JOURNAL OF GOVERNANCE AND PUBLIC POLICY

Journal of Governance and Public Policy
ISSN: 2460-0164 (print), 2549-7669 (Online)
Vol 11, No 1 (2024): Page no: 14-32

Big Data and Security: A Review of Social Media Risks and Insights for Indonesia

Ahmad Harakan [1*], Abdillah [2], Try Gustaf Said [3], Mujizatullah [4], Simon Gray [5]
[1,2,3] Universitas Muhammadiyah Makassar, Indonesia
[4] National Research and Innovation Agency, Indonesia
[5] University of Waikato, New Zealand
Corresponding Author: ahmad.harakan@unismuh.ac.id

Article Info

Article History;
Received:
2022-12-04
Revised:
2023-06-30
Accepted:
2023-09-08

Abstract: This article explores the intricacies of big data and its relationship with security, with the aim of mitigating potential security threats arising from social media platforms. The subsequent aim entails generating optimal strategies to propose to governmental entities for enhancing their efficacy in addressing security concerns pertaining to social media and its intersection with security. The present study commences by conducting a comprehensive survey of existing literature pertaining to social media security concerns and corresponding strategies for mitigating these issues. After conducting a comprehensive investigation, several significant discoveries were made and subsequently presented to aid stakeholders in better mitigating social media security risks. Numerous nations exist wherein the dynamics of government practices lack a robust social media security policy, and they exhibit skepticism towards endeavors aimed at constructing an efficient plan to mitigate social media security concerns. This study provides an overview of the existing arguments found in the literature and presents recommendations aimed at mitigating concerns related to social media security and technology. The present study also draws upon a comprehensive body of literature to identify and condense practical lessons. Further investigation and scholarly examination are necessary to explore strategies and pragmatic perspectives aimed at mitigating the potential risks associated with social media for the Indonesian government.

Keywords: *Social Media; Big Data Security; Security; Risk Mitigation Technique; Risk Mitigation Technique*

DOI: https://doi.org/10.18196/jgpp.v11i1.17038

INTRODUCTION

Continuous advancements are having a significant impact on how information technology affects people's lives (Liu J. et al., 2018; Buhalis, D., & Law, R., 2008). The integration of internet elements has become prevalent in various facets of life, serving as a means to enhance productivity and efficiency (Liu J. et al., 2018; Buhalis, D., & Law, R., 2008). Even those without specialized knowledge in these fields are familiar with the terms "technology" and "the internet" (Liu J. et al., 2018; Buhalis, D., & Law, R., 2008). This phenomenon is predicated on the extensive proliferation of internet connectivity, rendering it highly accessible. The field of Internet communication has also witnessed significant technological advancements. According to Barolli and Xhafa (2010), digital networks, which refer to interconnected networks, are not limited to usage on conventional devices like personal computers and laptops that are connected to the

internet. Instead, they are also extensively employed on smartphone devices. Specifically, the current advancements in mobile technology have expanded its functionality beyond communication. Users can now access a wide range of interconnected applications on the internet through their mobile devices. These applications encompass various domains, such as fintech, online gaming, shopping, mapping, banking, video and music streaming, health monitoring, and even dating. The proliferation of these applications is facilitated by their integration with communication features and the creation of social media platforms (Fan Z. et al., 2010; Yi X. et al., 2014). Nevertheless, the utilization of cloud computing by governments can potentially affect security, particularly in relation to internet-based data storage, the involvement of third-party entities, and the absence of a well-established legal framework at both national and international levels (Abd Al Ghaffar, H.-t.N, 2020). One issue that arises is the presence of social media, which is categorized as a platform for disseminating information and facilitating communication among influential individuals and the establishment of novel community networks (Barolli, L., & Xhafa, F., 2010; Fan, Z. et al., 2010; Yi, X. et al., 2014).

According to We Are Social and Hootsuite data, there were 49.48 million internet users (82% of the population) in January 2020, 1.2 million more (+2.4%) than in January 2019. There were 35 million users at the start of 2020, a 6.4% growth year on year (García-Ceballos, S. et al., 2021; Kraut, A. et al., 2020). In Indonesia, there are 160 million social media users out of a population of 272 million. Here, it is proven that everyone uses social media to stay connected, and that number will increase every year (Simangunsong, E., 2021). Despite the various benefits of technological developments, especially on social media, which can keep us connected even with people who are quite far away, there will definitely still be disadvantages in the form of threats that can disturb the comfort of users and also abuse the use of this social media (Liu, J. et al., 2018; Buhalis, D., & Law, R., 2008; Barrolli, L., & Xhafa, F., 2010). The development of social media, which originally served to make it easier for users to carry out social interactions using technology via the internet, then changed the way information was previously disseminated, becoming information dissemination that could be received by many users using social media, such as social media Facebook, Instagram, Twitter, WhatsApp, and the other social media groups (Barolli, L., & Xhafa, F., 2010; Fan, Z. et al., 2010; Yi, X. et al., 2014).

Research in 2019 by the media company We Are Social, in collaboration with Hootsuite, released data on the development of the number of internet users in Indonesia, revealing faster increase in internet users, namely as many as 20% compared to the number in 2018, and the release stated that there were 150 million social media users in Indonesia (García-Ceballos, S. et al., 2021; Kraut, A. et al., 2020; Simangunsong, E., 2021). In the previous year, 2018, the online community was shocked by the news that 87 million personal data of Facebook users were leaked by Cambridge Analytica Firm; moreover, around one million stolen personal data came from Indonesia (Kenzler, J., 2020; Christopoulou, A., 2019). Also, the results of the Alvara Research Center survey (Ahdiat, A., 2022) uncovered that Generation Z who accessed the internet in the range of 7-10 hours/day reached 20.9%, while the Millennial Generation was 13.7% and Generation X was only 7.1%. The Generation Z respondents who used the internet 11-13 hours/day reached 5.1%. Meanwhile, the Millennial Generation was 3%, and Generation X was only 2.4%. While Generation Z respondents who accessed the internet more than 13 hours/day reached 8%, the Millennial Generation and Generation X were only 3.7% and 2.6%, respectively. Furthermore, Generation X was recorded as the age group that rarely used the internet. Generation X respondents who were online for less than 1 hour/day were 18.4%. Meanwhile, the Millennial Generation and Generation Z were 13.7% and 8.6%, respectively. This survey was conducted through face-to-face interviews with 1,529 respondents from the Z, Millennial, and X generation age groups throughout Indonesia. This makes the role of social media very crucial in persuading and, at the same time, providing vulnerability to the current millennial generation.

Along with openness to data and information, protection of information is mandatory. In recent years, rapid development and lower costs in information and communication technology have made it more accessible and convenient (Liu J. et al., 2018; Buhalis, D., & Law, R., 2008; Barrolli, L., & Xhafa, F., 2010). As a result, the number of Internet users has exploded. Misuse of data is also a particular concern (Liu, J. et al., 2018; Buhalis, D. & Law, R., 2008; Barrolli, L., & Xhafa, F., 2010; Ahdiat, A., 2022). Many data breaches occur due to poor implementation or lack of security controls from both private and government institutions (Park S. et al., 2018; Alneyadi S.

et al., 2016; Romanosky S. et al., 2011; Kenzler J., 2020; Christopoulou, A., 2019; Ahdiat, A., 2022). This phenomenon makes many countries try to improve security requirements and implement them in their laws. However, most security frameworks are reactive and do not address relevant threats.

