JIPI (Jurnal Ilmu Perpustakaan dan Informasi) Vol. 10 No. 1 Tahun 2025
ISSN (online): 2528-021X
Page: 37-51

SOCIAL NETWORK SECURITY RESEARCH TRENDS: BIBLIOMETRIC ANALYSIS 2013-2023

Keysha Husna Muchtarom
Universitas Padjadjaran, Indonesia
E-mail: keysha21002@mail.unpad.ac.id*

Yunus Winoto
Universitas Padjadjaran, Indonesia

Tine Silvana Rachmawati
Universitas Padjadjaran, Indonesia

Receive : 06 Dec 2024
Accepted : 03 May 2025
Published: 23 May 2025
DOI : 10.30829/jipi.v10i1.22351

Abstract
This research discusses the development of trends regarding social network security research. Through the bibliometric analysis method by analyzing data found in the Scopus and Dimensions databases. Trend analysis of social network security research using the Scopus and Dimensions databases provides valuable insights. This research displays key information in the scopus and dimensions databases using the biblioshiny application. The findings show consistent interest and significant growth in this research. The research focus covers various aspects of social network security, reflecting the complexity of the topic. This research analyzes several points such as relevant authors, author collaboration, relevant sources, number of articles per year, and world cloud. Collaboration between researchers also proved important, with a high level of collaboration and significant international collaboration. The contributions of key researchers such as Zhang Z, Abraham A, Choo KKR, Li X, and Akhramovich V made a significant impact in this field. In addition, findings on the contributions of specific countries such as Korea, India, and China provide an overview of the distribution of social network security research globally. Frequently occurring keywords, such as "social networking (online)" and "network security," illustrate the research focus on security aspects in the context of online social networks. The findings provide guidance for researchers to understand future trends and directions of social network security research. Overall, this analysis provides important insights into the evolution and characteristics of social network security research. These findings can be used as a basis for further research, knowledge development, and guidance for practitioners in the field of social network security.

Keywords: *Social network security; Research trends; Bibliometric analysis; Scopus; Dimensions*

INTRODUCTION

The development of an increasingly modern era has triggered a transformation in the system, both directly and indirectly, including in the way people communicate. In the past, the communication process involved direct interaction between users to communicate. The limited reach between users was significant (Baskara & Hariyadi, 2014). However, advances in technology, especially the internet, have made it easy to overcome the limitations of distance,

time, and cost. The implementation of technology in terms of improving one of them in the fields of communication, business, sales and purchase of products is by using electronic commerce (e-commerce) (Adi, 2013). There are many factors that cause someone to access a website on an Internet site. Starting from low costs, quality types of goods, trust, easy transaction facilities, to several other factors (Sukma, 2013).

The development of information technology follows the progress of human civilization. This progress includes the development of information technology infrastructure, such as hardware, software, data storage technology, and communication technology (Darmawan & Ratnasari, 2020; Iksan et al, 2020). The rapid development of information technology has changed the way people interact and communicate with each other. Online social networks or social networks are platforms that help users share various types of content such as text, images, audio, video, and animation instantly to millions of people, which can have positive or negative impacts on society, and are used for business promotion, research data collection, news dissemination, sharing experiences, expressing political ideologies, providing film criticism, and various other interesting things (Peter, Begum, and Mercy 2022). Social networks have become an inseparable part of everyday life, allowing people to connect with friends, family, and communities around the world.

However, behind the ease and convenience offered by social networks, there are also risks that we need to overcome, so that social network security is a shared responsibility of society in a broader context. Social media security, amidst the rapid growth of digital interactions, highlights the complexity and urgency of data and privacy protection in the online ecosystem and personal freedom is the essence of privacy because privacy is the right of every individual that should be respected where in the current era of information technology, information about a person's privacy has been widely spread on the internet (Yel and Nasution 2022). The spread of privacy data can be caused by negligence or service providers. Social media is the main place for people to share moments, discuss ideas, and build networks. However, with this convenience, risks such as fraud, identity theft, and other cyber threats arise. Social media security includes proactive efforts to prevent and address these risks.

The success and security of users on the platform depends heavily on a deep understanding of the challenges and solutions in the context of cybersecurity (Gunawan 2021). One of the main aspects of social media security is protecting user security. Users must be able to maintain their privacy by controlling who can access their personal information and choosing the level of security that suits their preferences. This can be done through the privacy settings available on the social media platform. Users can limit who can see their posts and profiles, and choose to encrypt the messages and content they share. Some platforms also offer additional identity verification such as two-factor authentication.

The researcher conducted a review of previous research on three researchers to compare the differences and novelty of the researchers. The first study was conducted by Hakiki, Harahap, and Sulistyanto (2024) entitled Bibliometric Analysis of the Development of Communication Strategies on Social Media in Government Agencies in Cybersecurity analyzing the social media communication strategies of government agencies related to cybersecurity using Scopus data. Although it has similarities in discussing bibliometric analysis, the study focuses more on government communication strategies, while this study maps global social network security trends based on Scopus and Dimensions data with Biblioshiny. This provides broader insight into the development of social network security in general, not limited to social media.

