International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V72I12P108

Volume 72 Issue 12, 88-98, December 2024

Original Article

Evolution of Information Security and Data Privacy in Medical Systems: A Bibliometric Analysis (2010-2024)

Adam Muhudin[1*], Abdullahi Mohamud Osoble[1], Abdirahman Abdullahi Omar[1], Mohamed Abdirahman Addow[1], Osman Diriye Hussein[2]

[1]*Faculty of Computing, SIMAD University, Mogadishu, Somalia*.
[2]*Faculty of Engineering, SIMAD University, Mogadishu, Somalia*.

**Corresponding Author : adammuhudin@simad.edu.so*

Received: 03 September 2024 Revised: 06 November 2024 Accepted: 25 November 2024 Published: 25 December 2024

Abstract *- This paper describes the evolution of information security and data privacy in medical systems from 2010-2024. The protection of sensitive patient data, regarding which critical concern has been raised, is an imperative part of the healthcare world in these fast-growing digital times. This study explores the trends, research domains, highly-cited publications, and contributions of different countries and institutions in the concerned discipline. Using data derived from the Scopus database, this study has highlighted a significant increase in research output with regard to technological advancement and the raising of cybersecurity concerns in healthcare. The findings reveal that the research domain is collaborative, journal articles and conference papers dominate, and emerging influential scholars and sources are present. The paper further looks into thematic developments and highlights areas that call for further research, especially in advanced technologies like AI and blockchain, for better data security. This analysis, therefore, enhances insights for scholars, policymakers, and practitioners in efforts towards hardening medical systems against evolving cyber threats with the continued protection of patient privacy.*

Keywords *- Information security, Data privacy, Medical systems, Cybersecurity, Technological advancement.*

1. Introduction

The healthcare sector has experienced a profound transformation in recent years, propelled by technological advancements and the growing incorporation of digital systems [1]. This progression has resulted in notable enhancements in patient care, operational effectiveness, and data governance [2]. Nevertheless, it has presented new challenges [3], especially concerning information security and data privacy [4]. The safeguarding of sensitive medical information [5] has emerged as a significant issue [6] in light of the growing digitization, sharing, and analysis of healthcare systems and patient data [7]. Within healthcare data, two interrelated yet somewhat different concepts are information security and data privacy[4]. Information security involves the policies, practices, and technologies intended to ensure the security of healthcare information from unauthorized access, alteration, or destruction. This approach involves protecting health information in digital and physical forms to ensure that information is confidential, available, and accurate[5]. In contrast, data privacy concerns the rights and processes dealing with the collection, use, and sharing of personal data, focusing on ensuring that the sensitive information of individuals complies with legal standards regarding the protection of sensitive information[7]. While information security deals more with the mechanisms of protection, data privacy addresses how data is handled in a way that respects individual autonomy and complies with regulations concerning privacy. While many of those terms are used interchangeably, they serve different purposes [3]. Security information and data privacy in medical systems [8] moved from a goodwill option to an integral part of healthcare administration [9]. The adoption of electronic health records, telemedicine, and IoT devices [16] in healthcare has significantly increased the attack surface area of healthcare against cyber threats [10]. This, coupled with the increase in complexity, has led to various data breaches, unauthorized access, and other forms of cyberattacks, putting at risk patient privacy and safety [11]. Understanding the evolution of information security and data privacy practices in healthcare will, therefore, be important in formulating efficient ways to mitigate these risks [12]. This study conducts an extensive bibliometric analysis of developing information security and data privacy in medical systems from 2010 through 2024. By examining the trends, major research domains, and key publications in this period, the paper tries to provide insight into advances in security practice in the healthcare sector [19] and the challenges that have shaped the current landscape [13]. Moreover, regulatory structure variations [20], technological development [13], and changing risks all influence information security [21] and data privacy protocol evolution

in medical systems [14]. The results of this research will help us comprehend how the industry has changed in the past decade, highlighting the key areas that require further research and attention [15]. However, as far as modernization goes in the healthcare sector, it is important to ensure that patient information remains protected [18] and confidential [13]. This study will be an important source for scholars, policymakers, and practitioners working to strengthen the resilience of medical systems against active cyber threats [3, 17].

2. Literature Review

The literature review section provides a detailed review of previous findings and key studies in the Evolution of Information Security and Data Privacy in Medical Systems. This section highlights significant advancements, emerging trends, and central themes by analyzing a broad spectrum of academic contributions. This section synthesizes and critiques prior research, offering a comprehensive understanding that sets the stage for the procedural method used in our bibliometric analysis.

In 2019, a study by Y. Sun et al. [1] addressed critical privacy, security, and storage challenges within the background of growing digitization in healthcare, presenting the increase in risks to patient privacy due to the growth in the usage of EHRs, mobile and cloud based technologies. The paper highlights that, while all the regulations like HIPAA aimed at protecting patient information, making it compliant with a wide range of healthcare platforms is still quite an uphill task. Regarding the security of the systems holding medical data, the authors also mention the rapid increase in threats due to cyberattacks, such as phishing and ransomware attacks; they support using multi layered strategies, such as encryption and access controls.

Y. Sun et al. [1] discussed storage challenges, pointing to the limitations of traditional systems and the shift to cloud solutions for greater flexibility, though at the same time, arising risks such as data breaches and the so-called' data sovereignty problem'. As a counterbalance in this choice between accessibility and the need for security and compliance with laws, they have proposed an on-premises with cloud storage hybrid approach. Conclusively, the authors have proposed advanced encryption, blockchain technology, and improvement of access control mechanisms. Additionally, there is a greater call for collaboration across the board for healthcare providers, technology developers, and policymakers in an effort towards the realization of a more secure and efficient management of the data ecosystem, even as areas for future research are being identified for developing AI and machine learning to improve data security. In 2019, a study by AKM Iqtidar Newaz et al. [2] reviewed security and privacy challenges in modern healthcare systems. Such attacks on healthcare information systems include data breach incidents, denial of service, and ransomware, which, according to the authors, get great momentum with increasing integrations of sophisticated technologies into healthcare systems, such as IoT and cloud computing. They highlighted several vulnerabilities accompanying these technologies, underlining that as much as they provide enormous benefits related to efficiency and patient care, they equally increase the attack surface, making healthcare systems more vulnerable to cybersecurity threats.