For that reason, understanding existing social media security risks and mitigation approaches is required to acquire insights and build best practices to aid in more effectively tackling social media security threats. This study began by evaluating the many talks in the literature on social media security issues and mitigating measures. Following an exhaustive analysis, many critical findings were found and highlighted to assist governments in more effectively addressing social media security issues. This study's work sheds light on data security when utilizing social media.

RESEARCH METHOD

This study used a bibliometric analysis method with data sources from literature studies. The primary data used in this study came from the Scopus database. The Scopus database was the author's choice because it has complete data and is also one of the databases with the highest rating in the scientific field. To generate relevant discussions and conclusions, the authors utilized the VOSviewer analysis tool as a data processing tool. The VOSviewer analysis tool was also utilized to analyze search results in scopus.com.

The bibliometric analysis approach was employed in this research. Bibliometrics helps provide data sets that can be utilized by policymakers, academics, and other stakeholders to improve the quality of research (Hamidah I. et al., 2020). The bibliometric method is also a comprehensive and reliable way of reviewing and evaluating scientific publications to understand the development of certain topics (Nafi'ah et al., 2021). All data used in this study were retrieved from the Scopus database on November 26, 2022. In exploring the Scopus database, the researchers searched using three keywords: "Big Data Security", "Social-Media," and "Indonesia" in the last ten years (2006-2022). The search resulted in the discovery of 546 items related to the keywords "Big Data Security" and "Social Media," then focused on the keywords "Big Data Security" and "Social Media Risks." The result was 83 items, and there were 87 items related to the keywords "Big Data Security" and "Indonesia" without using a filter.

From 2006 to 2022, there were 546 (83 and 87 documents focusing on data security and risks in Indonesia) published articles indexed in the Scopus database related to data security on social media and risks. All search results data were stored in CSV files (Excel), which were then processed and checked using the VOSiewer program version 1.6.17. VOSviewer is a tool for displaying and analyzing trends in bibliometric maps (van Eck & Waltman, 2010). This program can display and describe bibliometric visual maps with unique data through identification and analysis of the types of analysis that can be visualized in VOSviewer, as illustrated in Figure 1.

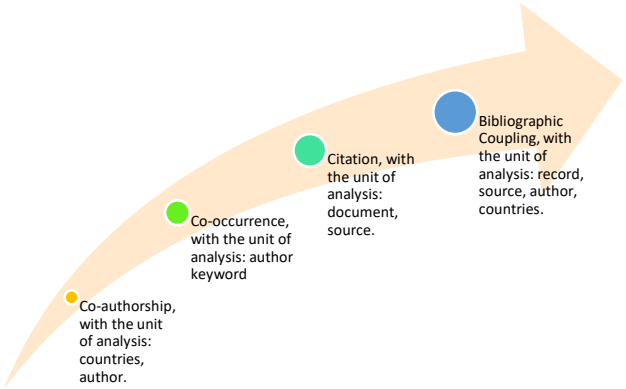


Figure 1. Types of Bibliometric Analysis Research Data at VOSviewer
Source: Processed by the Authors, 2022

Furthermore, the data collection was processed through the following steps to see the facts of previous research. These facts were analyzed to produce new findings that can contribute practically and theoretically to big data and security on social media risk in Indonesia, as depicted in Figure 2.

Figure 2. Bibliometric Analysis Data Process
Source: Processed by the Authors, 2022

RESULTS AND DISCUSSION

Mapping of Research Topics: An Overview

A total of 546 documents accessed in November 2022 regarding research on data security and social media risks were mapped and analyzed following the trend of search results for research publication data on Scopus. Each data or item displayed was based on search results, filtered on the scopus.com site, and then identified and analyzed utilizing the VOSviewer feature version 1.6.17. Data was then visualized following calculated weights and data trends. This also affected this research not to display less relevant data visualization on other items. Table 1 below presents the top 20 publishers (Documents by Source) that published studies on data security and social media risk studies at Scopus. The data becomes the researchers' record in identifying each research publication item in different trends and perspectives on data security issues in social media, as well as the risks and mitigation efforts carried out, as summarized in Table 1 and Figure 3.

Table 1. Top 20 Publishers (Documents by Source) with the Highest Influence on Data Security and Social Media Risk Studies in Scopus

No	Documents by Source	Documents	Citations	Total Link Strength
1	The Lancet	1	1,583	2
2	Jama	1	252	1
3	IEEE Transactions on Parallel and Distributed Systems	1	181	23
4	Information Systems Frontiers	1	53	0
5	Risk Analysis	1	48	0
6	Big Data and Cognitive Computing	1	46	5
7	Media, Culture and Society	1	46	0
8	P And T	1	45	0
9	Jama - Journal of the American Medical Association	1	44	0
10	BMC Public Health	1	34	1

Table 1. Top 20 Publishers (Documents by Source) with the Highest Influence on Data Security and Social Media Risk Studies in Scopus (cont')

No	Documents by Source	Documents	Citations	Total Link Strength
11	Annals of the New York Academy of Sciences	1	33	3
12	Www 2013 Companion - Proceedings of the 22nd International Conference on World Wide Web	1	29	0
13	Computers And Security	1	28	0
14	ECIS 2012 - Proceedings of the 20th European Conference on Information Systems	1	17	2
15	Proceedings - 2016 IEEE International Conference on Big Data, Big Data 2016	1	17	1
16	Fordham Law Review	1	14	0
17	Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare	1	13	0
18	Developments In Corporate Governance and Responsibility	1	11	1
19	Computer Science Review	1	10	0
20	Managing Risk and Information Security: Protect to Enable	1	10	0

Source: Processed from Scopus data, 2022

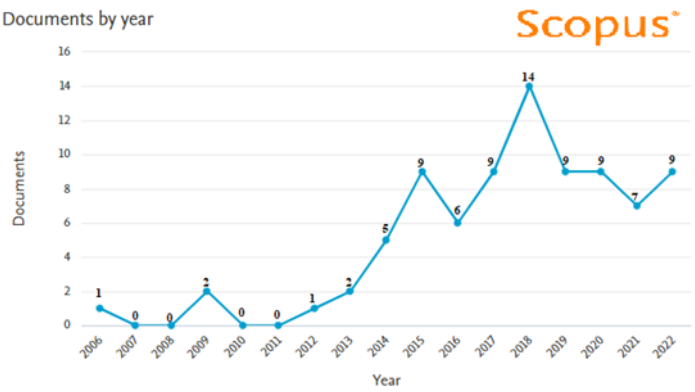


Figure 3. Number of Published Documents per Year on Security Data and Social Media Risks (2006-2022)
Source: Processed via Scopus, 2022

From several publishers (Documents by Source) that have published various studies on data security and social media risks that could be checked on, "The Lancet" and "Jama" are publishers with the most citations on Scopus. Figure 3 portrays the trend of increasing the number of documents every year in Scopus starting from 2006 to 2022 regarding the topic of data security and the risk of social media data. This trend was based on the results of search analysis on the Scopus website, and it was found that the trend in the number of articles in the Scopus database since 2013 has continued to increase even though the trend of increasing is still dynamic. This increase was influenced by developing issues, the level of cases of data leakage on social media, and the lack of response from global researchers.

