Borneo International Journal eISSN 2636-9826; Vol. 6 (1); 2023; 96-102
Published by *Majmuah Enterprise*
www.majmuah.com

Trends in Cyber Security Threat Research on Social Media: A Bibliometric Analysis

NOR NAEMATUL SAADAH ISMAIL[1] and MOHAMED ALI SAIP[2]

[1]*Awang Had Salleh Graduate School, School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA*
[2]*School of Computing, Universiti Utara Malaysia (UUM), 06010 Sintok, Kedah, MALAYSIA*
Email: naematul@hotmail.com | Tel: +60133215425

Received: March 25, 2023
Accepted: March 28, 2023
Online Published: March 29, 2023

Abstract

With more than 4.9 billion active users on social media as of January 2022, cybersecurity is becoming an increasingly crucial issue. As a result, there has been an increase in cybercrime, including attacks on people and businesses. Users of social media are subject to social and technical threats such as hacking, identity theft, and data leakage. To address these issues and defend against social engineering attacks, user education and increased cybersecurity threat awareness are crucial. Unfortunately, bibliometric analysis of cybersecurity threat literature is lacking, particularly when it comes to social media. This research intends to fill this vacuum by performing a bibliometric trend analysis of the literature that already exists on cybersecurity vulnerabilities in social media, with an emphasis on finding the most frequently cited papers and examining the chronological publishing history. This study intends to provide insight into the current state of this crucial topic and provide direction for further work in this area.

Keywords: cybersecurity threats; social media; social media threats; bibliometric analysis

1. Introduction

Cyber security can be defined as a technique for preventing unauthorized access to people's and organizations' assets. Social media platforms let individuals interact with each other around the worldwide. People and organizations use these websites for a wide range of purposes, like socializing, seeking for employment, extending their businesses, and sharing opinions and ideas (Hameed & Rahman, 2017). According to the latest data from Statista, as of January 2022, there were 4.9 billion active social media users worldwide as currently social networking is amongst the most popular activities that can be performed digitally. The tremendous numbers of social media's growth are driven the number of mobile devices globally increased. Usually, social media users spent their time approximately 144 minutes per day. Market leader Facebook, which currently has about 2.7 billion monthly active users, became the initial social network to exceed one billion registered accounts. This makes it the most popular social network globally. In June 2020, the top social media apps in the Apple App Store featured mobile messaging apps WhatsApp and Facebook Messenger, as well as the already mobile version of Facebook (Dixon, 2023). **Figure 1** below shows sixteen social media application with total numbers in millions as stated in Statista website. Currently, Facebook has the most user amongst the rest of social media application.

