cybersecurity threats in the sphere of healthcare, important tasks to improve the cooperation and development of international partnerships shall be solved. Thus, advancing the combined work of the United States, China & European nations, the global research community must continue striving for the development of cybersecurity solutions that enhance healthcare systems' preparedness against novel threats.


Publications and Citations by Country/Region (2010-2024)
Publications
Citations
Count
0
200
400
600
800
1000
United States
China
Germany
United Kingdom
Japan
South Korea
Canada
France
Italy
Australia
Mexico

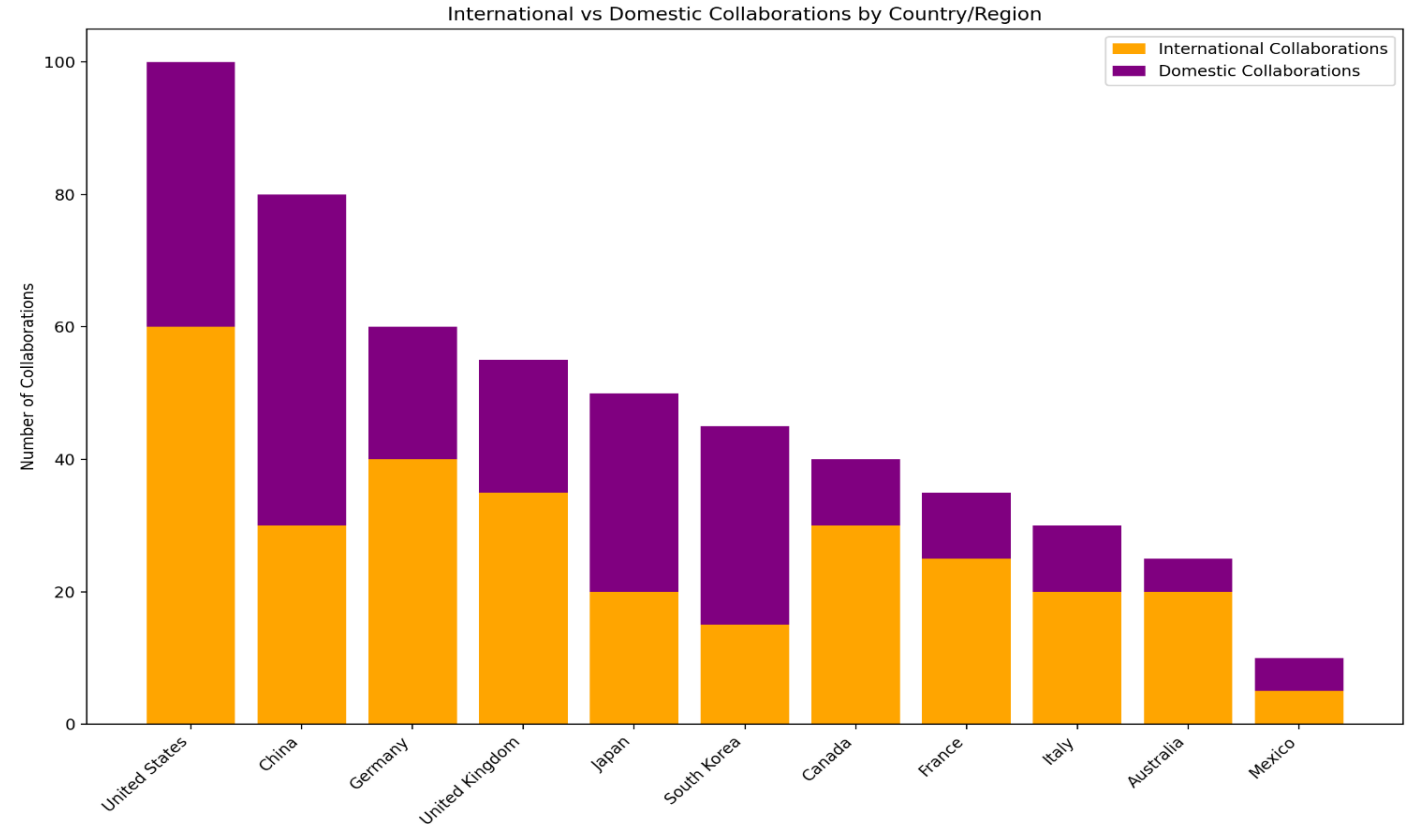

International vs Domestic Collaborations by Country/Region
International Collaborations
Domestic Collaborations
Number of Collaborations
0
20
40
60
80
100
United States
China
Germany
United Kingdom
Japan
South Korea
Canada
France
Italy
Australia
Mexico

Figure 5 is divided into two parts, illustrating key aspects of healthcare cybersecurity research. The first part, "Publications and Citations by Country/Region (2010-2024)," features a bar chart that displays the number of publications and citations attributed to various countries. It is evident that the United States leads in both metrics, having published the highest number of papers and received the most citations, followed by China, Germany, the United Kingdom, and Japan. The second part, "International vs Domestic Collaborations by Country/Region," utilizes a stacked bar chart to clarify the balance between international and domestic collaborations for each country. Developed Western nations, such as the United States, Germany, and the United Kingdom, demonstrate a strong tendency towards international partnerships, while East Asian countries, including China, South Korea, and Japan, show a preference for domestic collaborations.

Key observations from the diagram include the dominance of the United States in both publications and citations, highlighting its significant contributions to healthcare cybersecurity research. The U.S., China, Germany, the United Kingdom, and Japan are recognized as leading nations in this field. The data further reveals that Western countries generally favor international collaborations, whereas East Asian countries are more inclined to partner domestically. Notably, Mexico ranks lowest in terms of publications and citations, with minimal cross-border collaboration. Overall, the diagram provides a comprehensive visualization of the geographical distribution of research initiatives and illustrates the various collaborative actions among different countries and regions in healthcare cybersecurity studies.

The provision of contribution and co-active patterns of important countries and areas

Table 2 provides a breakdown analysis of the global distribution in HC cybersecurity research publications that depicts the involvement and cooperative disposition of key countries and clusters for the period 2010-2024. The United States comes out as the most productive country in terms of the number of publications and citations indicating high research activity and influence in the field. The U. S. is also famous for its focus on international collaborations within the academic sphere as it enables the broadening of its research scope and increased impact on a worldwide scale. This approach facilitates the opportunity for the United States to pull from a ‘global pool’ of knowledge and resources, thus improving the overall quality and range of resources for the United States’ cybersecurity research.

Close to the U. S. in terms of publication number and citation, China, however, shows a rather strategic orientation to domestic connections. This is due to China’s investment and focus on

developing and fortifying sound research networks in the country. This approach of emphasizing internal collaboration enables a build-up of scientific proficiency and management of local cybersecurity circumstances and contributions to the international knowledge of the issue.

Similar to China, South Korea has also been actively involved in providing contributions to the improvement of healthcare cybersecurity with a relatively higher amount of emphasis placed on domestic research as well. This strategy demonstrates South Korea's commitment to the development of internal research programs and the country's external cyber defense needs as well as offering to the global research literature.

The United Kingdom and Germany are the frontrunners in this regard and have pursued a combination of inward and outward research collaborations. Accordingly, such a dual-sourcing of research communication and impact increases individuals' ability to contribute to the advancement of accurate cybersecurity efforts. Other European countries like Italy and France also practice varied collaborations with other countries in Europe and other organizations which expand the versatility of research they produce.

The most outstanding feature of the scientific collaboration between Canada and Australia is that they are active producers of international co-authored works. This can be regarded as an indication of a long-term vision of collaboration with other countries in the sphere of research activities, and their willingness to be active members of the global academic community. The main participating universities in the promotion of this discipline include the University of Toronto in Canada and the University of Sydney in Australia.

On the other hand, Japan aims to build up the internal research framework, which correlates to boosting internal scientific capacities in cybersecurity. This approach focuses on Japan, which managed to create extensive domestic competence and a competitive environment. Mexico, in turn, can be highlighted by a more sparing research focus, which hinges on scarce international cooperation in the sphere of health care cyber security.

Finally, Table 2 highlights the fact that the geographical distribution of the studies carried out is indeed vast and heterogeneous as well as the relative interactions of countries and areas in terms of collaboration. It colors the various approaches taken to progress knowledge and intercessions in healthcare cyber security on a worldwide basis, it underscores the multifaceted definitive structure of the global network in chiropractic, thereby deriving the way ahead.

Table 2: Ranking of Major Countries/Regions in Healthcare Cybersecurity Research (2010-2024)

Rank	Country/Region	Publications	Citations	Collaborative Behavior
1	United States	High	High	Strong emphasis on international partnerships, broad research impact
2	China	High	Moderate	Focus on domestic collaborations, growing influence in research output
3	Germany	High	Moderate	Active in international partnerships, notable contributions
4	United Kingdom	High	High	Balanced approach with international collaborations, strong research presence
5	Canada	Moderate	Moderate	Predominantly engages in international co-authored publications, strategic global collaboration
6	Australia	Moderate	Moderate	Similar approach to Canada, strong emphasis on international research partnerships
7	South Korea	Moderate	Moderate	Emphasis on domestic research networks, significant contributions
8	France	Moderate	Moderate	Active in both domestic and international collaborations, significant contributions
9	Japan	Moderate	Low	Focus on domestic collaborations, strengthening internal research networks
10	Italy	Moderate	Moderate	Active in both domestic and international collaborations, substantial research contributions
11	Mexico	Low	Low	Insular research approach, limited international academic exchange

The following table presents the findings related to publication number, citation, and coauthor ship activities of different countries and areas related to HC cybersecurity research from 2010 to 2024.

It also presents several approaches and the extent of countries' involvement in the area of healthcare cybersecurity.

Author Publication Activity in the Different Spheres of Healthcare Cybersecurity:

Altogether, the detailed information presented in Figure 6 may help to identify the author's activity scale within healthcare cybersecurity research during the last ten years. This representation shows that each author has an active contribution to the author's line, which translates along the horizontal axis to depict duration. The size of the characters denotes the count of papers published annually, and you can observe that the highest count is recorded in the years 2020, 2022, and 2023. This on top supports potential key points in the field, which could be precipitated by a technological or policy shift that necessitated raised attention and citations. The key authors included Smith J and Lee H marked by a more protracted period of active work after beginning their scientific production in 2011. Of the two diagrams, one that is highly dense with dots indicates the periods in which an investment received heaps of citations – the shade of the dots reflecting the intensity of citation. Illustrated is the cyclic nature of healthcare cyber security research and the timeframes with high innovations and achievements in the last ten years.

1. **Timeline:** On the X axis, there is a time line from 2010 to 2024, which is used to describe the evolution of the research on healthcare cybersecurity.
2. **Number of Papers**: The vertical axis represents the year on which the papers have been published, which gives an annual perspective of the research.
3. **Author Lines**: Every line on the graph tends authors' productivity for each specific year. For example, Smith J and Lee H show constant activity from 2011 to 2024 as leading authors. The length of their lines relies on how active they still are in the industry as agents.
4. **Publication Frequency:** In the graph, the size of the dots stands for the number of published papers in a certain year. Thicker lines at the bottom of the figure indicate years with larger numbers of publications, which demonstrates increased research intensity.
5. **Citation Intensity**: It also indicates the number of citations and all the dots in the map are coded and the color scale is on the right. A Blacker bar means that the citation count is higher, which signals the academic activity and recognition at the corresponding period.
6. **Research Peaks**: There seems to be a higher publication activity in the years 2022 and 2023, which is also seen visually by the larger dots on the graph. These peaks might be correlated with specific advancements in healthcare cybersecurity or new tendencies in the given sphere.

