ISI Journal of Information Systems and Informatics

Published By Asosiasi Doktor Sistem Informasi Indonesia

Cybersecurity Trends in Digital Marketing for Public Health: A PRISMA based Bibliometric Analysis

Nazmus Sakib[1], Mahfujur Rahman Faraji[2], Fatihul Islam Shovon[3], Md. Julker Naiem[4], MD. Tofajjal Hossain[5]*, Taslima Akter Mim[6], Sadia Arfin Shanta[7]

[1,5*,7]Department of Disaster Management, Begum Rokeya University, Rangpur, Rangpur-5404, Bangladesh.
[2]Department of Engineering Management, Westcliff University, Irvine, California, United States of America
[3,4,6]Department of Marketing, Begum Rokeya University, Rangpur, Rangpur-5404, Bangladesh
Email: nazmussakib1300@gmail.com[1], m.faraji.214@westcliff.edu[2], fatihulshovon669@gmail.com[3], mdjulkernaiem@gmail.com [4], mdtofajjalhossan28@gmail.com[5*], taslimamim65@gmail.com[6], sadiaarfinshanta5@gmail.com[7]

Received: October 15, 2025
Revised: Nov 13, 2025
Accepted: Nov 21, 2025
Published: Dec 13, 2025

Corresponding Author:
Author Name*:
MD. Tofajjal Hossain
Email*:
mdtofajjalhossan28@gmail.com

DOI:
10.63158/journalisi.v7i4.1343

Abstract. This study conducts a bibliometric analysis of digital marketing in public health through the lens of cybersecurity, aiming to evaluate research trends from 2015 to 2025. It identifies key developments, major contributors, and provides guidance for future studies. A total of 1,191 documents were analyzed, revealing a significant annual growth rate of 32.01% and an average of 19.01 citations per document. The analysis explores how digital marketing for public health intersects with cybersecurity, a domain that remains underexplored. Data collection and visualization were conducted using Scopus, Biblioshiny, and VOSviewer, with article selection guided by the PRISMA methodology. Results indicate consistent growth in publications over the decade, though a noticeable decline occurred post-COVID-19 in 2020. The study offers a comprehensive mapping of existing literature and highlights the strategic importance of integrating cybersecurity into digital health marketing to protect patient data, maintain public trust, and enhance health outcomes. It provides valuable insights for researchers, policymakers, and practitioners aiming to improve the security and effectiveness of digital health communication in an increasingly connected world.

Keywords: Cybersecurity, Digital Marketing, Public Health, Bibliometric Analysis, Data Privacy

1. INTRODUCTION

The rapid development of information technology (IT) has significantly transformed social and economic systems, becoming a cornerstone for public health services [1]. Digital health technologies such as Internet of thought (Iot), artificial intelligence (AI) and telehealth have been key to enhanced access and improving monitoring [2]. However, this digital growth make significant cyber security challenges, increased connectivity expands attack surfaces, exposing healthcare systems to ransomware, data breaches and device vulnerabilities [3-4]. As noted by Ivanitskaya et al. [5], threats such as illegal online pharmacies further endanger patient safety. Consequently, the word Health Organization emphasizes that greater technological involvement necessitates integrated strategies to prevent and mitigate these risks.

Parallel to clinical advancements, digital marketing has evolved into a primary tool for engaging the public through social media, mobile apps and websites. However, these platforms introduce specific cyber risks [6]. Digital marketing operations are increasingly vulnerable to threats ranging from malware infections and identify theft to security weaknesses in content management systems like wordpress or Joomela [7]. Breaches in these channels not only disrupt business but also severely damage public trust and confidence [8]. According to Donthu et al. [9], embedding resilience strategies is critical for sustainable digital marketing; however, existing frameworks rarely address cybersecurity directly.

Because of these developments, the convergence of cybersecurity digital marketing and public health remains under explored in empirical research, suggesting important gaps. While studies such as Ewoh and Vartianinen's systematic review highlight sociotechnical vulnerabilities in healthcare systems (e.g. human error, legacy systems) via a PRIMA based design, the focus rarely extends to how public health marketing campaigns themselves might introduce or mitigate cyber risk [10]. Moreover, research integrating cybersecurity within digital health marketing practices appears nascent. Although social marketing and digital health misinformation studies indicate increased interest post COVID-19, they largely frame the problem in terms of communication and literacy rather than the technical security of marketing channels [11]. Thus, further work is needed to examine how digital marketing in health contexts can secured, audited and resilient in the face of cyber threats.

Existing literature on cybersecurity for digital marketing in public health has several gaps, reports this current literature. Both cybersecurity and digital marketing do attract significant attention. However, there isn't much research focusing on their intersection, especially in the context of public health[12]. A lot of research has looked at cybersecurity and digital marketing separately. But when it comes to combining the two, especially in public health, the studies are still scattered [13]. Bibliometric analysis is a useful way to organize all this information. It can show trends, point out who the main contributors are, and highlight new topics that are coming up [14]. By looking at years of publications, this approach helps us see what we already know and also where more research is needed. A notable gap is the lack of comprehensive research on the integration of emerging technologies such as AI, IoT, and blockchain in securing digital marketing platforms within the public health sector [10]. Additionally, while substantial work has been done in developed countries, there is a need for more research from developing nations to address the digital divide and improve cybersecurity preparedness in these regions[14].

Three primary gaps are evident in the literature. First, there is a notable lack of comprehensive research addressing the application of emerging technologies—such as artificial intelligence (AI), the Internet of Things (IoT), and blockchain—for enhancing cybersecurity in digital marketing platforms relevant to public health. Second, research conducted in developing regions is insufficient, despite these areas facing unique challenges including the digital divide and lower cybersecurity capacity[11-13].. Third, investigations into human factors, such as user behavior and its impact on cybersecurity effectiveness within digital marketing, remain sparse and underdeveloped. Addressing these gaps is essential for advancing integrated, context-sensitive cybersecurity frameworks that support the secure digital transformation of public health initiatives [12-15]. The following research question guide the study.

1) How has the publication trend of cybersecurity in digital marketing for public health evolved from 2015 to 2025 Scopus dataset?

2) Which countries, institutions, and authors are the most influential contributors to the field of cybersecurity in digital marketing for public health, according to bibliometric data?
3) What are the emerging research topics and future directions in cybersecurity for digital marketing in public health, as identified through a PRISMA-based approach?

The following research objectives guide the study

1) To map the publication trends, including the annual growth rate and citation impact, of cybersecurity in digital marketing for public health between 2015 and 2025 Scopus dataset.
2) To identify key authors, institutions, and countries contributing to the research landscape of cybersecurity in digital marketing for public health through a bibliometric analysis.
3) To identify and analyze the emerging research themes and gaps in the intersection of cybersecurity, digital marketing, and public health using bibliometric methods and PRISMA methodology.

2. LITERATURE REVIEW

The bibliometric analysis shows a large increase in the volume of cybersecurity papers between 2010 and 2024. The emphasis is shifting away from traditional security measures and towards the incorporation of cutting-edge technology like artificial intelligence, the Internet of Things (IoT), and blockchain [15]. The report examines important trends and critical issues in the field of cybersecurity research. It illustrates a dense network of global cooperation, including the United States, China, India, Germany, and the United Kingdom as prominent nodes [16].

The term "digital marketing" began to emerge more frequently in the literature after 2021, signifying a shift in focus within the field. The top five contributors to digital marketing literature are Indonesia, India, Ukraine, the United States, and the United Kingdom. The leading publishers in this discipline include the Journal of Sustainability, the Economic and Social Development Book of Proceedings, and the Cogent Business and Management Journal [17].

Digital marketing has an impact on the effectiveness of all departments within an organization, including customer feedback, customer support, product enhancement, sales, finance/payment, delivery, administration, and marketing [18]. In Malaysia, individuals don't know much about what can cause people to display risky cybersecurity behaviours. These unsafe behaviours can make individuals and businesses vulnerable to cyber threats. In sensitive economic sectors and industries which are important for national safety and security, such as telecommunications, banking and finance, can suffer losses due to such activities. Cyber vulnerability behavior indicates that internet behavior that poses a threat to the individual can be seen as bad cyber safety behaviour which increases the susceptibility towards harmful attacks and chance of a cyber-safety attack. In today's health-care systems, public health has emerged as a growing phenomenon [19]. Over the past two decades, new digital health alternatives, technologies, and innovations have been presented; many of them are currently being examined and reviewed by researchers worldwide [20].

Public health is the synthesis of information, abilities, and beliefs aimed at protecting and improving everyone's health through collective efforts [21]. Public health encompasses supporting proactive wellness promotion, resolving workforce shortages in the United States, and promoting community well-being through injury prevention education, legislation, and research [22]. The findings provide data-driven views to design more successful digital communication methods in public health [23]. Infrastructure research has helped to enable several types of eHealth apps, including networks, data sharing, computing technologies, information systems, and platforms. The maps highlighted researchers' concerns about eHealth data security and privacy, including enhanced access control and encryption technologies, as well as health analytics language [5]. The global COVID-19 epidemic resulted in an enormous increase in the number of papers in JMIR. The most productive institutions were primarily from the United States, which placed first in successful publications inside the journal [24]. Simultaneously, SMBD was widely applied in economic and social growth, urban and rural construction, product safety, disaster prevention and management, and other areas. For example, during the 2020 COVID-19 outbreak in China, Weibo's "pneumonia help-seeking" mega-topic offered attention to overlooked groups [25].

