Borneo International Journal eISSN 2636-9826; Vol. 6 (1); 2023; 80-86
Published by *Majmuah Enterprise*
www.majmuah.com

Cybersecurity Threat in Social Media: A Bibliometric Analysis

NUR A'FYFAH ZAIMY[1], MOHAMED ALI SAIP[2] and MAZNI FIKRI[3]

[1,2]*School of Computing, College of Arts and Sciences, Universiti Utara Malaysia (UUM), 06010 Changlun, Kedah, MALAYSIA*
[3]*Business Management Unit, Kedah Matriculation College, 06010 Changlun, Kedah, MALAYSIA*
Email: afyfahzaimy@gmail.com| Tel: +60145247803 |

Received: March 08, 2023
Accepted: March 11, 2023
Online Published: March 13, 2023

Abstract

Social media has become an integral part of modern-day communication and a ubiquitous source of information. However, its rapid adoption has also increased cybersecurity threats, making it crucial to understand the state of research on this topic. This bibliometric analysis aims to examine the state of research on cybersecurity threats in social media by answering two research questions. First, the study identifies the most cited research articles in this area using data retrieved from Scopus between 2011 and 2023. Second, the analysis explores the overall trend of publications on cybersecurity threats in social media over time. The analysis reveals the most influential research studies in the field and demonstrates the fluctuating trend in publications on cybersecurity threats in social media over the last decade. The findings can be useful for researchers and practitioners to track research trends over time. Also, these findings can be used to identify highly cited research papers.

Keywords: cybersecurity threats; social media; bibliometric analysis

1.0 Introduction

Billion people use social media to maintain personal and professional relationships, disseminate news and information, and enjoy entertainment (Asur & Huberman, 2010). People increasingly use social media daily to share information and express their views (Tanha, 2020). The many different functions social media sites serve today include social networking, advertising, information gathering, entertainment, and political engagement. Social media platforms have fostered new forms of networking and communication, enabling people to connect with others around the globe (Sawyer & Chen, 2012) and develop connections based on common goals, experiences, and beliefs. Businesses and marketers have also grown to rely heavily on social media (Appel et al., 2020) as a medium for customer engagement, brand visibility, and revenue generation. These platforms include Facebook, Twitter, and Instagram. However, social media has also raised concerns about privacy and security and spreading misinformation (Luo et al., 2021). Social media platforms collect information about their users. According to Ullah et al. (2022), the gathered information can be used for targeted advertising but also raises privacy and security concerns.

Ozkaya (n.d.) has claimed that social media has become a breeding ground for cybersecurity threats in today's world. Cybercriminals and threat actors can find various potential victims among the billions of people who use social media daily. Phishing, malware, data breaches, and identity theft are cybersecurity dangers (Jang-Jaccard & Nepal, 2014) affecting social networking sites. One of the biggest cybersecurity threats in social media is phishing attacks, where users are lured into providing their personal information or login credentials by clicking on malicious links or downloading infected attachments (Alkhalil et al., 2021). Identity theft and financial fraud are only two of the dire outcomes that can result from these attacks. Another significant issue in social media is malware infestations (Nakerekanti & Narasimha, 2019), when attackers employ social engineering strategies to deceive users into downloading or installing malicious software. The result might be the theft of private information or hackers' complete takeover of a system. Moreover, attackers can get unauthorized access to user data via data breaches on social networking platforms (Vemprala & Dietrich, 2019), including usernames, passwords, and other sensitive information.

These data breaches can result in the theft of large amounts of personal data, which can be used for identity theft or sold on the dark web. Hence, social media platforms are vulnerable to various other types of cyberattacks. As social media continues to evolve and new platforms emerge, cybercriminals and threat actors will likely continue to find new ways to exploit vulnerabilities in these platforms. Bibliometric analysis is a structured method of studying previously published publications to comprehend the development of literature (Shukla & Gochhait, 2020). Metrics and visualizations assist researchers in understanding developments in a particular field of study, where to go for reliable sources of information, and what is new in the study area (Shukla & Gochhait, 2020). There is a lack of bibliometric

studies on cybersecurity threat literature, especially in the realm of social media. A bibliometric trend study aims to better comprehend this broad topic's current state of affairs by analyzing the existing literature. Thus, this article will list the most often referenced studies on cybersecurity threats in social media. This study will also explain the overall pattern of publications in this area throughout time. Below is a list of the research questions that were made for the scope of this study to make sure that the discussion stays within those bounds.