Relating to these challenges, AKM Iqtidar Newaz et al. [2] discuss various defense mechanisms developed to protect healthcare systems. Therefore, they discussed different ways the data is secured, including encryption, IDS, and secure authentication. The authors have also emphasized the need for a multi-layered defense strategy that will combine the various security measures into comprehensive protection against diverse threats. They also called for continued research and development to match the growth in cyber threats in healthcare. They suggested that such efforts should be directed towards combining AI and ML to improve the detection and prevention of security breaches. In 2017, a study by Karim Abouelmehdi et al. [3] presented a critical review of big data security and confidentiality challenges in healthcare published in the Health Information Science and Systems journal. The authors present the challenges innate in managing huge volumes of healthcare data emanating from modern medical systems, focusing on the risks that could be unleashed about patient privacy and data security. They also observed that big data technologies in health care, as much as they provide enormous opportunities to enhance both patient outcomes and operational efficiencies, carry with them new vulnerabilities such as unauthorized access, data breaches, and misuse of sensitive information with regard to patients.

To this end, Karim Abouelmehdi et al. [3] examined the different security and privacy-enhancing technologies and strategies available to secure healthcare data. They further discussed how encryption, access control, and anonymization techniques can help maintain patient confidentiality while big data applications continue to be used for research and improvement in healthcare. The authors also indicate that strong data governance frameworks and regulatory mechanisms should be devised to support health organizations in managing big data properly and in conformity with all privacy laws and standards. They also call for further research in finding advanced security solutions, especially those implementing machine learning and artificial intelligence, in response to the new threats within healthcare's big data landscape. In 2014, a Farrukh Aslam Khan et al [4] study reviewed cloud computing and WBANs in healthcare. The researchers presented an overall framework that can help improve the security and privacy of patient data in a health environment using WBANs. This means that WBANs are increasingly integrated into healthcare systems for continuous monitoring and data acquisition, where sensitive patient information is involved. The paper deals with the possible novel risks from the transmission and storage of medical data

in cloud environments, considering that a security breach or unauthorized access could have profound effects. In resolving these challenges, the authors proposed using a framework that employs advanced encryption techniques coupled with protocols for secure data transmission, ensuring that the data at all levels of a patient's life is best protected. The framework also incorporates robust authentication methods to deter unauthorized access to healthcare data managed through WBANs and enhance security. In their article, Farrukh Aslam Khan et al [4] emphasized that there has to be a balance between the accessibility of patients' data to healthcare providers and the need for strict controls for privacy. The work represents part of the growing literature on how cloud technologies can be applied within the healthcare domain, with considerations for the paramount issues related to data security and the privacy of patients.

In 2014, a study by Harsh Kupwade Patil and Ravi Seshadri [5] discussed the most critical issues in healthcare related to big data: security and privacy. The authors examined the complexities that arise as health organizations increasingly rely on big data technologies to enhance patient care and operational efficiency. They highlighted the dual-edged nature of big data. While it offers significant benefits such as improved diagnostics and personalized treatments, it also poses considerable risks to the security and privacy of patient information.

The vast amount of sensitive healthcare data in marketplaces makes the sector an attractive target for cyber-attacks, data breaches, and unauthorized access. Harsh Kupwade Patil and Ravi Seshadri [5] thus discussed various different strategies and technologies to deal with these challenges. They proposed sound encryption methods, secure data storage solutions, and strict access control mechanisms to protect healthcare data from unauthorized access. Furthermore, the authors proposed the adoption of appropriate overall data governance frameworks that ensure compliance with privacy regulations and standards. The work reminds me of continuous innovative ways and alertness concerning healthcare data management, especially in a sector increasingly adopting and integrating big data technologies. Harsh Kupwade Patil and Ravi Seshadri [5] lend their voice to the broader debate on a balance between capitalizing on big data for advancement in healthcare and ensuring that patient information remains private and secure.

3. Methodology

The methodology for this bibliometric analysis involved research on the evolution of information security and data privacy in medical systems, embracing the period from 2010 to 2024. The bibliometric analysis hereby highlights trends, key research areas, influential publications, and the contributions of different countries and institutions in the field. This analysis will also give insight into how security practices in healthcare have evolved, particularly in response to technological advancement and emerging threats. The following subsections outline each step of our methodology in detail.

3.1. Data Collection and Search Strategy

The Scopus database was used for the current analysis due to its extensive coverage of peer-reviewed literature spanning various subjects, including medical, technical, and social sciences. Scopus is noted for the extensive number of journals indexed with conference proceedings and books, making it an ideal tool for capturing the heterogeneity of research in this area.

3.2. Search Strategy

The relevant articles related to the study were retrieved based on a systematic search using keywords related to medical systems, information security, and data privacy. The search string used was:

TITLE-ABS-KEY ("Healthcare Framework") AND TITLE-ABS-KEY ("Information Protection" OR "Safety" OR "Data Confidentiality") AND PUBYEAR > 2010 AND PUBYEAR < 2024

The search was limited to documents published between 2010 and 2024 to ensure a look into recent developments in the field. All search fields provided included the article title, abstract, and keywords for maximum relevance of results.

3.3. Data Screening and Preprocessing

Initially, 782 documents were identified in total. Following a comprehensive screening procedure, the documents were evaluated according to their relevance to the subject matter, accessibility of complete texts, and the quality of the research presented.

Documents not specifically pertinent to the evolution of information security and data privacy within medical systems, or those lacking adequate bibliometric data, were omitted from consideration. Consequently, the final dataset comprised 668 documents.

3.4. Data Analysis

Cleaning created a dataset subjected to a detailed bibliometric analysis based on various productivity, impact, and collaboration metrics. Analyses were conducted using Excel spreadsheets, VOSviewer, and the Bibliometrix package in R, specifically designed for such bibliometric analysis.