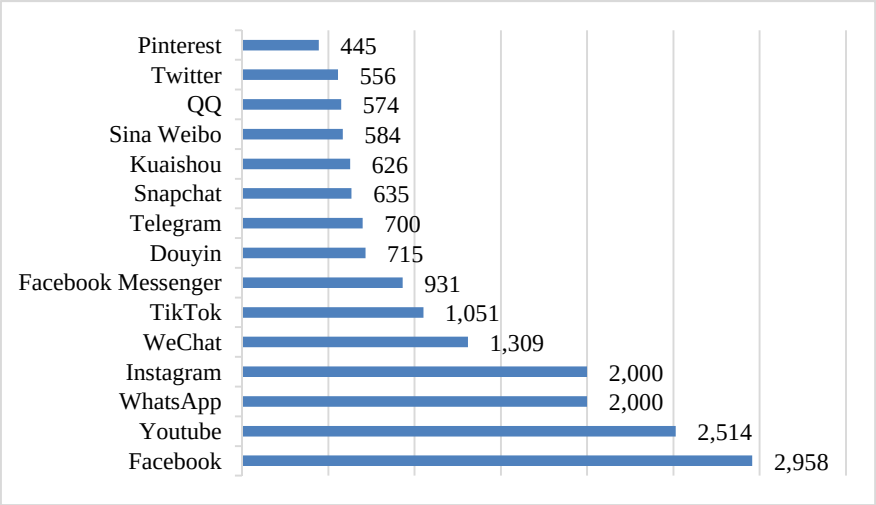

Figure 1: Numbers of active users in millions

As internet venues for information gathering and dissemination grew in popularity, so did the number of cybercrimes targeting groups of people as well as lone victims (Carley, 2020). The use of inadequate software, outdated security technologies, design faults, software bugs, readily accessible online hacking tools, a lack of public knowledge, high rates of financial return, are the causes of this enormous surge in cybercrime. The technical attackers develop more potent attack tools to investigate the target's vulnerabilities and then attack the victim (Rajasekharaiah, Dule, & Sudarshan, 2020).

As mentioned by (Herath, Khanna, & Ahmed, 2022) in their paper, social and technical are the risks for social media. While social risk can be escalate into another two level which are individual and professional. Some cyber threats that might occur to the individual are such loss of productivity, bullying, stalking, identity theft and personal information over exposed. Meanwhile, threats for professional person are such personal reputational damage, uneven personal branding, and data leakage. While the technical risks are such malicious software (malware), unlawful access to social media accounts, hacking, and disruption of services and password breaking. Besides that, some of malicious actions include using phoney accounts, cyberbullying, sexual assault, attacks using spear phishing and social engineering. Social networking sites can be particularly vulnerable to social engineering attacks due to the vast amount of circulating data and information. Training and increasing users' awareness of such threats is important for protecting against social engineering attacks (Albladi & Weir, 2020).

Bibliometric research on cybersecurity threat literature, particularly in the context of social media, is inadequate. To gain a better understanding of the current state of this vast subject, a bibliometric trend analysis is conducted by examining the available literature. The primary objective of this article is to identify the most frequently cited studies on cybersecurity threats in social media and to examine the general trend of publications in this field over time. The following list of research questions was developed to limit the scope of this study and ensure that the discussion remains within these parameters.

RQ1: What are the most frequently cited studies on cybersecurity threats in social media?

RQ2: What patterns can be observed in the publication history of these studies over time?

2. Methods

In this study, Scopus database has been used as our data collection sources. According to (Burnham, 2006), Scopus was founded by the Elsevier Co is an abstract and indexing database with full-text connections. The Hammerkop (Scopus umbretta) bird, which has reputedly outstanding navigational abilities, served as the model for the name Scopus. Back then in 2006, Scopus was developed two years before and working with 21 research institutions and more than 300 researchers and librarians during that time. The developers of Scopus claim that it is the "biggest single abstract and

indexing database ever developed" and that it indexes over 14,000 STM and social science volumes from 4000 publishers. However, Martin-Martin (2021) said that Scopus claims to cover over 76 million records.

The key focus of the search is "Cybersecurity threats in social media," and Scopus has been used to find pertinent materials. To select the most relevant articles about cybersecurity threats in social media, these keywords were entered into titles, abstracts and keywords of articles. From the earliest article, published in 2010, to the most recent ones, published in 2023, all of the retrieved works were organized by publication year. The query string's settings were as follows:

TITLE-ABS-KEY (cybersecurity AND threats AND in AND social AND media) AND PUBYEAR > 2009 AND (LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "English"))

The query returned 146 documents that suited with the provided criteria. Then, the 146 articles were analyzed by clicking the “Analyze results” features in the Scopus Journal. Then, the analyzed result has been exported in Microsoft Excel to perform the analysis. The first step involved performing a performance analysis to determine the research productivity in this field and the sources and types of documents that were retrieved. Second, citation analysis was carried out to determine the top ten most influential authors and articles. In order to establish the overall trend of published field research, a frequency analysis was lastly carried out.

3. Findings

Publication by Year

The volume of documents produced each year can be used to evaluate the productivity of this field of research. Figure 2 displays the distributions of the 146 documents based on the year of publication. The annual growth rate and cumulative growth rate are also summarized in Table 1. This publication's distribution by years shows the general direction of the research output in the field of social media cybersecurity concerns. Starting from 2011 until present year, which is 2023, the numbers of publications shows the ups and downs in frequency of publications. For the five recent years, shows more publications rather than the six early years starting from 2011. During that time, we believed that the number of social media users still low that’s why not many researchers find the importance of social media’s risk study.