The second study was conducted by Permatasari et al. (2023) entitled Bibliometric Analysis of Phishing Attacks and Social Media Using VOSviewer analyzing research trends related to phishing attacks on social media using Google Scholar with the co-occurrence method in VOSviewer. The study identified three main clusters related to phishing, information security, and data privacy on social media. The difference with the previous study is that it focuses on phishing and specific information security on social media, while this study is broader in analyzing social network security trends based on data from Scopus and Dimensions using Biblioshiny. The third study was conducted by Adriansyah and Anugrah (2024) entitled Bibliometric Analysis of Online Sales Company Security to Prevent Cybercrime analyzing research trends on cybersecurity in e-commerce businesses using VOSviewer, focusing on publication trends, frequently appearing keywords, and collaboration networks between researchers. This study identifies various cyber threats faced by e-commerce companies and highlights the need for more effective security strategies. Unlike previous research, the researchers analyzed social network security research trends using data from Scopus and Dimensions with Biblioshiny, thus providing a broader picture of academic developments in this field during the period 2013–2023.

This study aims to dig deeper and measurably into social network security research trends using a bibliometric analysis approach. By analyzing the existing scientific literature, this study attempts to identify patterns, main research focuses, and contributions of researchers and research institutions in developing social network security. The goal is to provide a clearer and more accurate picture of the dynamics of social network security, so that it can provide valuable insights for the development of more effective and responsive security strategies to the ever-evolving threats in the digital realm. Meanwhile, the benefits of this study are to provide insights for academics, researchers, and practitioners in designing more effective and adaptive social network security strategies to the ever-evolving digital threats.

Social Network Security and Social Network Crime

Network security is a system designed to protect a network from various external threats that have the potential to damage or disrupt the integrity, confidentiality, and availability of the network (Saputro 2016). The network security system functions as a layer of protection to prevent unauthorized access, cyber attacks, or other malicious actions that can disrupt network performance and stability. Meanwhile, social networks are one of the modern communication platforms that help users to interact remotely online, while also functioning as a medium for channeling hobbies and expressing creativity (Setianingsih and Aziz 2022). In addition, social networks are a space for sharing information, building communities, and expanding friendship or professional networks, all of which can be done easily and quickly through digital devices. Based on these two explanations, social network security is defined as an effort related to technology, policies, and strategies to protect social networking platforms from threats that can harm their users, such as data theft, account hacking, or misuse of personal information.

This security aims to maintain privacy, protect online interactions, and ensure that social networks remain a safe space for their users to communicate, share information, and express creativity without worrying about digital risks. The existence of fake identities, fraud, and cyber attacks pose a real threat to people's privacy and security in the online ecosystem. Cyber terrorism is an illegal activity that involves attacks on computers, networks, and the information stored in them. The purpose of the attack is to intimidate or coerce the government or society

for political and social purposes. In short, it can be interpreted as a form of terrorism carried out through cyberspace or by terrorists who utilize cyber technology. On the other hand, cyber terrorism is an act of individuals or groups that aims to launch cyber attacks (Lubis 2017). In addition to the role of platform providers, the role of the community is also very important in maintaining the security of social networks. Awareness of security risks and knowledge of good security practices must be an integral part of using social networks. The importance of user privacy in network security management is also an important aspect. In the context of social networks, there are a number of problems that users must face when their personal information is released to the public.

According to Oehri and Teufel (2012) in Gunawan (2021) user privacy is one of the most important aspects in network security management. In addition, user privacy is needed because it involves protecting personal data, having sensitive information, and user activities from potential threats. Potential threats such as unauthorized access, identity theft, or misuse of information by irresponsible parties. Maintaining user privacy not only increases trust in the network but also helps create a safe and trusted digital environment. This privacy protection can lead to privacy violations such as gossip, slander, and irresponsible sharing of news, photos, or videos.

According to Edwards (2015) in Gunawan (2021), awareness of information security can be defined as a person's understanding of security practices when using internet networking sites, as well as a recognition of the importance of protecting personal or group data, especially in an organizational context. The public needs to understand the importance of maintaining the confidentiality of personal information, such as using strong passwords and not sharing sensitive personal information carelessly. In addition, the public must also be active in reporting suspicious incidents or behavior that violates security rules to the authorities.

By maintaining the security of social networks, people can protect their privacy and personal information. This will provide a sense of security and confidence in exploring the digital world. Social network security also contributes to the quality of people's online experience, ensuring that their interactions on social networks are not disrupted by harmful attacks or fraud. In addition, with public awareness of social network security, we can build a responsible and supportive digital culture.

Overall, maintaining social media security is a shared responsibility of society. The development of information technology has provided great benefits in the way we interact and communicate. However, we must also be aware of the risks associated with using social media and play an active role in maintaining our security and privacy. With the right steps from social media platform providers, as well as active participation and awareness from the community, we can create an online ecosystem that is safe, trusted, and beneficial for all. According to Givan et al. (2021) in Andi Putra and Sutabri (2023) phishing is a form of cybercrime that involves fraud by deceiving victims. Usually, this crime is carried out via email or social media by sending fake links, creating fake websites, and the like. The goal is to steal important victim data, such as personal identity, passwords, PIN codes, and OTP (one time password) codes used in financial accounts such as mobile banking, internet banking, paylater services, digital wallets, and credit cards (Hartawan, Putra, and Muktiono 2020). Phishing is a fraudulent technique that has become a serious threat to social media security. In a phishing attack, an attacker pretends to be a trusted entity, such as a well-known company or organization, and tries to convince users to provide sensitive personal or financial information.

The main goal of a phishing attack is to steal passwords, credit card numbers, bank account information, or other sensitive data that can be used to carry out illegal activities or harm users. Social networking platform providers are aware of the threat posed by phishing and are trying to raise user awareness about this tactic. One of the efforts is to provide education to users on how to recognize the signs of phishing and protect themselves from such attacks. In this education, users are provided with information about the common characteristics of phishing attacks, such as unsolicited or suspicious messages asking for personal information, requests to click on suspicious links, or suspicious attachments in emails.