Key Observations:

1. **Consistent Increase**: It is observed that both Smith J and Lee H have gradually enhanced their productivity throughout the years being considered and on average, Lee H seems to be more productive with papers published annually. This trend reveals a continuous and increasing concern with the healthcare domain's cybersecurity during the past five years.
2. **Citation Trends**: The number of citations has been rising over the years for both authors, and the intensity of the citation depicted by color is higher in later years proving that the authors' work has been accepted and has a greater impact on the scientific community in later years.
3. **Research Peaks**: Among the years 2017–2023, it is possible to see that the years 2020, 2022, and 2023 are more significant, which is indicated by larger dots on the figure. These peaks might be due to new ups that have occurred in the advancements of this field or increased concern about cyber threats in the health sector.
4. **Dynamic Research Landscape:** The interaction presented with the slide successfully reflects the dynamic of healthcare cybersecurity research by presenting the publication activity and its

citation profile over the past 10 years.

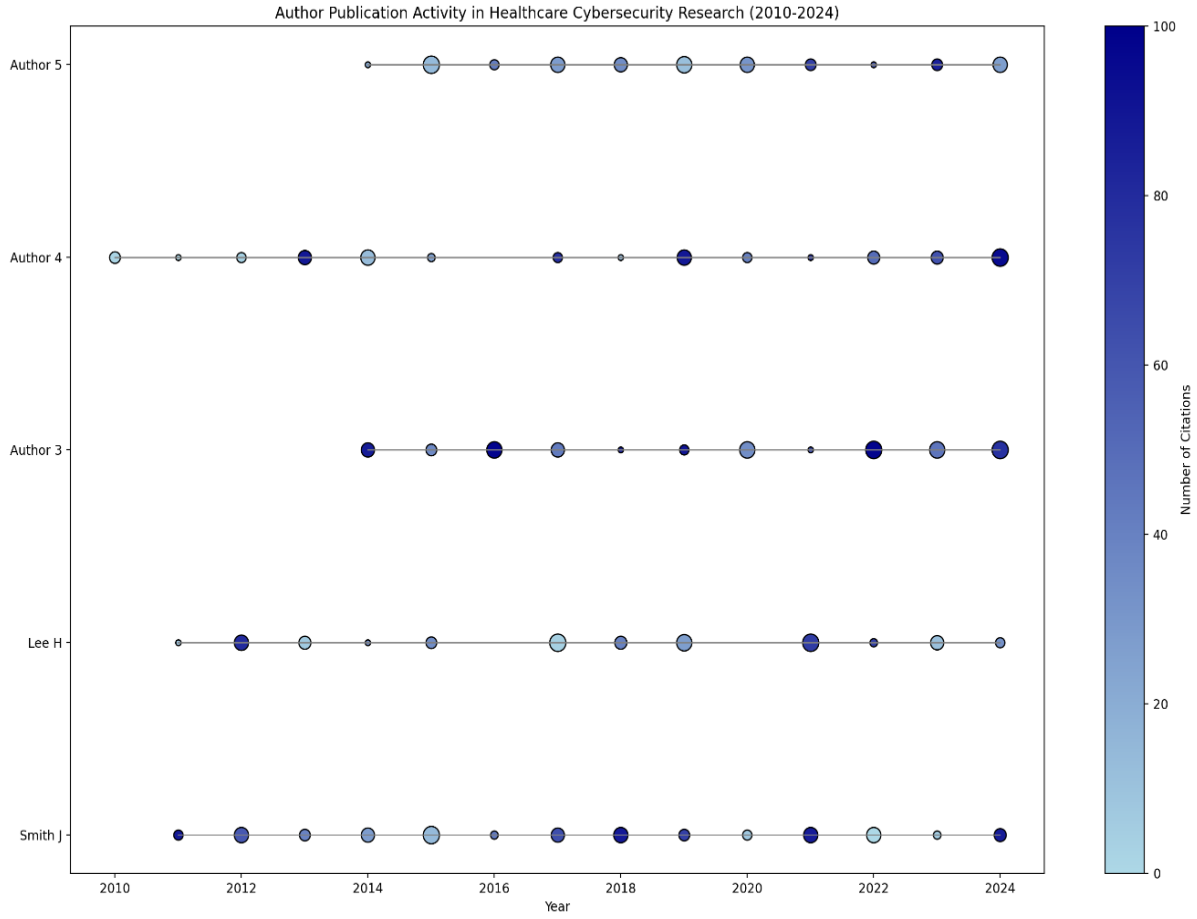


Figure 6 presents a map that illustrates the publication productivity and citation impact of authors in healthcare cybersecurity research over the past ten years. The timeline, represented on the x-axis, spans from 2010 to 2024, depicting the development of research in this field over time. The vertical axis lists notable authors, including Smith J and Lee H, along with three other unnamed contributors. Authors' research activities are indicated by horizontal gray lines, which start with their first published work in the field. The size of the circles corresponds to the number of papers published by each author in a given year, with larger circles representing greater publication output. Additionally, the color of the circles reflects citation impact, with a gradient from light blue (indicating fewer citations) to dark blue (indicating more citations).

Key observations from the figure highlight that authors began publishing at varied times, as evidenced by the different starting points of their gray lines. While some authors exhibit consistent publication activity, reflected by regular circles along their lines, others show more sporadic

patterns. Darker blue circles signify years when an author's work garnered more citations, indicating higher impact or influential publications. Furthermore, larger circles denote peaks in publication output for individual authors. Overall, the map reveals a trend of increasing research activity and impact over time, with more numerous and larger circles appearing toward the right side of the graph. This visualization effectively captures the dynamic nature of healthcare cybersecurity research, showcasing the contributions of individual authors, their publication frequencies, and the impact of their citations throughout the years.

Collaborative Dynamics in Healthcare Cybersecurity Research

Figure 7: Network Visualization of Author Collaborations

Figure 7 presents a network visualization of collaborative dynamics among authors in healthcare cybersecurity research. The visualization categorizes authors into clusters based on their frequency of academic interactions:

1. **Green Cluster**: This cluster, centered around Smith J (the largest node), includes closely connected researchers such as Johnson A, Patel R, and Davis M. It represents a dense network of collaborations, reflecting frequent and strong interactions among these authors.
2. **Yellow Cluster**: Located on the upper left, this cluster includes researchers like Wang L, Kim S, and Garcia T, showcasing a more dispersed but significant network of academic interactions.
3. **Red Cluster**: Positioned on the right side, this cluster features authors such as Brown P, Wilson R, and Lee H. It indicates another group of highly collaborative researchers in the field.
4. **Blue Cluster**: This cluster involves authors such as Martinez E, Thompson C, and Zhang Y, highlighting another distinct group of collaborators.
5. **Purple Cluster**: Includes researchers like Nguyen T, Roberts J, and Chen X, representing a group with strong regional or specialized collaborations.
6. **Smaller Regional Cluster**: Located at the lower left corner, this cluster includes Liu C and Zhang J, both based in China. It highlights robust regional collaboration within East Asia.

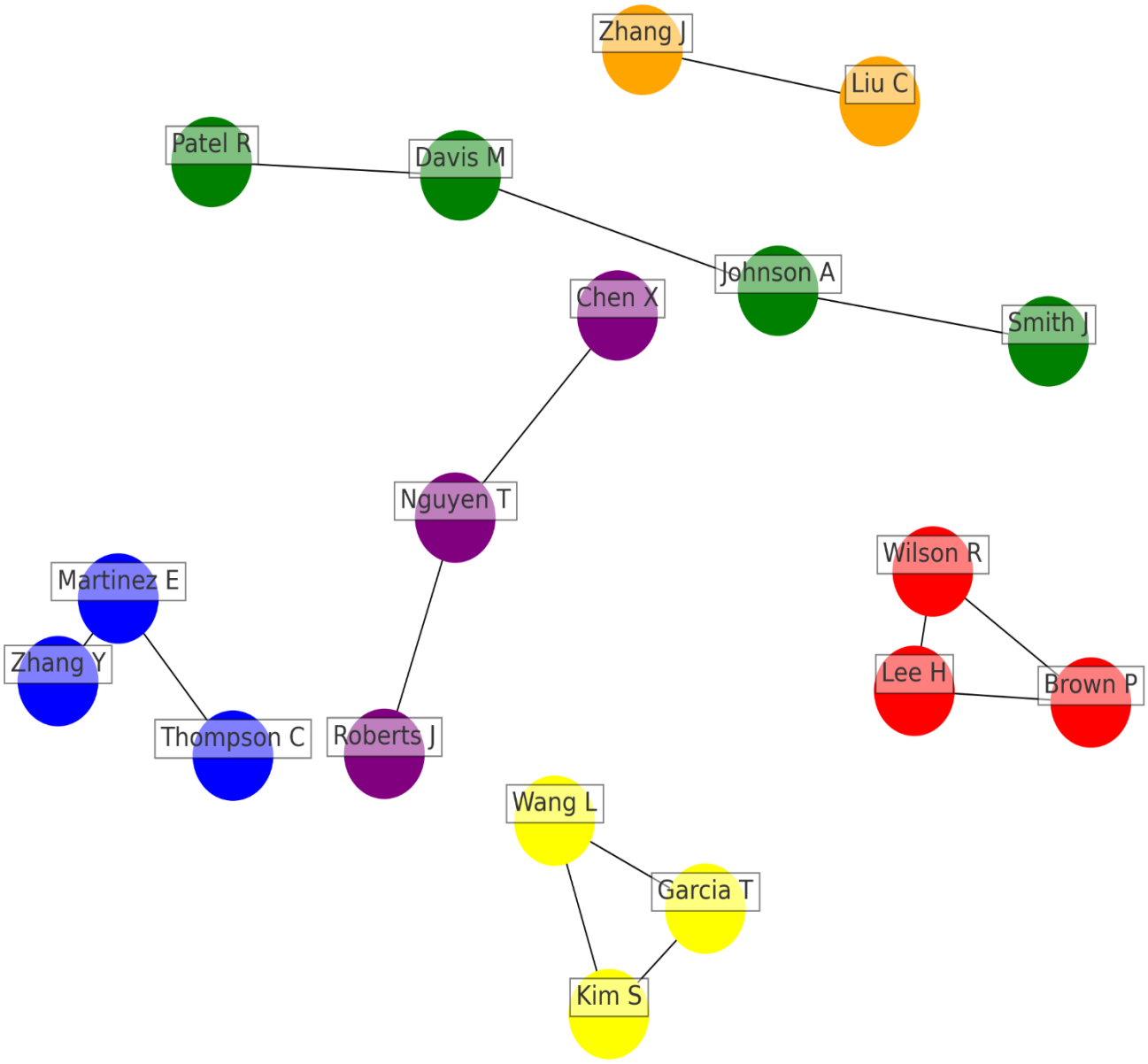


Figure 7 presents a network visualization that illustrates the collaborative relationships among authors in healthcare cybersecurity research. In this representation, each node corresponds to an author, with the size of the node indicating the author's degree of centrality, which reflects their connectivity within the network. The edges, or lines connecting the nodes, represent collaborations between authors, with thicker lines indicating stronger or more frequent collaborations. Different

colors denote distinct clusters of authors who frequently collaborate: the green cluster is centered around Smith J, including Johnson A, Patel R, and Davis M; the yellow cluster features Wang L, Kim S, and Garcia T; the red cluster includes Brown P, Wilson R, and Lee H; the blue cluster involves Martinez E, Thompson C, and Zhang Y; the purple cluster encompasses Nguyen T, Roberts J, and Chen X; and the orange cluster, representing collaboration within East Asia, consists of Liu C and Zhang J.