RQ1: What are the most cited research articles in the field of cybersecurity threats in social media?

RQ2: What is the overall trend of publication in this field over time?

2.0 Methodology

For this analysis, data was culled from the Scopus database. According to Schotten et al. (2017), Scopus, one of the largest abstract and citation databases of peer-reviewed literature, was constructed by Elsevier starting in 2002 and launched in 2004. Since then, it has added many articles before its start date (Thelwall & Sud, 2022). Scopus is utilized to search for relevant documents with the topic of "Cybersecurity threats in social media" as the primary emphasis. These keywords were searched in titles and abstracts as input to find the most pertinent articles about cybersecurity threats in social media. All the retrieved works were sorted by publication year, from the earliest pieces in 2011 to the most recent ones in 2023. Following were the settings for the query string:

TITLE-ABS-KEY (cybersecurity AND threats AND in AND social AND media) AND PUBYEAR > 2010 AND PUBYEAR < 2024 AND (LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "cr") OR LIMIT-TO (DOCTYPE , "re")) AND (LIMIT-TO (LANGUAGE , "English"))

The search yielded 157 documents matching the criteria provided. Then, the 157 papers were analyzed through the 'Analyze results' feature in Scopus. A bibliometric analysis was explicitly carried out to determine the most frequently referenced research in this area and its overall publication pattern over time. The first step was to conduct a citation analysis to determine the ten most influential articles in the field. Finally, a frequency analysis was conducted to determine the overall trend of published field studies.

3.0 Results

3.1 Most Productive and Highly Cited Articles

Among all 157 papers obtained, Table 1 summarizes the top ten publications with the highest number of citations based on the keywords of cybersecurity threats in social media. Columns in Table 1 consist of 'Author,' 'Title,' and 'Year' of the paper that has been published, 'ToD' means the type of documents, and 'TC' is the total of citations. The number of the highest citation found in Scopus based on the related keywords is the paper written by Jang-Jaccard and Nepal, with 380 citations. The type of document Jang-Jaccard and Nepal wrote is a conference paper in 2014. Using developing technologies, including social media, cloud computing, mobile applications, and critical infrastructure, Jang-Jaccard and Nepal (2014) examined novel cyber threat patterns and provided speculative insights on potential future study areas. Next is the paper by Westerlund (2019), with 183 citations from 2011 to 2023. The study by Westerlund (2019) examines deep fakes and offers market prospects to cybersecurity and AI entrepreneurs in the fight against medium forgeries and false news.

Research by Sun et al. (2019) is the third most cited paper in the journal. It examines the emergence of cybersecurity incidents by evaluating recent sample works published during the dominant period. It also discusses problems and potential future paths in the area. Moreover, a paper by Mittal et al. (2016) has received 112 citations, while research by Orabi et al. (2020) has received 61 citations. In addition, both conference papers written by Caramancion (2020) and Le et al. (2019) have the same citation number, with 19 from 2011 to 2023. All ten of these highly-cited studies discuss or conduct research into some aspect of the growing field of cybersecurity threats. Nine of the studies also incorporated the ever-changing medium of social media and its security into their research. In fact, only one paper (Mackey and Liang, 2013) focused solely on cyber threats without mentioning social media at all. In light of this, anyone interested in researching cybersecurity threats in the social media sphere should start with these articles.