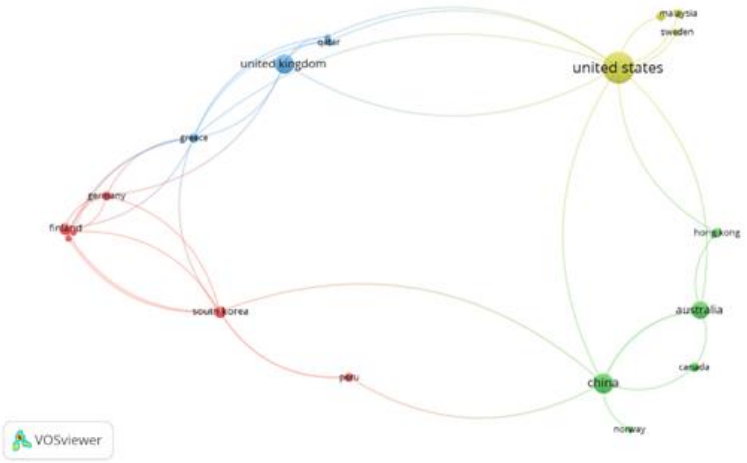
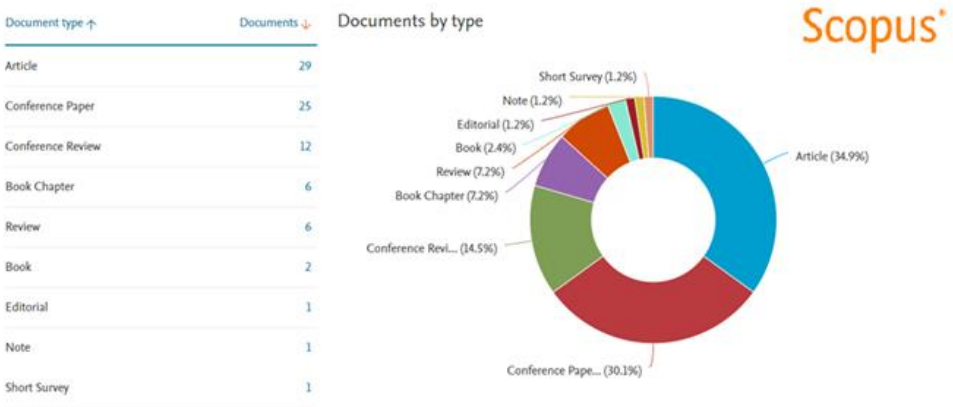


Figure 4. Top 10 Countries with Most Publications Regarding Data Security and Social Media Risks (Analyze Type: Co-authorships (countries))
Source: Processed via VOSviewer, 2022

Figure 4 demonstrates that the top ten countries with the most published documents studied and published about data security on social media and the risks by authors from countries, such as the United States (USA), with a total of 22 documents, then China with nine documents, and followed by India and United Kingdom (UK) with eight publication documents. Other countries were Australia with seven documents, Finland and South Korea with three documents, and Canada, Germany, and Greece with two documents, respectively. This confirms that studies on data security and social media risks are still lacking in Indonesia. Accordingly, this impacts the difficulty of developing a strategy in dealing with data leaks on social media by the Indonesian government and formulating appropriate policies.



Document type	Documents
Article	29
Conference Paper	25
Conference Review	12
Book Chapter	6
Review	6
Book	2
Editorial	1
Note	1
Short Survey	1

Figure 5. Types of Documents with the Most Publications Regarding Data Security and Social Media Risks
Source: Processed via Scopus, 2022

In Figure 5 above, several types of publication documents had several documents related to data security issues and social media risks. Such types of publication documents included Articles (29 documents), Conference Paper (25 documents), Conference Reviews (12 documents), Book Chapter (6 documents), Review (6 documents), Book (2 documents), Editorial (1), Short Survey (1), and Note (1 document). From that, it can be said that there is still a lack of publications regarding data security issues and social media risks in the era of rapid and difficult-to-control information and technology development.

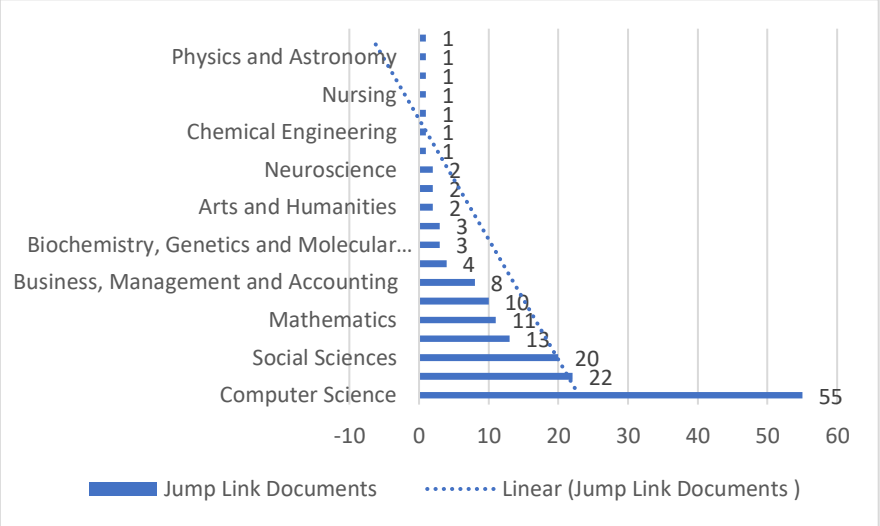


Figure 6. Most Publication Subject Area Regarding Data Security and Media Risk
Source: Processed via Scopus, 2022

Figure 6 illustrates the top ten subject areas of publications containing documents on the topic of data security and social media risks. Fields of study, such as Computer Science, are areas of interest to researchers with 55 documents, the most from other fields of study. Then, there is the Social Science Subject Area, which is a field of study that is in great demand and includes studies and research on data security and the risks of social media. Although it is dominant, the data above also indicates that the study of data security and social media risks needs to be understood in various contexts by observing other fields of study. The complexity of the problem of data security on social media and the risks that become a transition in the era of information and technology development in the world need to be examined carefully, and study perspectives in other fields to find the right ideas and foundations in formulating strategies to deal with this one problem are necessary. In social science, many researchers started to realize the urgency of data security on social media in Indonesia. This tendency is seen that researchers in fields of study, such as Social Sciences, need documents or results of research in other fields to build ideas and analysis. It is envisaged that this would give insight into existing understandings of social media security risks and mitigation approaches, allowing for the collection of insights and development of best practices to aid in more effectively tackling social media security issues.

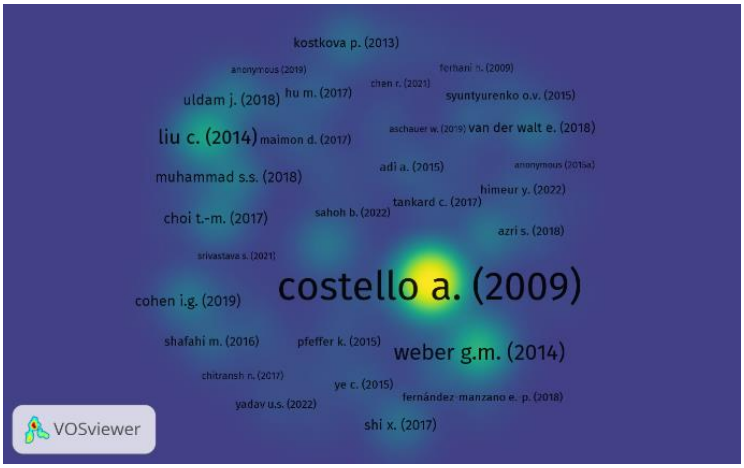


Figure 7. Top 5 Documents with Highest Citation Strength on Scopus Regarding Data Security and Social Media Risks (Analyze Type: Citation (document source))
Source: Processed via VOSviewer, 2022

Figure 7 above depicts the depth (density) of the most frequently cited documents to form a basic understanding of data security issues in social media and their risks. Top 5 authors with high document citations are: (1) Costello A. (2009) as many as 1583 citations; (2) Weber G.M. (2014) as many as 252 citations; (3) Liu C. (2014) as many as 181 citations; (4) Muhammad S.S. (2018) 53 citations; and (5) Choi T.-M. (2017) as many as 48 citations. The number of citations is claimed to be a document that is quite influential for global researchers in viewing studies related to data security on social media and its risks. A publication document that influences other published documents can be seen in the number of citations; the more citations of a document, the greater the influence on the research topic under study. The results of this research study based on these data regarding data security on social media and the risks suggest that this phenomenon makes many countries try to increase data security requirements on social media. Misuse of data is also a particular concern in this case. Many data breaches occur due to poor implementation or lack of control (Price, W. N., & Cohen, I. G., 2019; Hongjun, Z. et al., 2014; Paquette, S. et al., 2010; Pearson, S., & Benameur, A., 2010; Osborn, E., & Simpson, A., 2018).

