**Bulletin of Electrical Engineering and Informatics**
Vol. 12, No. 1, February 2023, pp. 587~596
ISSN: 2302-9285, DOI: 10.11591/eei.v12i1.4460 

# Privacy during epidemic of COVID-19: a bibliometric analysis

**Auwal Shehu Ali[1,2], Zarul Fitri Zaaba[1], Manmeet Mahinderjit Singh[1]**
[1]School of Computer Sciences, Universiti Sains Malaysia, Pulau Pinang, Malaysia
[2]Department of Computer Sciences, Bayero University, Kano, Kano State Nigeria

**Article Info**

***Article history:***

Received Jul 24, 2022
Revised Sep 30, 2022
Accepted Oct 24, 2022

***Keywords:***

Privacy
COVID-19
Bibliometric
Contact tracing app
Privacy preserving

**ABSTRACT**

1226 articles on privacy and COVID-19 were published by authors from 69 countries in this year's issue. COVID 19's privacy is now the focus of many researchers' attention. The present body of knowledge on privacy for COVID-19 digital technologies has been thoroughly analyzed, and a concise overview of research status and future developments can be gleaned. This paper conducted a bibliometric examination of privacy using the Scopus dataset. Utilizing VOSviewer software, the relevant literature papers published on this topic were examined to determine the field's development history, research hotspots, and future directions. Over time, there has been a rise in the number of studies published in privacy for COVID-19, particularly after 2020, and the growth rate has been steadily increasing. Regarding published research, the United States and China lead the pack. These articles appeared in primarily English-language journals and conference proceedings. Privacy and COVID-19 research was mostly computer science. The most used terms in privacy and COVID-19 were data privacy and humans. This paper examines the evolution of privacy and COVID-19 research and indicates current research priorities and future research goals. Furthermore, the privacy and COVID-19 study seem to be a promising sphere as this study identifies 26 domains.



***Corresponding Author:***

Zarul Fitri Zaaba
School of Computer Sciences, Universiti Sains Malaysia
11800 Pulau Pinang, Malaysia
Email: zarulfitri@usm.my

## 1. INTRODUCTION

The most prominent issue humanity has recently experienced in terms of viral infection is the current outbreak of COVID-19, triggered by SARS-CoV-2 (severe acute respiratory syndrome coronavirus 2). Even as the nation aspired for quick COVID-19 vaccine rollouts in 2021, researchers' expectations may be limited by the pandemic. In this epidemic, millions were infected and died [1]. Even with widespread immunizations, still, the daily cases keep on resurfacing. The pandemic has resulted in the loss of many jobs. It has closed many entertainments, educational, sporting, religious, tourist, and public establishments worldwide. Different research approaches are proposed to minimize the economic impact of the pandemic. The number of COVID-19 papers is 20 times higher than prior viral diseases [2].

Information and communication technology (ICT) is the only option for people to be socially engaged or keep their enterprises going in these uncertain times. There are numerous social networks (SNs) through which people may stay in touch with their contacts, post photos and videos of their activities, find new acquaintances, or even conduct business online. They can enroll in classes, attend religious services, or work remotely using these methods. To decrease the consequences of this outbreak and limit the disease's transmission as rapidly as possible, governments in many countries have developed several digital technologies as a solution, like intelligent device

apps, internet-based frameworks, and unified platforms like contact tracing apps. These digital systems gather massive volumes of personal data in many states to achieve many goals (such as locating the disease's covert transmission routes, preventing its further spread, and predicting future trends).

Moreover, authorities have utilized digital solutions to prevent clinical staff from experiencing stress and for effective resource planning, considering the incidence of COVID-19 [3]. These data are vital for the fight against the outbreak. However, collecting these data can be vulnerable to manipulation or abuse if adequate attention to individual privacy is not made amidst the recent spike in digital activity. In a certain way, privacy concerns have pushed digital advancements under tremendous pressure [4]. Privacy violations have considerably increased because of the widespread using technology to fight COVID-19. As a result, there is an inescapable necessity to shift focus away from data-first and toward privacy-first [5]. Privacy considerations make it difficult for many governments worldwide to get consumers to use pandemic-related apps [6].