Table 1: Top 10 Most Cited Papers

Author	Title	Year	ToD	TC
Jang-Jaccard, J., Nepal, S.	A Survey of Emerging Threats in Cybersecurity	2014	Conference Paper	380
Westerlund, M.	The Emergence of Deepfake Technology: A Review	2019	Review	183
Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L.Y., Xiang, Y.	Data-Driven Cybersecurity Incident Prediction: A Survey	2019	Article	156
Mittal, S., Das, P.K., Mulwad, V., Joshi, A., Finin, T.	CyberTwitter: Using Twitter to Generate Alerts For Cybersecurity Threats and Vulnerabilities	2016	Conference Paper	112
Orabi, M., Mouheb, D., Al Aghbari, Z., Kamel, I.	Detection of Bots in Social Media: A Systematic Review	2020	Article	61
Linkov, I., Anklam, E., Collier, Z.A., DiMase, D., Renn, O.	Risk-Based Standards: Integrating Top-Down and Bottom-Up Approaches	2014	Article	55
DIonisio, N., Alves, F., Ferreira, P.M., Bessani, A.	Cyberthreat Detection from Twitter using Deep Neural Networks	2019	Conference Paper	37
Mackey, T.K., Liang, B.A.	Pharmaceutical Digital Marketing and Governance: Illicit Actors and Challenges to Global Patient Safety and Public Health	2013	Article	32
Caramancion, K.M.	An Exploration of Disinformation As a Cybersecurity Threat	2020	Conference Paper	19
Le, B.-D.,	Gathering Cyber Threat Intelligence From Twitter Using Novelty	2019	Conference Paper	19

Wang, G., Nasim, M., Babar, M.A.	Classification

3.2 Trend of Publication Frequency

The number of publications from 2011 to 2023 indicates the field's research output. Figure 1 displays the publication trend of the 157 papers by year. The yearly publication trend percentage and its cumulative percentage are both summarized in Table 2. Trends in research output related to keywords; 'cybersecurity threats,' 'in,' and 'social media' are reflected in this publication distribution by year. Two publications were published in 2011; however, that number fell to zero in 2012 in the related area. In 2013, there were three articles about cybersecurity and associated threats, and this pattern persisted through 2014. A few studies, like that by Kelic et al., were released in 2013 to assess the economic effects of cybersecurity risks and provide guidance in selecting appropriate cybersecurity policies. There was a rise of four and five articles in 2015 and 2016 on cybersecurity issues and social media research, demonstrating how seriously people take the security risks posed by social media. The number of papers published has increased since 2013, albeit at a slower rate in both 2017 and 2020. In 2021, when there are 37 publications, the number of publications is at its peak. The number of articles is anticipated to continue to rise in the coming year. It is due to cybersecurity risks being one of the active study fields, growing social media platform usage globally, and concerns about its security, despite decreasing publication in 2022 and 2023.

Table 2: Trend of Yearly Publications

Year	Number of Publications	Percentage (N = 157)	Cumulative Percentage
2011	2	1.27	1.27
2012	0	0	1.27
2013	3	1.91	3.18
2014	3	1.91	5.09
2015	4	2.55	7.64
2016	5	3.18	10.82
2017	1	0.64	11.64
2018	9	5.73	17.19
2019	30	19.11	36.3
2020	27	17.20	53.5
2021	37	23.57	77.07
2022	31	19.75	96.82
2023	5	3.18	100.00