Mapping of Research Topics on Data Security, Social Media Risks, and Mitigation Techniques in Indonesia

Following the trend of Scopus search results for research publication data, 87 documents accessed in November 2022 pertaining to data security research, social media risks, and mitigation techniques in Indonesia were mapped and analyzed. Every piece of data or item presented was derived from search results and filtered on the scopus.com website. Subsequently, it was identified and analyzed utilizing version 1.6.17 of the VOSviewer feature. After that, the data were visualized graphically using computed weights and trends. This also impacts the research by preventing the display of data visualization on less pertinent elements.

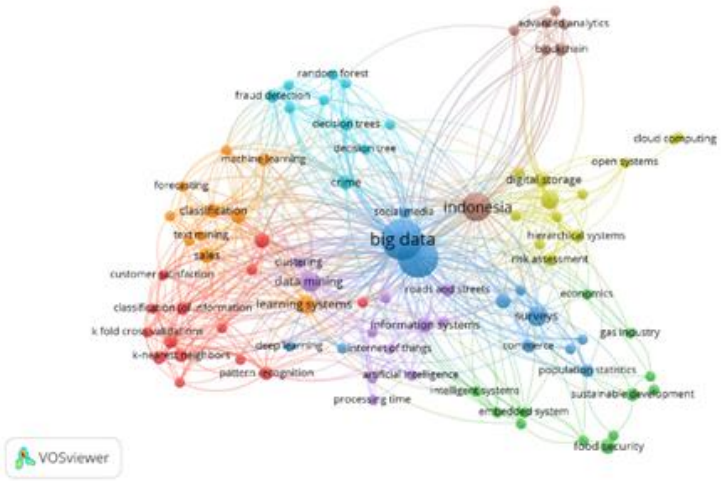


Figure 8. Analysis via VOSviewer (Analyze Type: Co-occurrence (All Keywords))
Source: Processed via VOSviewer, 2022

In a search through VOSviewer in Figure 8, with as many as 87 research documents indexed in Scopus regarding data security issues and social media risks in Indonesia, eight (8) clusters of trending keyword topics in previous research on this topic were found. This is the basis for identifying problems and creating strategies for data security issues and social media risks in Indonesia, as well as the findings of this study. The eight clusters were divided into the following. The first theme cluster (red): research issues that are of serious concern to this cluster are classification information, customer satisfaction, graphic methods, Instagram, kfold cross-validations, k-nearest neighbors, learning algorithms, motion compensation, naive Bayes, nearest neighbor search, pattern recognition, query processing, and sentiment analysis. The second cluster (green): research issues that are of serious concern to this cluster are economics, embedded systems, financial services, food security, food supply, industrial gas, intelligent systems, monitoring, network security, and sustainable development. The third cluster (blue):

research issues that are of serious concern to this cluster are big data, commerce, deep learning, official statistics, population statistics, regression analysis, security of data, social media, social network analysis, social networking (online) surveys, and tourism statistics. The fourth cluster (yellow): research issues that are of serious concern to this cluster are cloud computing, database systems, digital storage, hierarchical systems, information security, information management, open systems, personal data protection, and risk assessment. The fifth cluster (purple): research issues that are of serious concern to this cluster are artificial intelligence, clustering, data mining, data warehouses, decision-making, information systems, information use, internet of things (IoT), motor transportation, processing time, and roads and streets. The sixth cluster (light blue): research issues that are of serious concern to this cluster are crime, data handling, decision trees, finance, fraud detection, machine learning approach, and predictive analytics. The seventh cluster (orange): the research issues that are of serious concern to this cluster are classification methods, classification techniques, forecasting, learning systems, machine learning, sales, support vector machines, and text mining. The eighth cluster (brown) is the last in this cluster, which is a serious concern on the topic of advanced analytics, big data analytics, blockchain, data acquisition, data analytics, Indonesia, and interoperability. Each cluster becomes a reference for research issues, which become perspectives for building research that contributes practically and theoretically to future research.

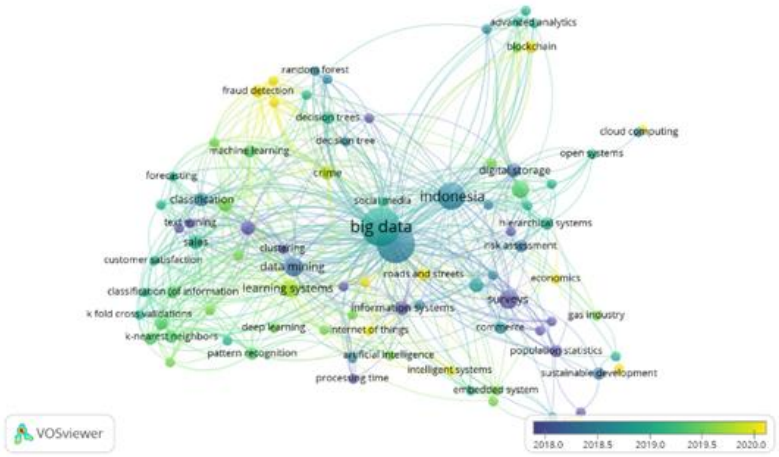


Figure 9. Analysis via VOSviewer (Analyze Type: Co-occurrence (All Keywords))
Source: Processed via VOSviewer, 2022

The appearance is not much different from what is shown in Figure 9; the results of the visualization (Overlay Visualization) display that there have been several research issue trends since 2020 that have become a concern in Indonesia. Some of the research issues are (1) Financial services in data network security in Indonesia; (2) Economic risk assessment in the social media market; (3) Intelligent system related to information management of online media crimes; (4) Data security on the Internet of Things (IoT); and (5) Froud detection and machine learning approaches in learning systems and crimes on social media. From some of the research issue trends that have been researched regarding data security and social media risks in Indonesia, it can be said that studies are still needed to support existing studies while simultaneously understanding data security issues and social media risks that are appropriate in Indonesia. As a result, it is necessary to review other relevant topics to assist researchers in explaining data security issues and social media risks in Indonesia, and it is advisable to review the previous data in Table 2. The research documents related to case studies on data security and social media risks in Indonesia can be observed in Table 2.