Since many countries embrace big data and AI, group privacy breaches are more likely than individual ones in this global epidemic. There was an event in South Korea in which the spread of COVID-19 was traced to a lesser-known religious sect (the Shincheonji church) [7]. Consequently, the government had access to a vast amount of raw data, such as transactions, credit card use, mobile id, social security numbers, and going to pharmacies that members made of the Shincheonji church. Because of these invasions of privacy and the involvement in their personal life brought about by the harsh actions taken against them by the government of South Korea, several members have taken their own lives. The equilibrium between public security and personal privacy is significantly supported via the law in countries like Singapore, but this can contribute to many adverse effects during the era of post-COVID-19 because of the massive information transformation into the digital world [8]. Without legislative tools for COVID-19 like catastrophes, protecting privacy from corporate and government exploitation is difficult [9]. The volume and diversity of personal data acquired have expanded, which may assist corporate/political players in demanding more intrusive data for political advertisement. Post-COVID-19, privacy and cybersecurity risks will undoubtedly increase along with digitization [10].

Recently, a significant attempt has been undertaken to solve privacy issues arising from technology services linked to COVID-19, together with information collection and analysis, to halt the pandemic. Prominent and noteworthy research and technology initiatives like Apple's and Google's contact tracking systems, which are decentralized and respect users' privacy [11], Tracing people through their phone calls without compromising their privacy [12], and privacy-safe monitoring of possible COVID-19 infections [13], personal data privacy protection law [14], consent-based data processing [15], utilization of personal information based on user consent [16], and methods of statistical disclosure control [17], RDA-recommended data sharing [18], responsible data governance [19], Protocols for protecting personal information using blockchain technology [20], clustering without disclosing personal information [21], AI-driven software for privacy protection [22], and methods for protecting individual privacy based on differences in identifiability [23] are some instances.

Previous studies related to privacy in the scope of COVID-19 examined a range of essential topics, like privacy concerns in technological approaches, privacy-preserving techniques and approaches for medical information, privacy specifications amid the electronic surge, private data confidentiality frameworks, ethical considerations with ICT used to combat the disease outbreak, balancing privacy, and protecting the public from the epidemic, and privacy issues in contact-tracing apps. Sowmiya *et al.* [24] conducted a survey and found privacy and security concerns with contact-tracing apps intended to stop the spread of COVID-19. They also provided helpful suggestions for protecting personal data in the cloud. Vadrevu *et al.* [25] examined various cutting-edge techniques for protecting privacy in video surveillance and medical record. Using a set of eight questions, Zeinalipour and Claramunt [26] examined the primary post-COVID-19 privacy concerns with contact-tracing apps. Their study provides valuable insight into the advantages and disadvantages of contact-tracing apps.

Schmidtke [27] explored the privacy concerns and limitations of deploying digital solutions utilizing location data to contain COVID-19 outbreaks. The author emphasized the necessity of context-specific models when tackling privacy concerns in preventing COVID-19-like pandemics. Shuja *et al.* [28] explored COVID-19 open-source data privacy. The authors proposed an information unification to address the pandemic and anonymity to protect user privacy. Sihombing *et al.* [29] examined privacy protection measures in 9 countries. Some other scholars have also published assessments of the COVID-19-era privacy protection mechanisms specific to each country [30]–[32].

In addition, some prior works have centered on the measuring of privacy threats [33], the type of digital solution (for instance, centralized or decentralized) [34], public acceptance of digital apps [35], privacy concerns of technological advancements in COVID-19 context [36], concerns over aggressive use of ICT in the face of a global epidemic [37], and privacy concerns in healthcare during COVID-19 period [38].