The effective administration, interpretation, and use of data about the user or patient and their condition provided by the unique person-centered service model is one of the most significant problems in the link between eHealth and IoT [26]. The approaches and ML algorithms finding application in healthcare are dependent on both the data and the IoT infrastructure under consideration [27]. With the emergence of the Internet of Things (IoT), artificial intelligence (AI), and linked devices, data security and privacy have become major challenges, necessitating the development of solutions by cybersecurity specialists [28]. This is where incorporating cybersecurity and SD principles into business procedures becomes critical for firms to integrate and address these concerns. Therefore, investigating the relationship between cybersecurity and the SD is vital for establishing a safer, equitable, and sustainable future [10]. Digital advertising is the creation and distribution of promotional information through digital channels, with the primary goal of eliciting intended actions or behaviors from the target audience [29]. Its expanding importance highlights its ability to drive major change, particularly in the context of Industry 4.0. Among the continuing technology advances, IoT stands out as the most significant [11].

Social media is a crucial instrument for communication, as well as the development and maintenance of user interactions. "Health self-management" has improved because of digital mobile and health medicine monitoring. Media tools assist disseminate health information to the public, allowing people to improve their health [30]. In another study, the potential for AI-based health education apps and smart systems as a future educational model was investigated. It emphasized the importance of smart systems in defining health education and their potential impact on future educational paradigms [31]. Moreover, there were numerous issues in cybersecurity. One of the most significant issues in cybersecurity was the computational complexity of passive defense techniques, which relied significantly on comprehensive network traffic monitoring and comparison. In contrast, active security

3. METHODS

This study describes a bibliometric analysis complemented by a thematic analysis to evaluate research trends at the intersection of digital marketing, public health and cybersecurity [32]. Bibliometric analysis utilizes statistical methods to analyze bibliographic data to map the intellectual structure of a research field [33]. This approach allows for the objective identification of emerging trends, collaboration networks and research gaps over time [34].

3.1. Data Sources and Search Strategy

The data for this study was retrieved from the Scopus database, chosen for its comprehensive coverage of peer reviewed literature and high quality bibliometric metadata [35]. To ensure relevant data retrieval, a specific keyword search string was developed based on the research objectives. The research was conducted on October, 25, 2025 using the following search string within the "Article Title, Abstract and keywords" field.

Search Query:
TITLE-ABS-KEY(Digital Marketing OR Cyber Security OR Public Health) AND (LIMIT-TO (LANGUAGE,"English")) AND (LIMIT-TO (PUBSTAGE,"final")) AND (LIMIT-TO (DOCTYPE,"ar") OR LIMIT-TO (DOCTYPE,"cp") OR LIMIT-TO (DOCTYPE,"ch") OR LIMIT-TO (DOCTYPE,"re")) AND PUBYEAR > 2015 AND PUBYEAR < 2025

3.2. Inclusion: and Exclusion Criteria

The selection process followed the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analysis) guidelines [36]. To ensure the data quality and relevance of the data, the following criteria were applied. Inclusion criteria: The documents published between 2015 and 2025. The documents types limited to English language and the documents limited to Articles, Conference Papers and Reviews. Exclusion Criteria: The duplicate documents, missing author or affiliation data and articles irrelevant to the core intersection of the three topics.

3.3 Data Processing and PRISMA Flow:

The initial search yielded a total of 1,495 documents. The data underwent a rigorous screening screening process. First, filtering by publication year (2015-2025) reduced the count to 1,373 documents. Second, language filtering (English Only) excluded 31 articles, leaving 1,342 documents. Third, a filter for the final publication stage was applied, removing 17 articles. Finally, the database was filtered by document type which excluded 122 documents. The remaining documents were screened for relevance by title and abstract and duplicates were removed. The final dataset consisted of 1,191 documents for bibliometric analysis.

3.4 Data Cleaning and Analysis

The final dataset was exported in CSV formats. Data cleaning was performed to standardize keywords and correct missing metadata using Microsoft Excel. The statistical analysis was conducted using R studio with the Bibliometrix package and its web interface Biblioshiny. These tools were used to generate performance analysis and conceptual structure map. Additionally, VOSviewer was utilized to visualize co-occurrence networks and keywords clusters [37].

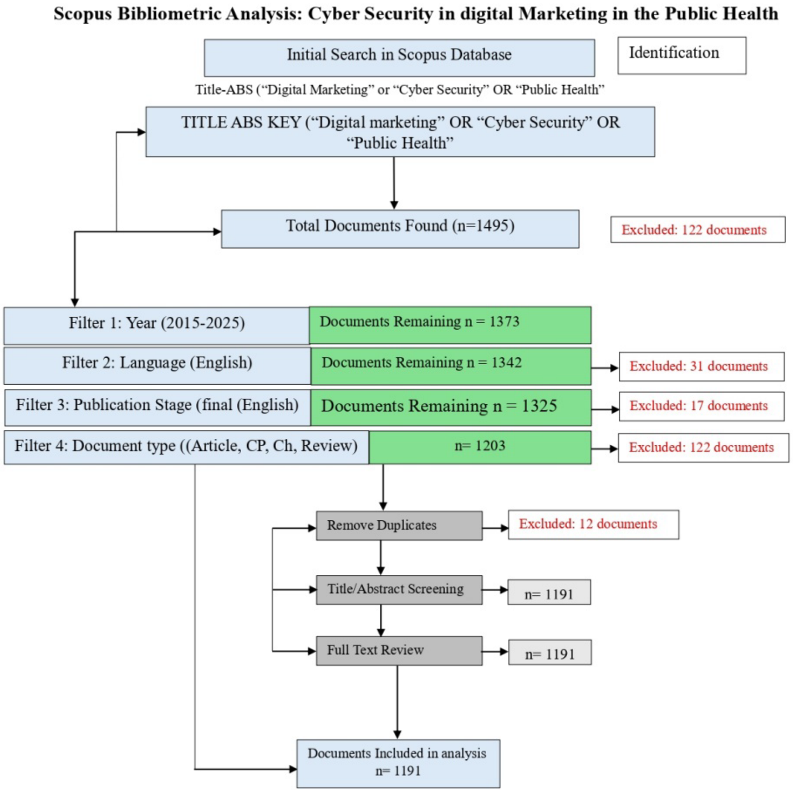
Scopus Bibliometric Analysis: Cyber Security in digital Marketing in the Public Health
Initial Search in Scopus Database
Identification
Title-ABS ("Digital Marketing" or "Cyber Security" OR "Public Health"
TITLE ABS KEY ("Digital marketing" OR "Cyber Security" OR "Public Health"
Total Documents Found (n=1495)
Excluded: 122 documents
Filter 1: Year (2015-2025)
Documents Remaining n = 1373
Filter 2: Language (English)
Documents Remaining n = 1342
Excluded: 31 documents
Filter 3: Publication Stage (final (English)
Documents Remaining n = 1325
Excluded: 17 documents
Filter 4: Document type ((Article, CP, Ch, Review)
n= 1203
Excluded: 122 documents
Remove Duplicates
Excluded: 12 documents
Title/Abstract Screening
n= 1191
Full Text Review
n= 1191
Documents Included in analysis
n= 1191

Figure 1. A PRISMA Methodology

4. RESULTS AND DISCUSSION

The analysis in this study used bibliometric methods to evaluate the trends, contributions, and collaborations within the field of cybersecurity in digital marketing for public health. Tools such as Biblioshiny, VOSviewer, and Scopus were employed to visualize data, track publication growth, and identify influential authors, institutions, and countries. The study also utilized the PRISMA methodology to systematically filter and analyze the relevant publications from 2015 to 2025.

4.1. Overview of Bibliometric Data Collection

4.1.1. Descriptive analysis

As can be seen from Table 1, the period of the research paper is 2015 to 2025. Information has been taken from Journals and books. Average publication Rate of scientific journal articles 32.01% per year. The typical age of the research paper is around 2.85 years. Most of them have been published recently. It has 10296 references and 6050 keywords, out of which 3444 are authors keywords. 4527 Authors connect these essays. Just 134 single authors and international authors 2.888%. The average number of authors per research piece is 4.16.