The results of articles publication trend of the cybersecurity threats in social media shows the unstable trend that can be described as starting from the year 2011 started with one published article, since than it seems to be increases in two years excluded the year 2012 with no article get published. Meanwhile the trend seems to go down as only two articles in 2015 and increased by two in 2016. Then it went down a little bit before started to increase in 2018. The trend shows increasing pattern in 2018 and 2019. The most published was in the year 2021 with 35 publications in total. Nevertheless, it went down again in 2022 with 29 publications. It is possible to have the increasing trend by the end of this 2023.

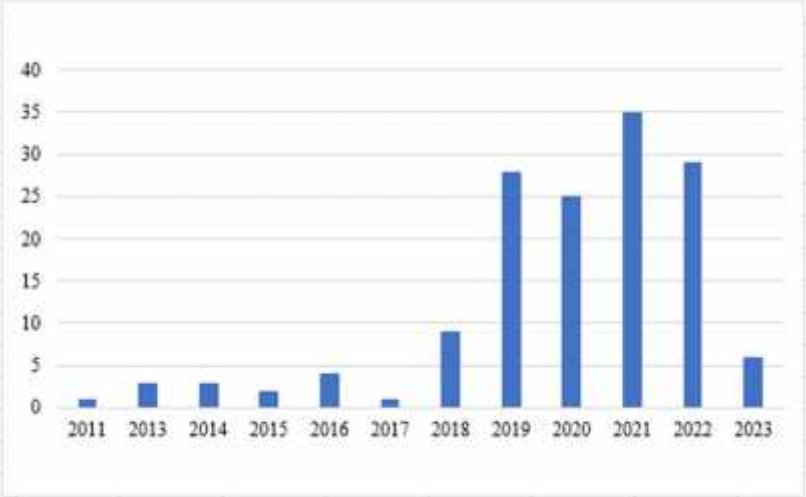

Figure 2: Numbers of publication per year

Table 1 : Yearly publications and cumulative percentage

Year	Number of Publications	Percentage (N=146)	Cumulative Percent
2011	1	0.685	0.685
2012	0	0	0.685
2013	3	2.055	2.740
2014	3	2.055	4.795
2015	2	1.370	6.164
2016	4	2.740	8.904
2017	1	0.685	9.589
2018	9	6.164	15.753
2019	28	19.178	34.932
2020	25	17.123	52.055
2021	35	23.973	76.027
2022	29	19.863	95.890
2023	6	4.110	100.000

Document Type and Sources

For the type of document, only two type has been limited to during the articles finding which are conference paper and article in journal. Thus, **Figure 3** shows the distribution of type of document analyzed. 60.27% are from article publish in journal while 39.73% are from conference paper. From analysis result , **Figure 3** also determined the sources type of the document are from journals and conferences.