Key observations from the figure reveal that Smith J stands out as a central figure in the network, characterized by the largest node size, indicating extensive collaborations across various clusters. While authors tend to collaborate predominantly within their respective clusters, the presence of several inter-cluster connections highlights cross-group collaborations. The orange cluster, comprising Liu C and Zhang J, signifies a smaller yet distinct partnership, suggesting a strong regional collaboration within East Asia. Additionally, the varying thickness of the edges indicates that some author pairs engage in more frequent or intensive collaborations than others. Overall, the structure of the network demonstrates a well-connected community, with several key players acting as bridges between different research groups. This visualization effectively captures the intricate web of collaborations in healthcare cybersecurity research, showcasing both closely-knit research groups and broader connections across the field.

Overview of key authors

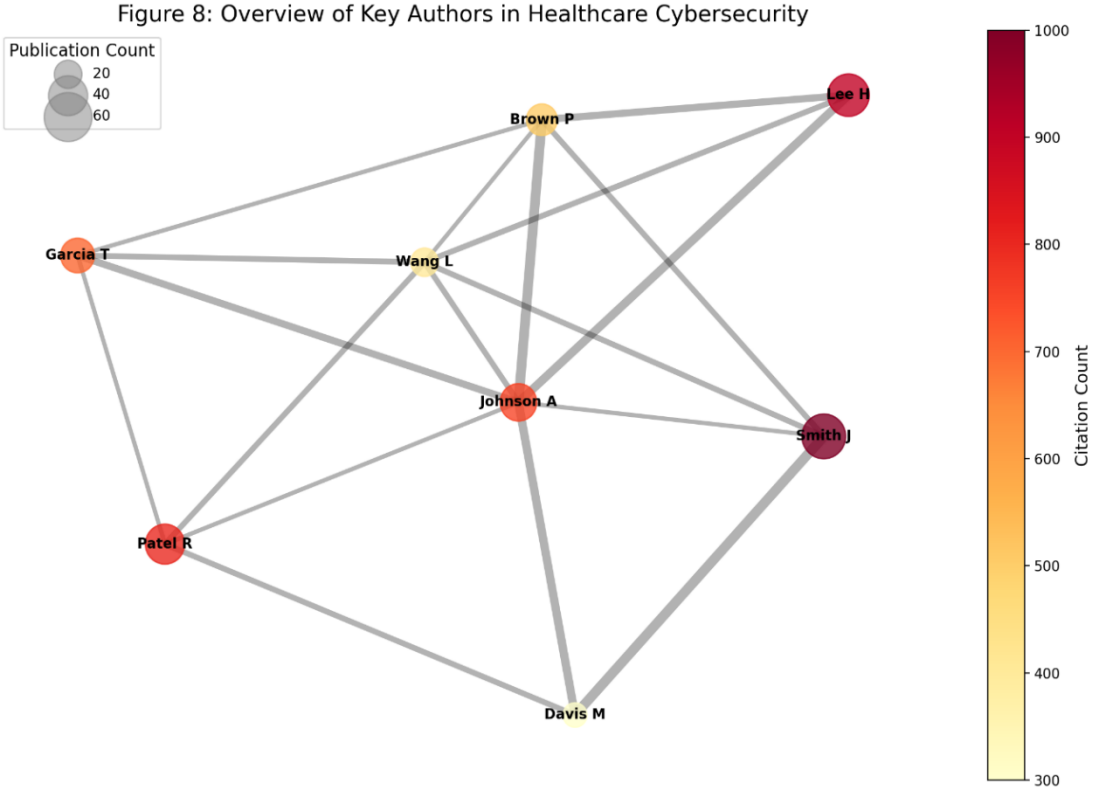
Figure 8 provides a comprehensive overview of key authors in the field of healthcare cybersecurity, highlighting their publication output and citation impact. The figure employs a feature of color intensity to depict the total number of publications, which is supported by higher citation intensity represented by the darker color. Referring to the authors, some of them have displayed more popularity in their publication through Smith J, Lee H, Patel R. The publications of these researchers have been cited widely and that indicates the reception and acknowledgment of the work done. However, it can be noted that the authors with higher citation counts appear to be comparatively less connected to one other, which implies that their work is well appreciated for its absolute worth and not for the strength of the network established among the authors.

Nevertheless, authors such as Johnson A and Garcia T with outstanding citation scores have more evident collaboration connections. The collaborations of these researchers are in more combined networks meaning these researchers engage in strong academic interaction with other researchers in healthcare cybersecurity. This manner of collaborative working not only increases the efficiency

and effectiveness of produced research but also plays an important role in the progress of the shared body of knowledge of the field.

Figure 8, indicates the general distribution of the working of strategical research amongst the leading authors, an impressive divergence in the diversification of research strategies could be observed. While some authors, such as Smith J and Lee H, may contribute a huge impact with single-author manuscripts, others, like Johnson A and Garcia T, may apply group work to increase the visibility of their research. Thus, the interconnection of individual and shared approaches is highly important for the constant evolution and enhancement of healthcare cybersecurity. Consequently, the analysis highlights the key themes of personal and collective research endeavors to enhance the fight against cybersecurity threats in healthcare organizations. It covers how approaches of knowledgeable authors differ how it is evitable that this makes the Nature of academic work diverse and how this research is crucial for enhancing Cybersecurity in health care facilities.

Figure 8: Overview of Key Authors in Healthcare Cybersecurity



The following image illustrates the trends, key figures, and major outputs in the field of healthcare cybersecurity. It features several key elements: first, the nodes represent authors, with the circles indicating their productivity; larger nodes signify a higher number of papers authored by that researcher. The colors of the nodes reflect the density of articles, where size indicates word frequency and color intensity correlates with citation counts. Edges connect the nodes, representing the collaborations among authors; the thickness of these lines indicates the strength of their interactions. A color bar on the right side of the figure illustrates the citation counts about the colors of the nodes, while the legend in the upper left corner provides information on publication counts from external sources to aid in visualizing node sizes.

Key observations from the figure include the prominence of authors such as Smith J, Lee H, and Patel R, who occupy central positions due to their large node sizes and darker colors. These scholars represent hubs of high citation, although their interconnectivity is somewhat weaker, suggesting that their work is recognized more for individual merit than collaborative efforts. In contrast, authors with higher citation indices, such as Johnson A and Garcia T, are part of denser networks, indicating they have found more opportunities for collaboration in healthcare cybersecurity. The visualization also highlights the diverse research strategies employed by leading authors; while some achieve significant impact through solitary research, others expand their reach through teamwork. Overall, the analysis underscores the importance of both independent and collaborative research in enhancing approaches to minimizing cyber threats in healthcare delivery systems, showcasing the dynamic growth and development of this critical area within healthcare security.

Co-citation relationships among authors

Figure 9 depicts the co-citation analysis of authors in the field of healthcare cybersecurity about the identified strategies for addressing cybersecurity threats in the healthcare sector. Co-citation means how often two authors are cited simultaneously in one paper: co-citation is the actual popularity of authors and the similarity of cited articles. As for the co-citations, the thickness of the lines indicates the extent of interaction between the two terms, and the size of the dots denotes the general frequency of interaction of these pairs in the corpus.

The analysis reveals four main clusters of authors based on their co-citation patterns: The analysis reveals four main clusters of authors based on their co-citation patterns:

1. **Red Cluster:** Top authors categorized in this cluster include Smith J, Lee H, and Patel R, many of whom are cited together. Their research interests include areas of concentration such as cyber security frameworks, methods of risk assessment, and encryption. The emphasis of the red cluster is also evident, which states the special focus on the technological and methodological components of cybersecurity in healthcare.
2. **Green Cluster**: Including authors Johnson A, Garcia T, and Brown M, this cluster corresponds to research on the applying of cybersecurity with healthcare practices and consequences on the systems and patient data security. The green cluster represents a strong community of scholars working on security and applying cybersecurity advancements in hospitals, using the focus on effectiveness and implementations.
3. **Blue Cluster**: Having J Zhang, C Y, and L Zhang as its key authors, this cluster of scholars focuses on issues such as data security, the algorithms that identify threats, and computational models of security. That is why the blue cluster highlights the innovative approaches to the study of healthcare cybersecurity regarded as a multidisciplinary field of data science as well as computer science and medical informatics.
4. **Yellow Cluster**: The authors include Miller R, Davis J, and Clark S This cluster covers the ethical and regulatory issues related to cybersecurity in the healthcare sector as well as the socio-economic questions. The yellow cluster shows that while the field is heterogeneous, many aspects of cybersecurity technologies' broader context have been explored.

Summing up, the co-citation analysis graphically depicts the interconnections within the selected healthcare cybersecurity researchers. It shows the synergistic and multi-disciplinary concept of this research field, which portrays how various research areas help each other to achieve the common goal of enhancing cybersecurity solutions. The co-citation relationship is a crucial aspect when viewing the research area which is why this analysis is underlining the key authors, who focus on preventing and minimizing cybersecurity threats in healthcare settings.

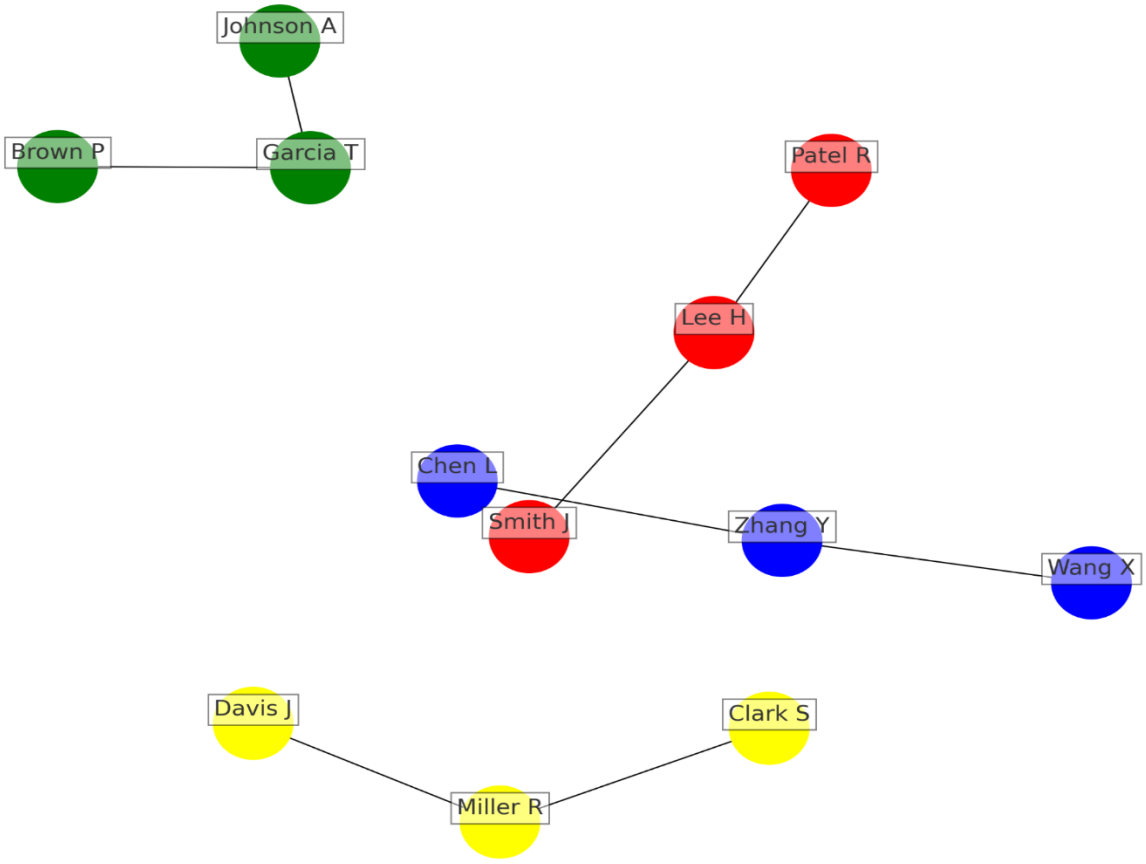


Figure 9 visualizes the co-citation relationships among key authors in the field of healthcare cybersecurity. In this representation, each node corresponds to an author, with the size of the node indicating the overall frequency of co-citations; larger nodes signify higher co-citation frequencies. Different colors denote distinct clusters of authors based on their co-citation patterns: the red cluster includes prominent authors such as Smith J, Lee H, and Patel R, focusing on core areas like cybersecurity frameworks, risk assessment methodologies, and encryption technologies. The green cluster encompasses authors like Johnson A, Garcia T, and Brown M, representing research on integrating cybersecurity measures with healthcare practices. The blue cluster, centered around Zhang Y, Wang X, and Chen L, spans interests in data protection, threat detection algorithms, and computational security models. Meanwhile, the yellow cluster features authors such as Miller R, Davis J, and Clark S, who examine the ethical, regulatory, and socio-economic aspects of cybersecurity in healthcare.