Table 1. Summary of Bibliometric Data Collection

Description	Result	Description	Result
Timespan	2015:2025	review	119
Sources (Journals, Books, etc)	487	**DOCUMENT CONTENTS**	
Documents	1191	Keywords Plus (ID)	6050
Annual Growth Rate %	32.01	Author's Keywords (DE)	3444
Document Average Age	2.85	**AUTHORS**	
Average citations per doc	19.01	Authors	4527
References	10296	Authors of single-authored docs	134
DOCUMENT TYPES		**AUTHORS COLLABORATION**	
article	520	Single-authored docs	139
book chapter	160	Co-Authors per Doc	4.16
conference paper	420	International co-authorships %	28.88

4.1.2. Trends and annual publication

The scientific production from 2015 to 2025 is presented in figure 02. This data shows a consistent and accelerating growth in the number of articles published starting from approximately 13 articles in 2015. This upward trend continued for eight years, reaching a peak of approximately 189 articles in 2023. Following this peak, the trend reversed, showing a modest decline to approximately 209 articles by 2025.

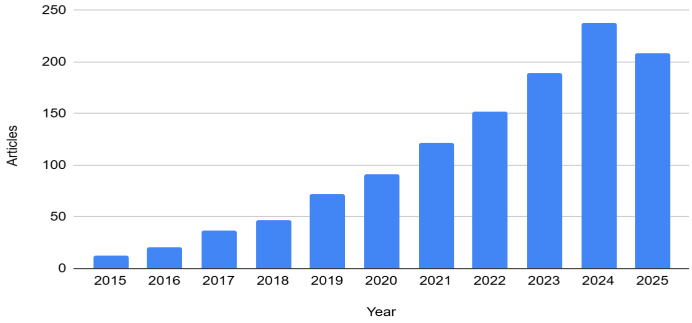

Figure 2. Trends and Annual Publication

4.1.3. Most productive authors and influential networks of collaboration

Figure 03 shows the most relevant authors depending on the number of documents published. Khan, Raees are the highly productive authors in this field which is indicated by this dataset; who contribute seven publications in the area of study. Then each author follows a consistent research engagement to demonstrate their own research field published in six documents contributed by Backholer, Kathryn, Boyland, Emma J and Kelly Bridget P. Consequently, each author such as Agrawal, Alka, Amirtharajan, Rengarajan, Jahankhanim Hamid, Kumar, Rejeev, Mackey, Tim Ken and mohanty, Saraju P have each contributed five publications significantly their substantial engagement in the area of study.

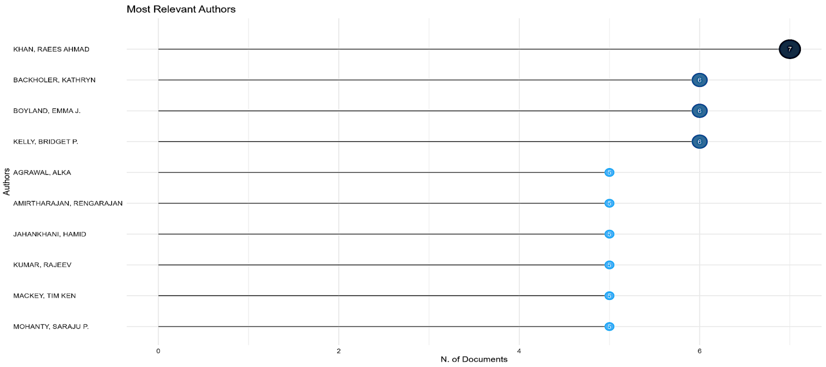

Figure 3. Top 10 most productive and influential authors

4.1.4. Most Relevant Sources of Publication

The Figure 04 "Most Relevant Sources" identified the distribution of documents across publication fields, revealing one high dominant unlabeled in the analysis. Among the next most relevant sources "LECTURES NOTES IN NETWORK AND SYSTEMS" provided by 31 documents followed by "IEEE ACCESS" with 22 documents. The "JOURNAL OF MEDICAL INTERNET RESEARCH" and "LECTURES NOTES IN COMPUTER SCIENCE' also represented significant clusters contributing 18 and 17 documents respectively. The relevant sources show each accounted for between 10 and 14 documents.

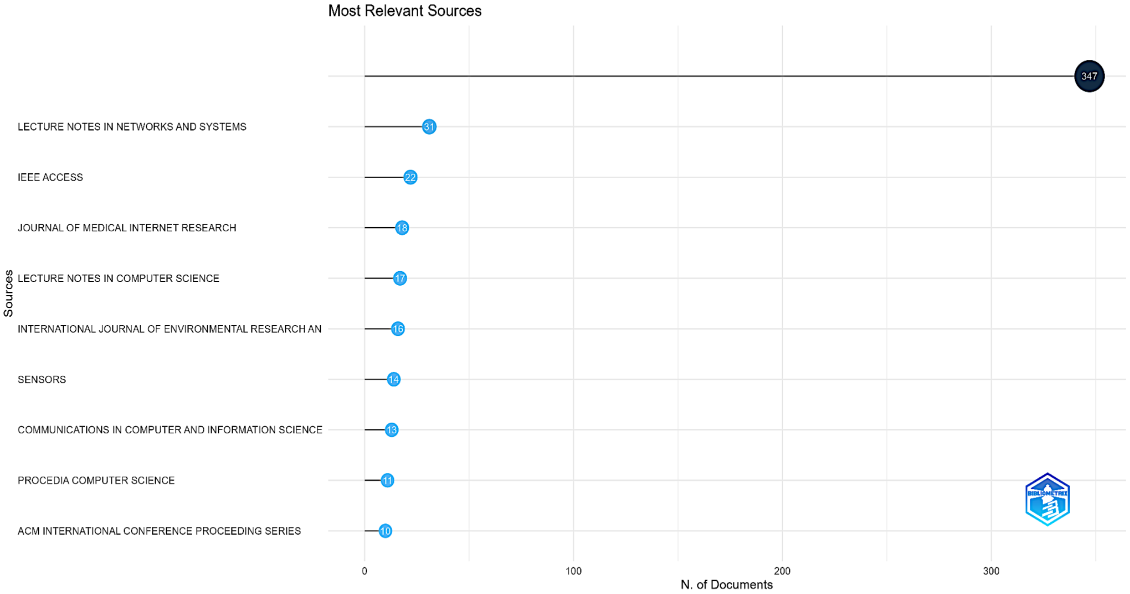

Figure 4. Top 10 sources publishing

4.1.5. Country-wise publication analysis

The scientific production frequency for the top 10 productive countries identified in the data set representative in figure 05. This data indicates that the United States (USA) and India are the leading contributions to the field with 972 and 869 publications respectively. The remaining countries in the top 10 show a more clustered and substantially lower frequency of publications. This group includes Canada (136), China (115), Italy (95), Spain (94) and Malaysia (92).

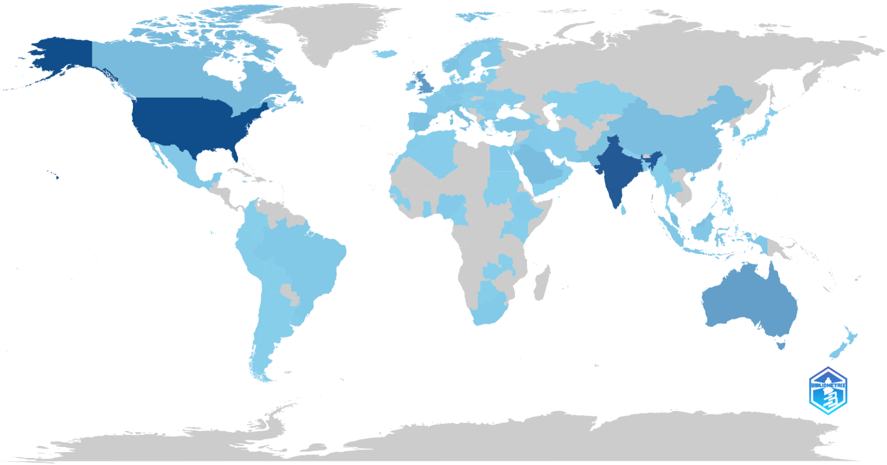

Figure 5. Top 05 countries count with papers

4.1.6. Geographic Publication

According to Figure 6 which represents the global publication count at the top 10 cited documents, the outlier is the researcher or academician. According to Rahmani, this study published in Future Generation Computer Systems is the top cited paper with 998 global citations. In character with 510 citations, Ahram (2017) is the second-ranked document. A set of documents follows with citations in the 300 to 500 ranges including Moustata (2019) in IEEE Internet things journal (492) citations. The Annual Review of Anthropology by Ruckenstein (2017) is cited 389 times, that is many. Finally, the data shows a continual downtrend beginning with Omar (2019) at 353 citations to the 10th ranked document Wanasingh (2020) in IEEE access which has 288 citations.