Table 2. Top 15 Study Documents on Data Security, Social Media Risks, and Mitigation Techniques in Indonesia

No	Document Title	Authors	Year	Source	Citation
1	Theorizing spatial dynamics of metropolitan regions: A preliminary study in Java and Madura Islands, Indonesia	Buchori, I., Sugiri, A., Maryono, M., Pramitasari, A., Pamungkas, I.T.D.	2017	Sustainable Cities and Society 35, pp. 468-482	26
2	Immutable ubiquitous digital certificate authentication using blockchain protocol	Rahardja, U., Hidayanto, A.N., Putra, P.O.H., Hardini, M.	2021	Journal of Applied Research and Technology, 19(4), pp. 308-321	17
3	Customer Churn Analysis and Prediction Using Data Mining Models in the Banking Industry	Karvana, K.G.M., Yazid, S., Syalim, A., Mursanto, P.	2019	2019 International Workshop on Big Data and Information Security, IWBIS 2019 8935884, pp. 33-38	12
4	Hybrid cloud: Bridging of private and public cloud computing	Aryotejo, G., Kristiyanto, D.Y., Mufadhol	2018	Journal of Physics: Conference Series 1025(1),012091	12
5	Big data for government policy: Potential implementations of bigdata for official statistics in Indonesia	Pramana, S., Yuniarto, B., Kurniawan, R., (...), Hasyyati, A.N., Indriani, R.	2018	Proceedings - WBIS 2017: 2017 International Workshop on Big Data and Information Security 2018-January, pp. 17-21	11
6	Sentiment Analysis of the Covid-19 Virus Infection in Indonesian Public Transportation on Twitter Data: A Case Study of Commuter Line Passengers	Sari, I.C., Ruldeviyani, Y.	2020	2020 International Workshop on Big Data and Information Security, IWBIS 2020 9255531, pp. 23-28	9
7	Improving Data Security, Interoperability, and Veracity using Blockchain for One Data Governance, Case Study of Local Tax Big Data	Wibowo, S., Sandikapura, T.	2019	Proceeding - 2019 International Conference on ICT for Smart Society: Innovation and Transformation Toward Smart, 8969805 Region, ICISS 2019	8
8	Enhanced tele ECG system using Hadoop framework to deal with big data processing	Ma'Sum, M.A., Jatmiko, W., Suhartanto, H.	2017	2016 International Workshop on Big Data and Information Security, IWBIS 2016 7872900, pp. 121-126	8

Table 2. Top 15 Study Documents on Data Security, Social Media Risks, and Mitigation Techniques in Indonesia (cont')

No	Document Title	Authors	Year	Source	Citation
9	Instagram Sentiment Analysis with Naive Bayes and KNN: Exploring Customer Satisfaction of Digital Payment Services in Indonesia	Sudira, H., Diar, A.L., Ruldeviyani, Y.	2019	2019 International Workshop on Big Data and Information Security, IWBIS 2019, 8935700, pp. 21-26	8
10	Strategic Collaboration ICT in the online Transportation Services in Jakarta Area	Purba, J.T., Samuel, S., Purba, A.	2020	IOP Conference Series: Materials Science and Engineering, 918(1),012206	7
11	ISMS planning based on ISO/IEC 27001:2013 using analytical hierarchy process at gap analysis phase (Case study: XYZ institute)	Candra, J.W., Briliyant, O.C., Tamba, S.R.	2018	Proceeding of 2017 11th International Conference on Telecommunication Systems Services and Applications, TSSA 2017, 2018-January, pp. 1-6	7
12	Marketing strategy for renewable energy development in Indonesia context today	Arafah, W., Nugroho, L., Takaya, R., Soekapdjo, S.	2018	International Journal of Energy Economics and Policy 8(5), pp. 181-186	7
13	Employee commitment and service performance	Wulandari, S.S.	2019	Human Systems Management 37(4), pp. 381-386	6
14	Application of text mining for classification of textual reports: A study of Indonesia's national complaint handling system	Surjandari, I., Megawati, C., Dhini, A., Sanditya Hardaya, I.B.N.	2016	Proceedings of the International Conference on Industrial Engineering and Operations Management 8-10 March 2016, pp. 1147-1156	6
15	Semantic Segmentation on LiDAR Point Cloud in Urban Area Using Deep Learning	Wicaksono, S.B., Wibisono, A., Jatmiko, W., Gamal, A., Wisesa, H.A.	2019	2019 International Workshop on Big Data and Information Security, IWBIS 2019 8935882, pp. 63-66	5

Source: Processed from Scopus data, 2022

Table 2 presents that only a few published research documents covering topics around data security and social media risks in Indonesia would be explored in this study based on their citation strength on Scopus. The research signifies that there is still very little interest in studying these topics. Nevertheless, some research results obtained from the seven documents above are deemed necessary to develop further research, and the research results are mapped as follows. In Buchori I. et al.'s (2017) research, the utilization of GIS-based and tabular data that applied spreadsheet operations detailed at the sub-district level in several special areas on Java and Madura Islands as metropolitan areas had an impact on the security vulnerability of population data. So as not to cause data leaks impacting the community and distrusting local government institutions, it is necessary to assist the community's data security strategy. A study by Rahardja U. et al. (2021) suggests the era of the world's technology and information revolution, the

potential for social media crimes, and the vulnerability of data security problems in Indonesia, so this research encourages the role of blockchain, which plays a role in increasing the security of e-certificate data. In addition, Karvana K.G.M. et al.'s (2019) research argued for data security issues, especially among banking industry customers in Indonesia, could apply analysis and prediction methods called "data mining model" and "Churn customer prediction," where the use of classification techniques from data mining produces machine learning models. The results of this modeling can be used by companies that will implement strategic actions to prevent customer churn. Research from Aryitejo G. et al. (2018) further raised the problem of low data security in Cloud Computing, which is commonly used in the start-up business world in Indonesia as a cloud service provider (CSP), offering a Hybrid Cloud Deployment Model (HCDM). It has characteristics as an open source, which is one of the secure cloud computing models so that HCDM can solve data security problems. In Pramana S. et al.'s (2018) study, it is argued that big data management in Indonesia is the speed and frequency of data creation and collection, so institutions such as the Indonesian government are responsible for today's flood of data. It is also known that the amount of digital data available is currently projected to increase by 40% per year. Therefore, to face this challenge, the concept of "Big Data for Development" is offered, which refers to the identification of big data sources that are relevant to the policies and planning of the Indonesian government's development program.

Additionally, Sari I.C. and Ruldeviyani Y.'s (2020) research stated that to see the accuracy of the correctness of data and measure opinion sentiment on social media (commuter-line), the "Naïve Bayes" method can be used, which outperforms the decision tree. Specifically, a study by Wibowo S. and Sandikapura T. (2019) put forward PERPRES (Presidential Regulation) No. 39 of 2019 concerning One Data Indonesia, which is intended to regulate data generated by central and regional agencies to support development planning, implementation, evaluation, and control, including one of which is regional taxes. This is to manage Big Data containing data from the central and regional governments of Indonesia. Besides, Sudira H. et al. (2019) asserted that internet penetration and social media trends have generated many data. The use of digital payment services (Go-Pay, Ovo, and LinkAja), which are currently widespread in Indonesia, is a challenge in itself. Hence, it has an impact on data security vulnerabilities and social media risks for people in Indonesia. Furthermore, in their research, Purba J.T. et al. (2020) pointed out the rise of financial technology collaborations used in online transportation applications, which are now widely implemented by a number of transportation companies in Indonesia. Their research concludes that the adoption of FinTech as a means of payment is growing rapidly in economic transactions. Second, developing technology, with the presence of the internet, big data, cellular, and computing power, is clearly driving innovation in online transportation services. From the several research explorations on cases in Indonesia described above, none really recommends efforts to mitigate data security problems in community digital activities on social media. This is a record for Indonesian researchers to increase the publication of research on data security and risk issues on social media to conduct in-depth research.