Privacy and COVID-19 research began in 2020. Scholars have since adopted this term to study the development of related technologies. This study uses bibliometrics to analyze scientific publications on

health privacy. The bibliometric analysis examines research domain knowledge structure and growth using associated publications. These will be significant and valuable findings to help the researchers or scholars comprehend the policy changes and related development within the domain.

This work is organized as follows: in section 2, the method of literature identification, searching, filtering process and analysis were discussed. In section 3, results and a discussion of the findings were presented. Finally, section 4 summarizes the concluding remarks of this review.

## 2. METHOD

This research obtained all its data from the Scopus database as of July 2022. The Scopus database has been used since it is the "biggest single abstract and indexing database ever developed" [39] and also the most excellent accessible abstract and citation source for searching publications [40], respectively. Some of the statistical summariess have been gathered from the manuscripts that have been collected. These results include the following: type of access, year of publication, name of the researcher, subject area, type of document, the title of the source, keywords, affiliation, country, type of source, and type of language.

## 3. DISCUSSIONS AND RESULT

The information that was gathered was evaluated to establish the following: type of document, type of source, yearly growth, type of languages, subject areas, keywords, individual country productivity, authorships, and several citations. The majority of the findings are presented using percentages and frequency distributions. For the annual increase, we provided information in the form of yearly documents, along with their frequencies, percentages, and percentage distribution, through July 1, 2022.

This section is determined to explain the finding of the study and provide a thorough analysis. Several visual elements (such as tables, graphs, and figures) can be used to illustrate findings and facilitate comprehension [14], [15]. The discussion may be broken up into several sub-sections.

### 3.1. Document and source type

First, document types and source types were identified from the data. Sources include journals, conference proceedings, book series, books, and trade publications. Conference papers listed as sources were distinct from those listed as documents [41]. Conference papers are papers that were first given at conferences but were later expanded into full-length journal articles. Even though the document type was originally a conference paper, it has since been published in other formats, such as conference proceedings or a book chapter. The research revealed six distinct publication forms covering topics related to privacy and COVID-19: journals, conference proceedings, book series, trade journals, books, and undefined. Table 1 shows that 58.16% of publications appeared in journals, whereas 27.16% were presented in conferences. The other documents are around 15%, with each category having some% of the total records. The lowest among them were undefined, with less than 1%. Table 2 presents four document types. The article has the highest representation among the document type at (51.79%), followed by the conference paper with 33.69%. Book chapters and reviews also produce a sizable amount of resources, accounted for 7.34% and 7.18%, respectively.

Table 1. Source category

| Source category | Frequency | Percentage (%) |
|---|---|---|
| Journals | 713 | 58.16 |
| Conference proceeding | 333 | 27.16 |
| Book series | 96 | 7.83 |
| Book | 72 | 5.87 |
| Trade journal | 9 | 0.73 |
| Undefined | 3 | 0.24 |
| Total | 1226 | 100.00 |

Table 2. Document category

| Document category | Frequency | Percentage (%) |
|---|---|---|
| Article | 635 | 51.79 |
| Conference paper | 413 | 33.69 |
| Book chapter | 90 | 7.34 |
| Review | 88 | 7.18 |
| Total | 1226 | 100.00 |

### 3.2. Year of publication

The first research on privacy and COVID-19 was published in 2020 by Bradford, Aboy, and Liddell [42] in their paper titled, "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes". The number of publications covering this topic has been rising, and this trend is expected to continue through 2021. On the other hand, it was significantly raised as shown in Figure 1. From Figure 1, it can be observed that publications related to privacy and health issues, in general, have been increasing twice their size; this is because of the privacy concerns during lockdown have been an increase. The year 2022 is predicted to have the most significant number of publications since the pandemic began. The year 2023 is still a ways off, but several articles have already been planned and indexed in the Scopus database.