In addition, users are also given practical advice on steps they can take to protect themselves from phishing attacks. One of these is to not click on suspicious links in emails or social media messages. Data security is also a major concern in social networks. Users' personal data stored on social networking platforms must be properly protected to prevent unauthorized access. This involves using data encryption, protection against cyberattacks, and actively monitoring for potential security breaches. Social networking platform providers use multiple layers of security, including firewalls, end-to-end encryption, and automated threat detection to protect user data. They also have dedicated security teams to monitor and respond quickly to security threats. It is important for social networking platform providers to have clear policies about user security and privacy. They should commit to protecting users' personal information, provide easy-to-use privacy settings, and provide transparency about how user data is used and stored. Many social networking platforms have updated their privacy policies to meet the increasing requirements of data protection laws.

Social Network Security Strategies

In order to maintain social media security, it is also important to follow common security practices that are widely accepted in the digital world. First, use strong and unique passwords for social media accounts. Avoid using passwords that are easy to guess or related to personal information. Second, avoid sharing sensitive information publicly on social media platforms. Do not provide phone numbers, home addresses, or financial information publicly unless necessary. Third, check the privacy policies and privacy settings on the social media platforms you use. Make sure you understand who can see your information and how your data is used. Fourth, be wary of unknown or suspicious friend or follow requests. Do not accept friend requests or follow accounts that seem suspicious. Fifth, avoid clicking on suspicious or unknown links on social media platforms. These links can direct you to malicious websites or try to steal your personal information. Sixth, update the software and applications you use with the latest versions that contain security fixes. Seventh, use two-factor authentication options when available. This adds an extra layer of security by requiring verification through a device other than your password. Eighth, be careful about sharing personal information through private messages. Make sure you communicate with people you know and trust. Ninth, report suspicious accounts or content to the social network platform provider. By reporting suspicious activity, you help protect yourself and other users from potential threats. Tenth, use policy updates and notifications from the social network platform provider. It is important to stay up-to-date with policy changes and security updates provided by the platforms you use.

Knowledge of social network security research trends is essential given the complexity of ever-evolving threats and ever-changing technology. Research in the information security domain continues and is a major focus of research that can be developed through the examination of several in-depth studies. This research is not only limited to related disciplines

such as computer systems, information systems, computer science, informatics engineering, and information technology, but also involves various fields of science in an integrated manner according to needs, such as management, social science, law, and ethics (Nasution 2018). Developments in social network security not only cover technical aspects, but also explore relevant legal, ethical, and regulatory concepts. By understanding research trends, security practitioners can anticipate new developments, design more effective protection strategies, and prepare for responses to threats that may emerge in the future. It also enables stakeholders, both from academic and industry practitioners, to jointly contribute to improving security and privacy standards in the online world.

RESEARCH METHOD

Etymologically, the term bibliometrics in Indonesian or bibliography in English consists of two words, namely biblio which means book or bibliography, and metrics which means measurement (Royani and Idhani 2018). Bibliometrics is considered a measurement tool for analyzing books, journals, and other scientific publications. This method is often used to evaluate research performance, identify scientific trends, and understand publication and citation patterns in a particular field. Bibliometrics utilizes data such as the number of publications, the number of citations, and relationships between authors or institutions to generate deeper insights into the dynamics of scientific knowledge.

Bibliometric methods have undergone many developments and advances thanks to the use of computer-based data processing technology (Wedhatama, Hanoum, and Prahardika Prihananto 2021). In recent years, the number of publications utilizing bibliometric methods has also increased significantly. This is not only influenced by the computerized process, but also by the need for bibliometric methods to process certain volumes of data so that the results can be statistically reliable.

Blank spaces in a topic can create novelty in research with the above topics. The gap in a research topic in certain years can create unique novelty, because the situation of society in each year is different. Scopus was chosen as the main database because it has a wide coverage, accredited journals, and is rich in authors and citations. Scopus is a citation and abstract database managed by experts in their fields, covering 39,744 active scientific journals, 29,683 conference proceedings, 1,499 book series with 59,698 volumes, more than 300 trade publications, and more than 8,000 articles published by international publishers, based on information from the official Scopus website (www.scopus.com) accessed on June 3, 2020 (Hakim 2020). In addition, the Dimensions database was also chosen where Dimensions has a digital object identifier (DOI) index, covering millions of studies, 6 million grants, and 142 million patents. Data from Dimensions is used for descriptive and evaluative bibliographic analysis. The topics in this study are interrelated, so the bibliometric method is applied to analyze the relationship between topics, both large-scale and subtopics (Ryandono et al. 2022).

Summary of the research data sources used by the researcher are as follows; (1) Research Database comes from Scopus and Dimensions; (2) Searching Period starts from 2013 to 2023; (3) Language = English; (4) Searching Keyword = "Social Network Security"; (5) Document Type = Article; and (6) Sample Size = 82. The method used in this research consists of the following five stages. This study begins the process of determining search keywords by searching the Scopus and Dimensions databases on December 8, 2023. The researcher uses the search keyword TITLE ("Social Network Security") with the aim of detailing and filtering

scientific literature that focuses on social network security. The search results in the Scopus database showed 29 related documents, which were then filtered based on the search "Article title" and limited to the publication year range from 2009 to 2023. The search results in the Dimensions database showed 29 related documents, which were then filtered based on the search "title and abstract" and limited to the publication year range from 2003 to 2023 and limited to the publication type "Article". After filtering, the number of documents was focused on articles with a relevant publication time range. Data from Scopus will be analyzed using R Studio and Biblioshiny. Biblioshiny is a network analysis-based software that helps map and visualize networks and bibliometric maps effectively. The Biblioshiny application makes it easy for users to display, obtain, and process statistical data from bibliographic searches without having to understand how to code programs (López, Marín, and Pérez 2024).