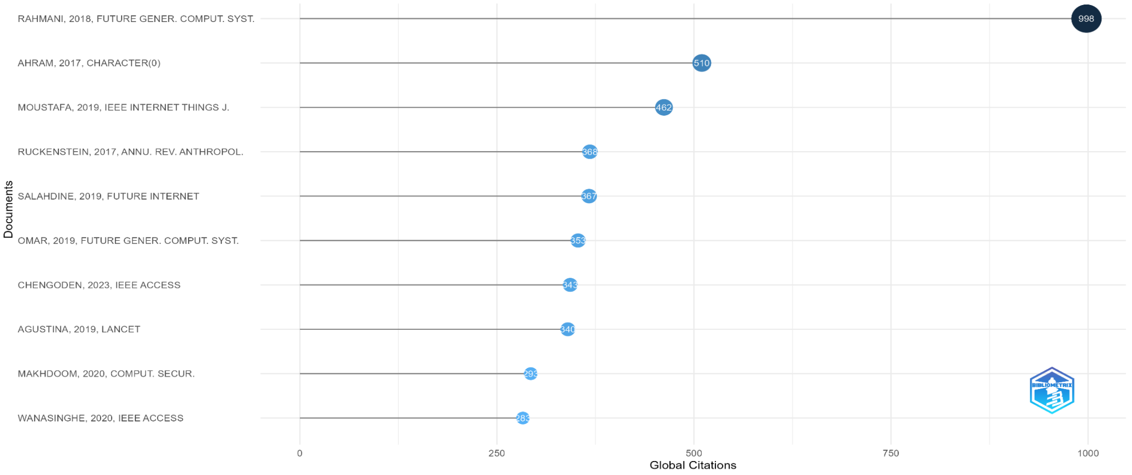

Figure 6. Geographical distribution of number of publications

4.1.7. Global Research Collaboration

Figure 07 displays a bibliometric network map of international research maps which reveals co-authorship links between countries in the dataset. The size of the node is proportional to the country's productivity and the lines between nodes indicate collaborative co-authorship. The top productive countries in this dataset followed by the United States, India and Iran, Australia, China, Spain, and Saudi Arabia are also significant prominently in this field. Firstly, The purple colour cluster is led by the United States, India and Australia. The red colour represents Euro-Centric features with strong links between Spain, Italy, France, Germany and Portugal. Thirdly, the yellow/orange cluster displays the Middle-East and Asia including Saudi-Arabia, Pakistan, Malaysia, Japan, The Arab Emirates and Bangladesh. Fourthly, the blue coloured cluster is led by East Asia including Asia, China and Hong-kong and also Includes Qatar. Finally, European, Mediterranean and African nations including Norway, Greece, Turkey and South Africa are represented by green clusters.

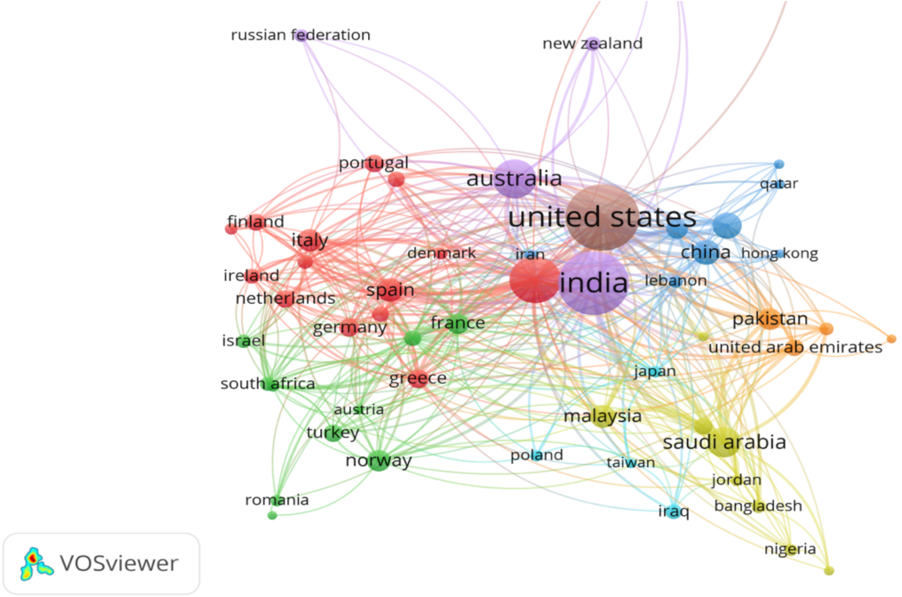

Figure 7. The best joint ventures among nations

4.2. Institutional Affiliation analysis and Join Networks

In this research, the analysis of trends in cybersecurity within digital marketing for public health shows figure 08 that worldwide many Universities and research Institute played vital role in this case. According to bibliography analysis, Deakin University achieved top position by publishing the maximum number of research articles (41). The Institute plays a leading vital role in digital health and cyber security. In the not reported category, 34 studies did not specify any institutional affiliation, indicating independent and multidisciplinary research efforts. La trobe University and Vellore Institute of technology, ranked 3rd and 4th position after publishing 24 and 20 papers respectively. Overall, Australian and Indian institutions are especially active in this research area. Their research proves that, Use of Cyber security in Digital marketing is not only commercial but also plays a vital role in protecting public health information.

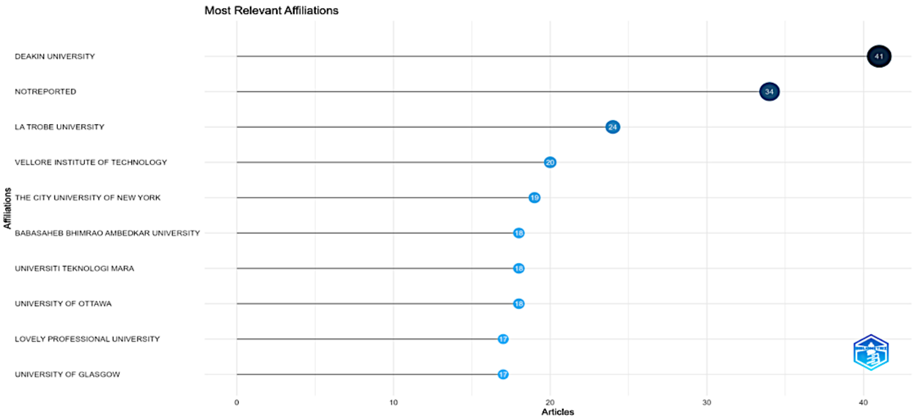

Figure 8. Top 10 most contributing institutions

4.3. Keyword Cloud and Author Keywords

4.3.1. Keyword Cloud

Figure 09 displays a keyword cloud which highlights the frequency of keywords appearing in these documents. This dataset identified “cyber security”, as the most dominant and central topics or keywords. The secondary tier is most frequent keywords including healthcare, human network security, marketing, public health and social media. Lastly, the significant keyword is related to specific technologies such as “internet of things”, “blockchain”, “digital storage”, “artificial intelligence”, “data privacy”, and “electronic health record".

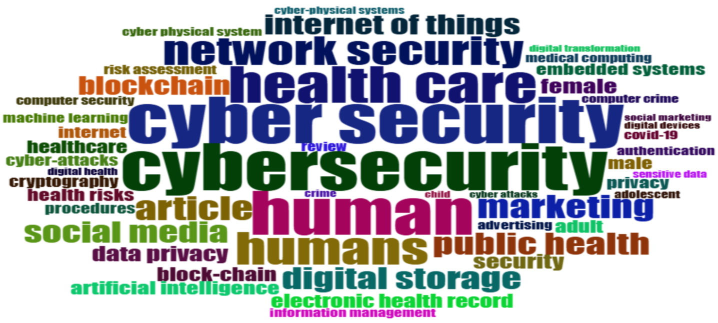

Figure 9. Keyword Cloud

4.3.2. Author Keywords

Figure 10 represents the tree map visualization of the keyword; the area of each rectangle is directly proportional to the frequency of keyword that clear a visual comparison of the significant dominant's topics. In this analysis, the most prominent keyword is cybersecurity (n=305, 6%), and its variants cyber security (n=302, 6%) are the significant keywords dominating this dataset. Following these keywords is related to human factors and health are also high performance "human" appears as a major keyword (n=283, 6%) along with "healthcare" (n=237, 5%), "human" (n=209, 4%).