Using the aforementioned tools, we analyzed various aspects of the extracted data. These analytical steps ensured a comprehensive examination of the bibliometric data, providing valuable insights into research trends, influential contributions, and collaborative patterns in the evolution of information security and data privacy in medical Systems.

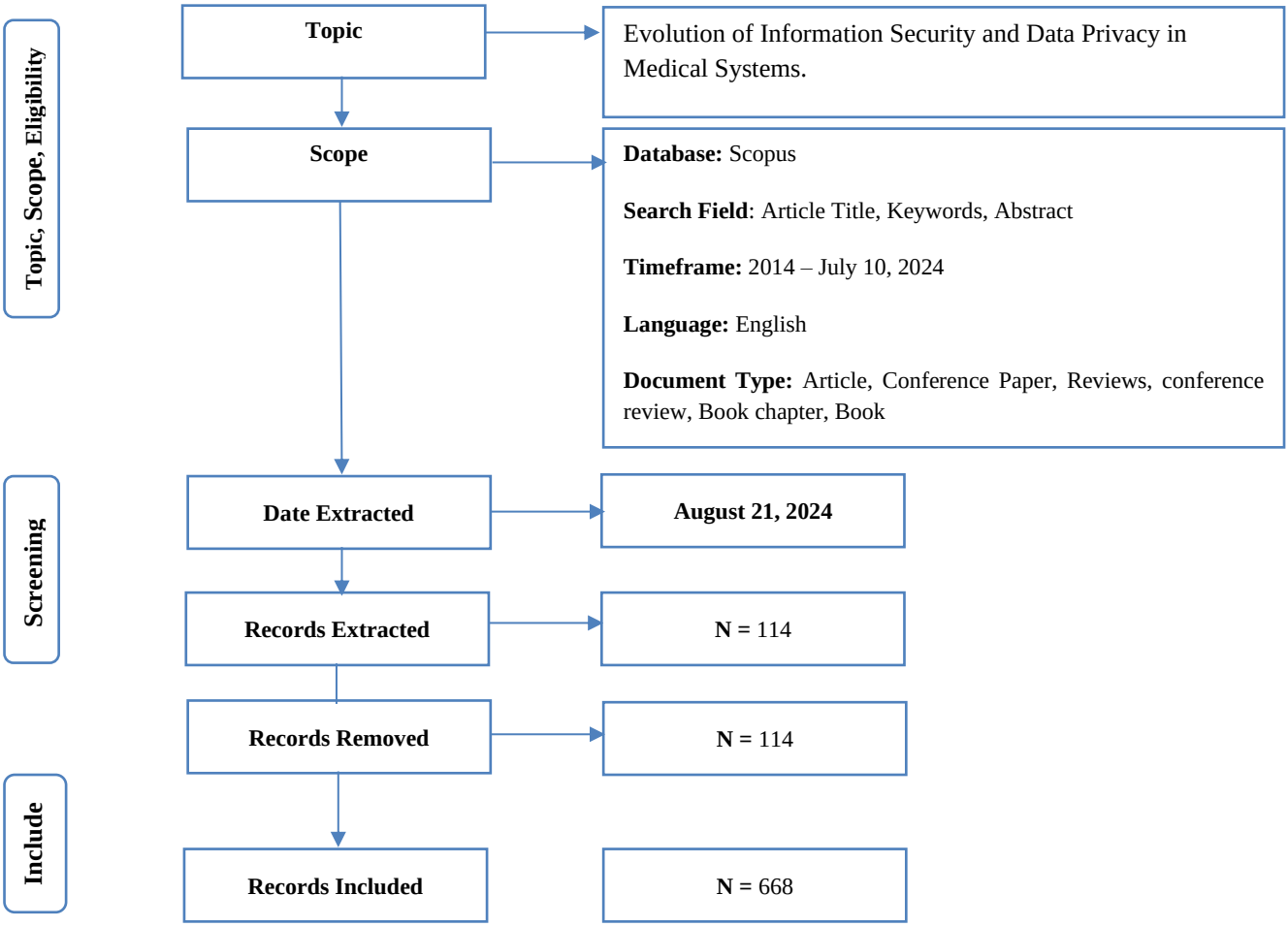

Fig. 1 Search and data screening strategy

4. Results and Discussion

4.1. Descriptive Analysis

Bibliometric analysis within 2010-2024 gives insight into the rapid growth and international collaboration in research on information security and data privacy in medical systems. The growth, from 668 documents drawn from 421 sources at an average annual growth rate of 10.92%, is steep.

This area of research is relatively young, with an average document age of 4.36 years and 14.71 citations per document. Collaboration is strong, with 3.8 co-authors per document on average and a high international co-authorship of 23.35%. The lion's share of the output is disseminated as journal articles and conference papers, revealing the fast-moving and interdisciplinary nature of the field. The data generally indicate a strong and dynamic research community dealing with key security and privacy questions in medical systems.

4.2. Document Type

Figure 2 shows the documents included in this review on information security and data privacy in medical systems. The figure shows that journal articles are the most frequent category, with 339 entries. This prevalence reveals that academic peer-reviewed journals form the main channel of research dissemination, reflecting the high quality and great impact the publications have on academia. With 235 entries, conference papers represent the second most frequent document type, suggesting that this field is dynamic, with active discussions and debates taking place at conferences. These events allow researchers to get immediate feedback and collaboration that, in many instances, can result in expanding conference papers into journal articles.

Besides, the presence of different document types, like book chapters and retracted articles, gives flavor to the research setting. The 44 book chapters realize that at least some research works are being compiled into comprehensive compilations. At the same time, the small numbers of retracted papers indicate the need to maintain ethical standards and accuracy in this sensitive area. Figure 3, showing the number of papers and citations per year from 2010 to 2024, provides a clear view of the growth trajectory in information security and data privacy in medical systems.