RESULT AND DISCUSSION

Key Information

Table 1
Main Information Database Scopus and Dimension

Timespan	2009:2023	2003:2024
Sources (Journals, Books, etc)	28	49
Documents	29	53
Annual Growth Rate %	5.08	0
Document Average Age	5.03	4.23
Average citations per doc	13.45	13.53
References	1	1
Keywords Plus (ID)	197	18
Author's Keywords (DE)	87	18
Authors	84	164
Authors of single-authored docs	3	5

Source: Biblioshiny, 2023

In this study, a bibliometric analysis was conducted by analyzing two databases, the table above is the result of the Scopus database from 2009-2023 and Dimensions from 2003-2024 to investigate the trend of social network security research. A total of 28 Scopus sources, including journals and books, were utilized in reviewing 29 documents. While Dimensions sources as many as 49 sources, involving journals and books, were utilized in reviewing 53 documents.

From the results of the analysis, it was revealed that the average annual growth rate of Scopus reached 5.08%, while Dimension 0 data showed consistent interest in this topic during the study period. In addition, the average age of Scopus documents was 5.03 years, while the average age of Dimensions documents was 4.23 reflecting the continued relevance of the research.

In terms of influence and acceptance in the scientific community, each Scopus document was cited an average of 13.45 times, while Dimensions documents were cited an average of 13.53 times indicating the importance of these findings in the social network security literature. Although the number of references per document is relatively low, only one, this may reflect the

focus on primary literature and more recent research. Regarding keyword usage in Scopus, there are 197 additional keywords (ID) and 87 keywords from authors (DE). Meanwhile, regarding keyword usage in Dimensions, there are 18 additional keywords (ID) and 18 keywords from authors (DE), reflecting the diversity and complexity of aspects given attention in the social network security literature. Finally, the Scopus study involved 84 authors, with 3 documents written by a single author. Meanwhile, the Dimensions study involved 164 authors, with 5 documents written by a single author, indicating a significant level of collaboration in this research community. This bibliometric analysis provides in-depth insights into the trends of social network security research during the study period and can be a basis for further understanding in the development of social network security literature in the future.

Author Analysis

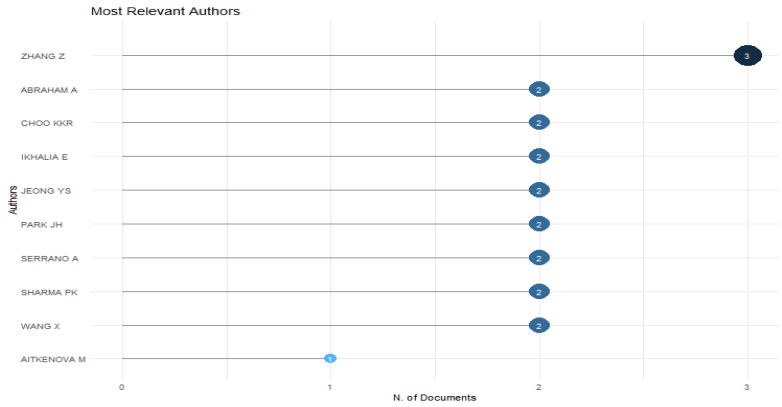

Figure 1. Most Relevant Authors From the Scopus Database
Source: Biblioshiny, 2023

In the scope of this study, an analysis was carried out as shown in the image above which was carried out in the Scopus database on researcher contributions by evaluating the author collaboration table and related articles. Zhang Z stands out as the main contributor with 3 articles, contributing 0.95 to the comparison of fractionalized articles. Abraham A, although only contributing 2 articles, showed a significant impact of his contribution with a higher fractionalized value of 1.2. Choo KKR, Ikhalia E, Jeong YS, Park JH, Serrano A, and Sharma PK each have 2 articles with varying fractionalized values, reflecting the varying levels of contribution in each related article. Wang X also participated with 2 articles, giving a fractionalized value of 0.45. Aitkenova M contributed one article with a fractionalized value of 0.125.

Meanwhile, the author analysis in the database dimensions of this study highlights a number of researchers who have had a significant impact on the social network security literature. Li X and Zhang Z each contributed 3 articles, with fractionalized values of 0.642857143 and 0.95, respectively, indicating substantial contributions to the literature on social network security. Akhramovich V and Akhramovych V, with 2 articles each, stood out with very high fractionalized values of 2 and 1.2, respectively, reflecting significant contributions to this research. Other researchers, such as Boroojeny AE, Chitsaz H, Choo KR, Gallagher SR, Hu Y, and Jeong Y, also made quite diverse contributions, with 2 articles each and varying fractionalized values, reflecting varying levels of contributions to the literature on social network security.