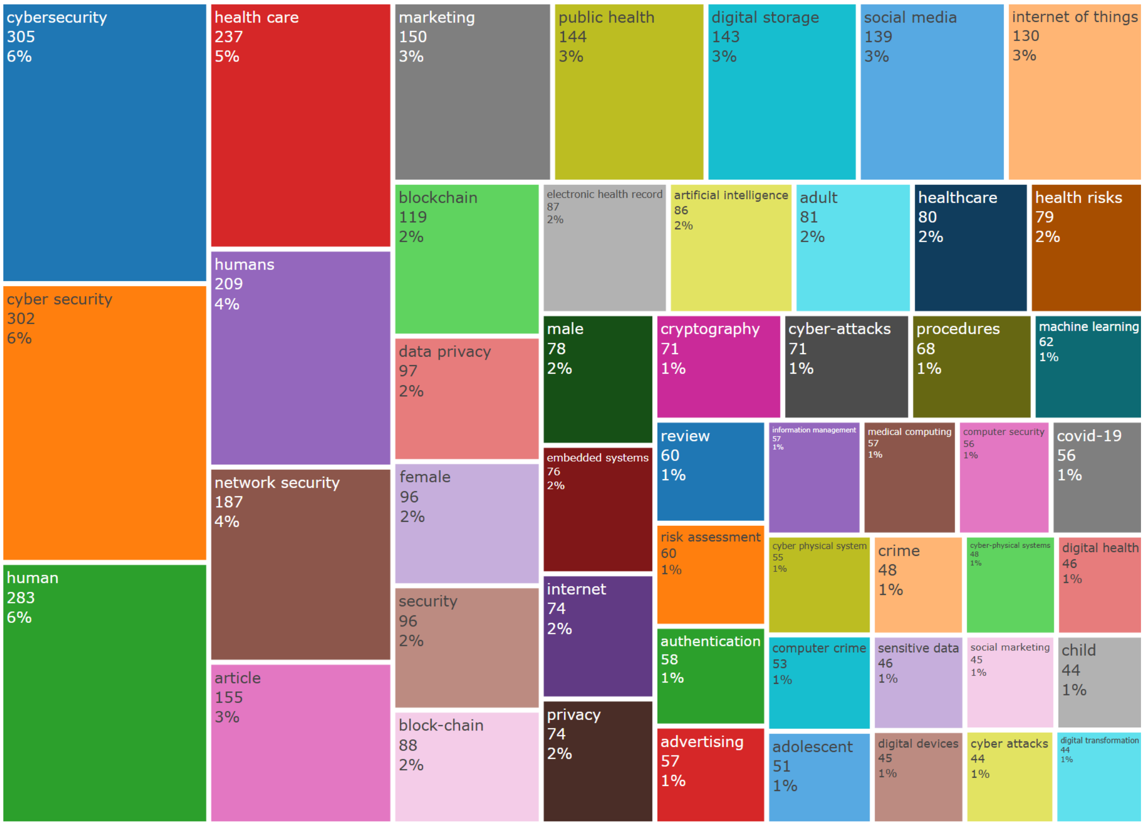

Figure 10. Most frequently used author-keywords

4.3.3. Top 10 keywords

Table -03 shows the most frequent keywords used in the research. According to the result "Cyber security "and "cybersecurity " these two words are used most (302 & 305). It proves that cyber security is the main of this research area. In the next place there is "Human " (283)"health care"(237) and "humans" (209), which shows that humanity and health care is also given importance."Network security " (187) and "digital storage " (143)" words indicate the technological side.On the other hand, "marketing " (150)" and "public health " (144) words means that nowadays Cyber security terms are related to marketing and public health. Also, the presence of the word "article" (155) shows that many studies are literature-based or data-analytic. Overall, these keywords indicate that research topics include cyber security, healthcare,Created a connection between the human element and digital marketing.

Table 2. Top 10 keywords

Terms	Frequency
Cybersecurity	607
human	283
health care	237
humans	209
network security	187
article	155
marketing	150
public health	144
digital storage	143

4.4. Networks analysis

4.4.1. Author based bibliographical coupling network

Figure 11 reveals the diagram between thematic clusters derived form a coupling analysis. This analysis represents the structural theme of the research. The upper-right quadrant represents both high centrality and high impact which indicate the well-developed and central theme of the research domain. The upper-left quadrant cluster is defined by the themes of "blockchain" (conf 60%), "internet of things (57.4%) and security (conf 33.3%) which indicates the highly developed and impactful research field. The lower right quadrant represents the transversal or foundational cluster which is strongly associated with "healthcare" (conf 80%), security (conf 44%) with a minor link cyber security (conf 25%). This analyzes finding that not highly developed as a distinct research theme. The lower-left quadrant shows peripheral themes and less development. This analyze represent the characterized by machine learning (conf 80%), cyber security (conf 75%) and blockchain (conf 40%).

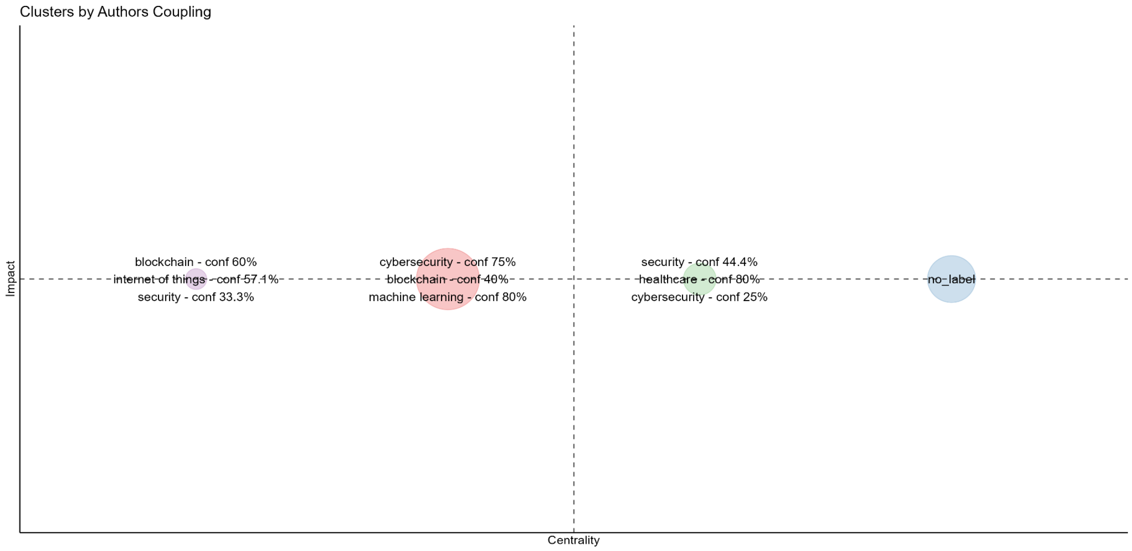

Figure 11. Bibliographic-coupling network of top influential authors

4.4.2. Keyword co-occurrence network

Figure 12 represent the network visualization map of keyword occurrence. In this analysis, each node presents a keyword and the size of the node is proportional for frequency of occurrence. This cluster appearing on the left is centered on the core concept of cyber security, healthcare and cyber security. Then the primary node represents the technical and infrastructural keywords including "network security", "internet of things (IOT)", "blockchain", "digital storage", "machine learning", "cyber-physical systems and cryptography. The Second cluster on the right is dominated by human with large node for "humans". This cluster brings together the social demographic and user centric aspects of the research including public health, social media, marketing health, digital health and demographic identifies such as female, male, adult and child. The findings of this analysis are the set of bridge connections between the two clusters an important interdisciplinary nexus. The health care is connecting strongly to the human. It is also analyze the significant research that integrates the technical security of healthcare systems with human and public health outcomes.

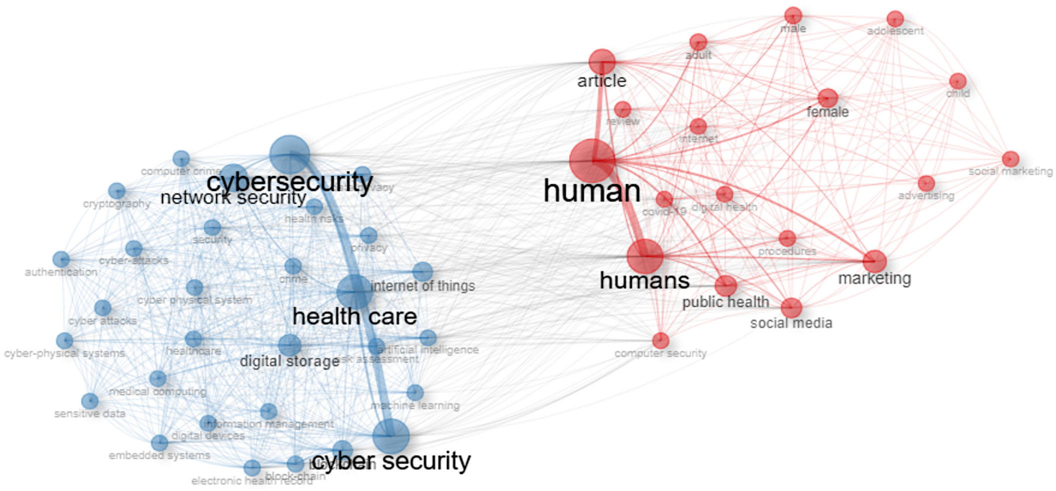

Figure 12. Network of top keywords co-occurring

4.4.3. Trend of Keywords

According to the bibliometric analysis it shows, in recent years Research in public health in cyber security with digital marketing has grown rapidly. Studies in 2016–2018, mainly focused on advertising, criteria and social communication. Between 2018 and 2020, studies were done on internet and health. The pandemic highlights the need for more security and cyber security in the digital care system. The increasing use of the terms "cyber security", "electronic health record", "block-chain", and "sensitive data" in 2022–2025 suggests that health information security is now a key focus of research. Overall, Cyber security has been established as an important and growing research area in improving public health through digital marketing.