Total	**157**	**100.00**

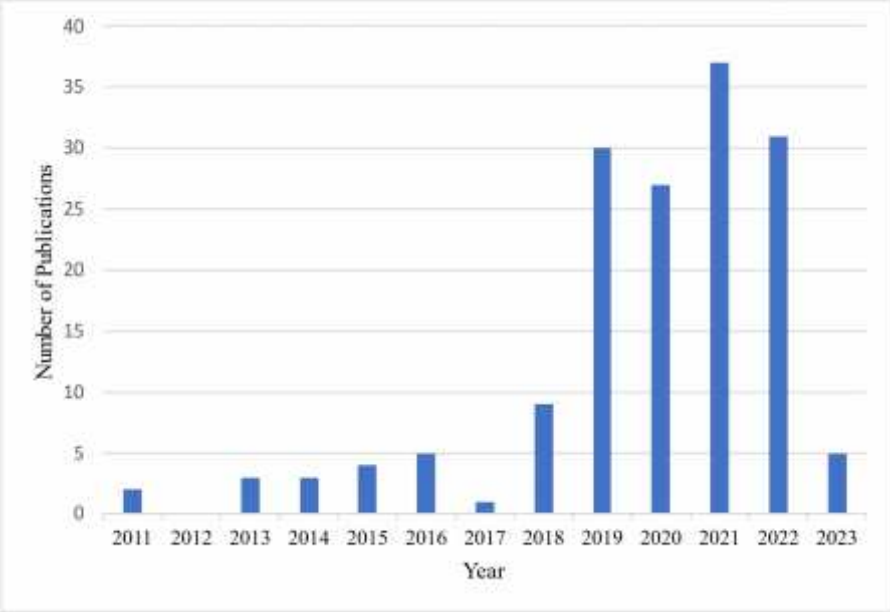

Figure 1: Overall Trend of Publications Yearly

4.0 Discussion

Scopus bibliometric analysis of cybersecurity threats in social media sheds light on the most-cited research publications and the general publishing trend in this area over time. The findings of the study have important implications for the field of cybersecurity threats in social media and can guide future research efforts. The study found that the most cited research articles in the field of cybersecurity threats in social media focused on developing technologies such as social media with its novel security threat patterns. They also provided theoretical insights on potential future study areas. According to the results, researchers have paid much attention to these issues, indicating they are crucial to the area. Future researchers might use the most frequently cited publications as a jumping-off point to develop and broaden their knowledge of these topics.

The results of an analysis of the publication trend in the field of cybersecurity threats in social media through time show the number of publications has fluctuated over the years, with 2021 seeing the most, followed by 2022 seeing to be dropped, for reasons that are not entirely clear. This tendency, however, signals that the study of cybersecurity threats in social media will swiftly evolve and become increasingly significant, given the perpetual security vulnerabilities in every social media platform. The bibliometric analysis used in this study also has several strengths, such as the ability to search the literature in the field of cybersecurity threats in social media in a comprehensive manner thanks to the incorporation of Scopus and the provision of a reliable and accurate analysis of the literature. Nevertheless, the bibliometric methods employed in this analysis have caveats, such as their utter reliance on the thoroughness and precision of Scopus's metadata.

Suggestions for future research in the field of cybersecurity threats in social media include a focus on emerging social media platforms and their unique security challenges, as well as the effectiveness of current security measures in protecting users' data and privacy. Additionally, interdisciplinary research that examines the social, cultural, and economic factors that influence cybersecurity threats in social media can provide a more comprehensive understanding of the complex nature of these threats. Therefore, the bibliometric analysis conducted using Scopus has provided valuable insights into cybersecurity threats in social media. The study findings have important implications for the field and can guide future research efforts. Overall, this study provides a foundation for future research on cybersecurity threats in social media.

5.0 Conclusions

The bibliometric analysis provides an overview of the existing literature on cybersecurity threats in social media. The research areas and methods provide insights into the most cited papers and overall trend publications from 2011 to 2023. However, several research gaps exist, which require attention from researchers. Future research should focus on emerging social media platforms, their unique security challenges, and the effectiveness of current security measures in protecting users' data and privacy. Moreover, interdisciplinary research can provide a more comprehensive understanding of the complex nature of cybersecurity threats in social media. Ultimately, this analysis can contribute to developing effective strategies to mitigate cybersecurity risks in social media platforms.

Acknowledgements

The authors thank all School of Computing and Kedah Matriculation College members who invented this study. This study was conducted for the Cybersecurity in Social Media Project.

References

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*(March), 1–23. https://doi.org/10.3389/fcomp.2021.563060

Appel, G., Grawel, L., Hadi, R., & Stephen, A. T. (2020). The Future of Social Media in Marketing. *Journal of the Academy of Marketing Science*, *48*, 79–95. https://doi.org/10.1007/s11747-019-00695-1

Asur, S., & Huberman, A. B. (2010). Predicting the Future With Social Media. *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology*, 492–499. https://doi.org/10.1109/WI-IAT.2010.63

Caramancion, K. M. (2020). No An Exploration of Disinformation As a Cybersecurity Threat. *Proceedings - 3rd International Conference on Information and Computer Technologies, ICICT 2020*, 440–444. https://doi.org/10.1109/ICICT50521.2020.00076

Jang-Jaccard, J., & Nepal, S. (2014). A Survey of Emerging Threats in Cybersecurity. *Journal of Computer and System Sciences*, *80*(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Kelic, A., Collier, Z. A., Brown, C., Beyeler, W. E., Outkin, A. V, Vargas, V. N., Ehlen, M. A., Judson, C., Zaidi, A., Leung, B., & Linkov, I. (2013). Decision Framework for Evaluating the Macroeconomic Risks and Policy Impacts of Cyber Attacks. *Environment Systems and Decisions*, *33*(4), 544–560. https://doi.org/10.1007/s10669-013-9479-9