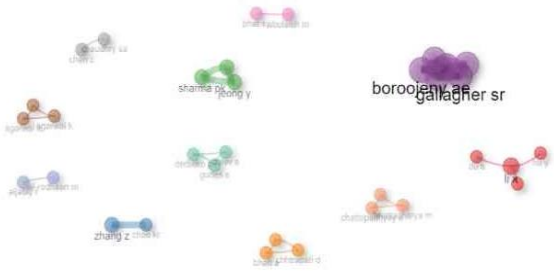

Figure 2. Author's Collaboration Network in Database Dimensions
Source: Biblioshiny, 2023

As shown in the figure above, this study explores the framework of author collaboration on the Dimensions database by analyzing several key parameters of the main nodes. In the figure, a group of nodes collaborating as one entity is referred to as a cluster, where each node in the network belongs to one cluster. Several researchers, such as Li X, Hu Y, Chen H, Du S, Zhang Z, Choo KR, Jeong Y, Park JH, Sharma PK, Boroojeny AE, Chitsaz H, Gallagher SR, Sahinalp SC, Sharifi-Zarchi A, Shrestha A, Bhatt A, Chaudhari SP, Chhtrapati D, Agarwal A, Agarwal K, Gourav A, Abulaish M, Bhat SY, Chaudhry SA, Chen C, Derbeko P, Dolev S, Gudes E, Bhattacharya M, Chattopadhyay S, Das AK, Al-Rodhaan M, and Aljably R, play key roles in this collaboration network. These nodes are grouped into different clusters with Betweenness, Closeness, and PageRank attributes. For example, Li X is included in cluster 1 with Betweenness value of 3, Closeness 0.333, and PageRank 0.058. Zhang Z, Choo KR, Jeong Y, Park JH, and Sharma PK form clusters 2 and 3, with certain characteristics that reflect the unique roles and contributions of each researcher in the collaboration network.

While in the Scopus database on the network structure by evaluating several key parameters for a number of main nodes. Some of the researchers who attracted attention in this analysis include names like Zhang Z, Choo KKR, Wang X, Guo W, Gupta BB, Jing J, Liu E, Liu Z, Ikhalia E, Serrano A, Arreymbi J, Bell D, Louvieris P, Jeong YS, Park JH, Sharma PK, Loia V, Abraham A, Elbarawy Y, Hassanien AE, Akaichi J, Ali Alqahtani A, Dhouioui Z, Bharati TS, Kumar C, Ji S, Liu Y, Aitkenova M, Aktayeva A, Beissekov A, Konyrkhanova A, Al-Sayyed R, Al-Zoubi AM, Alqatawna J, and Madain A. These nodes are grouped into different clusters by considering attributes like Betweenness, Closeness, and PageRank. Zhang Z stands out in cluster 1, showing his central role with a Betweenness value of 10 and a Closeness of 0.125. Meanwhile, several other researchers, including Ikhalia E, Serrano A, Jeong YS, and others, are spread across various clusters with attributes that reflect their unique roles and positions in the network.

Journal Analysis

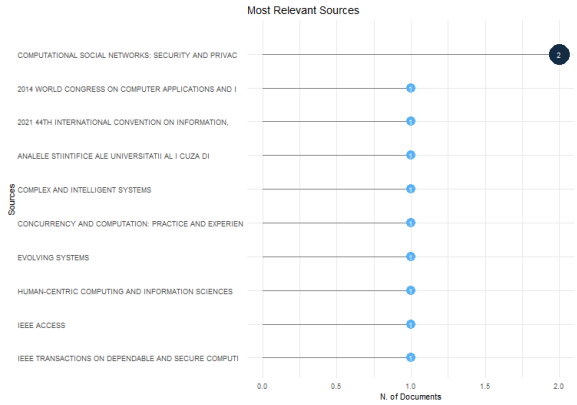

Figure 3. Most Relevant Sources in Database Scopus
Sumber: Biblioshiny, 2023

The researcher conducted an analysis on the Scopus database of sources used in research on social network security. A table has been presented to display the number of articles originating from each source. One example of the classical analytical law in bibliometrics is knowing the order of journals that publish articles in order from the largest to the smallest number. This is used to group and identify core journals. In addition, this journal ordering facilitates the recognition of the difference between "core" journals that publish most articles, and "subsequent areas". From the results of the analysis, it was found that the source entitled "COMPUTATIONAL SOCIAL NETWORKS: SECURITY AND PRIVACY" is the main contributor to social network security research with two relevant articles. This source has a significant impact on the development of knowledge in the field. In addition, several other sources also make important contributions to social network security research by each contributing one relevant article. These sources include "2014 WORLD CONGRESS ON COMPUTER APPLICATIONS AND INFORMATION SYSTEMS, WCCAIS 2014," "2021 44TH INTERNATIONAL CONVENTION ON INFORMATION, COMMUNICATION AND ELECTRONIC TECHNOLOGY, MIPRO 2021 - PROCEEDINGS," "ANALELE STIINTIFICE ALE UNIVERSITATII AL I CUZA DIN IASI - SECTIUNEA STIINTE ECONOMICE," "COMPLEX AND INTELLIGENT SYSTEMS," "CONCURRENCY AND COMPUTATION: PRACTICE AND EXPERIENCE," "EVOLVING SYSTEMS," "HUMAN-CENTRIC COMPUTING AND INFORMATION SCIENCES," "IEEE ACCESS," and "IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING." Although the number of articles originating from these sources is only one, they still make an important contribution to the development of knowledge in the field of social network security. Overall, it can be concluded that the most influential primary source in social network security research is "COMPUTATIONAL SOCIAL NETWORKS: SECURITY AND PRIVACY" with two relevant articles. In addition, other sources also make important contributions with one relevant article each.