Table 1. Descriptive analysis

Description	Results
MAIN INFORMATION ABOUT DATA	
Timespan	2010:2024
Sources (Journals, Books, etc)	421
Documents	668
Annual Growth Rate %	10.92
Document Average Age	4.36
Average citations per doc	14.71
References	22470
DOCUMENT CONTENTS	
Keywords Plus (ID)	4166
Author's Keywords (DE)	1868
AUTHORS	
Authors	2054
Authors of single-authored docs	53
AUTHORS COLLABORATION	
Single-authored docs	55
Co-Authors per Doc	3.8
International co-authorships %	23.35
DOCUMENT TYPES	
Article	339
Book	4
Book Chapter	44
Conference paper	235
Conference review	11
Editorial	3
Erratum	1
Retracted	5
Review	26

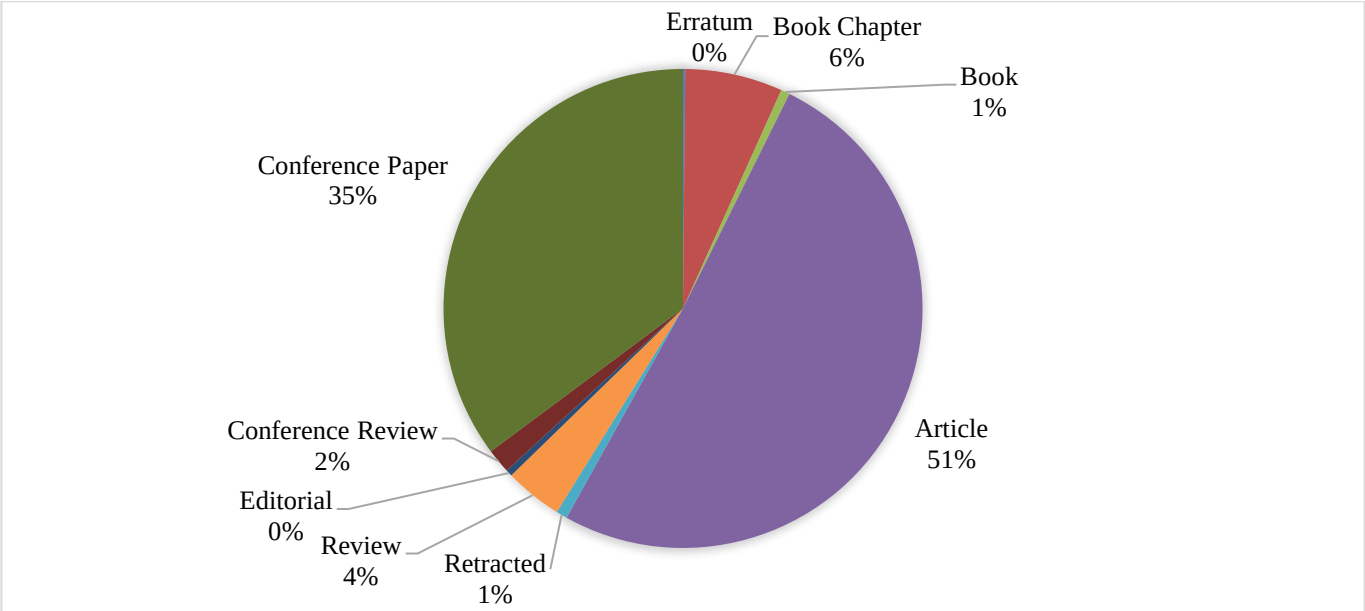

Fig. 2 Document type

4.3. Publications and Citations Trends

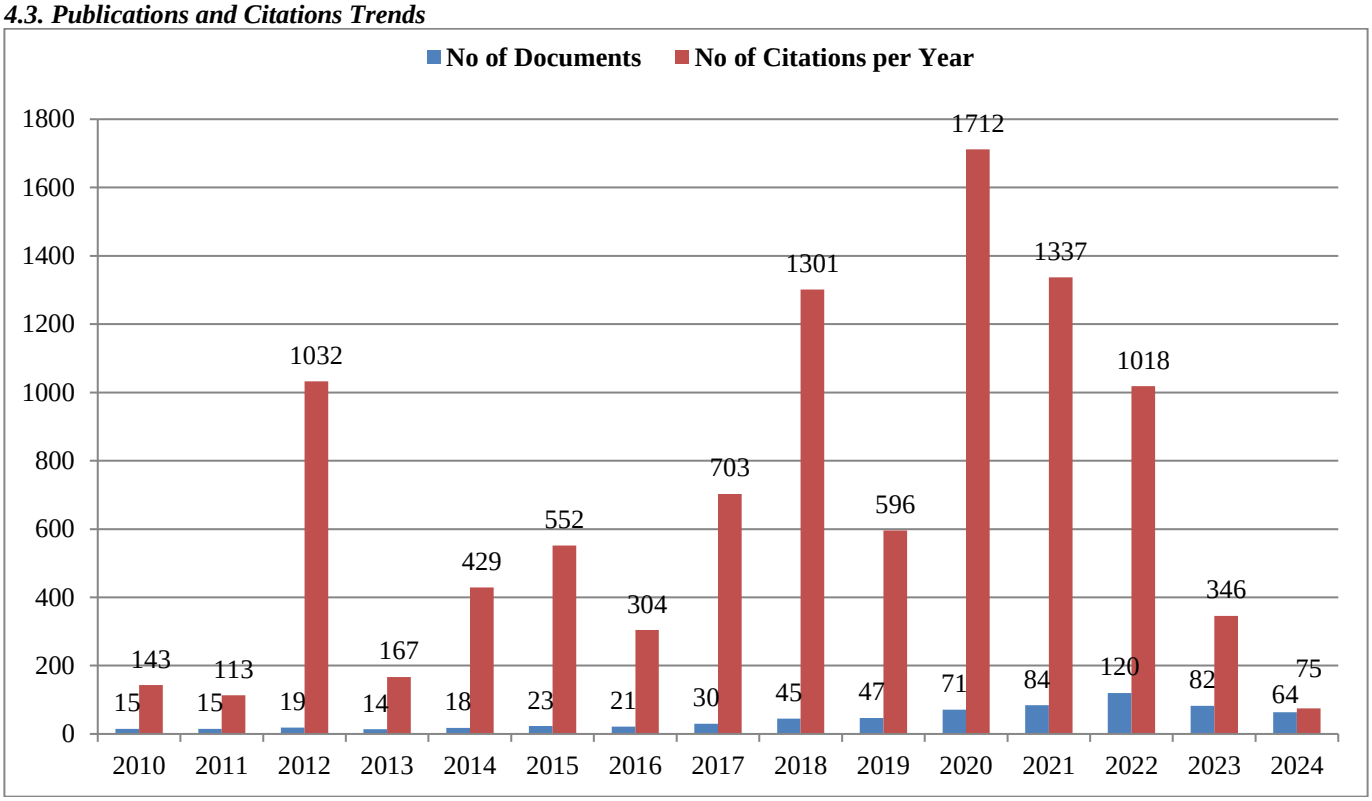

Fig. 3 Publications and citations trend

From 2010 to 2015, the number of publications on information security and data privacy in medical systems grew slowly, with annual figures ranging from 14 to 23 documents. This steady increase indicates that the topic gradually gained interest within the academic community. However, from 2016 onward, there was a notable rise in publications, nearly doubling within a few years. This surge likely reflects the increasing importance of cybersecurity in the healthcare sector, driven by technological advancements and growing concerns over data breaches and patient privacy.

The peak in 2022, with 120 documents, marks the height of this trend, showing the topic's prominence in academic and industry discussions. Citations per year follow a different pattern, with significant peaks in 2013, 2019, and particularly in 2020, where 1712 citations were recorded. The 2020 peak suggests that research during this period was highly influential, possibly due to the global focus on healthcare systems during the COVID-19 pandemic, which brought data security and privacy issues into sharper focus. The observed decline in publications and citations by 2024 might indicate a shift in research focus or that the field has reached a more mature phase where the rapid growth has stabilized.