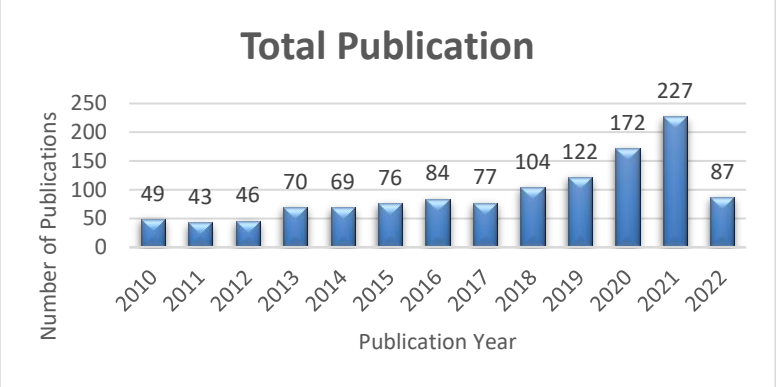



Figure 1. Summary of publications by year

### 3.3. Documents language

As can be seen from Table 3, nearly all of the retrieved papers were originally published in English (99.43%). Only a small fraction of the documents analyzed were written in languages outside English; they were Portuguese, Dutch, French, and Italian.

Table 3. Languages used

| Language | Frequency | Percentage (%) |
|---|---|---|
| English | 1226 | 99.43 |
| Portuguese | 3 | 0.24 |
| Dutch | 2 | 0.16 |
| French | 1 | 0.08 |
| Italian | 1 | 0.08 |
| Total | 1233 | 100.00 |

### 3.4. Subject area

The research also categorized the published papers by topic. The majority of the research on privacy and COVID-19 were in computer science, which represented 29.54% of the total records, followed by medicine (19.18%), engineering (12.77%), social sciences (9.77%), and mathematics (4.17%). The other subject areas covered privacy, and COVID-19 research is tabulated in Table 4.

Table 4. Subject area

| Subject area | TP | Percentage (%) |
|---|---|---|
| Computer science | 659 | 29.54 |
| Medicine | 428 | 19.18 |
| Engineering | 285 | 12.77 |
| Social sciences | 218 | 9.77 |
| Mathematics | 93 | 4.17 |
| Decision sciences | 89 | 3.99 |
| Health professions | 82 | 3.68 |
| Business, management, and accounting | 61 | 2.73 |
| Nursing | 54 | 2.42 |
| Biochemistry, genetics, and molecular biology | 47 | 2.11 |

### 3.5. Keyword analysis

The VOSviewer software [43], a tool for creating and visualizing bibliometric networks, created a network between the author keywords and the publications that used them. Figure 2 shows a network visualization of the authors' keywords. The relationships between the keywords are illustrated using colour, square size, text size, and the thickness of connecting lines. Keywords that share the same hue, for instance, appeared to be grouped. Therefore, in this research, privacy, COVID-19, pandemic, digital contact tracing, pandemics, and coronavirus infection have the same colour (yellow), indicating a close association between the terms and their frequent cooccurrence together. Considering the frequency of occurrences (after data cleaning on the author keywords), the keywords such as privacy and human were the most used in the privacy and COVID-19 study. The top 20 keywords used in the privacy and COVID-19 research are shown in Table 5.