Le, B.-D., Wang, G., Nasim, M., & Babar, M. A. (2019). Gathering Cyber Threat Intelligence From Twitter Using Novelty Classification. *Proceedings - 2019 International Conference on Cyberworlds, CW 2019*, 316–323. https://doi.org/10.1109/CW.2019.00058

Luo, H., Cai, M., & Cui, Y. (2021). Spread of Misinformation in Social Networks: Analysis Based on Weibo Tweets. *Security and Communication Networks*, 23. https://doi.org/10.1155/2021/7999760

Mittal, S., Das, P. K., Mulwad, V., Joshi, A., & Finin, T. (2016). CyberTwitter: Using Twitter to Generate Alerts For Cybersecurity Threats and Vulnerabilities. *Proceedings of the 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2016*, 860–867. https://doi.org/10.1109/ASONAM.2016.7752338

Nakerekanti, M., & Narasimha, V. (2019). Analysis on Malware Issues in Online Social Networking Sites (SNS). *Conference: 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS)*, 335–338. https://doi.org/10.1109/ICACCS.2019.8728536

Orabi, M., Mouheb, D., Al Aghbari, Z., & Kamel, I. (2020). Detection of Bots in Social Media: A Systematic Review. *Information Processing and Management*, *57*(4). https://doi.org/10.1016/j.ipm.2020.102250

Ozkaya, E. (n.d.). *Cybersecurity Challenges in Social Media* [Charles Sturt University]. https://researchoutput.csu.edu.au/ws/portalfiles/portal/24720950/Erdal_Ozkaya_DIT_Theses_Cybersecurity_Challenges_in_Social_Media.pdf

Sawyer, R., & Chen, G. M. (2012). The Impact of Social Media on Intercultural Adaptation. *Intercultural Communication Studies*, *21*(2), 151–169.

Schotten, M., Aisati, M. el, Meester, W. J. N., Steiginga, S., & Ross, C. A. (2017). A Brief History of Scopus: The World's Largest Abstract and Citation Database of Scientific Literature. In *In Research Analytics*. Auerbach Publications. https://www.taylorfrancis.com/chapters/edit/10.1201/9781315155890-3/brief-history-scopus-world-largest-abstract-citation-database-scientific-literature-michiel-schotten-hamed-el-aisati-wim-meester-susanne-steiginga-cameron-ross

Shukla, G., & Gochhait, S. (2020). Cyber Security Trend Analysis using Web of Science: A Bibliometric Analysis. *European Journal of Molecular & Clinical Medicine*, *7*(6), 2567–2576.

https://ejmcm.com/article_4083_a8e8731dd5ab757b65ea243cb9af2a12.pdf

Sun, N., Zhang, J., Rimba, P., Gao, S., Zhang, L. Y., & Xiang, Y. (2019). Data-Driven Cybersecurity Incident Prediction: A Survey. *IEEE Communications Surveys and Tutorials*, *21*(2), 1744–1772. https://doi.org/10.1109/COMST.2018.2885561

Tanha, M. A. (2020). Exploring the Credibility and Self-Presentation of Insta Micro-Celebrities in Influencing the Purchasing Decisions of Bangladeshi Users. *SEARCH Journal of Media and Communication Research*, *12*(2), 1–20. https://www.researchgate.net/publication/343524327_Exploring_the_credibility_and_self-presentation_of_Insta_micro-celebrities_in_influencing_the_purchasing_decisions_of_Bangladeshi_users

Thelwall, M., & Sud, P. (2022). Scopus 1900–2020: Growth in Articles, Abstracts, Countries, Fields, and Journals. *Quantitative Science Studies*, *3*(1), 1–17. https://doi.org/10.1162/qss_a_00177

Ullah, I., Boreli, R., & Kanhere, S. S. (2022). Privacy in Targeted Advertising on Mobile Devices: A Survey. *International Journal of Information Security*. https://doi.org/10.1007/s10207-022-00655-x

Vemprala, N., & Dietrich, G. (2019). A Social Network Analysis (SNA) Study On Data Breach Concerns Over Social Media. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 7186–7193. https://core.ac.uk/download/pdf/211327978.pdf

Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review*, *9*(11), 39–52. https://doi.org/10.22215/TIMREVIEW/1282