Meanwhile, in the Dimensions database on research sources used in the field of social network security. The table presented in the article displays the number of articles originating from each source. The results of the analysis show that several sources have a significant contribution to social network security research. The most prominent primary sources are "CYBERSECURITY EDUCATION SCIENCE TECHNIQUE," "IEEE ACCESS," "JOURNAL OF COMPUTATIONAL BIOLOGY," and "THE JOURNAL OF SUPERCOMPUTING," each of which has 2 relevant articles. This shows that these sources have an important role in the development of knowledge in the field of social network security.

In addition, several other sources also made important contributions by contributing 1 relevant article each. These sources include "ACM SIGKDD EXPLORATIONS NEWSLETTER," "ANNALS OF THE ALEXANDRU IOAN CUZA UNIVERSITY - ECONOMICS," "APPLIED SCIENCES," "ASIAN JOURNAL OF AGRICULTURAL EXTENSION ECONOMICS & SOCIOLOGY," "COLLECTION INFORMATION TECHNOLOGY AND SECURITY," and "COLLECTION OF SCIENTIFIC WORKS OF THE MILITARY INSTITUTE OF KYIV NATIONAL TARAS SHEVCHENKO UNIVERSITY." Although the number of articles originating from these sources is only one, they still make important contributions to the development of knowledge in the field of social network security. Overall, it can be concluded that "CYBERSECURITY EDUCATION SCIENCE TECHNIQUE," "IEEE ACCESS," "JOURNAL OF COMPUTATIONAL BIOLOGY," and "THE JOURNAL OF SUPERCOMPUTING" are the most influential primary sources with 2 relevant articles each in social network security research. Other sources also make important contributions with 1 relevant article each.

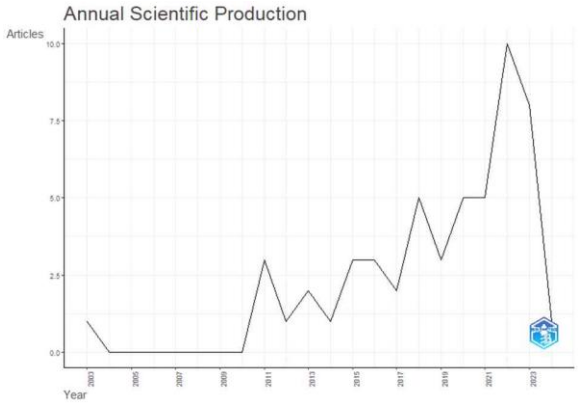

Figure 4. Annual Scientific Production in Database Dimensions

Through the bibliometric analysis of the table above obtained from the Dimensions database which displays the number of articles related to social network security based on the year of publication, several interesting findings can be found. The research trend in social network security has developed significantly during the observed time period. At the beginning of the period, from 2003 to 2008, no articles were published in this field. However, from 2009 to 2011, there was a sharp increase with the emergence of 3 articles in 2011. After that, the number of articles continued to fluctuate but with a general trend showing an increase. In 2018 and 2021, the highest number of articles was recorded with 5 articles each. 2022 was the peak of the increase with 10 articles, while 2023 was still quite high with 8 articles. However, in 2024, the number of articles decreased again to 1 article.

The conclusion that can be drawn from this analysis is that the research trend in social network security has experienced rapid growth during the observed time period. In recent years, there has been a significant increase in the number of articles published, indicating an increasing interest and focus in this field. Meanwhile, a bibliometric analysis of the number of articles related to social network security obtained from the Scopus database based on the year of publication, can reveal some interesting findings. The research trend in social network security has varied over time. At the beginning of the observed period, namely from 2009 to 2011, there were no articles published in this field. However, from 2012 to 2019, there was a significant increase in the number of articles published, peaking in 2019 with 5 articles. After 2019, there was a slight decrease in the number of articles published in 2020, only 1 article, before increasing again in 2021 with 3 articles. In 2022 and 2023, the number of articles

remained relatively stable with 3 and 2 articles, respectively. It can be concluded that social network security has become an increasingly important research topic over the past decade. Although there are fluctuations in the number of articles published each year, the general trend shows increasing interest and focus in social network security research.

Figure 5. Word Cloud in Database Scopus
Sumber: Biblioshiny, 2023

In the bibliometric analysis of the table above obtained from the Scopus database showing the frequency of terms frequently used in social network security research, there are several interesting findings. Social network security research covers a variety of topics relevant to security and privacy. The existence of diverse social phenomena can produce innovation in the research topics to be observed. The most frequently appearing term is "social networking (online)" with a frequency of 14, followed by "network security" with a frequency of 13. This shows that social network security research often focuses on the security aspect in the context of online social networks. Furthermore, the term "security and privacy" appears 5 times, indicating the importance of the security and privacy aspects in this study. The term "learning systems" appears 4 times, indicating a relationship between social network security and learning systems. Several other terms that appear with lower frequencies include "data privacy," "human computer interaction," "social network," "social sciences computing," and others.

This shows the variety of topics and approaches in social network security research. From this analysis, it can be concluded that social network security research covers various aspects such as security, privacy, human-computer interaction, and system learning. The focus on online social networking security and data protection is also evident through the high frequency of terms such as “social networking (online)” and “network security.”