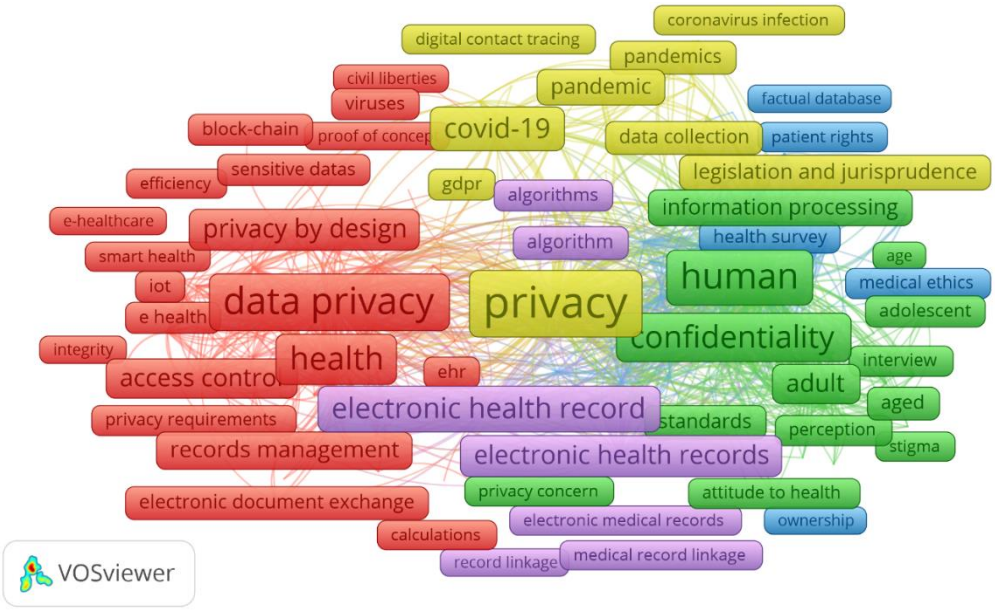



Figure 2. Keyword maps analysis

Table 5. Keywords

| Keyword | Frequency |
|---|---|
| Privacy | 594 |
| Data privacy | 383 |
| Human | 333 |
| Health | 241 |
| Confidentiality | 218 |
| Article | 195 |
| Health care | 195 |
| Electronic health record | 154 |
| Security | 136 |
| Privacy-preserving | 132 |
| COVID-19 | 117 |

### 3.6. Geographical distribution

Scholars from 79 various countries published the collected articles. Table 6 shows the top 20 nations in the privacy and COVID-19 publications. The U.S published the most documents with 353 publications, followed by China (127), India (115), and Canada (96). The United States topped the list for total citations with 3026, followed by China (1872).

### 3.7. Citation analysis

Moreover, we utilized Harzing's Publish or Perished application to look for citation metrics associated with the retrieved information. This application uses data extracted from the Scopus database to analyze the citation score and total citations for each publication based on sources found in Google Scholar. Table 7 summarizes the retrieved documents' citation metrics as 1st July 2022. The summary provides

information on the total number of citations produced each year and the number of citations made by each author and article.

The top 20 cited articles in privacy and COVID-19 were listed in Table 8 (in appendix). An article entitled "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online" by Bansal, Zahedi, and Gefen [44] obtained the most significant number of citations overall, with a total of 529 citations, according to the Scopus database (44 citations per year) [45], [46]. The same paper also acquired the maximum number of citations, with a total of 900 citations and 75 citations each year, according to the total citations tracked by Google Scholar as of the 1st of July 2022.

Table 6. Top 10 countries contributed to privacy and COVID-19 publications

| Country | Total publication | Total citation |
|---|---|---|
| United States | 353 | 3026 |
| China | 127 | 1872 |
| India | 115 | 1300 |
| Canada | 96 | 651 |
| United Kingdom | 84 | 1083 |
| Australia | 80 | 828 |
| Germany | 65 | 664 |
| Saudi Arabia | 40 | 349 |
| South Korea | 34 | 350 |
| Netherlands | 33 | 313 |

Table 7. Metrics

| Reference date | 1/7/2022 |
|---|---|
| Publication years | 2010-2022 |
| Citation years | 12(2010-2022) |
| Papers | 1226 |
| Citations | 15593 |
| Citations/year | 1299.42 |
| Citations/paper | 12.72 |
| Citations/author | 5602.78 |
| Papers/author | 525.66 |
| Authors/paper | 3.36 |
| h_index | 59 |
| g_index | 94 |
| hc_index | 54 |
| hI_index | 13.81 |
| hI_norm | 32 |