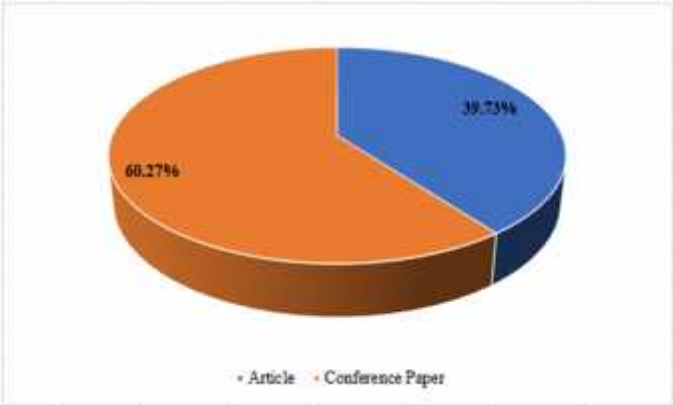

Figure 3 : Document types and sources

Impactful Articles

Table 2 displays the top 10 most highly cited article in cybersecurity threats in social media of the 146 documents retrieved. The table shows the authors' name, the articles' title, publication year, type of document (ToD) and the citations numbers that refers to TC. The most cited article belongs to Julian Jang-Jaccard and Surya Nepal which is 386 citations. In their conference paper, the survey was focused on information system aspects which are vulnerabilities in existing technologies and the potential threats in the future. The future threats such as social media, cloud computing, smartphone technology and critical infrastructure can possibly infect with malware (Jang-Jaccard & Nepal, 2014). Second highest citation is the article from journal that written by Nan Sun, Jun Zhang, Paul Rimba, Shang Gao, Leo Yu Zhang, and Yang Xiang with 158 citations. The survey performed by (Sun et al., 2019) using a set of data to examines the developing research by evaluating recent representative publications that published during the dominant period to predict cybersecurity incidents.

Meanwhile, the third most cited article with 113 citation is a conference paper from (Mittal, Das, Mulwad, Joshi, & Finin, 2016) suggest a tool that searches Twitter for cybersecurity information and analyses it to act as an open-source intelligence (OSINT) source. They analyze real-time information update from tweets. Then they encoded the obtained intelligence using the Semantic Web RDF and utilize SWRL rules to analyze the retrieved intelligence to provide alerts for security experts.

While article form (Orabi, Mouheb, Al Aghbari, & Kamel, 2020) received 64 citations. The authors provided a general review of social media bot assaults, existing detection techniques, and difficulties in the field by performing systematic review that was conducted using a pre-determined search strategy and included literature related to social media bot identification techniques. The next most cited article from (Linkov, Anklam, Collier, DiMase, & Renn, 2014) with 55 citations while article by (DIonisio, Alves, Ferreira, & Bessani, 2019) hit 38 citations that proposed a tool using deep neural networks to process cybersecurity threat from tweets collected from Twitter; a social media platform. Next article written by (Mackey & Liang, 2013) received 32 citations. Lastly, the least three cited articles that have been cited 19 times are written by (Hellmeier, 2016), (Caramancion, 2020), and (Le, Wang, Nasim, & Babar, 2019).

From these ten most cited article in cybersecurity threat in social media, nine of them are examined the security of social media, a dynamic medium. Only one study performed by Mackey and Liang's (2013), completely disregarded social media in favor of focusing on cyberthreats. Thus, these articles are a good place to start for anyone who wants to learn more about the cybersecurity concerns associated with social media.

Table 2: Top 10 most cited article

Author	Title	Year	ToD	TC
Jang-Jaccard J., Nepal S.	A survey of emerging threats in cybersecurity	2014	Conference Paper	386
Sun N., Zhang J., Rimba P., Gao S., Zhang L.Y., Xiang Y.	Data-Driven Cybersecurity Incident Prediction: A Survey	2019	Article	158
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	113
Orabi M., Mouheb D., Al Aghbari Z., Kamel I.	Detection of Bots in Social Media: A Systematic Review	2020	Article	64
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	38
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

Hellmeier S.	The Dictator's Digital Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes	2016	Article	19
Caramancion K.M.	An exploration of disinformation as a cybersecurity threat	2020	Conference Paper	19
Le B.-D., Wang G., Nasim M., Babar M.A.	Gathering cyber threat intelligence from twitter using novelty classification	2019	Conference Paper	19

4. Discussion

Social media is a platform for exchanging personal information and interacting with others, making it a prominent target for cybersecurity threats in recent years. The study's insights can guide future research efforts and have huge consequences for the field of cybersecurity concerns in social media. The survey discovered that social media, a new technology with novel security threat patterns, was the subject of the most-cited academic articles in the topic of cybersecurity threats in social media. They also gave theoretical explanations of potential new research fields. The findings show that researchers have given these topics a lot of thought, which suggests that they are important to the field. The bibliometric analysis employed in this study also has a few advantages, including the capacity to conduct a thorough literature search in cybersecurity threats in social media due to the inclusion of Scopus and the provision of a trustworthy and accurate analysis of the literature. However, there are limitations to the bibliometric techniques used in this analysis, such as their complete reliance on the accuracy and completeness of Scopus's metadata.