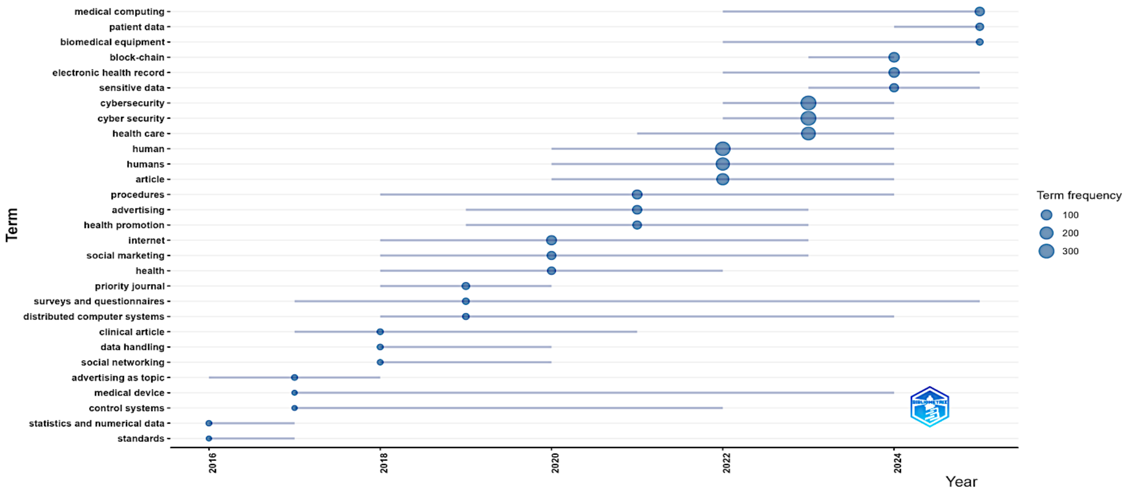

Figure 13. Trend of Top 20 Keywords

4.5. Conceptual Structure Mapping

According to the bibliometric analysis, public health, human related issues (humans, humans) and Digital marketing (marketing, social media, internet) -these three elements are at the center of Cyber security research. "Human " and Humans these two words used the highest number (283 and 209), indicating that people and Their behavior are the main focus of research in public health systems. "Public concern" and "Social media" categories show high centrality. In other words, digital media and social media play an important role in public health information broadcast. Further, marketing and internet indicate that digital marketing has now become a powerful weapon in the telecasting system of public health information. For that, the importance of cyber security is increasing, because storing and managing people's health information online is now a major challenge. In other words, we can say that with the need for development regarding digital marketing in public health, the importance of cyber security research is rapidly increasing and it has now become one of the most active research trends.

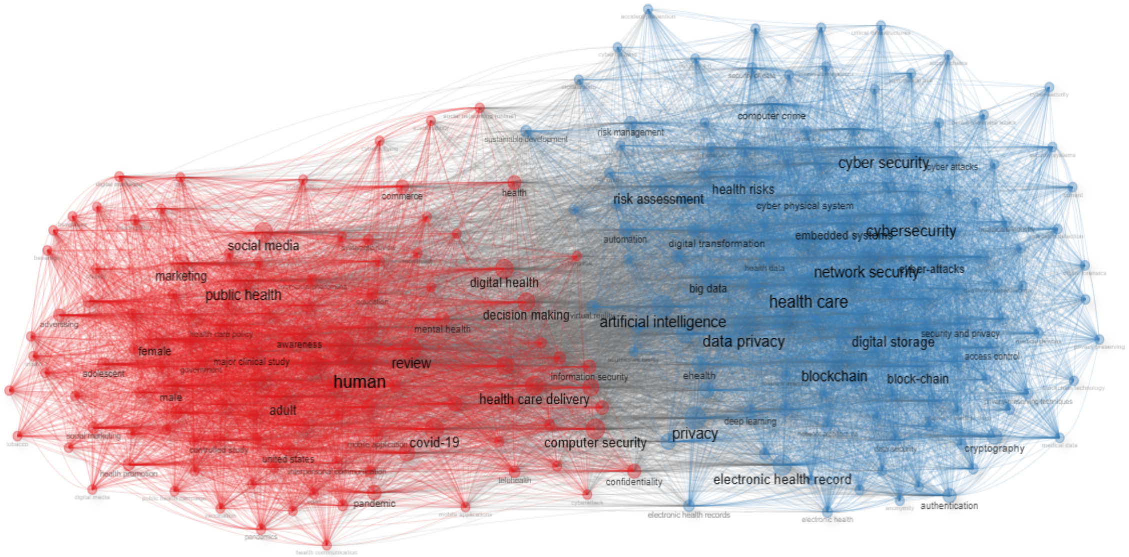

Figure 14. Conceptual structure map

4.6. Discussions

This study gives a bibliometric analysis of cybersecurity, digital marketing, public health linking. It analyses general trends, key contributors and other research avenues. These days everything is digital. In the same way, public health systems are using digital marketing strategies to better engage patients [33]. However, this digital transformation simultaneously exposes public health platforms to growing cybersecurity risks. This analysis highlights that the integration of emerging technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), and blockchain in cybersecurity is becoming critical to safeguarding sensitive health data, as identified by several researchers [12]. While these technologies offer promising solutions but also introduce new vulnerabilities that require urgent attention in both research and practical implementation. This technology dependent transformation brings threats that cause not only economic loss but also directly compromise public health security and the privacy of personal information [34].

Analysis of publications between 2015 and 2025 demonstrates a gradual increase in research linking cybersecurity and digital health. Notably, the COVID-19 pandemic post 2020 marked a pivotal turning point in this trend. During the pandemic increasing dependency on telemedicine, E-health, online Health communication and digital campaigns exposed the health sector to greater cyber risk. This has compelled researchers and policymakers to focus on effectively integrate cyber security into digital health systems [35].

The USA and India have emerged as top contributors in this research sector, indicating major economies are prioritizing practical research at the intersection of Cyber security and digital health marketing [37]. The recurrence of keywords like "Human" and "Humans" in the analysis signifies that the ultimate goal of cybersecurity in public health is the protection of people and their information [38]. Digital marketing and social media have recently become effective tools for public health campaigns [39]. However, alongside information dissemination, risks such as fake news, malware, phishing and data theft are escalating. Consequently, cyber security in digital marketing is now a technical necessity but also a social responsibility.

The discussion reflects that the development of digital public health systems and cyber security are complementary to each other [23]. When correctly coordinated, they multiply public health protection, information privacy and human trust. Therefore, future research requires extensive international cooperation, robust policies, and the development of user-oriented security systems to ensure a safe, equitable and sustainable digital health environment.

One of the critical contributions of this study is the identification of research gaps. Despite extensive independent research on cybersecurity and digital marketing, the convergence of these fields within public health remains in its infancy [41]. The study emphasizes the growing need for interdisciplinary collaboration among cybersecurity experts, digital marketer's and public health practitioners. Results also indicate global cooperation is needed especially in developing countries to ameliorate the digital divide of the preparedness for cyber security [13]. In addition, human factors generally emphasized in the study are mostly neglected by similar technical and cybersecurity studies due to the behavior of users. Future research should emphasize creating strong cybersecurity frameworks that prioritize user needs and can adapt to the digital health evolution.

This research fundamentally connects 3 important areas cybersecurity, digital marketing and public health. It redefines cybersecurity as a strategic trust catalyst in digital public health platforms. It affects the protection of patient personal data, transparency and digital ethics in the healthcare sector and directly affects the engagement of audiences and the effectiveness of campaigns [12]. Researchers can identify and describe conceptual clusters through bibliometric mapping which establishes the relationships between key issues like data privacy, cybersecurity awareness, harmful information related to health, digital market tools etc. In the end, it proposes a conceptual model that bolsters the trust and confidence in the usage of digital marketing in healthcare over cybersecurity. The bibliometric analysis reveals key thematic clusters around cybersecurity, emerging technologies (AI, IoT, blockchain), public health, and human factors, which together frame the theoretical basis for future research. These keywords not only represent active research hotspots but also delineate critical avenues for advancing knowledge, including the development of user-centric security frameworks, integration of cutting-edge technologies for enhanced protection, and addressing regional disparities in cybersecurity preparedness. Future research directions thus naturally extend from the conceptual connections embedded in these thematic keywords, emphasizing an interdisciplinary approach to secure digital marketing platforms in public health settings.

Theoretically, this study opens the door to several academic research areas: The effectiveness of digital marketing tools or systems used in public health information dissemination depends on security measures [42]. Cybersecurity laws and their implementation create trust in users by reducing the potential for harm in the use of digital marketing in the health sector [12]. Technology Cybersecurity knowledge, digital health campaigns, apps or various related platforms act as an important regulator [43]. It explains in detail how cybersecurity laws and their implementation affect various stakeholders including patients, marketers, policy makers, and governments [44]. By reviewing international and historical research on this topic, this study identifies common problems and solutions and points the way for future research.