## 4. CONCLUSION

This article provides a bibliometric review to understand better the trends, historical thinking, predictions, and contributions found in the privacy and COVID-19 literature. This research examines how privacy studies expanded in the last 11 years with more COVID-19 articles. 2020 saw 172 publications, up from 104 in 2018. As of June 2022, the total number of privacy and COVID-19 publications was 87. Privacy and COVID-19 articles had 3.65 authors on average. This research also illustrates that the scope primarily covered in the privacy and COVID-19 study is related to data privacy and humans based on the authors' keywords in their work. Other possible subjects worth investigating include privacy and contact tracing apps, the privacy policy of IoT, privacy and blockchain, medical informatics, and privacy-preserving that can be conducted as future works. The U.S has the most publications and citations compared to Canada and the UK. We advocate conducting privacy and COVID-19 research in developing nations because of the technology's global impact. The study's findings and projections opine that COVID-19 and privacy will serve as the impetus for a number of long- and short-term policy changes, necessitating researchers' theoretical and empirical focus.

Our research is restricted in several ways due to the characteristics of the database that was utilized. Even though Scopus is a vast database, there are still unindexed journals whose papers may have been disregarded. This study only focused on privacy and COVID-19 based on document titles. Thus, all additional privacy and COVID-19-related publications without the title were likewise discarded. There is no ideal search query; there is a possibility of obtaining false positive and negative results. Our citation analysis used Scopus and Google Scholar data. Total publications and citations are only correct at search time. This research is one of the first to delve into the specific bibliometric indicators of privacy and COVID-19.

## APPENDIX

Table 8. Top 20 articles in privacy and COVID-19 study

| S/No | Paper title | Authors | Years | Journal name | Cited by | Cites per year | GSc* Cites by | GSc* cites per year |
|---|---|---|---|---|---|---|---|---|
| 1 | The impact of personal dispositions on information sensitivity, privacy concerns, and trust in disclosing health information online | G. Bansal, F. "Mariam" Zahedi, and D. Gefen | 2010 | Decision Support Systems | 529 | 44.08 | 900 | 75.00 |
| 2 | Security and privacy in electronic health records: A systematic literature review | J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval | 2013 | Journal of Biomedical Informatics | 384 | 32.00 | 660 | 55.00 |
| 3 | Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology | G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella | 2018 | Sustainable Cities and Society | 329 | 27.42 | 495 | 41.25 |
| 4 | Security and Privacy in Smart Health: Efficient Policy-Hiding Attribute-Based Access Control | Y. Zhang, D. Zheng, and R. H. Deng | 2018 | IEEE Internet of Things Journal | 249 | 20.75 | 297 | 24.75 |
| 5 | Unaddressed privacy risks in accredited health and wellness apps: A systematic cross-sectional assessment | K. Huckvale, J.T. Prieto, M. Tilney, P.-J. Benghozi, and J. Car | 2015 | BMC Medicine | 227 | 18.92 | 390 | 32.50 |
| 6 | A review of the state-of-the-art privacy-preserving approaches in the e-Health clouds | A. Abbas and S. U. Khan | 2014 | IEEE Journal of Biomedical and Health Informatics | 226 | 18.83 | 336 | 28.00 |
| 7 | Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain | A. Zhang and X. Lin | 2018 | Journal of Medical Systems | 219 | 18.25 | 334 | 27.83 |
| 8 | Availability and quality of mobile health app privacy policies | A. Sunyaev, T. Dehling, P. L. Taylor, and K. D. Mandl | 2015 | Journal of the American Medical Informatics Association | 194 | 16.17 | 350 | 29.17 |
| 9 | Health information privacy concerns, antecedents, and information disclosure intention in online health communities | X. Zhang, S. Liu, X. Chen, L. Wang, B. Gao, and Q. Zhu | 2018 | Information and Management | 171 | 14.25 | 223 | 18.58 |
| 10 | Patients want granular privacy control over health information in electronic medical records | K. Caine and R. Hanania | 2013 | Journal of the American Medical Informatics Association | 169 | 14.08 | 281 | 23.42 |
| 11 | Privacy and Security in Mobile Health Apps: A Review and Recommendations | B. Martínez-Pérez, I. de la Torre-Díez, and M. López-Coronado | 2015 | Journal of Medical Systems | 167 | 13.92 | 317 | 26.42 |
| 12 | A privacy preserving three-factor authentication protocol for e-Health clouds | Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He | 2016 | Journal of Supercomputing | 159 | 13.25 | 193 | 16.08 |
| 13 | Information Technology-Based Tracing Strategy in Response to COVID-19 in South Korea - Privacy Controversies | S. Park, G. J. Choi, and H. Ko | 2020 | JAMA - Journal of the American Medical Association | 156 | 13.00 | 296 | 24.67 |
| 14 | Is deidentification sufficient to protect health privacy in research? | M. A. Rothstein | 2010 | American Journal of Bioethics | 147 | 12.25 | 235 | 19.58 |
| 15 | Privacy-preserving personal health record using multi-authority attribute-based encryption with revocation | H. Qian, J. Li, Y. Zhang, and J. Han | 2014 | International Journal of Information Security | 145 | 12.08 | 199 | 16.58 |