As cybersecurity threats in social media are constantly evolving, it is important to identify emerging threats and trends in the field and explore the intersection between social media and cybersecurity in new areas even though the trend seems to be ups and downs. This is maybe due to keywords that has been used while performed the article searched. Thus, in future, other researchers might be expanded this search scope, use multiple search keywords. Other than that, researchers might performed co-citation and bibliographic coupling analyses. These analyses can help to discover patterns of research collaboration and identify the most important books and authors in the social media are. Moreover, analyze keywords and abstracts, network visualization utilizing method and identifying emerging threats and trends can be performed.

5. Conclusion

This bibliometric analysis provides valuable insights into the current state of research on cybersecurity threats in social media. It highlights important research themes and suggests areas where further research is needed. Insights into the most popular papers and overall trend publications from 2009 to 2023 are provided by the research areas and methodologies. There are, however, several research gaps that need to be filled. Future studies should concentrate on new social media platforms, their distinct security issues, and the efficiency of existing security controls in safeguarding user data and privacy. Moreover, multidisciplinary research can offer a more thorough knowledge of the intricate nature of social media cybersecurity vulnerabilities. In the end, this study can aid in the creation of successful plans to reduce cybersecurity threats in social media platforms.

Acknowledgement

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of Cyber Security in Social Media Research Project. This work was supported by Universiti Utara Malaysia.

References

Albladi, S. M., & Weir, G. R. S. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1). https://doi.org/10.1186/s42400-020-00047-5

Burnham, J. F. (2006). Scopus database: A review. *Biomedical Digital Libraries*, *3*, 1–8. https://doi.org/10.1186/1742-5581-3-1

Caramancion, K. M. (2020). 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

Carley, K. M. (2020). Social cybersecurity: an emerging science. *Computational and Mathematical Organization Theory*, *26*(4), 365–381. https://doi.org/10.1007/s10588-020-09322-9

DIonisio, N., Alves, F., Ferreira, P. M., & Bessani, A. (2019). Cyberthreat Detection from Twitter using Deep Neural Networks. *Proceedings of the International Joint Conference on Neural Networks*, *2019-July*(July), 1–8. https://doi.org/10.1109/IJCNN.2019.8852475

Dixon, S. (2023). Number of social media users worldwide from 2017 to 2027. Retrieved March 15, 2023, from https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

Hameed, K., & Rahman, N. (2017). Today's social network sites: An analysis of emerging security risks and their counter measures. *International Conference on Communication Technologies, ComTech 2017*, 143–148. https://doi.org/10.1109/COMTECH.2017.8065764

Hellmeier, S. (2016). The Dictator's Digital Toolkit: Explaining Variation in Internet Filtering in Authoritarian Regimes. *Politics and Policy*, *44*(6), 1158–1191. https://doi.org/10.1111/polp.12189

Herath, T. B. G., Khanna, P., & Ahmed, M. (2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. *Journal of Cybersecurity and Privacy*, *2*(1), 1–18. https://doi.org/10.3390/jcp2010001

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

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

Linkov, I., Anklam, E., Collier, Z. A., DiMase, D., & Renn, O. (2014). Risk-based standards: Integrating top-down and bottom-up approaches. *Environment Systems and Decisions*, *34*(1), 134–137. https://doi.org/10.1007/s10669-014-9488-3

Mackey, T. K., & Liang, B. A. (2013). Pharmaceutical digital marketing and governance: Illicit actors and challenges to global patient safety and public health. *Globalization and Health*, *9*(1). https://doi.org/10.1186/1744-8603-9-45

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

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), 102250. https://doi.org/10.1016/j.ipm.2020.102250

Rajasekharaiah, K. M., Dule, C. S., & Sudarshan, E. (2020). Cyber Security Challenges and its Emerging Trends on Latest Technologies. *IOP Conference Series: Materials Science and Engineering*, *981*(2). https://doi.org/10.1088/1757-899X/981/2/022062

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