Based on the analysis and identification of researchers in the previously described Systematic Literature Review (SLR) study, it can be said that internet penetration trends and social media trends in Indonesia offer a variety of interesting opportunities and challenges. Consequently, the utilization of social media for the administration of big data has expanded substantially in recent years in Indonesia. Given the frequency and rate at which data is generated and accumulated, institutions, including the Indonesian government, are presently accountable for the deluge of information. Furthermore, it is widely recognized that the annual growth rate of digital data availability is presently estimated to be 40%. On the other hand, it is unfortunate to note that social media sites, such as YouTube, Facebook, Instagram, TikTok, Twitter, and LinkedIn, can pose various risks and serious security threats to unwary users and their organizations. However, this is not accompanied by efforts to mitigate data security vulnerabilities and knowledge of the risks of excessive information in Indonesia. Accordingly, it is necessary to develop key insights (insight into challenges and opportunities) in dealing with these problems. Publications regarding data security and the risk of crime on social media in cases in Indonesia should be, thus, increased. Insights from the research results become knowledge about the risks of social media activities and improve the security of individual data in cyberspace.

Social Media Risks and Big Data Security in Indonesia: Challenges and Opportunities

A recent global study noted by He W. (2012) surveyed 4,640 IT security practitioners and revealed data security problems on social media in 12 countries. He also mentioned that an effective social media security policy is a social media security strategy to reduce social media security risks. A recent study by Jensen M. L. et al. (2017) unveiled that social media sites are ten times more effective at delivering malware and stealing information than previously popular email delivery methods. Prajapati A. and Gupta S. (2021) also listed more than 43,000 malicious files related to social networking sites. The number of malicious programs were received by Kaspersky Labs targeting popular social networking sites such as Twitter and Instagram (He, W., 2012).

However, it is unrealistic to prohibit people from using social media tools, such as YouTube, Facebook, Instagram, TikTok, Twitter, and LinkedIn, because many people need to utilize social media for activities related to work, school, and study. Also, despite the risks of social media, the study by Bertot J.C. (201) and Shafqat N. and Masood A. (2016) stated that many national governments do not have the necessary security controls and policies that can be implemented to address the risks and information security issues posed by the use of social media. As more countries/national governments become increasingly concerned about the potential information security implications of social media use, many countries/governments are implementing their social media security policies effectively.

Further studies from Obar J.A. and Oeldorf-Hirsch A. (2020) and Masur P. K. and Scharkow M. (2016) revealed that data security policies on social media are not always effective for society. The study findings are that many people and some institutions do not understand security policies and underestimate security risks even though they receive written security policies and have been briefed. In the case of Indonesia, Pramana S. et al.'s (2018) research asserted that for the management of big data in Indonesia, where there is the speed and frequency of data creation and collection, institutions such as the Indonesian government are responsible for the flood of data today. Related to that, Presidential Regulation No. 39 of 2019 concerning One Data Indonesia is intended to regulate the current excess data while at the same time ensuring the security of public data using social media. Furthermore, a study by Herath T. and Rao H. R. (2009) uncovered that even when users know the security policy, they often ignore it to achieve what they want due to time pressure, inadequate knowledge, or different motivations. Encouraging users to engage in safe online behavior is also difficult because some people's mentality and way of thinking are linked to risk perception. Thus, more research is needed to develop more effective strategies to minimize the security risks posed by social media. Several reasons why it is important to protect personal data can be seen in Figure 10.

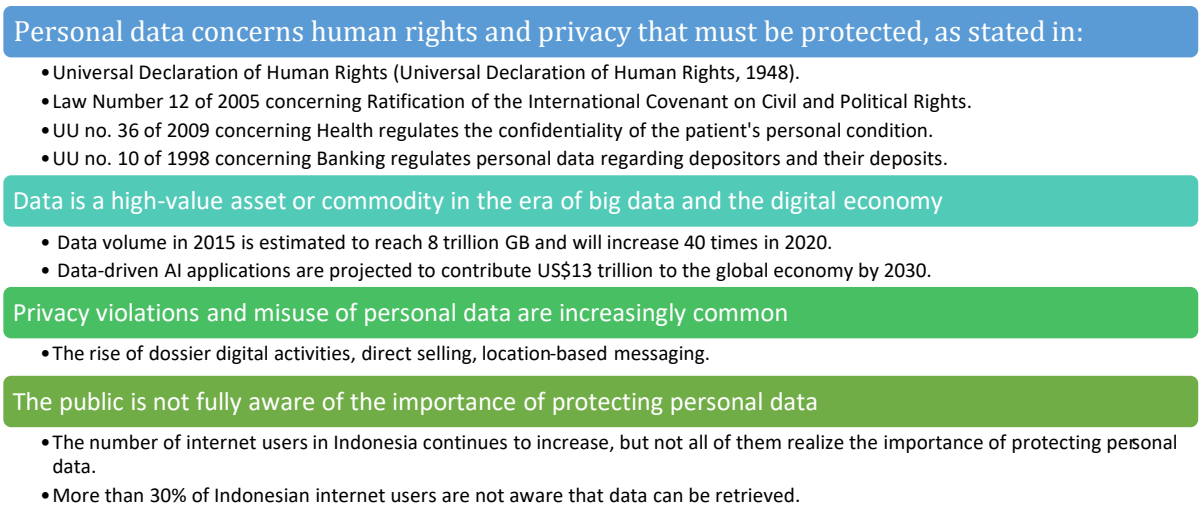


Figure 10. Fundamentals of Data Protection
Source: Sri Adiniangsih S.E., 2019

Based on Figure 10 above, the reasons why it is important to protect personal data are that: (1) Personal data concerns human rights and privacy, which must be protected; (2) Data is a high-value asset or commodity in the current era of big data and digital economy; (3) Cases of violation of privacy and misuse of personal data are increasingly occurring; and (4) The public is not fully aware of the importance of protecting personal data. Nowadays, social media sites like Facebook provide users with the ability to maintain their web pages and share content with their personal connections (Baruah T. D., 2012; Akram W. & Kumar R., 2017). Social media also brings many benefits to today's digital society. However, because people and institutions are increasingly using social media to communicate with work, school, and college, this raises data security risks in social media (Dwivedi Y. K. et al., 2021; Carr C. T. & Hayes R. A., 2015). The dilemma of data security is also that the too-strict adoption of social media technology is hindered by security problems due to various security incidents, such as loss of confidential data and malware. To reduce the potential risks caused by using social media for the community, Sotiriadis M.D. (2017) and Wang Y. et al. (2016) suggested that strategies to deal with social media risks need to focus on wiser and smarter usage behavior.

CONCLUSION

In the identification and analysis of this study, little thought/insight to improve and expand social media security strategies in journal publishing was found. Consequently, this is still lacking to be able to understand the risks of data security and crime on social media, such as information theft and Malware virus attacks, which is the reason for the need to increase publications regarding data security and the risks of crime on social media in cases in Indonesia. From the several exploratory research studies on cases in Indonesia previously described, none really recommended efforts to mitigate data security problems in community digital activities. The insights from the research result in knowledge about the risks of social media activities and improving the security of individual data in cyberspace. Data security issues are also widely recognized, as the adoption of social media technology is hampered by security issues caused by various insider threats, such as confidential data and malware. Several studies suggest that social media risk management strategies need to focus on wiser and smarter recognition behavior to reduce the potential risks caused by social media use.