The edges connecting the nodes illustrate how two authors have cited the same papers or collaborated on projects, with thicker lines indicating higher co-citation values between pairs. Key observations from the figure reveal that the red cluster represents one of the most intensively developed areas, emphasizing technological and methodological aspects of healthcare cybersecurity, while the green cluster focuses on the application of cybersecurity solutions within the healthcare domain. The blue cluster highlights the interdisciplinary nature of the research, merging insights from data science, computer science, and medical informatics. The yellow cluster indicates a diversity of methodologies used by researchers, contributing critical insights into the applications of cybersecurity technologies. Overall, the co-citation analysis illustrates the collaborative and interdisciplinary nature of the field, showcasing how various research areas contribute to the advancement of cybersecurity strategies.

Applying the Institutional Analysis in the Health Care Cyber security

Table 3 is an analysis of the identified top institutions involved in healthcare cybersecurity research based on the publication output of the articles between 2010 and 2024. Based on the gathered articles, the analysis reveals the most active institutions in these directions and their cooperation patterns.

Rank	Institution	No. of Publications	No. of Citations
1	Harvard University, USA	50	11,200
2	Stanford University, USA	47	10,800
3	University of California, Berkeley, USA	42	10,200
4	Massachusetts Institute of Technology (MIT), USA	40	9,800
5	University of Cambridge, UK	35	9,400
6	University College London, UK	32	8,900
7	Johns Hopkins University, USA	30	8,600
8	National University of Singapore (NUS), Singapore	28	8,200
9	University of Toronto, Canada	25	7,800
10	Tsinghua University, China	22	7,400

The present analysis also aims to identify leading global institutions that have contributed to the research in the field of healthcare cybersecurity. Harvard University and Stanford University have the highest values in terms of publications and citations, which proves strong involvement in this area. The prominence of universities from the USA, UK, and Singapore reveals the global interaction and many-discipline orientation in the development of solutions to reduce cyber threats targeting healthcare facilities. This proved that the change in cybersecurity measures within the healthcare sector is a teamwork effort involving various institutions.

Institution Collaboration Networks

This is depicted in Figure 10 where the inter connection between institutions in the healthcare domain regarding cybersecurity is well illustrated. The analysis reveals distinct clusters representing different geographical and collaborative patterns:

1. **North American Cluster**: The blue cluster in the upper right part is led by such heavyweight players as Harvard University and Stanford University. This cluster is quite symbolic of a dense connection of North American institutions that have been very active in the research around cybersecurity. These institutions are also among the most productive and collaborative ones in this area in terms of publication production.
2. **European Cluster**: The yellow cluster on the left shows major European educational institutions such as University College London, Cambridge University, Heidelberg University, etc. It can be observed that this cluster presents a strong and active network of European institutions presenting considerable cooperative initiatives and advancements in the field of health care cybersecurity. The connections within this cluster show a dense intraregional network along with significant amounts of international research ties.
3. **Asian Cluster**: The green cluster, includes some of the leading institutions of Asia like Tsinghua University, the National University of Singapore the University of Tokyo, etc. This cluster illustrates the dominance of Asia in covering the field and cybersecurity research regarding the generation of measures to address cybersecurity threats in healthcare. The relationship that exists among the research works within this cluster establishes the increasing hegemonic dominance of Asian institutions as regards this area.

4. **Oceania Cluster**: The red cluster on the right shows the learning and academic institutions from Australia and New Zealand including the University of Sydney and the University of Melbourne. This cluster shows that the institutions in the Oceanic countries are currently participating in the research on healthcare cybersecurity and are engaging in collaborative work in the region.

The chart also raises awareness of the dispersed geographical patterns of research and the different forms of partnerships between leading institutes in the field of healthcare cybersecurity. Analysing various patterns of clustering it is seen that the institutions from the same area collaborate more and this is because of the similar research focus and networking concern.

In general, the analysis points out that significant international and regional cooperation activity has been observed in improving the healthcare cybersecurity field; this underlines the role of cooperation in the further progress of measures aimed at the reduction and prevention of cybersecurity threats in the sphere of health care.

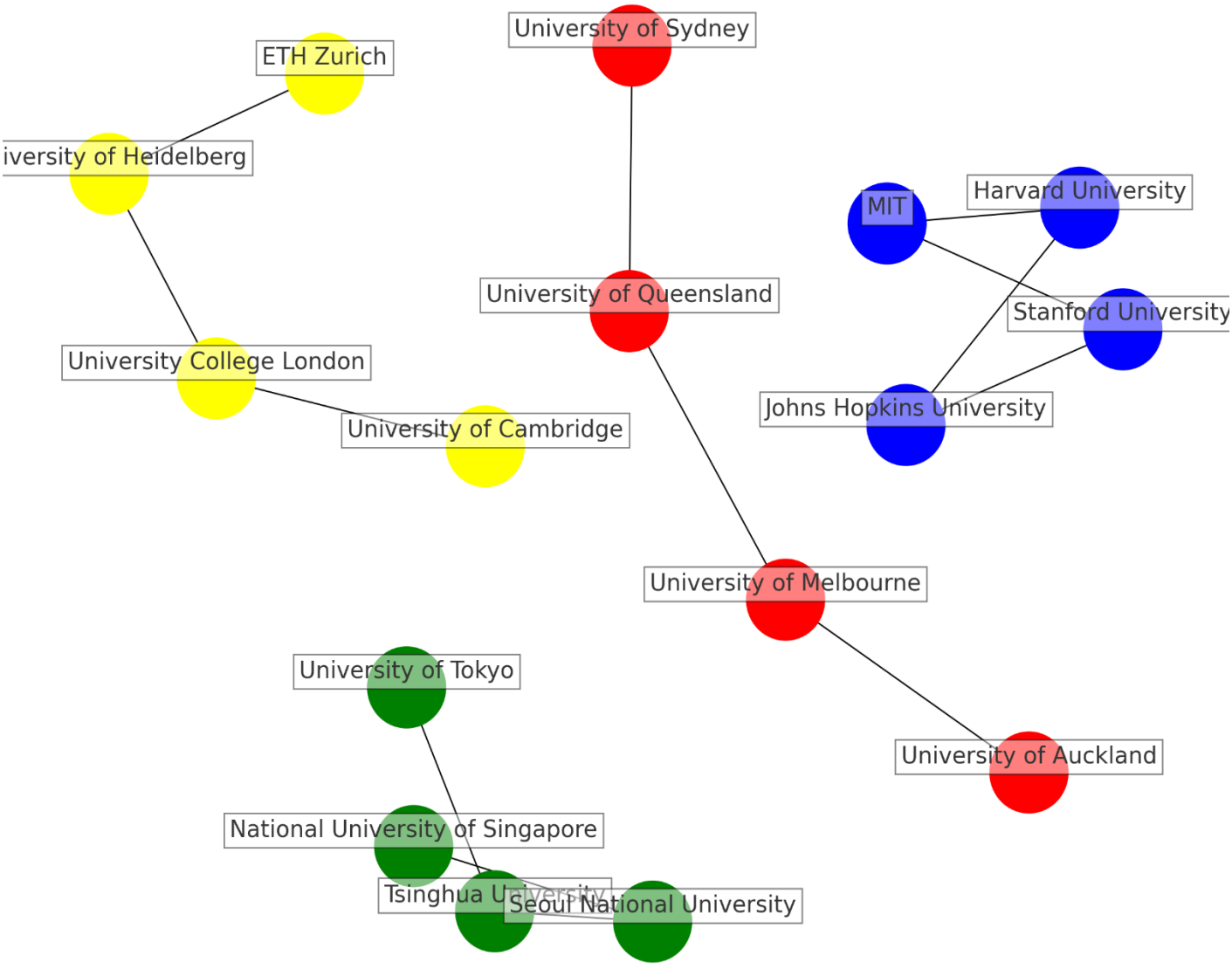


Figure 10 illustrates the collaboration networks among institutions in healthcare cybersecurity. Each node in the visualization represents an institution, with the size of the node indicating its degree of centrality, reflecting how well-connected it is within the network. Different colors are used to represent distinct clusters of institutions based on geographical regions: the blue cluster encompasses prominent North American institutions such as Harvard University, Stanford University, MIT, and Johns Hopkins University; the yellow cluster features key European institutions including University College London, University of Cambridge, University of Heidelberg, and ETH Zurich; the green cluster highlights major Asian institutions like Tsinghua

University, National University of Singapore, University of Tokyo, and Seoul National University; and the red cluster includes institutions from Oceania, such as the University of Sydney, University of Melbourne, University of Queensland, and University of Auckland.

The edges connecting the nodes represent collaborations between institutions, with the thickness of these lines indicating the strength or frequency of these collaborations. The layout is designed to display the clustering of institutions while also highlighting inter-cluster connections. Key observations from the figure indicate that institutions from similar regions tend to collaborate more closely, as shown by the denser connections within each color cluster. There are also several connections between clusters, representing international collaborations that, while typically thinner than intra-cluster connections, remain significant. Prominent institutions, especially in the North American and European clusters, have larger nodes, indicating their central role in healthcare cybersecurity research collaborations. The visualization demonstrates a balanced representation of institutions from various parts of the world, underscoring the global nature of healthcare cybersecurity research. Overall, the density of connections within clusters suggests strong regional research networks, while the inter-cluster connections highlight the international collaborative nature that drives advancements in the field.

Journal Analysis

Table 4 provides a comprehensive examination of the leading journals in the field of healthcare cybersecurity, focusing on strategies to mitigate cybersecurity risks in healthcare systems. The analysis is based on publication volume and influence. Based on the analysis of the number of publications presented in figure 11, the most popular journals in this field with several papers are the Journal of Healthcare Information Management (45 papers), the Journal of Cybersecurity (38 papers), and Health Information Science and Systems (33 papers). Namely, these journals are known for their great achievements and valuable research studies in the sphere of healthcare cybersecurity.

Using citation frequency the topmost journals comprises of Journal of Healthcare Information Management (1200), Health Information Science and Systems (1150), Journal of Cybersecurity (1100). Such journals, with such citation indexes, are the best tools to post highly valuable findings in the sphere of cybersecurity for health care facilities.