Table 8. Top 20 articles in privacy and COVID-19 study (continue)

| S/No | Paper title | Authors | Years | Journal name | Cited by | Cites per year | GSc* Cites by | GSc* cites per year |
|---|---|---|---|---|---|---|---|---|
| 16 | Views on health information sharing and privacy from primary care practices using electronic medical records | G. Perera, A. Holbrook, L. Thabane, G. Foster, and D. J. Willison | 2011 | International Journal of Medical Informatics | 143 | 11.92 | 243 | 20.25 |
| 17 | Exploring the far side of mobile health: Information security and privacy of mobile health apps on ios and android | T. Dehling, D.-W. Inf, F. Gao, S. Schneider, and A. Sunyaev | 2015 | JMIR mHealth and uHealth | 138 | 11.50 | 251 | 20.92 |
| 18 | Publishing data from electronic health records while preserving privacy: A survey of algorithms | A. Gkoulalas-Divanis, G. Loukides, and J. Sun | 2014 | Journal of Biomedical Informatics | 135 | 11.25 | 215 | 17.92 |
| 19 | Analysis of the security and privacy requirements of cloud-based electronic health records systems | J. JPC Rodrigues, I. de la Torre, G. Fernández, and M. López-Coronado | 2013 | Journal of Medical Internet Research | 128 | 10.67 | 194 | 16.17 |
| 20 | Healthchain: A Blockchain-Based Privacy Preserving Scheme for Large-Scale Health Data | J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu | 2019 | IEEE Internet of Things Journal | 122 | 10.17 | 158 | 13.17 |

*GSc=Google Scholar

## REFERENCES


[1] A. Majeed and S. O. Hwang, "A Comprehensive Analysis of Privacy Protection Techniques Developed for COVID-19 Pandemic," *IEEE Access*, vol. 9, pp. 164159–164187, 2021, doi: 10.1109/ACCESS.2021.3130610.

[2] C. S. Wagner, X. Cai, Y. Zhang, and C. V. Fry, "One-Year In: COVID-19 Research at the International Level in CORD-19 Data," *SSRN Electronic Journal*, 2021, doi: 10.2139/ssrn.3874974.

[3] Y. Nishimura *et al.*, "Burnout of Healthcare Workers Amid the COVID-19 Pandemic: A Follow-Up Study," *International Journal of Environmental Research and Public Health*, vol. 18, no. 21, p. 11581, Nov. 2021, doi: 10.3390/ijerph182111581.