The dynamics in discussions about the security risks of social media are often distorted, fragmented, and disseminated through various outlets, such as newspapers, technical journals, news articles, and corporate websites. The authors conducted an in-depth literature review of 87 documents indexed in Scopus regarding data security and social media risks to consolidate the ongoing discussion in recommending data security policy references to prevent information theft and fight malware attacks on social media more effectively. As a result of this research, the authors have provided several recommendations to help communities and institutions reduce the risk of piracy on social media.

ACKNOWLEDGMENT

The authors acknowledge the financial support from Universitas Muhammadiyah Makassar, Indonesia, and thank the collaborating institutions for this research and the article publishing process.

REFERENCES

Ahdiat, A. (2022). Survei: Pecandu Internet Terbanyak dari Kalangan Gen Z. [online] available at https://databoks.katadata.co.id/datapublish/2022/06/29/survei-pecandu-internet-terbanyak-dari-kalangan-gen-z accessed on November 2022

Akram, W., & Kumar, R. (2017). A study on positive and negative effects of social media on society. *International Journal of Computer Sciences and Engineering*, 5(10), 351–354. https://doi.org/10.26438/ijcse/v5i10.351354

Alneyadi, S., Sithirasenan, E., & Muthukkumarasamy, V. (2016). A survey on data leakage

prevention systems. *Journal of Network and Computer Applications*, 62, 137–152. https://doi.org/10.1016/j.jnca.2016.01.008

Arafah, W., Nugroho, L., Takaya, R., & Soekapdjo, S. (2018). Marketing Strategy for Renewable Energy Development In Indonesia Context Today. *International Journal of Energy Economics and Policy*, *8*(5), 181-186.

Aryotejo, G., & Kristiyanto, D. Y. (2018, May). Hybrid cloud: bridging of private and public cloud computing. *Journal of Physics: Conference Series*, 1025, 012091. https://doi.org/10.1088/1742-6596/1025/1/012091

Barolli, L., & Xhafa, F. (2010). Jxta-overlay: A p2p platform for distributed, collaborative, and ubiquitous computing. *IEEE Transactions on Industrial Electronics, 58*(6), 2163–2172. https://doi.org/10.1109/TIE.2010.2050751

Baruah, T. D. (2012). Effectiveness of Social Media as a tool of communication and its potential for technology enabled connections: A micro-level study. International journal of scientific and research publications, 2(5), 1-10.

Bertot, J. C., Jaeger, P. T., & Hansen, D. (2012). The impact of policies on government social media usage: Issues, challenges, and recommendations. *Government information quarterly*, *29*(1), 30–40. https://doi.org/10.1016/j.giq.2011.04.004

Buchori, I., Sugiri, A., Maryono, M., Pramitasari, A., & Pamungkas, I. T. (2017). Theorizing spatial dynamics of metropolitan regions: A preliminary study in Java and Madura Islands, Indonesia. *Sustainable cities and society*, *35*, 468–482. https://doi.org/10.1016/j.scs.2017.08.022

Buhalis, D., & Law, R. (2008). Progress in information technology and tourism management: 20 years on and 10 years after the Internet—The state of eTourism research. *Tourism Management, 29*(4), 609–623. https://doi.org/10.1016/j.tourman.2008.01.005

Candra, J. W., Briliyant, O. C., & Tamba, S. R. (2017, October). ISMS planning based on ISO/IEC 27001: 2013 using analytical hierarchy process at gap analysis phase (Case study: XYZ institute). In *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)* (pp. 1-6). IEEE. https://doi.org/10.1109/TSSA.2017.8272916

Carr, C. T., & Hayes, R. A. (2015). Social media: Defining, developing, and divining. *Atlantic journal of communication*, *23*(1), 46–65. https://doi.org/10.1080/15456870.2015.972282

Choi, T. M., & Lambert, J. H. (2017). Advances in risk analysis with big data. *Risk Analysis, 37*(8), 1435–1442. https://doi.org/10.1111/risa.12859

Christopoulou, A. (2019). The Information disorder Ecosystem: A study on the role of Social Media, the Initiatives to tackle disinformation and a Systematic Literature Review of False Information Taxonomies. International Hellenic University, 1-82. https://repository.ihu.edu.gr//xmlui/handle/11544/29381

Costello, A., Abbas, M., Allen, A., Ball, S., Bell, S., Bellamy, R., ... & Patterson, C. (2009). Managing the health effects of climate change: Lancet and University College London Institute for Global Health Commission. *The Lancet, 373*(9676), 1693–1733. https://doi.org/10.1016/S0140-6736(09)60935-1

Dwivedi, Y. K., Ismagilova, E., Hughes, D. L., Carlson, J., Filieri, R., Jacobson, J., ... & Wang, Y. (2021). Setting the future of digital and social media marketing research: Perspectives and research propositions. *International Journal of Information Management*, *59*, 102168. https://doi.org/10.1016/j.ijinfomgt.2020.102168

Fan, Z., Kalogridis, G., Efthymiou, C., Sooriyabandara, M., Serizawa, M., & McGeehan, J. (2010, April). The new frontier of communications research: smart grid and smart metering. In *Proceedings of the 1st International Conference on Energy-Efficient Computing and Networking* (pp. 115-118). https://doi.org/10.1109/MNET.2014.6863125

García-Ceballos, S., Rivero, P., Molina-Puche, S., & Navarro-Neri, I. (2021). Educommunication and Archaeological Heritage in Italy and Spain: An Analysis of Institutions' Use of Twitter, Sustainability, and Citizen Participation. *Sustainability, 13*(4), 1602. https://doi.org/10.3390/su13041602

Hamidah, I., Sriyono, S., & Hudha, M. N. (2020). A Bibliometric analysis of COVID-19 research using VOSviewer. *Indonesian Journal of Science and Technology*, 34–41. https://doi.org/10.17509/ijost.v5i2.24522

He, W. (2012). A review of social media security risks and mitigation techniques. *Journal of Systems and Information Technology*, *14*(2), 171–180. https://doi.org/10.1108/13287261211232180

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European journal of information systems, 18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Hongjun, Z., Wenning, H., Dengchao, H., & Yuxing, M. (2014, August). Survey of research on information security in big data. In Anais do III Brazilian Workshop on Social Network Analysis and Mining (pp. 267-272). SBC.

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems, 34*(2), 597–626. https://doi.org/10.1080/07421222.2017.1334499

Karvana, K. G. M., Yazid, S., Syalim, A., & Mursanto, P. (2019, October). Customer churn analysis and prediction using data mining models in banking industry. In *2019 International Workshop on Big Data and Information Security (IWBIS)* (pp. 33-38). IEEE. https://doi.org/10.1109/IWBIS.2019.8935884

Kenzler, J. (2020). Cambridge Analytica and the Public Sphere: An Investigation of Political Manipulation in the Digital Age (Master's thesis). Tampere University. https://core.ac.uk/download/pdf/288313141.pdf

Kraut, A., Kohalmi, L., & Toth, D. (2020). Digital dangers of smartphones. JE-Eur. Crim. L., 36. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jeeucl2020&div=8&id=&page=

Liu, C., Chen, J., Yang, L. T., Zhang, X., Yang, C., Ranjan, R., & Kotagiri, R. (2014). Authorized public

auditing of dynamic big data storage on cloud with efficient verifiable fine-grained updates. *IEEE Transactions on Parallel and Distributed Systems, 25*(9), 2234–2244. https://doi.org/10.1109/TPDS.2013.191