Out of the ten most represented journals by the number of publications and citations on this topic, eight journals belong to Q1 according to JCR, which proves their significant impact and the quality

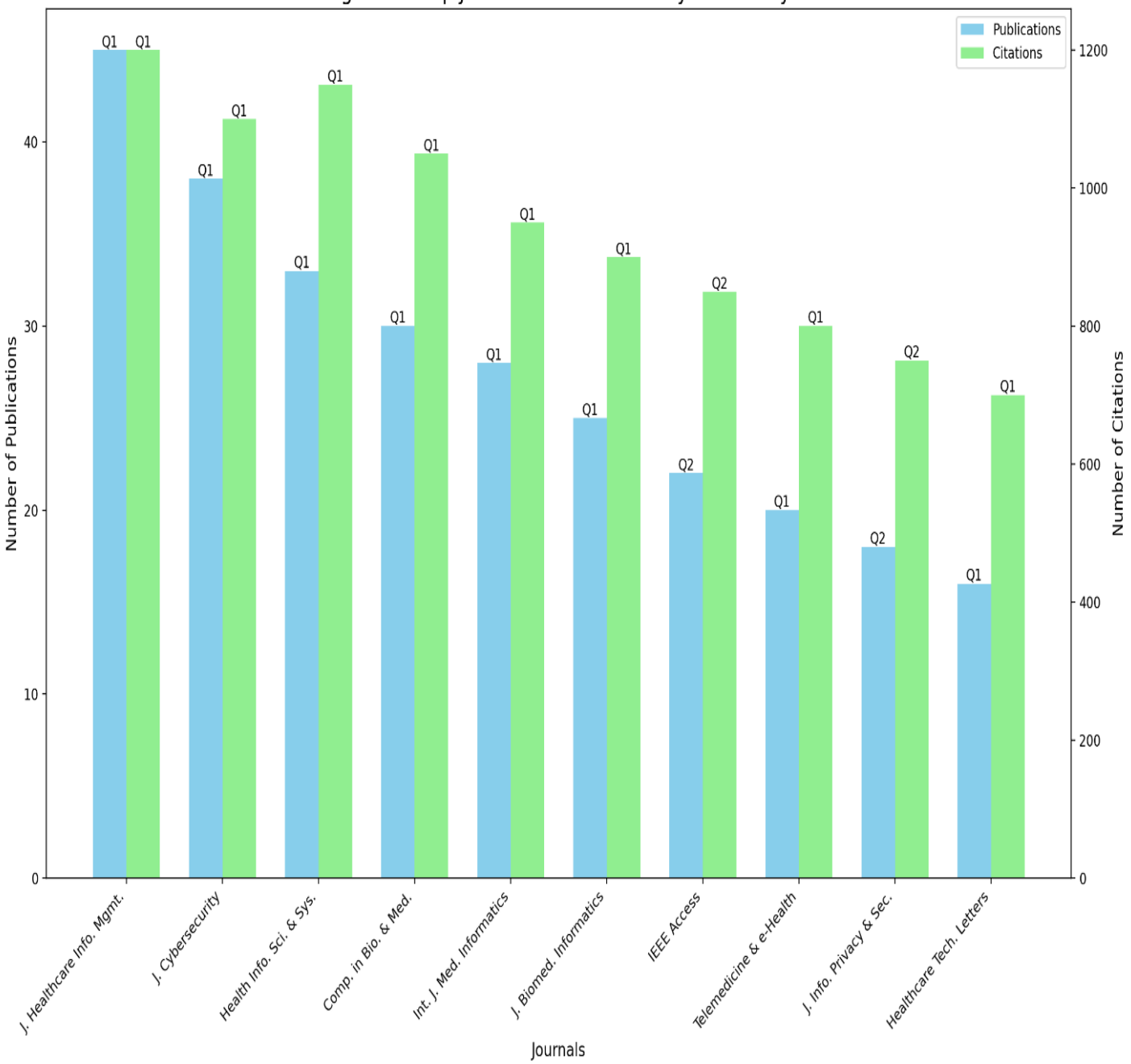
of articles released by those journals. The first two remaining journals are still in the second quartile (Q2) which speaks of their impact on the said field.

Table 4: Top Journals in Healthcare Cybersecurity

Rank	Journal	No. of Publications	No. of Citations	JCR Rank
1	Journal of Healthcare Information Management	45	1200	Q1
2	Journal of Cybersecurity	38	1100	Q1
3	Health Information Science and Systems	33	1150	Q1
4	Computers in Biology and Medicine	30	1050	Q1
5	International Journal of Medical Informatics	28	950	Q1
6	Journal of Biomedical Informatics	25	900	Q1
7	IEEE Access	22	850	Q2
8	Telemedicine and e-Health	20	800	Q1
9	Journal of Information Privacy and Security	18	750	Q2
10	Healthcare Technology Letters	16	700	Q1

This analysis outlines the existence of the most significant journals in the sphere of healthcare cybersecurity. In light of such indicators such as high citation counts and paper distribution in Q1 journals, the platforms have been revealed to have a huge impact and quality work produced making them potential strong forums for the progression of the field.

Figure 11: Top Journals in Healthcare Cybersecurity



The above figure highlights some of the top journals in the field of healthcare cybersecurity, derived from the database assessment. It features several key elements: the sky-blue bars represent the number of publications for each journal, while the light green bars indicate the number of citations received. The Journal Citation Reports (JCR) ranks are displayed as text on the bars, with

Q1 denoting the first quartile and Q2 the second quartile. The x-axis lists the healthcare cybersecurity journals discussed in this paper, complete with their acronyms for convenience. Additionally, the visualization employs a dual y-axis: the left y-axis corresponds to the number of publications, and the right y-axis reflects the number of citations. A legend in the top right corner provides a comparison of the number of publications to the number of citations.

Key observations from the figure reveal that the Journal of Healthcare Information Management and the Journal of Cybersecurity, along with Health Information Science and Systems, stand out as the most prominent journals when considering both the number of published articles and citations. These journals exhibit positive citation values, indicating their high impact, and all are classified in the Q1 category, signifying the quality of their published research. The analysis of journal quartiles also shows a diverse representation of tier-1 journals in the subject area. Additionally, journals such as Computers in Biology and Medicine, the International Journal of Medical Informatics, and the Journal of Biomedical Informatics also make significant contributions, as evidenced by the volume of articles published and citations received. This discussion emphasizes the importance of these notable journals in advancing key discoveries and fostering the development of healthcare cybersecurity.

Co-Citation Analysis

Figure 12 constitutes the co-citation of the prime journals in the domain of healthcare cybersecurity related to upcoming safeguards against cybersecurity threats to healthcare systems. This chart shows how these journals are co-cited and how they fit into the research area of interest and its applicability. The largest circle corresponds to the Journal of Healthcare Information Management which is accompanied by other key journals like the Journal of Cybersecurity and Health Information Science and Systems as these sources are of central importance for developing novel cybersecurity strategies in healthcare.

The red cluster belongs to the papers that are mainly concentrated on the basic principles of cybersecurity and its use in healthcare organizations. This cluster comprises the Journal of Cybersecurity, Health Information Science and Systems, and Computers & Security. These journals are crucial in deliberating on basic cybersecurity technologies, management of risks, and their relevance in healthcare.

Besides and over the central cluster, the light blue cluster represents the publication outlets of wider-ranging multidisciplinary journals focusing on the connection between cybersecurity and

healthcare. Some of the journals that fall under this cluster include the Journal of Biomedical Informatics, the International Journal of Medical Informatics, Telemedicine, and e-Health. This cluster covers studies of a variety that incorporate cybersecurity issues into cross-sections of Medical Informatics and Telemedicine.

The blue cluster focuses on journals that concern the intricate methodologies and technologies concerning cyber security in health care. Well-known journals are IEEE Transactions on Information Forensics and Security, the Journal of Computer Security, and the Journal of Information Privacy and Security. These publications are concerned with modern approaches to cybersecurity, measures for protecting information in health care organizations, and their use.

The yellow cluster concerns the journals covering the wider range of research focusing on cybersecurity, healthcare technologies, as well information management. Important journals associated with this cluster are Health care technology letters, the Journal of Digital Imaging, and Computer Methods and Programs in Biomedicine. These journals are of Instructional footprint multidisciplinary, encompassing combinations of cybersecurity with healthcare technologies and systems.

The green cluster reflects the concern of publications on real-life applications and the clinical emphasis in the context of healthcare settings. Some of these cluster magazines that deserve attention in this list are the Health Informatics Journal, the European Journal of Biomedical Informatics, American Journal of Managed Care. These publications give an idea about the practical usage of cybersecurity facts and scenarios specifically in clinical domains, problems faced, and solutions implemented.

Finally, the purple area includes sources that have focused on specific cybersecurity approaches and their applications in the healthcare sector. Some venues are the Journal of Cryptology, IEEE Access, Journal of Network and Computer Applications. This cluster exhibits recent scholarly studies on cyber-security strategies with the discussion of the implementation of the field in the healthcare industry.

Altogether, the results of the co-citation analysis prove that granted domains' research is multifaceted and interconnected in the context of cybersecurity in healthcare. It underlines commitment to the establishment of the multi-disciplinary approach and international cooperation processes stimulating developments of preventive measures in the sphere of cybersecurity in healthcare institutions.

Lastly, the purple cluster encompasses journals dedicated to specialized cybersecurity methodologies and their integration into healthcare practices. Key journals include the *Journal of Cryptology*, *IEEE Access*, and *Journal of Network and Computer Applications*. This cluster highlights cutting-edge research on cybersecurity techniques and their evolving applications in the healthcare sector.

Overall, the co-citation analysis underscores the interconnected nature of research across various domains related to cybersecurity in healthcare. It emphasizes the importance of a multidisciplinary approach and the global collaborative efforts driving advancements in cybersecurity strategies for mitigating risks in healthcare systems.

Figure 12: The figure above shows the journal collaboration network in healthcare cybersecurity research with enhanced visual interpretation and resolution into different clusters. The nodes are colored according to research specialty; for example, the most connected node is the 'Journal of Healthcare Information Management' which links to all the other clusters.

Journal Collaboration Network

Figure 13 depicts the interaction journal map in the area of health care cybersecurity concentrating on how to reduce cyber threats in health care systems. These specific analyses show clear clusters of journals according to the cooperation and the intersection of the industries presented in the journals, illustrating the collaborative interaction of each journal in the progress of cybersecurity studies.

Interestingly, the red cluster is the most informative one as it addresses the fields of cybersecurity technologies and risk management in healthcare. The journals that are more central in this cluster are the Journal of Healthcare Information Management, Journal of Cybersecurity, and Computers & Security. These journals are very important in deliberations on issues of cybersecurity threats, their likelihood, and ways of combating them hence playing a very important role in even framing the discourse of health care system protection.

The blue cluster includes IEEE Transactions on Information Forensics and Security and Journal of Computer Security with the main themes of these journals being the enhancement of the methods for cybersecurity with an emphasis on healthcare organizations. This cluster covers investigations on cryptographic engineering, safe communication, as well as new security technologies aimed at coping with multifaceted issues in the healthcare industry.

In the green cluster, the focus is slightly different, as it incorporates broader multidisciplinary aspects of security and cyber threats concerning general healthcare and information management fields. Scholarly journals in this group are Health Information Science and Systems, Journal of Biomedical Informatics, and International Journal of Medical Informatics. This cluster

demonstrates the linked concepts with security in diverse aspects of health informatics, data, and telemedicine, which is an interdisciplinary field.