4.4. Most Contributing Countries

The VOSviewer network visualization shows the serious contributions of countries involved in the bibliometric analysis of "Evolution of Information Security and Data Privacy in Medical Systems." It leads, fronted by India and China, with big and central nodes to show their high volume of research output and strong collaborative ties with other nations. Also, the United States assumes a strategic position, as suggested by its big node size and the numerous links that point to heavy involvement in international collaborative research. Further, the development of the visualization can be seen through robust collaborative networks: India also collaborates with Bangladesh and Iraq, while China connects with Malaysia, Japan, and other close neighbors. Similarly, the United States is outstanding for its strong collaboration with countries like Italy, South Korea, and Japan. In fact, the United States forms, so to say, the core of developing global research collaborations in this domain. Other emerging contributors are Malaysia, Turkey, and Saudi Arabia, the smaller nodes on the map. Although their research output is relatively small in volume, these countries have begun to show interest in this crucial area. The contributors are from a wide geographical dispersion covering Asia, Europe, North America, and the Middle East. This indeed emphasizes that information security and data privacy issues related to medical systems are core global problems. Such wide participation shows the connectedness and cooperation in research in this area and how established and emerging contributors are very important for the advancements in the field. Analysis of challenges in data security within the realm of health shows that it is a global workout that has been increasingly driven by various countries in different parts of the world.