CONCLUSION

Based on the analysis of social network security research trends using the Scopus and Dimensions databases, there are several important findings that can be described. First, interest in this topic shows quite good consistency, with an average annual growth rate of 5.08% in Scopus, while data from Dimensions shows a stable pattern even though it does not record an annual growth rate. The number of articles and citations per document from both databases shows that the literature on social network security has a significant impact in its field. Second, based on the Scopus database, Zhang Z stands out as the main contributor with 3 articles, contributing 0.95 to the fractionalized article comparison, while based on the dimensions database, Li X and Zhang Z each contributed 3 articles, with fractionalized values of 0.642857143 and 0.95. Third, this study also has contributions from principal researchers, such as Zhang Z in the Scopus database and Li X and Zhang Z in the Dimensions database, which have a great impact on both databases. Fourth, based on the Scopus database, “COMPUTATIONAL SOCIAL NETWORKS: SECURITY AND PRIVACY” is the main contributor, while based on the

dimensions database, the most prominent main source is "CYBERSECURITY EDUCATION SCIENCE TECHNIQUE". Fifth, in the dimensions data in 2018 and 2021, the highest number of articles was recorded with 5 articles each, while in the Scopus database it peaked in 2019 with 5 articles. Sixth, keyword analysis reveals a variety of topics of concern, such as "social networking (online)" which is the most dominant term, followed by "network security" and other terms such as "security and privacy" and "learning systems," which shows a complex and broad scope of research. Overall, these findings provide in-depth insights into the evolution, characteristics, and contributions of social network security research, which can be used to identify future research directions and provide guidance for researchers and practitioners in this field.

SUGGESTION

Based on the bibliometric analysis, suggestions for the development of social network security research include increasing national and international collaboration, exploring under-explored topics such as legal aspects and new technologies, and using more diverse analysis methods. Utilizing data from various databases and focusing on practical solutions to improve user security and privacy are also important. In addition, studies to raise public awareness and understand the influence of social network security on social dynamics are expected to enrich research in this field. These steps are expected to contribute to scientific literature and society.

THANK YOU-NOTE

This research can be carried out well thanks to the assistance of various parties.

REFERENCES

Adriansyah, Rizky Adin, dan Aldof Faris Anugrah. 2024. "Analisis Bibliometrik Keamanan Perusahaan Penjualan Online Untuk Terjadinya Kejahatan Siber." Jurnal Sistem Informasi Dan Informatika (Simika) 7(2):113–20. doi: 10.47080/simika.v7i2.3185.

Andi Putra, Yusuf, dan Tata Sutabri. 2023. "Analisis Penyadapan Pada Aplikasi Whatsapp Dengan Menggunakan Metode Sinkronisasi Data." Blankika: Jurnal Multidisiplin 1(2):131–40. doi: 10.57096/blantika.v2i1.8.

Edwards, Keith. 2015. "Mengkaji Kesadaran Keamanan, Privasi Informasi, dan Perilaku Keamanan Pengguna Komputer Rumahan." Disertasi: Sekolah Tinggi Teknik dan Komputasi Universitas Nova Southeastern.

Givan, Bryan, Rizky Amalia, Abdurrachman, Imelda Sari, Slamet Heri Winarno, dan Arman Syah Putra. 2021. "Efektif Penggunaan E-Money Melalui Belanja Online Di E-Commerce." Jurnal Internasional Penelitian Pendidikan & Ilmu Sosial (IJERSC) 2(6):1692–97.

Gunawan, Hendro. 2021. "Pengukuran Kesadaran Keamanan Informasi Dan Privasi Dalam Media Sosial." Jurnal Muara Sains, Teknologi, Kedokteran, Dan Ilmu Kesehatan 5(1):1–8.

Hakiki, Dikhy, Hamida Syari Harahap, dan Ari Sulistyanto. 2024. "Analisis Bibilometrik Perkembangan Strategi Komunikasi Di Media Sosial Pada Instansi Pemerintahan Dalam Keamanan Siber." Jurnal Keamanan Nasional X(1):135–48.

Hakim, Lukmanul. 2020. "Analisis Bibliometrik Penelitian Inkubator Bisnis Pada Publikasi Ilmiah Terindeks Scopus." Pengadaan: Jurnal Ilmiah Manajemen 8(2):176–89.

Hartawan, Muhammad Syarif, Arman Syah Putra, dan Ayub Muktiono. 2020. "Konsep Smart City untuk Integrated Citizen Information Smart Card atau ICISC di DKI Jakarta." Jurnal

Internasional Sains, Teknologi & Manajemen 1(4):364–70. doi: 10.46729/ijstm.v1i4.76.

Khairifa, F., Kholil, S., Syam, AM & Mujtahid, NM. (2025). Mitigating food waste and household waste management: The potential for redistributing surplus food in the policy communication of Medan City government. IOP Conference Series: Earth and Environmental Science 1445 (1), 012047

López, Alejandro Carlos Campina, Antonio Alejandro Lorca Marín, dan Ma Ángeles de las Heras Pérez. 2024. "Indagación, Modelización y Pensamiento Computacional: Un Análisis Bibliométrico Con El Uso de Bibliometrix a Través de Biblioshiny." Revista Eureka Sobre Enseñanza dan Pengungkapan Las Ciencias 21(1). doi: 10.25267/Pdt.

Lubis, Rizky Reza. 2017. "Potensi Pengguna Internet Indonesia Dalam Penanggulangan Radikalisasi Siber." Jurnal Pertahanan & Bela Negara 7(2):19–34. doi: 10.33172/jpbh.v7i2.177.