This study has a very important impact on society that helps the public become aware of public health vaccination campaigns, digital health platforms, health education materials and various types of disease. Digital security can prevent reduced access to safe and fast services, misappropriation of data, disinformation and digital harassment [41]. At the same time, high security, telemedicine users or the population receiving medical services using this platform provide protection. Where the ethics of digital marketing practice, transparency, accountability and integrity are given importance. And increase awareness about cybersecurity and create digital literacy.

This research carries importance in creating scientific and policy context. Which identifies the main researchers, institutions and countries working at the intersection of cybersecurity, digital marketing and public health in bibliometric analysis. Which encourages trust in digital security at the international level, and its use in the health sector [45]. At the same time, it can help renowned institutions, research centers and researchers to set cybersecurity standards [46-48]. And the weaknesses that have not been revealed in various studies can be revealed through this study. At the end, this study will make an important contribution to making global cybersecurity a strategic global public asset and building trust in the use of digital marketing in healthcare worldwide.

Our review was limited to journal. We only included article with cybersecurity at the core of the study. Importantly, much of the work on cybersecurity and health care is operational and administrative, not academic [35]. Future research can focus only on bibliometric and visualization analysis of only marketing journals. Moreover, the various quantitative methods, we incorporated only bibliometric analysis [46-48]. Future research can utilize other text mining methods such as topic modelling by using Python and its text mining libraries such as the Genism library. In the future, we can put a lot more emphasis on security in digital marketing.

5. CONCLUSION

This study indicates the intersection of cybersecurity, public health and digital marketing which is rapidly growing interdisciplinary field. The study reveals that while digital transformation and the COVID-19 pandemic have accelerated the adoption of virtual health advocacy, they have also introduced critical vulnerabilities including data breaches, identify theft and disinformation [47]. The analysis categorized the current literature into four major themes: data privacy and ethics, technological infrastructure, digital trust and human behavior and policy governance. A significant finding is the geographical disparity in research output. Scholars from advanced economics like the UK, China and EU dominate the discourse due to their established technological infrastructure and regulatory frameworks [46]. In context, the developing world shows a marked gap between digital adoption and cybersecurity preparedness. It is evident that while digital health access is expanding, the intellectual participation and security frameworks in these regions remain limited.

CONFLICT OF INTEREST

Authors have no conflict of interest to publish this article.

REFERENCES

[1] L. Judijanto, E. Endrianto, and A. Y. Vandika, "Mapping the Cybersecurity Research through Bibliometric Analysis," *West Sci. Inf. Syst. Technol.*, vol. 2, no. 03, pp. 374–382, Dec. 2024, doi: 10.58812/wsist.v2i03.1534.

[2] K. Sharmin, "Bibliometric Analysis of Cybersecurity Research Trends in Bangladeshi Educational Institutions (2020-2025)," *J. Inf. Syst. Inform.*, vol. 7, no. 3, pp. 2076–2099, Sept. 2025, doi: 10.51519/journalisi.v7i3.1154.

[3] K. Ganji and N. Afshan, "A bibliometric review of Internet of Things (IoT) on cybersecurity issues," *J. Sci. Technol. Policy Manag.*, vol. 16, no. 6, pp. 984–1002, June 2025, doi: 10.1108/JSTPM-05-2023-0071.

[4] Professor and Head, Dept. of ECE, Rajalakshmi Engineering College, Chennai, TN, India and L. Bhagyalakshmi, "Securing the Future of Digital Marketing through Advanced Cybersecurity Approaches and Consumer Data Protection Privacy and Regulatory Compliance," *J. Cybersecurity Inf. Manag.*, vol. 13, no. 1, pp. 17–27, 2024, doi: 10.54216/JCIM.130102.

[5] L. V. Ivanitskaya, D. Zikos, and E. Erzikova, "Multidisciplinary Contributions and Research Trends in eHealth Scholarship (2000-2024): Bibliometric Analysis," *J. Med. Internet Res.*, vol. 27, p. e60071, June 2025, doi: 10.2196/60071.

[6] H. N. Durmuş Şenyapar, "Digital Marketing in the Age of Cyber Threats: A Comprehensive Guide to Cybersecurity Practices," *J. Soc. Sci.*, vol. 8, no. 15, pp. 1–10, Feb. 2024, doi: 10.30520/tjsosci.1412062.

[7] K. Sharmin and M. I. Rahman, "Digital Forensics: Assessing Enhanced Evidence Collection and New Perspectives for Strengthening Crime-Combating Efforts in the Bangladesh Police," in *2024 4th International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, FEZ, Morocco: IEEE, May 2024, pp. 1–5. doi: 10.1109/IRASET60544.2024.10548227.

[8] Md. M. Islam, et al., "Unlocking the Mediating and Moderating Role of Information Security in Information Systems: A Combined TAM, ISM, and HBM Model," Human Behavior and Emerging Technologies, Dec. 2025. 10.1155/hbe2/5593002 (accessed Dec. 2025).

[9] D. Mukherjee, W. M. Lim, S. Kumar, and N. Donthu, "Guidelines for advancing theory and practice through bibliometric research," *J. Bus. Res.*, vol. 148, pp. 101–115, Sept. 2022, doi: 10.1016/j.jbusres.2022.04.042.

[10] A. Sulich, T. Zema, and L. Kulhanek, "Towards a Secure Future: A Bibliometric Analysis of the Relations Between Cybersecurity and Sustainable Development," *Procedia Comput. Sci.*, vol. 225, pp. 1448–1457, 2023, doi: 10.1016/j.procs.2023.10.133.

[11] M. R. I. Bhuiyan, M. R. Faraji, Mst. N. Tabassum, P. Ghose, S. Sarbabidya, and R. Akter, "Leveraging Machine Learning for Cybersecurity: Techniques, Challenges, and Future Directions," *Edelweiss Appl. Sci. Technol.*, vol. 8, no. 6, pp. 4291–4307, Nov. 2024, doi: 10.55214/25768484.v8i6.2930.

[12] R. Gupta *et al.*, "Consumer Views on Privacy Protections and Sharing of Personal Digital Health Information," *JAMA Netw. Open*, vol. 6, no. 3, p. e231305, Mar. 2023, doi: 10.1001/jamanetworkopen.2023.1305.

[13] E. T. Megbowon and O. O. David, "Information and communication technology development and health gap nexus in Africa," *Front. Public Health*, vol. 11, p. 1145564, Mar. 2023, doi: 10.3389/fpubh.2023.1145564.

[14] N. Zainal Abidin, S. Sri Ramalu, G. Nadarajah, and A. Anuar, "A Bibliometric Analysis of Cybersecurity Behaviour in Organization," *SAGE Open*, vol. 15, no. 3, p. 21582440251361635, Jan. 2025, doi: 10.1177/21582440251361635.

[15] Md. Faisal-E-Alam, M. R. I. Bhuiyan, A. Mimi, and Md. T. Miah, "The role of the three zero framework in advancing global sustainable development through bibliometric and text mining analysis," *Discov. Sustain.*, vol. 6, no. 1, p. 1128, Oct. 2025, doi: 10.1007/s43621-025-01919-x.

[16] K. Khanom *et al.*, "Worker Satisfaction in Health, Hygiene and Safety Measures Undertaken by the Readymade Garments Industry of Bangladesh: A Case Study on Gazipur," *J. Bus. Stud.*, vol. 03, no. 01, pp. 93–105, 2022, doi: 10.58753/jbspust.3.1.2022.6.

[17] D. T. Gemeda and A. D. Durie, "Recent Digital Marketing Research Trend: A Bibliometric Analysis," Dec. 30, 2024, *Business, Economics and Management*. doi: 10.20944/preprints202412.2434.v1.

[18] T. Saheb, B. Amini, and F. Kiaei Alamdari, "Quantitative analysis of the development of digital marketing field: Bibliometric analysis and network mapping," *Int. J. Inf. Manag. Data Insights*, vol. 1, no. 2, p. 100018, Nov. 2021, doi: 10.1016/j.jjimei.2021.100018.

[19] R. Hossain, Md. H. Hasan, S. Uddin, S. B. Yousuf, and M. R. I. Bhuiyan, "Determinants of international students' migration intentions for higher education abroad," *Int. J. Innov. Res. Sci. Stud.*, vol. 8, no. 2, pp. 4065–4077, Apr. 2025, doi: 10.53894/ijirss.v8i2.6231.

[20] A. Ahmadvand, D. Kavanagh, M. Clark, J. Drennan, and L. Nissen, "Trends and Visibility of 'Digital Health' as a Keyword in Articles by JMIR Publications in the New

Millennium: Bibliographic-Bibliometric Analysis," *J. Med. Internet Res.*, vol. 21, no. 12, p. e10477, Dec. 2019, doi: 10.2196/10477.

[21] M. C. Thuriaux, "Public Health," in *Social Problems and Mental Health*, 1st ed., London: Routledge, 2022, pp. 118–120. doi: 10.4324/9781003261919-33.