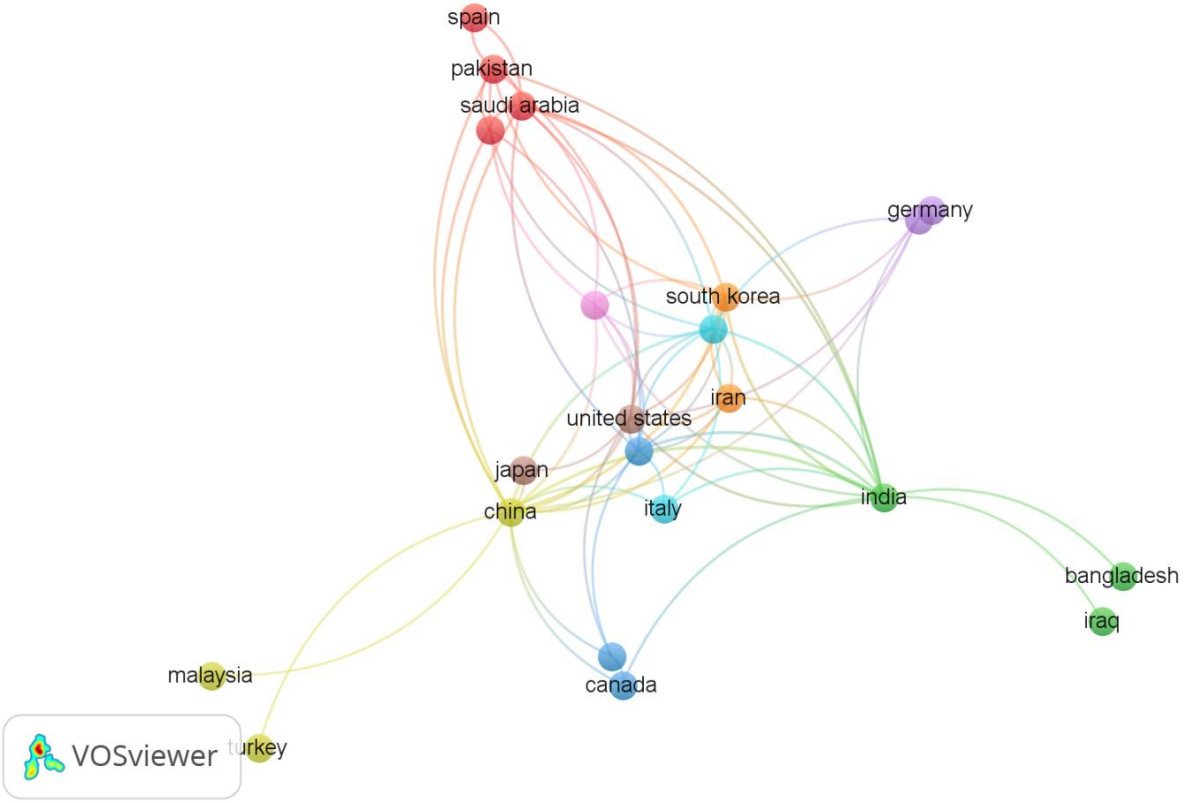

Fig. 4 Contributing countries

Table 2. Top ten most influential authors

Author	h_index	g_index	m_index	TC	NP	PY_start
LIU J	6	10	0.5	190	10	2013
WANG J	6	8	0.429	199	8	2011
ZHANG Y	6	10	0.75	101	11	2017
CHEN C-L	5	5	0.455	191	5	2014
CHOO K-KR	5	5	0.833	175	5	2019
HASEEB K	5	5	1	191	5	2020
LI Y	5	8	0.833	84	8	2019
MA J	5	5	0.556	140	5	2016
REHMAN A	5	6	1	196	6	2020
SABA T	5	5	1	189	5	2020

Table 3. Top ten most influential sources

Source	h_index	g_index	m_index	TC	NP	PY_start
Journal Of Medical Systems	16	26	1.231	827	26	2012
IEEE Access	11	18	1.833	362	18	2019
Security And Communication Networks	6	7	1	139	7	2019
Electronics (Switzerland)	5	5	0.714	122	5	2018
IEEE Internet Of Things Journal	5	5	1.25	297	5	2021
Multimedia Tools And Applications	5	6	0.714	154	6	2018
Sensors (Switzerland)	5	5	0.625	91	5	2017
Future Generation Computer Systems	4	4	0.571	346	4	2018
IEEE Journal Of Biomedical And Health Informatics	4	4	0.667	96	4	2019
IEEE Transactions On Industrial Informatics	4	4	0.571	297	4	2018

4.5. Influential Authors

The figure illustrates the top 10 most influential authors in the field. It shows the top contributors ranked by their bibliometric indicators: h-index, g-index, m-index, total citations (TC), and number of publications (NP). These metrics reflect a wide understanding of each author's productivity, impact, and influence. Among the researchers, LIU J has the most outstanding h-index of 6 and a g-index of 10, with a total of 190 citations for 10 publications, reflecting the continuity and significance of his contribution to the field. It follows from the h-index that at least 6 of his publications have received no less than 6 citations, while the g-index indicates a broader distribution of citations across his published articles. The trend followed in the starting publication years-PY_start-of leading authors follows the trend from 2011 to 2020. It points out that there are more mature scholars and, at the same time, new entrants who are gaining significant results over a short period. Researchers like HASEEB K and REHMAN A possess higher m-index values of 1, representing contributions with a continuous and substantial relation towards professional years. The combination of senior and junior scholars represents a dynamic, evolving community of scholarship in the information security and data privacy of medical systems.

4.6. Influential Sources

Primary sources of information security in medical systems and data privacy for 2010-2024 were considered. It was found that the Journal of Medical Systems has the highest h-index value with a very high total number of citations. At the same time, it holds the leading position in the diffusion of highly cited documents in the area under consideration. Furthermore, IEEE Access has rapidly emerged as a significant resource, notwithstanding its relatively recent inception in 2019. The journal's elevated m-index indicates its swift gathering of impactful publications, positioning it as a distinguished participant within the field. In turn, Security and Communication Networks and Electronics from Switzerland record more modest outputs with impacts. While fewer in number, the concentration on well-focused quality research is evidenced through the citation scores, which are less frequent but worthy once published, contributing to the field and helping to illustrate diversity in the vehicles driving growth and development of knowledge in medical data security. The analysis underlines the relevance of both the established and the emerging sources in framing the ongoing discourse in this critical area of study.

4.7. Keyword Co-occurrence

India, China, and the United States are the leading contributors to this scholarship on information security and data privacy in medical systems. Large nodes and a high level of linkages with other countries depict this. Indeed, these countries produce high output volumes, while their collaborations with other countries run deep, especially between Asia and North America. While the United States acts as a nodal point for most countries, India and China are extending their friendship with regional and international partners such as Japan, South Korea, and Germany. This precisely gives an idea of these nations' in-depth contributions toward developing the discipline and sharing knowledge. For instance, nodes like Malaysia, Turkey, Bangladesh, and Iraq are smaller, which indicates the emergence of contributions in the area. Such countries, though at subordinate commanding positions, are becoming more and more active with localized research areas, so to say. Another focused contribution to the network comes from the Middle Eastern and European countries like Saudi Arabia and Germany; the connections are few but prominent. In other words, this visualization infers the international collaborative character of research in the domain represented by a mix of established contributors and up-and-coming participants coming together to address key challenges in medical data security.

4.8. Influential Affiliations

The illustration depicting influential affiliations underscores prominent institutions spearheading investigations in information security and data privacy within medical systems. Notably, Xidian University and Hainan University emerge as particularly distinguished due to their substantial volume of published research. This indicates that these universities possess robust research initiatives in cybersecurity, presumably bolstered by targeted funding, dedicated research teams, or strategic partnerships. This means that the research in this field is global, given the diverse geographical representations of these institutions from China to Malaysia and the United States. This could also be helpful for healthcare data security to take over as a global problem; the identified institution can always remain resource centers for young researchers who may seek collaboration or opportunities to pursue their research.

4.9. Thematic Evaluation

This thematic map provides an overall framework for understanding the main research themes related to information security and data privacy in medical systems. The "Motor Themes" quadrant, which involves terms like "human," "humans," and "article," would indicate a representation that these subjects are of high relevance and highly developed.

This shows that research on these topics is currently leading the game, as these are the bases from which many academic discourses and innovations have been harnessed. The prominence of these themes underlines their critical importance and shows how extensive the research attention has been. Finally, the "Emerging or Declining Themes" quadrant represents themes that show higher centralities and less development, such as "medical systems", "health care", and "network security". Perhaps this indicates that the theme has either just initiated during the preliminary phase of evolution or is in the declining phase of importance in academic discourse.