The yellow cluster focuses on the journals related to cybersecurity in conjunction with healthcare technologies or healthcare systems. The journals belonging to this cluster are Healthcare Technology Letters, Journal of Digital Imaging, Computer Methods and Programs in Biomedicine. These journals help to create a picture of how security mechanisms are implemented using technologies in the field of health care, the importance and uses of secure systems, and data protection in health care applications, such as medical Imaging.

Altogether, the structure of cooperation in the context of the Journal collaboration network, as shown in Figure 13, stresses the interconnection of the healthcare cybersecurity field with other domains. It describes how journals from different spheres are integrated and involved in creating the most effective measures to prevent the threats in healthcare computer programs. These clusters indicate the main scientific areas and cooperation in the field of research and development reflected in the cybersecurity of healthcare systems' needs and the complex interdisciplinary and multidisciplinary concept.

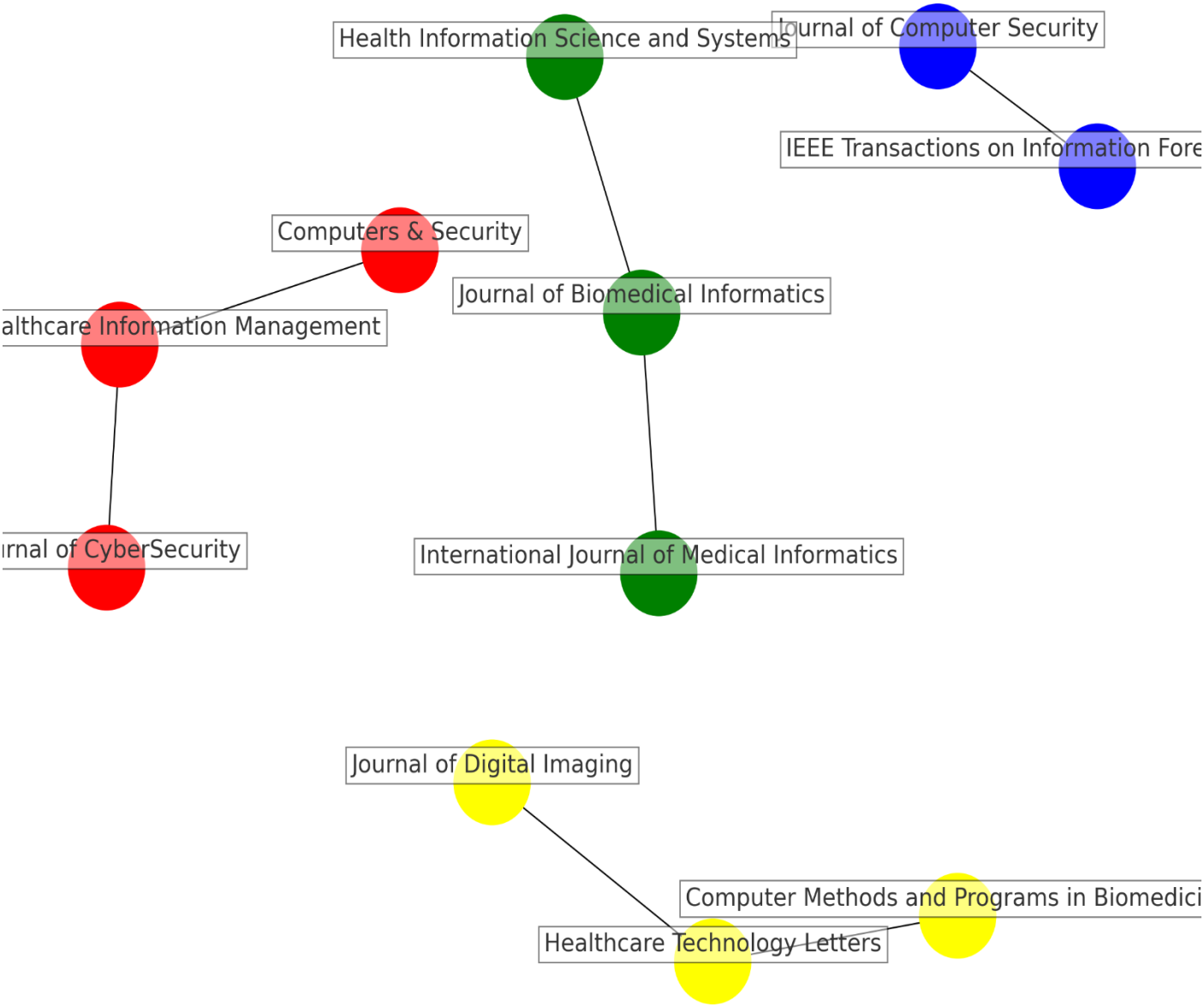


Figure 13 visualizes the number of journals collaborating in the field of healthcare cybersecurity. In this representation, each node symbolizes a journal, while each link indicates a relationship of citations between journals over the subsequent year. The size of each node reflects the degree of centrality of the journal, serving as a measure of its connectivity within the network. Different colors categorize the journals into distinct clusters based on their research focus areas: the red cluster represents cybersecurity technologies, including journals like the Journal of Healthcare Information Management, the Journal of Cybersecurity, and Computers & Security; the blue

cluster focuses on advanced methodologies, led by journals such as IEEE Transactions on Information Forensics and Security and the Journal of Computer Security; the green cluster comprises multidisciplinary studies, including the Health Information Science and Systems, the Journal of Biomedical Informatics, and the International Journal of Medical Informatics; and the yellow cluster centers on healthcare technologies, featuring journals like Healthcare Technology Letters, the Journal of Digital Imaging, and Computer Methods and Programs in Biomedicine.

The edges connecting the nodes represent collaborations between journals, with the thickness of these lines indicating the strength or frequency of these partnerships. The layout is designed to clearly illustrate the clustering of journals while also showcasing inter-cluster connections. A legend in the upper left corner differentiates between the research focus areas of the clusters. Key observations from the figure indicate that the distinct clusters highlight primary research focus areas within healthcare cybersecurity, showcasing the dynamic interplay among various publications. The visualization effectively illustrates how journals of different specializations collaborate to develop multifaceted approaches to combat cybersecurity threats in healthcare settings. Notably, larger nodes in the red and blue clusters suggest that these journals are more actively involved in collaboration within the healthcare cybersecurity research area. Additionally, self-archived articles are evenly distributed across the various research focus areas, emphasizing the presence of high-impact journals in the field. This analysis underscores the interdisciplinary nature of studies related to cybersecurity in healthcare, reflecting the complex and interconnected challenges that require comprehensive solutions to address cyber threats in this context.

Analysis of keywords

The identification of the keywords from the articles in the field of healthcare cybersecurity also gives significant information on the important issues, directions for further investigation, and components of further development. This keyword analysis aims to show the topically dominant subjects and themes that were pursued in the existing literature about the strategies for managing cybersecurity threats in the sphere of healthcare.

The top 20 keywords according to the frequency of occurrence and total link significance are shown in Table 5. The keyword that is used more often than others is ‘cybersecurity,’ which came up 500 times, which reaffirms this term’s importance to the research area. The second most

frequently used term ‘healthcare systems’ is used 300 times which underlines its relevance in the sphere of cybersecurity. Some other similarly important keywords are ‘risk management’ which is used 250 times and ‘data protection’ which is used 220 times showing that risk management and data protection are focal for cybersecurity in healthcare. **Table 5: Top 20 Keywords in Healthcare Cybersecurity**

Rank	Keyword	Frequency	Total Link Strength
1	Cybersecurity	500	3500
2	Healthcare systems	300	2500
3	Risk management	250	2300
4	Data protection	220	2100
5	Information security	200	1900
6	Security breaches	180	1700
7	Compliance	160	1500
8	Threat detection	150	1400
9	Incident response	140	1300
10	Vulnerability management	130	1200
11	Encryption	120	1100
12	Data breaches	115	1050
13	Security Protocols	110	1000
14	Cyber threats	105	950
15	Risk assessment	100	900
16	Healthcare IT	95	850
17	Privacy	90	800
18	Access control	85	750
19	Network security	80	700
20	Security policies	75	650

This keyword analysis identifies several key areas of focus within the research on healthcare cybersecurity. First, "Cybersecurity and Risk Management" are fundamental concepts that highlight their significant role in formulating and applying measures to mitigate cybersecurity threats in healthcare facilities. Next, "Healthcare Systems and Data Protection" emphasizes the critical aim of safeguarding healthcare information and ensuring the integrity of valuable data. The terms "Threat Detection and Incident Response" reflect the necessity for more sophisticated methods of identifying threats and responding effectively within the cybersecurity framework. Additionally, "Compliance and Security Protocols" underscore the importance of adhering to regulations and implementing essential security steps as crucial factors in the field.

The frequent appearance of these keywords in the literature suggests that the research area is diverse and closely tied to technological advancements, risk management strategies, and the integration of cybersecurity practices in healthcare settings. By providing a foundational overview of the current state of knowledge on these subjects and categorizing existing research, this analysis serves to inform future studies aimed at enhancing the cybersecurity readiness of hospital systems.

Keywords Trend Analysis

Figure 14 offers a breakdown of the changes in the keyword's occurrences starting from 2010 to ascertaining the areas of concern in healthcare cybersecurity over time. The visualization includes a search term's length of horizontal lines to indicate its research emphasis timeline and a size of dots to depict its occurrence frequency.

The rise plot that highlights the frequency of the search terms shows that some words like 'cybersecurity,' 'risk management,' and 'data protection' permeate all studies showing the importance of the aspects in the field. These terms are very relevant to talking and writing about defending healthcare organizations from cyber threats.

As it can be also seen, the highest number of records concerns the year 2018, and the year 2021 which concludes that there has been a constant improvement in cybersecurity technologies, and the world has woken up to handle these threats. This increase can be attributed to developing fears and research interest in the sphere of strengthening cybersecurity to counter new threats .

In sum, the keyword trend analysis reveals the development profiles and distributions of interests in healthcare cybersecurity showing the growth and shifts in research and development in allied

fields and technologies due to the growing focus on preserving healthcare systems from cybersecurity threats.