Liu, J., Yang, F., & Ren, L. (2018). Study on Reliability Evaluation Method Based on Improved Monte Carlo Method. In *E3S Web of Conferences* (Vol. 64, p. 04008). EDP Sciences. https://doi.org/10.1051/e3sconf/20186404008

Ma'Sum, M. A., Jatmiko, W., & Suhartanto, H. (2016, October). Enhanced tele ECG system using Hadoop framework to deal with big data processing. In *2016 International Workshop on Big Data and Information Security (IWBIS)* (pp. 121-126). IEEE. https://doi.org/10.1109/IWBIS.2016.7872900

Masur, P. K., & Scharkow, M. (2016). Disclosure management on social network sites: Individual privacy perceptions and user-directed privacy strategies. *Social Media+ Society*, *2*(1), 2056305116634368. https://doi.org/10.1177/2056305116634368

Muhammad, S. S., Dey, B. L., & Weerakkody, V. (2018). Analysis of factors that influence customers' willingness to leave big data digital footprints on social media: A systematic review of literature. *Information Systems Frontiers, 20*(3), 559–576. https://doi.org/10.1007/s10796-017-9802-y

Nafi'ah, B. A., Roziqin, A., Suhermanto, D. F., & Fajrina, A. N. (2021). The Policy Studies Journal: A Bibliometric and Mapping Study from 20152020. *Library Philosophy and Practice,* 2021, 1–18. https://digitalcommons.unl.edu/libphilprac/5881/

Obar, J. A., & Oeldorf-Hirsch, A. (2020). The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society*, *23*(1), 128–147. https://doi.org/10.1080/1369118X.2018.1486870

Osborn, E., & Simpson, A. (2018). Risk and the small-scale cyber security decision making dialogue—a UK case study. *The Computer Journal, 61*(4), 472–495. https://doi.org/10.1093/comjnl/bxx093

Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government information quarterly*, 27(3), 245–253. https://doi.org/10.1016/j.giq.2010.01.002

Park, S., Akatyev, N., Jang, Y., Hwang, J., Kim, D., Yu, W., ... & Kim, J. (2018). A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement. *Digital Investigation,* 24, S93-S100. https://doi.org/10.1016/j.diin.2018.01.012

Pearson, S., & Benameur, A. (2010, November). Privacy, security and trust issues arising from cloud computing. In 2010 IEEE Second International Conference on Cloud Computing Technology and Science (pp. 693-702). IEEE. https://doi.org/10.1109/CloudCom.2010.66

Prajapati, A., & Gupta, S. (2021). A Survey: Data Mining and Machine Learning Methods for Cyber Security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7*(2), 24–34. Internet Archive. https://doi.org/10.32628/cseit217212

Pramana, S., Yuniarto, B., Kurniawan, R., Yordani, R., Lee, J., Amin, I., ... & Indriani, R. (2017, September). Big data for government policy: Potential implementations of bigdata for official statistics in Indonesia. In *2017 International Workshop on Big Data and Information Security (IWBIS)* (pp. 17-21). IEEE. https://doi.org/10.1109/IWBIS.2017.8275097

Price, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature medicine*, 25(1), 37–43. https://doi.org/10.1038/s41591-018-0272-7

Purba, J. T., Samuel, S., & Purba, A. (2020, September). Strategic Collaboration ICT in the online Transportation Services in Jakarta Area. In *IOP Conference Series: Materials Science and Engineering* (Vol. 918, No. 1, p. 012206). IOP Publishing. https://doi.org/10.1088/1757-899X/918/1/012206

Rahardja, U., Hidayanto, A. N., Putra, P. O. H., & Hardini, M. (2021). Immutable Ubiquitous Digital Certificate Authentication Using Blockchain Protocol. *Journal of applied research and technology*, *19*(4), 308–321. https://doi.org/10.22201/icat.24486736e.2021.19.4.1046

Romanosky, S., Telang, R., & Acquisti, A. (2011). Do data breach disclosure laws reduce identity theft? Journal of Policy Analysis and Management, 30(2), 256–286. https://doi.org/10.1002/pam.20567

Sari, I. C., & Ruldeviyani, Y. (2020, October). Sentiment analysis of the COVID-19 virus infection in Indonesian public transportation on Twitter data: A case study of commuter line passengers. In *2020 International Workshop on Big Data and Information Security (IWBIS)* (pp. 23-28). IEEE. https://doi.org/10.1109/IWBIS50925.2020.9255531

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security*, *14*(1), 129.

Simangunsong, E. (2021). Identifying Personal Characteristics of Social Media Entrepreneurs in Indonesia. *Jurnal ASPIKOM, 6*(2), 360–372. https://doi.org/10.24329/aspikom.v6i2.934

Sotiriadis, M. D. (2017). Sharing tourism experiences in social media. *International Journal of Contemporary Hospitality Management, 29*(1), 179–225. https://doi.org/10.1108/IJCHM-05-2016-0300

Sri Adiningsih, S. E. (2019). *Transformasi ekonomi berbasis digital di Indonesia: lahirnya tren baru teknologi, bisnis, ekonomi, dan kebijakan di Indonesia*. Gramedia Pustaka Utama.

Sudira, H., Diar, A. L., & Ruldeviyani, Y. (2019, October). Instagram sentiment analysis with naive Bayes and KNN: exploring customer satisfaction of digital payment services in Indonesia. In *2019 International Workshop on Big Data and Information Security (IWBIS)* (pp. 21-26). IEEE. https://doi.org/10.1109/IWBIS.2019.8935700

Surjandari, I., Megawati, C., Dhini, A., & Hardaya, I. B. N. S. (2016, March). Application of text mining for classification of textual reports: a study of Indonesia's national complaint handling system. In *6th International Conference on Industrial Engineering and Operations Management (IEOM 2016)*. http://ieomsociety.org/ieom_2016/pdfs/320.pdf

Van Eck, N., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for bibliometric mapping. *Scientometrics*, *84*(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

Wang, Y., Min, Q., & Han, S. (2016). Understanding the effects of trust and risk on individual behavior toward social media platforms: A meta-analysis of the empirical evidence. *Computers in Human Behavior,* 56, 34–44. https://doi.org/10.1016/j.chb.2015.11.011

Weber, G. M., Mandl, K. D., & Kohane, I. S. (2014). Finding the missing link for big biomedical data. *Jama, 311*(24), 2479–2480. https://doi.org/10.1001/jama.2014.4228

Wibowo, S., & Sandikapura, T. (2019, November). Improving data security, interoperability, and veracity using blockchain for one data governance, case study of local tax big data. In *2019 International Conference on ICT for Smart Society (ICISS)* (Vol. 7, pp. 1-6). IEEE. https://doi.org/10.1109/ICISS48059.2019.8969805

Wicaksono, S. B., Wibisono, A., Jatmiko, W., Gamal, A., & Wisesa, H. A. (2019, October). Semantic segmentation on lidar point cloud in urban area using deep learning. In *2019 International Workshop on Big Data and Information Security (IWBIS)* (pp. 63-66). IEEE. https://doi.org/10.1109/IWBIS.2019.8935882

Wulandari, S. S. (2018). Employee commitment and service performance. *Human Systems Management*, *37*(4), 381–386. https://doi.org/10.3233/HSM-17122

Yi, X., Liu, F., Liu, J., & Jin, H. (2014). Building a network highway for big data: architecture and challenges. *IEEE Network, 28*(4), 5–13. https://doi.org/10.1145/1791314.1791331