Fig. 5 Keyword co-occurrence network

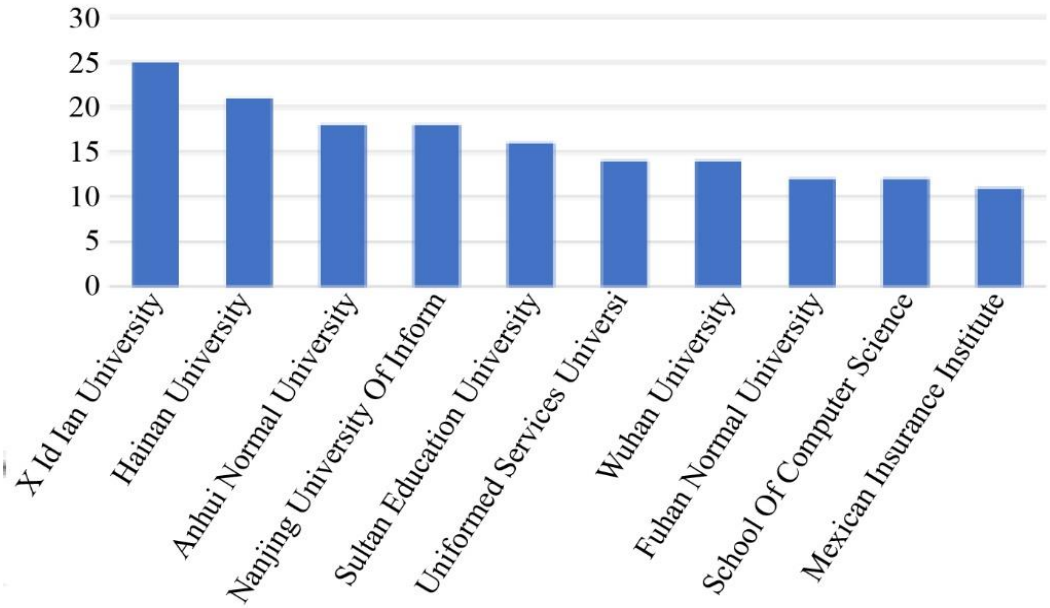

Fig. 6 Influential affiliations

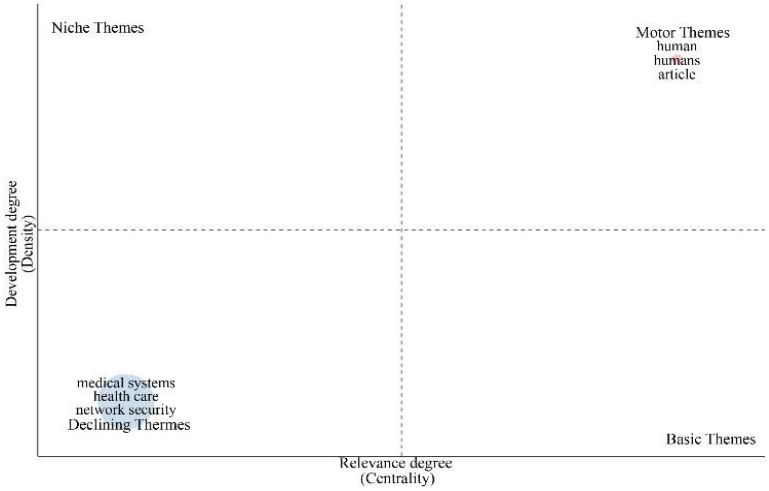

Fig. 7 Thematic evaluation

The absence of themes across the "Basic" and "Niche" quadrants underlines the possibility that the discipline is primarily concerned with a small set of entrenched topics, with limited attention devoted to emerging areas. It, therefore, appears from this study that while essential topics are well entrenched, there is, in fact, scope for investigation and development of topics that can become of importance in the future.

5. Limitations of the Study

Despite the comprehensive approach employed, the limitations of the present research are manifold. First, concerning sources, the study relies exclusively on the Scopus database for bibliometric data. Though an excellent data source, covering most peer-reviewed literature publications, it does not cover all relevant publications that may appear in regional or specialized journals not indexed by Scopus. This may result in an incomplete overview of the global research landscape related to information security and data privacy in medical systems. Future studies should also involve additional databases, such as Web of Science or Google Scholar, to capture a wider data set. The proposed search strategy for the review contains specific keywords; this might lead to selection bias. Since the choice of keywords determines the scope of literature retrieved, there is a possibility that despite trying to be comprehensive, some pertinent studies may have been excluded inadvertently due to variations in terminology used or differences in indexing practices across journals. This limitation may result in underrepresenting some subfields or emerging topics that are articulated using alternative terminologies. Finally, the whole study relies mostly on quantitative bibliometric indicators, such as the number of publications, citation rate, and h-index value, which are inadequate to make proper assessments, whether in productivity or even the impact of research. These valuable metrics cannot represent the qualitative elements of the research: substantive content, practical implications, or the innovative contributions of the analyzed studies. Thus, the analysis may not fully represent the depth and practical relevance of the developments in information security and data privacy for medical systems.

6. Conclusion and Research Directions

The manuscript, therefore, presents a critical bibliometric review of information security and data privacy evolution within medical systems from 2010-2024. The results indicate an increase in research activity that correlates with the importance of cybersecurity in healthcare as the sector continues to experience rapid digital transformation. The analysis showed that journal articles and conference papers have been the dominant categories; the most substantial contributions now come from countries such as India, China, and the United States. This study also covers the collaborative nature of this research field, pointing to highly influential authors, journals, and institutions in driving discourse within the research area of medical data security. The study highlights key trends within the domain, such as the increased integration of advanced technologies like AI and blockchain, which have furthered data security and privacy. These are deemed critical technologies in dealing with the complex challenges that arise from the digital transition of health. This report also emphasizes the importance of multi-layer defense mechanisms in safeguarding sensitive patient information from various cyber threats that continue to increase. Even with this good growth trend, the study further observes that continuous innovation and dynamic adaptation to the rapidly changing landscape of cybersecurity challenges within the healthcare context are required for such growth.