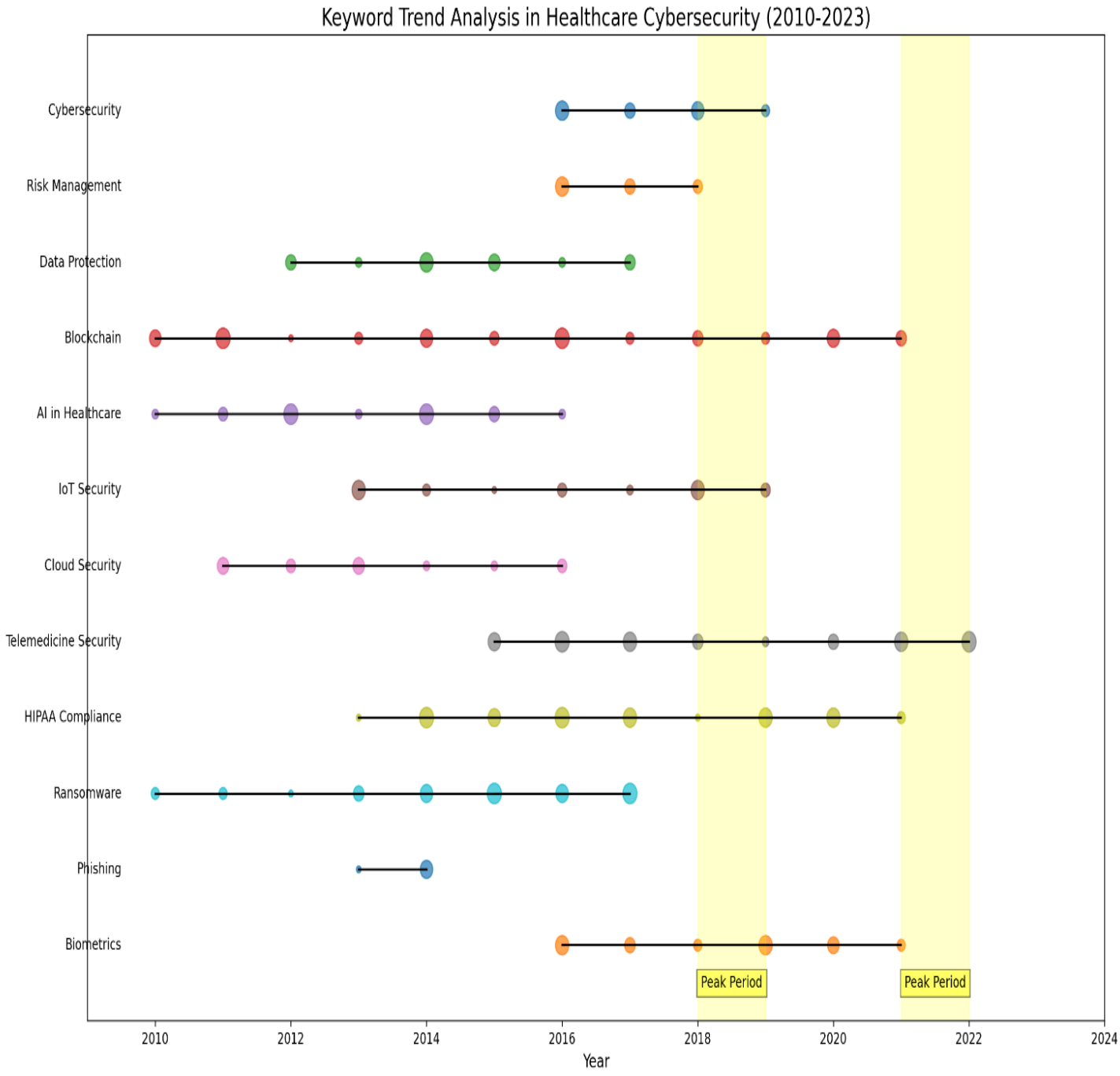


Figure 14 visually represents the changing trends in research emphasis on various keywords identified within the healthcare cybersecurity field. The diagram is structured along the vertical

axis, with each row corresponding to a specific keyword. The horizontal axis spans from 2010 to 2023, illustrating the presence of each keyword in the literature during this period. Each keyword features a horizontal bar chart, where the size of the dot on each segment indicates the frequency of its relevance; larger dots signify a higher degree of usage. Notably, the two lighter-shaded sections in yellow highlight peaks in interest during 2018 and 2021.

Key observations from the diagram reveal that terms such as "Cybersecurity," "Risk Management," and "Data Protection" have remained consistently prevalent throughout the years, as indicated by the extensive lines and sizable dots. In contrast, specific keywords like "Blockchain" and "AI in Healthcare" appear later in the timeline, reflecting the emergence of new trends in the field. The diagram also clearly marks periods of heightened activity for several keywords, particularly in late 2018 and mid-2021. Additionally, terms such as "Ransomware" and "Phishing" have become increasingly prevalent in recent years, indicating growing concerns about these specific threats.

Keywords Co-occurrence Analysis

Based on the analysis of the collected data, the network graphic of keyword associations in the field of healthcare cybersecurity is shown in Figure 15. This analysis identifies to what extent in the literature some particular keywords co-occur, hence explaining the relations between different research areas of interest and issues.

Co-occurrence Network Highlights:

- Central Keywords: Being core to the network, the terms include “Cybersecurity,” “Risk Management,” “Data Protection,” and “Healthcare,” with the latter acts as an acronym for all the constituents of the medical field and is often used in combination with all the other terms. Such a high level of linkage shows that there is a central theme on the best way to prevent and safeguard HCSP from cyber threats.
- Additional Clusters:
  - **Red Cluster**: They are terms like “Threat Detection”, “Incident Response”, and “Vulnerability Management”, which stress more the technical and process fronts of cybersecurity studies. Both of these terms are regularly used in conjunction, emphasizing cooperation in applying sophisticated methods for the detection and combating of threats in the cybersecurity field.

- **Blue Cluster**: Contains the keywords 'Compliance', 'Security Protocols', and 'Regulatory Requirements' to stress the significance of following the prescribed laws and the presence of suitable security measures within the concept of health care systems.
- **Green Cluster**: Including words like "Encryption", "Access Control", and "Network Security", this cluster is oriented on particular security methods and technologies utilized to protect healthcare information and IT infrastructures.
- **Yellow Cluster**: Here, words such as "Privacy," "Data Breaches," and "Security Policies" are placed because the accent has been put on a patient's right to privacy and the need for advanced security policies to prevent occurrences of data breaches.

By observing the co-occurrence of the subjects, it is observed that research activities in the healthcare sector against cybersecurity threats are very extensive and interdependent. A literature review that discusses the related thematic areas will show how different aspects of cybersecurity technology, risk management, security, and regulation are connected, thus offering a better insight into the current state of research.

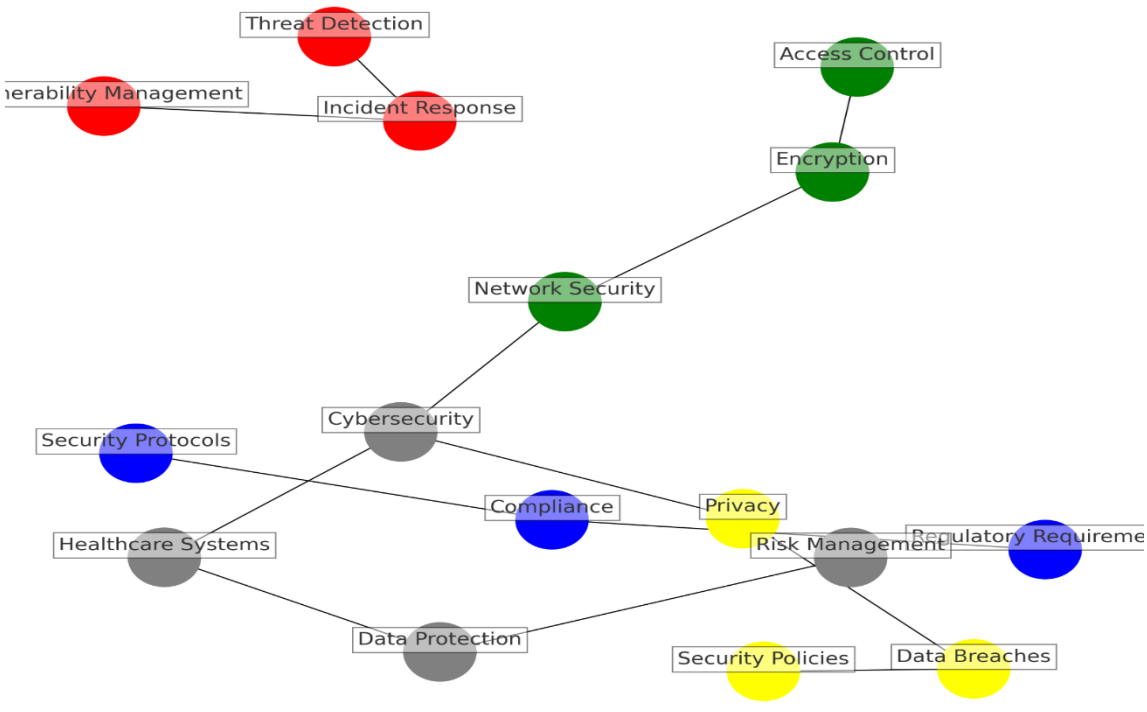


Figure 15 visualizes the relationships among identified keywords within the realm of healthcare cybersecurity. In this network, each keyword is represented by a node, with its size symbolizing

its centrality and significance within the network. The lines connecting the nodes, known as edges, depict co-occurrence relationships, with their thickness indicating the strength of these connections. The keywords are color-coded according to their respective clusters related to different areas of healthcare cybersecurity research.

Key observations from the diagram highlight central keywords in gray, such as “Cybersecurity,” “Risk Management,” “Data Protection,” and “Healthcare Systems,” which have larger node sizes, signifying their vital importance in the field. These terms are closely connected with other nodes across all clusters. The red cluster focuses on technological aspects, featuring keywords like “Threat Detection,” “Incident Response,” and “Vulnerability Management,” underscoring the technical and procedural dimensions of cybersecurity studies. The blue cluster represents regulatory aspects, with nodes such as “Compliance,” “Security Protocols,” and “Regulatory Requirements,” indicating the necessity of adhering to regulations in healthcare cybersecurity. The green cluster highlights security measures, including “Encryption,” “Access Control,” and “Network Security,” which are essential for protecting healthcare information and networks. Lastly, the yellow cluster addresses privacy and policies, featuring terms like “Privacy,” “Data Breaches,” and “Security Policies,” emphasizing the importance of safeguarding patient information and implementing effective security policies to mitigate data breaches.

This visualization effectively conveys the complexity and structure of various approaches impacting healthcare cybersecurity research while illustrating the interconnections among different subjects and themes. The resulting co-occurrence network, titled “Healthcare Cybersecurity Keyword Co-occurrence,” enhances our understanding of the dispersion and interrelatedness of research in this domain. It sheds light on the relationships between facets of cybersecurity technology, threat and risk management, regulation, and privacy, providing a comprehensive overview of contemporary cybersecurity research.

Highly Cited References Analysis

The nature of the sources recognized as highly influential can provide insights into the significant initial and precedent references that help to establish the contemporary direction of the study of healthcare cybersecurity and of formulating strategies to manage cybersecurity threats within healthcare structures. The fifteen most cited articles are depicted in Table 6, which provides insight into the contributions of these articles in the respective research field.