Mafriza, A., Sayekti, R., & Syam, A. M. (2022). Strategy for implementation of the senayan library management system (SLIMS) automation system at SMK Negeri 1 Stabat. International Journal of Cultural and Social Science, 3(2), 300-309

Manurung, AK., Sayekti, R & Syam, AM. (2024). Analisis Pemanfaatan Jurnal Elektronik Sebagai Sumber Belajar Oleh Mahasiswa Universitas Muhammadiyah Sumatera Utara. Jurnal Ilmiah Wahana Pendidikan 10 (17), 178-186

Nasution, Mahyuddin K. M. 2018. Keamanan Informasi.

Oehri, Caroline, dan Stephanie Teufel. 2012. "Budaya Keamanan Media Sosial-Dimensi Manusia dalam Manajemen Media Sosial." Dalam Keamanan Informasi untuk Afrika Selatan 4(1):1–5.

Permatasari, Riyandini Devi Intan, Anisa Rahmah, Fithrotuz Zuhroh, Tsabita Rizqiina Putri Hidayat, dan Nur Aini Rakhmawati. 2023. "Analisis Bibliometrik Mengenai Serangan Phishing Pada Media Sosial Menggunakan Vosviewer." Jurnal Ilmiah Informatika Komputer 28(3):230–40. doi: 10.35760/ik.2023.v28i3.9514.

Peter, M. Chandrakumar, M. Sharmila Begum, dan A. Rahmat Tak Bernoda. 2022. "Analisis Masalah Keamanan Dan Privasi Di Jejaring Sosial." Jurnal Hasil Negatif Farmasi 13(9):4333–50. doi: 10.47750/pnr.2022.13.S09.541.

Pratiwi, R. A., Ritonga, S., & Syam, A. M. (2024). Strategi Perpustakaan Dalam Meningkatkan Aksesibilitas Layanan Kepada Anak Tunanetra Di Sekolah Dasar Luar Biasa Negeri (SDLBN) 117709 Kampung Baru Labuhan Batu. CENDEKIA: Jurnal Ilmu Sosial, Bahasa dan Pendidikan, 4(1), 272-288.

Rahmah, S., Sayekti, R., Syam, A.M. (2024). Pemanfaatan Jurnal Terakreditasi Nasional Dalam Penulisan Tugas Akhir Oleh Mahasiswa UIN Sumatera Utara. Madani: Jurnal Ilmiah Multidisiplin 2 (8), 368-376.

Ritonga, A. R., Education, I. R., Zein, A., Syam, A. M., & Ohorella, N. R. (2023). Misconceptions of Jihad: A Constructivist Review of the Meaning of Struggle in Islam in the Modern Era: Analysis of the verses al-Amwaal wa al-Nafs.

Rusdi, M., Sebayang, V.A., Kholil, S., & Syam, A.M. (2024). Islam and the Ethics of War: Deconstructing Jihad through the Principle of Humanism in Theological Discourses

Royani, Yupi, dan Dukariana Idhani. 2018. "Analisis Bibliometrik Jurnal Penelitian Kelautan di Indonesia." Media Pustakawan 25(4):63–68.

Ryandono, Muhammad Nafik Hadi, Imron Mawardi, Lina Nugraha Rani, Tika Widiastuti, Ririn Tri Ratnasari, dan Akhmad Kusuma Wardhana. 2022. "Tren Topik Penelitian Terkait Daging Halal sebagai Komoditas antara Scopus dan Web of Science: Tinjauan Sistematis."

Penelitian F1000 11(1562):1562. doi: 10.12688/f1000research.123005.1.

Saputro, Agil. 2016. "Implementasi Sistem Keamanan Jaringan Dengan Menggunakan Intrusion Detection Sistem (IDS) Studi Kasus: Universitas Satya Negara Indonesia." Universitas Satya Negara Indonesia.

Saraan, M. I. K., Rambe, R. F. A. K., Syam, A. M., Suhendar, A., Dalimunthe, M. A., & Sinaga, R. P. K. (2024, May). The application of fertilizer subsidies in the context of coffee plantations in Pollung Sub-District, Humbang Hasundutan District, North Sumatra Province. In IOP Conference Series: Earth and Environmental Science (Vol. 1352, No. 1, p. 012012). IOP Publishing.

Setianingsih, Frida Eka, dan Fauzan Aziz. 2022. "Pengaruh Media Sosial Instagram Terhadap Minat Beli Online Di Shopee." Jurnal Administrasi Bisnis 11(2):107–16.

Siregar, N.Z & Syam, A.M. (2024). The Influence of Digital Library Service Quality On Student Satisfaction. PERSPEKTIF: Journal of Social and Library Science 2 (2), 40-48.

Wedhatama, Odrifaza Girindra, Syarifa Hanoum, dan Prahardika Prihananto. 2021. "Studi Bibliometrik Pada Penelitian Manajemen Sumber Daya Manusia Di Bidang Perawatan Kesehatan (Healthcare)." Jurnal Sains Dan Seni ITS 10(1). doi: 10.12962/j23373520.v10i1.60391.

Yani, E.A & Syam, A.M. (2024). Implementasi Personal Information Management (PIM) Mahasiswa Tingkat Akhir Pada Program Studi Ilmu Perpustakaan. Reslaj: Religion Education Social Laa Roiba Journal 6 (8), 4454–4467

Yel, Mesra Betty, dan Mahyuddin K.M. Nasution. 2022. "Keamanan Informasi Data Pribadi Pada Media Sosial." Jurnal Informatika Kaputama 6(1):92–101.