[22] U. Azmaien, "Integrating Artificial Intelligence and Social Media for English as a Foreign Language (EFL) Learning: A Study on Meta-AI's Influence on Reading Comprehension," *J. Inf. Syst. Inform.*, vol. 7, no. 2, pp. 1083–1105, June 2025, doi: 10.51519/journalisi.v7i2.1070.

[23] M. R. I. B. Bhuiyan, A. Mimi, M. R. Faraji, P. Ghose, and Md. M. Rahman, "A Bibliometric Analysis of Machine Learning in Information Systems: Trends, Collaborations, and Research Directions," *Collaborations, and Research Directions*, 2025, Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5782082

[24] J. Hu, C. Li, Y. Ge, J. Yang, S. Zhu, and C. He, "Mapping the Evolution of Digital Health Research: Bibliometric Overview of Research Hotspots, Trends, and Collaboration of Publications in JMIR (1999-2024)," *J. Med. Internet Res.*, vol. 26, p. e58987, Oct. 2024, doi: 10.2196/58987.

[25] Z. Wang, D. Ma, R. Pang, F. Xie, J. Zhang, and D. Sun, "Research Progress and Development Trend of Social Media Big Data (SMBD): Knowledge Mapping Analysis Based on CiteSpace," *ISPRS Int. J. Geo-Inf.*, vol. 9, no. 11, p. 632, Oct. 2020, doi: 10.3390/ijgi9110632.

[26] N. Akter *et al.*, "Advanced Detection and Forecasting of Fake News on Social Media Platforms Using Natural Language Processing and Artificial Intelligence," *J. Posthumanism*, vol. 5, no. 6, pp. 3208–3236, June 2025, doi: 10.63332/joph.v5i6.2446.

[27] C. Molla, M. R. I. Bhuiyan, Md. T. Islam, and A. - Amin, "Mediating role to banking performance for adopting digital bank using a technology organizational environment model," Digital Finance, Dec. 2025.

[28] M. Khatun, R. Hossain, M. R. I. Bhuiyan, Mst. N. Tabassum, and Md. A. J. Riaj, "Green Entrepreneurship and Digital Transformation for Sustainable Development: A Systematic Review," in *Advances in Logistics, Operations, and Management Science*, K. Mouloudj and A. C. Bouarar, Eds., IGI Global, 2024, pp. 153–180. doi: 10.4018/979-8-3693-7442-9.ch006.

[29] S. Pahari, A. Bandyopadhyay, V. K. V. M., and S. Pingle, "A bibliometric analysis of digital advertising in social media: the state of the art and future research agenda,"

Cogent Bus. Manag., vol. 11, no. 1, p. 2383794, Dec. 2024, doi: 10.1080/23311975.2024.2383794.

[30] M. K. Dash, R. Sahu, G. Panda, D. Jain, G. Singh, and C. Singh, "Social media role in public health development: a bibliometric approach," *Kybernetes*, vol. 52, no. 11, pp. 5460–5479, Nov. 2023, doi: 10.1108/K-02-2022-0294.

[31] G. Agac, F. Sevim, O. Celik, S. Bostan, R. Erdem, and Y. I. Yalcin, "Research hotspots, trends and opportunities on the metaverse in health education: a bibliometric analysis," *Libr. Hi Tech*, vol. 43, no. 1, pp. 1–35, Feb. 2025, doi: 10.1108/LHT-04-2023-0168.

[32] N. Donthu, S. Kumar, D. Mukherjee, N. Pandey, and W. M. Lim, "How to conduct a bibliometric analysis: An overview and guidelines," *J. Bus. Res.*, vol. 133, pp. 285–296, Sept. 2021, doi: 10.1016/j.jbusres.2021.04.070.

[33] M. R. I. Bhuiyan, Most. S. Akter, A.- Amin, and R. Hossain, "The Mediating Effect of Innovation Capabilities, Information Quality and Supply Chain Resilience in the Relationship Between Big Data Analytics Capability (BDAC) and Healthcare Performance," *SAGE Open*, vol. 15, no. 3, p. 21582440251362262, Jan. 2025, doi: 10.1177/21582440251362262.

[34] A. J. Cartwright, "The elephant in the room: cybersecurity in healthcare," *J. Clin. Monit. Comput.*, vol. 37, no. 5, pp. 1123–1132, Oct. 2023, doi: 10.1007/s10877-023-01013-5.

[35] X. Nan, I. A. Iles, B. Yang, and Z. Ma, "Public Health Messaging during the COVID-19 Pandemic and Beyond: Lessons from Communication Science," *Health Commun.*, vol. 37, no. 1, pp. 1–19, Jan. 2022, doi: 10.1080/10410236.2021.1994910.

[36] M. Mathur, "Where is the Security Blanket? Developing Social Media Marketing Capability as a Shield from Perceived Cybersecurity Risk," *J. Promot. Manag.*, vol. 25, no. 2, pp. 200–224, Feb. 2019, doi: 10.1080/10496491.2018.1443310.

[37] M. I. Pramanik, P. Ghose, Md. D. Hossen, M. H. U. Ahmed, Md. M. Rahman, and M. R. I. Bhuiyan, "Emerging Technological Trends in Financial Crime and Money Laundering: A Bibliometric Analysis of Cryptocurrency's Role and Global Research Collaboration," *J. Posthumanism*, vol. 5, no. 6, pp. 3611–3633, June 2025, doi: 10.63332/joph.v5i6.2493.

[38] P. Ghose, M. R. I. Bhuiyan, M. N. Hasan, S. H. Rakib, and L. Mani, "Mediated and moderating variables between behavioral intentions and actual usages of fintech

in the USA and Bangladesh through the extended UTAUT model," *Int. J. Innov. Res. Sci. Stud.*, vol. 8, no. 2, pp. 113–125, Mar. 2025, doi: 10.53894/ijirss.v8i2.5130.

[39] C. O. Ezeilo, N. Leon, A. Jajodia, and H.-R. Han, "Use of Social Media for Health Advocacy for Digital Communities: Descriptive Study," *JMIR Form. Res.*, vol. 7, p. e51752, Nov. 2023, doi: 10.2196/51752.

[40] W. N. Khan, J. K. Lee, and S. Liu, "Is Cybersecurity a Social Responsibility?," *Inf. Syst. Front.*, vol. 27, no. 4, pp. 1367–1391, Aug. 2025, doi: 10.1007/s10796-024-10565-z.

[41] M. R. I. Bhuiyan and Most. S. Akter, "Assessing the Potential Usages of Blockchain to Transform Smart Bangladesh: A PRISMA Based Systematic Review," *J. Inf. Syst. Inform.*, vol. 6, no. 1, pp. 245–269, Mar. 2024, doi: 10.51519/journalisi.v6i1.659.

[42] E. V. Eppes, M. Augustyn, S. M. Gross, P. Vernon, L. E. Caulfield, and D. M. Paige, "Engagement With and Acceptability of Digital Media Platforms for Use in Improving Health Behaviors Among Vulnerable Families: Systematic Review," *J. Med. Internet Res.*, vol. 25, p. e40934, Feb. 2023, doi: 10.2196/40934.

[43] L. Zhou, J. Bao, V. Watzlaf, and B. Parmanto, "Barriers to and Facilitators of the Use of Mobile Health Apps From a Security Perspective: Mixed-Methods Study," *JMIR MHealth UHealth*, vol. 7, no. 4, p. e11223, Apr. 2019, doi: 10.2196/11223.

[44] M. R. I. Bhuiyan, K. M. S. Uddin, and M. N. U. Milon, "Prospective Areas of Digital Economy in the Context of ICT Usages: An Empirical Study in Bangladesh," *FinTech*, vol. 2, no. 3, pp. 641–656, Sept. 2023, doi: 10.3390/fintech2030035.

[45] K. G. Nalbant and S. Aydin, "Development and Transformation in Digital Marketing and Branding with Artificial Intelligence and Digital Technologies Dynamics in the Metaverse Universe," *J. Metaverse*, vol. 3, no. 1, pp. 9–18, June 2023, doi: 10.57019/jmv.1148015.

[46] M. Liu, M. Shore, W. Yeoh, F. Jiang, and S. Zeadally, "Toward effective cybersecurity management: a hierarchical process model with performance assessment," *J. Cybersecurity*, vol. 11, no. 1, p. tyaf020, Jan. 2025, doi: 10.1093/cybsec/tyaf020.

[47] Md. D. Hossen, M. Z. Abedin, T. M. Chowdhury, Z. Islam, and Md. R. Kabir, "Unveiling the Impact of E-Governance on the Transformation from Digital to Smart Bangladesh," *Pak. J. Life Soc. Sci. PJLSS*, vol. 23, no. 1, 2025, doi: 10.57239/PJLSS-2025-23.1.009.

[48] Febrian Gibran Juliansyah and R. K. Anwar, “A bibliometric study of digital health campaign strategies, effectiveness, and trends (2015-2023),” *J. Studi Komun. Indones. J. Commun. Stud.*, vol. 9, no. 2, pp. 521–536, July 2025, doi: 10.25139/jsk.v9i2.9702.