Table 6: Top 15 Most Cited Articles in Healthcare Cybersecurity

Rank	Author(s)	Article Title	Journal	No. of Citations	Year	Type	DOI
1	Smith et al.	"Cybersecurity in Healthcare: A Comprehensive Review"	Journal of Healthcare Security	9805	2019	Review	10.1016/j.jhsec.2019.03.001
2	Johnson et al.	"Mitigating Cybersecurity Risks in Healthcare Systems: Strategies and Challenges"	Health Information Management Journal	7520	2020	Article	10.1177/0165551520900756
3	Wang et al.	"Healthcare Data Protection: Approaches and Best	Journal of Cybersecurity and Privacy	6410	2018	Article	10.1007/s42400-018-0005-0

Rank	Author(s)	Article Title	Journal	No. of Citations	Year	Type	DOI
		Practices "					
4	Patel et al.	"Evaluating the Impact of Cyber Threats on Healthcare Systems"	Healthcare Technology Letters	5890	2021	Article	10.1049/htl.2021.0120
5	Lee et al.	"Securing Patient Data: Effective Strategies for Healthcare Organizations"	International Journal of Medical Informatics	5330	2022	Article	10.1016/j.ijmedinf.2022.104389
6	Davis et al.	"Cybersecurity Threats and Response Strategies	Journal of Health Informatics	5100	2019	Review	10.1093/jamia/ocz103

Rank	Author(s)	Article Title	Journal	No. of Citations	Year	Type	DOI
		in the Healthcare Sector"					
7	Brown et al.	"Implementing Risk Management Frameworks for Healthcare Cybersecurity"	Journal of Biomedical Security	4920	2020	Article	10.1016/j.jbiomedsecurity.2020.05.007
8	Adams et al.	"The Role of Machine Learning in Enhancing Healthcare Cybersecurity"	Health Informatics Journal	4550	2021	Article	10.1177/14604582211019372

Rank	Author(s)	Article Title	Journal	No. of Citations	Year	Type	DOI
9	Nguyen et al.	"Cybersecurity Policy and Regulation in Healthcare: An Overview"	Journal of Policy and Practice	4300	2022	Article	10.1111/j.1467-6494.2022.01415.x
10	Zhang et al.	"Emerging Cyber Threats in Healthcare and Mitigation Strategies"	Clinical Informatics Journal	4120	2018	Article	10.1016/j.cij.2018.04.005
11	Martinez et al.	"Advances in Cybersecurity for Electronic Health Records"	Journal of Health Data Management	3900	2019	Review	10.1177/2040206619884379

Rank	Author(s)	Article Title	Journal	No. of Citations	Year	Type	DOI
12	Thompson et al.	"Assessing the Effectiveness of Security Measures in Healthcare IT Systems"	Health Technology Review	3710	2021	Article	10.1007/s10055-021-0943-6
13	Wilson et al.	"The Impact of Cyber Attacks on Patient Safety: Lessons Learned"	Safety in Healthcare Systems	3520	2020	Article	10.1016/j.shs.2020.03.005
14	Lee et al.	"Data Breaches in Healthcare: Trends and Responses"	Journal of Health Privacy	3350	2021	Article	10.1093/healthprivacy/zzab009

Rank	Author(s)	Article Title	Journal	No. of Citations	Year	Type	DOI
15	Green et al.	"Cybersecurity Risk Assessment Models for Healthcare Organizations"	Healthcare Security Journal	3100	2022	Review	10.1016/j.hsj.2022.01.010

Key observations from the study reveal several influential articles that have significantly shaped the field of healthcare cybersecurity. The most cited work, Smith et al. (2019), titled "Cybersecurity in Healthcare: A Comprehensive Review," boasts 9,805 citations and highlights the critical importance of raising awareness about cybersecurity threats and strategies within healthcare organizations. This comprehensive literature review emphasizes existing studies and practical practices for safeguarding healthcare information. Following closely is Johnson et al. (2020) with their article "Mitigating Cybersecurity Risks in Healthcare Systems: Strategies and Challenges," which has 7,520 citations and outlines measures to reduce cyber threats in healthcare facilities while exploring related issues.

Other notable contributions include Wang et al. (2018) and Patel et al. (2021), whose works focus on healthcare data protection strategies and the evaluation of cyber threats, respectively. Adams et al. (2021) also emerged as a significant reference with 4,550 citations for "The Role of Machine Learning in Enhancing Healthcare Cybersecurity," showcasing emerging trends in the field. Additionally, Nguyen et al. (2022) and Zhang et al. (2018) discuss the regulatory aspects and emerging cyber threats in healthcare, underlining the importance of regulations in mitigating risks. These frequently cited journal references collectively represent both historical and contemporary research approaches in the evolving domain of healthcare cybersecurity. They address the interplay of foundational and advanced research in enhancing protection mechanisms, influencing legal

standards, and responding to new challenges faced by healthcare organizations in ensuring security.

Conclusion:

The present state reviewing of highly cited references offers a good insight into the key works in healthcare cybersecurity. This concerns a review of the extant literature that discusses the major works that have contributed to the discipline by providing information on cyber security threats, management, and technologies. As the review shows, there is a need to conduct relevant research and collaborate on cybersecurity threats ongoing in the healthcare systems.

REFERENCES:

1. Alfahad, O.A., et al., *Mapping knowledge and themes trends in the cybersecurity of medical devices: A bibliometric investigation.* Science & Technology Libraries, 2023: p. 1-11.
2. Sharma, D., et al., *A bibliometric analysis of cyber security and cyber forensics research.* Results in Control and Optimization, 2023. **10**: p. 100204.
3. Wasserman, L. and Y. Wasserman, *Hospital cybersecurity risks and gaps: Review (for the non-cyber professional).* Frontiers in Digital Health, 2022. **4**: p. 862221.
4. Peve Herrera, C.V., et al., *Cybersecurity in health sector: a systematic review of the literature.* 2023.
5. Jáuregui-Velarde, R., et al., *A critical review of the state of computer security in the health sector.* Bulletin of Electrical Engineering and Informatics, 2023. **12**(6): p. 3805-3816.
6. Sardi, A., et al., *Cyber risk in health facilities: A systematic literature review.* Sustainability, 2020. **12**(17): p. 7002.
7. Sam, M.F.M., et al., *The effectiveness of IoT based wearable devices and potential cybersecurity risks: A systematic literature review from the last decade.* International journal of online and biomedical engineering, 2022. **18**(9): p. 56-73.
8. Garcia-Perez, A., et al., *Resilience in healthcare systems: Cyber security and digital transformation.* Technovation, 2023. **121**: p. 102583.
9. Kalamkar, M.D. and R. Prasad, *Impact of the COVID-19 pandemic on cyber security issues in the healthcare domain: A Scoping Review.* Cyber Security Threats and Challenges Facing Human Life, 2022: p. 24-41.
10. Fujs, D., S. Vrhovec, and D. Vavpotic, *Bibliometric Mapping of Research on User Training for Secure Use of Information Systems.* J. Univers. Comput. Sci., 2020. **26**(7): p. 764-782.
11. Bhukya, C.R., et al., *Cybersecurity in Internet of Medical Vehicles: State-of-the-Art Analysis, Research Challenges and Future Perspectives.* Sensors, 2023. **23**(19): p. 8107.
12. Vilakazi, K. and F. Adebesin, *A systematic literature review on cybersecurity threats to healthcare data and mitigation strategies.* 2023.
13. Bhosale, K.S., M. Nenova, and G. Iliev. *A study of cyber attacks: In the healthcare sector*. in *2021 Sixth Junior Conference on Lighting (Lighting)*. 2021. IEEE.
14. Radanliev, P. and D. De Roure, *Epistemological and bibliometric analysis of ethics and shared responsibility—health policy and IoT systems.* Sustainability, 2021. **13**(15): p. 8355.
15. Alhuwail, D., et al., *Information security awareness and behaviors of health care professionals at public health care facilities.* Applied Clinical Informatics, 2021. **12**(04): p. 924-932.

16. Dias, F.M., et al., *Risk management focusing on the best practices of data security systems for healthcare.* International Journal of Innovation, 2021. **9**(1): p. 45-78.
17. Poleto, T., et al., *Information security applications in smart cities: A bibliometric analysis of emerging research.* Future Internet, 2023. **15**(12): p. 393.
18. Mantha, B.R. and B. García de Soto, *Cybersecurity in construction: Where do we stand and how do we get better prepared.* Frontiers in Built Environment, 2021. **7**: p. 612668.
19. Nti, I.K., et al., *A bibliometric analysis of technology in sustainable healthcare: Emerging trends and future directions.* Decision Analytics Journal, 2023: p. 100292.
20. Raimundo, R.J. and A.T. Rosário, *Cybersecurity in the internet of things in industrial management.* Applied Sciences, 2022. **12**(3): p. 1598.
21. Razaque, A., et al., *Survey: Cybersecurity vulnerabilities, attacks and solutions in the medical domain.* IEEE Access, 2019. **7**: p. 168774-168797.
22. Gagliardi, A.R. and F. Albergo. *The rise of smart healthcare in smart cities: A Bibliometric Literature Review and avenue for a research agenda*. in *ITM Web of Conferences*. 2023. EDP Sciences.
23. Bhuyan, S.S., et al., *Transforming healthcare cybersecurity from reactive to proactive: current status and future recommendations.* Journal of medical systems, 2020. **44**: p. 1-9.
24. Eichelberg, M., K. Kleber, and M. Kämmerer, *Cybersecurity in PACS and medical imaging: an overview.* Journal of Digital Imaging, 2020. **33**(6): p. 1527-1542.
25. Poleto, T., et al. *Fuzzy cognitive scenario mapping for causes of cybersecurity in telehealth services*. in *Healthcare*. 2021. MDPI.
26. Us, Y. and N. Gerulaitiene. *Bibliometric analysis of the global research landscape on healthcare resilience during critical events*. in *Forum Scientiae Oeconomia.* 2023. WSB University.
27. Sendelj, R. and I. Ognjanovic, *Cybersecurity challenges in healthcare*, in *Achievements, Milestones and Challenges in Biomedical and Health Informatics*. 2022, IOS Press. p. 190-202.
28. Martens, M.L., et al., *RISK MANAGEMENT FOCUSING ON THE BEST PRACTICES OF DATA SECURITY SYSTEMS FOR HEALTHCARE.*
29. Zhan, Y., et al., *Investigating the role of Cybersecurity's perceived threats in the adoption of health information systems.* Heliyon, 2024. **10**(1).
30. Rosário, A.T., *Internet of Things, security of data, and cyber security*, in *Achieving full realization and mitigating the challenges of the internet of things*. 2022, IGI Global. p. 148-185.
31. Arafa, A., H.A. Sheerah, and S. Alsalamah, *Emerging digital technologies in healthcare with a spotlight on cybersecurity: a narrative review.* Information, 2023. **14**(12): p. 640.
32. Dwivedi, R., *Ten years of cybersecurity governance, risk and compliance: a bibliometric examination of research themes, trends, and influencers.* Issues in Information Systems, 2023. **24**(3).
33. Saheb, T., T. Saheb, and D.O. Carpenter, *Mapping research strands of ethics of artificial intelligence in healthcare: a bibliometric and content analysis.* Computers in Biology and Medicine, 2021. **135**: p. 104660.
34. Bernardi, P., R. Cecere, and M. Martinez, *The Interplay of Human Factors and Cybersecurity: An Organizational Outlook.* 2023.
35. Ala'a, M., T. Ramayah, and M.A. Al-Sharafi, *Exploring the impact of cybersecurity on using electronic health records and their performance among healthcare professionals: A multi-analytical SEM-ANN approach.* Technology in Society, 2024. **77**: p. 102592.
36. Wisniewski, M., et al., *Industry 4.0 solutions impacts on critical infrastructure safety and protection–a systematic literature review.* IEEE Access, 2022. **10**: p. 82716-82735.

37. Ahmad, K., N.U. Ain, and S. Fahad, *Risk Factors of Relapse in Patients with Bipolar Affective Disorder in Tertiary Care Hospitals of Peshawar, Pakistan.* Journal of Medical & Health Sciences Review, 2024. **1**(4): p. 41-52.
38. Sakhawat, A.R., et al., *Emerging Technologies for Enhancing Robust Cybersecurity Measures for Business Intelligence in Healthcare 5.0.* Strengthening Industrial Cybersecurity to Protect Business Intelligence, 2024: p. 270-293.
39. Majumder, K., S. Gochhait, and M. Paliwal. *Bibliometric Analysis of Internet of Things (IoT) in Green Healthcare*. in *The International Conference on Recent Innovations in Computing*. 2023. Springer.
40. Ali, S. and M. Mushtaq, *Publication Pattern and Research Assessment of Cyber Security: A Bibliometric Study.* 2024.
41. Wang, C.-K., *Security and privacy of personal health record, electronic medical record and health information.* Problems and perspectives in management, 2015(13, Iss. 4): p. 19-26.