This study is limited in several ways: first, the reliance on the Scopus database may have excluded worthy research not indexed in this database; second, such exclusion could affect the analysis in one way or another. At the same time, reliance on some keywords may have resulted in a selection bias and diminished representativeness of the findings of the literature review. The paper also emphasizes numerical metrics, such as publication count and citation rate, without looking further into what was said in those publications; this might have led to underestimating the research's practical implications and real-world impacts. These are shortcomings, which may also hint at specific trends in further research: checking additional sources, conducting a keyword search using a wider strategy, and refining an approach to evaluating the efficiency of security practices in medical systems.

Funding Statement

SIMAD University generously funded this research. The support provided by SIMAD University was instrumental in the successful completion of this study, enabling comprehensive data collection, analysis, and dissemination of findings related to the bibliometric analysis of the Evolution of Information Security and Data Privacy in Medical Systems. The authors express their sincere gratitude for this valuable contribution.

References

[1] Yingnan Sun, Frank P-W. Lo, and Benny Lo, "Security and Privacy for The Internet of Medical Things Enabled Healthcare Systems: A Survey," *IEEE Access*, vol. 7, pp. 183339-183355, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[2] AKM Iqtidar Newaz et al., "A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses," *ACM Transactions on Computing for Healthcare*, vol. 2, no. 3, pp. 1-44, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Karim Abouelmehdi et al., "Big Data Security and Privacy in Healthcare: A Review," *Procedia Computer Science*, vol. 113, pp. 73-80, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[4] Farrukh Aslam Khan et al., "A Cloud-Based Healthcare Framework for Security and Patients' Data Privacy Using Wireless Body Area Networks," *Procedia Computer Science*, vol. 34, pp. 511-517, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[5] Harsh Kupwade Patil, and Ravi Seshadri, "Big Data Security and Privacy Issues in Healthcare," *In 2014 IEEE International Congress on Big Data*, Anchorage, AK, USA, pp. 762-765, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[6] Bradley A. Malin, Khaled El Emam, and Christine M. O'Keefe, "Biomedical Data Privacy: Problems, Perspectives, and Recent Advances," *Journal of The American Medical Informatics Association*, vol. 20, no. 1, pp. 2-6, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[7] Anam Sajid, and Haider Abbas, "Data Privacy in Cloud-Assisted Healthcare Systems: State of The Art and Future Challenges," *Journal of Medical Systems*, vol. 40, no. 6, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[8] Josh Benaloh et al., "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," *CCSW '09: Proceedings of the 2009 ACM Workshop on Cloud Computing Security*, Chicago Illinois USA, pp. 103-114, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[9] José Luis Fernández-Alemán et al., "Security and Privacy in Electronic Health Records: A Systematic Literature Review," *Journal of Biomedical Informatics*, vol. 46, no. 3, pp. 541-562, 2013. [CrossRef] [Google Scholar] [Publisher Link]

[10] William J. Gordon, Adam Fairhall, and Adam Landman, "Threats to Information Security: Public Health Implications," *The New England Journal of Medicine*, vol. 377, no. 8, pp. 707-709, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[11] Cynthia Dwork, "Differential Privacy: A Survey of Results," *International Conference on Theory and Applications of Models of Computation*, Xi'an, China, vol. 4978, pp. 1-19, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[12] Aqeel Sahi, David Lai, and Yan Li, "A Review of the State of the Art in Privacy and Security in the eHealth Cloud," *IEEE Access*, vol. 9, pp. 104127-104141, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Osman Diriye Hussein, and Husein Osman, "IoT-Based Air Quality Management in Somalia," *International Journal of Electronics and Communication Engineering*, vol. 11, no. 3, pp. 77-86, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] David Kotz, "A Threat Taxonomy for mHealth Privacy," *Third International Conference on Communication Systems and Networks (COMSNETS 2011)*, Bangalore, India, pp. 1-6, 2011. [CrossRef] [Google Scholar] [Publisher Link]

[15] Eirini C. Schiza et al., "Data Protection Issues of Integrated Electronic Health Records (EHR)," *In XIV Mediterranean Conference on Medical and Biological Engineering and Computing 2016*, Paphos, Cyprus, Springer, Cham, pp. 787-790, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ajit Appari, and M. Eric Johnson, "Information Security and Privacy in Healthcare: Current State of Research," *International journal of Internet and enterprise management*, vol. 6, no. 4, pp. 279-314, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[17] Shahid Latif et al., "A Blockchain-Based Architecture for Secure and Trustworthy Operations in The Industrial Internet of Things," *Journal of Industrial Information Integration*, vol. 21, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Suveen Angraal, Harlan M. Krumholz, Wade L. Schulz, "Blockchain Technology: Applications in Health Care," *Circulation: Cardiovascular Quality and Outcomes*, vol. 10, no. 9, pp. 1-3, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[19] Federico Cabitza, Raffaele Rasoini, Gian Franco Gensini, "Unintended Consequences of Machine Learning in Medicine," *JAMA*, vol. 318, no. 6, pp. 517-518, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[20] Catherine Dinh-Le et al., "Wearable Health Technology and Electronic Health Record Integration: Scoping Review and Future Directions," *JMIR mHealth and uHealth*, vol. 7, no. 9, pp. 1-13, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[21] Mirza Mansoor Baig, Hamid GholamHosseini, and Martin J. Connolly, "Mobile Healthcare Applications: System Design Review, Critical Issues and Challenges," *Australasian Physical & Engineering Sciences in Medicine*, vol. 38, pp. 23-38, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[22] Kit Huckvale et al., "Unaddressed Privacy Risks in Accredited Health and Wellness Apps: A Cross-Sectional Systematic Assessment," *BMC Medicine*, vol. 13, pp. 1-13, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[23] Joseph Jeremiah Adekunle et al., "AI Shield: Leveraging Artificial Intelligence to Combat Cyber Threats in Healthcare," *Iconic Research and Engineering Journals*, vol. 8, no. 3, pp. 184-195, 2024. [Google Scholar] [Publisher Link]