[4] G. Newlands, C. Lutz, A. Tamò-Larrieux, E. F. Villaronga, R. Harasgama, and G. Scheitlin, "Innovation under pressure: Implications for data privacy during the Covid-19 pandemic," *Big Data & Society*, vol. 7, no. 2, p. 205395172097668, Jul. 2020, doi: 10.1177/2053951720976680.

[5] R. A. Fahey and A. Hino, "COVID-19, digital privacy, and the social limits on data-focused public health responses," *International Journal of Information Management*, vol. 55, p. 102181, Dec. 2020, doi: 10.1016/j.ijinfomgt.2020.102181.

[6] F. Hassandoust, S. Akhlaghpour, and A. C. Johnston, "Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective," *Journal of the American Medical Informatics Association*, vol. 28, no. 3, pp. 463–471, Mar. 2021, doi: 10.1093/jamia/ocaa240.

[7] N. Y. Ahn, J. E. Park, D. H. Lee, and P. C. Hong, "Balancing Personal Privacy and Public Safety During COVID-19: The Case of South Korea," *IEEE Access*, vol. 8, pp. 171325–171333, 2020, doi: 10.1109/ACCESS.2020.3025971.

[8] H. O'Connor, W. J. Hopkins, and D. Johnston, "For the greater good? Data and disasters in a post-COVID world," *Journal of the Royal Society of New Zealand*, vol. 51, no. sup1, pp. S214–S231, May 2021, doi: 10.1080/03036758.2021.1900297.

[9] A. Zwitter and O. J. Gstrein, "Big data, privacy and COVID-19 – learning from humanitarian expertise in data protection," *Journal of International Humanitarian Action*, vol. 5, no. 1, p. 4, Dec. 2020, doi: 10.1186/s41018-020-00072-6.

[10] F. Almeida, J. Duarte Santos, and J. Augusto Monteiro, "The Challenges and Opportunities in the Digitalization of Companies in a Post-COVID-19 World," *IEEE Engineering Management Review*, vol. 48, no. 3, pp. 97–103, Sep. 2020, doi: 10.1109/EMR.2020.3013206.

[11] K. Michael and R. Abbas, "Behind COVID-19 Contact Trace Apps: The Google–Apple Partnership," *IEEE Consumer Electronics Magazine*, vol. 9, no. 5, pp. 71–76, Sep. 2020, doi: 10.1109/MCE.2020.3002492.

[12] S. Nisar, M. A. Zuhaib, A. Ulasyar, and M. Tariq, "A Privacy-Preserved and Cost-Efficient Control Scheme for Coronavirus Outbreak Using Call Data Record and Contact Tracing," *IEEE Consumer Electronics Magazine*, vol. 10, no. 2, pp. 104–110, Mar. 2021, doi: 10.1109/MCE.2020.3038023.

[13] S. Nisar, M. A. Zuhaib, A. Ulasyar, and M. Tariq, "A robust tracking system for COVID-19 like pandemic using advanced hybrid technologies," *Computing*, May 2021, doi: 10.1007/s00607-021-00946-6.

[14] S. McLennan, L. A. Celi, and A. Buyx, "COVID-19: Putting the General Data Protection Regulation to the Test," *JMIR Public Health and Surveillance*, vol. 6, no. 2, p. e19279, May 2020, doi: 10.2196/19279.

[15] M. Ienca and E. Vayena, "On the responsible use of digital data to tackle the COVID-19 pandemic," *Nature Medicine*, vol. 26, no. 4, pp. 463–464, Apr. 2020, doi: 10.1038/s41591-020-0832-5.

[16] B. M. Knoppers *et al.*, "Modeling consent in the time of COVID-19," *Journal of Law and the Biosciences*, vol. 7, no. 1, Jul. 2020, doi: 10.1093/jlb/lsaa020.

[17] S. Sauermann, C. Kanjala, M. Templ, and C. C. Austin, "Preservation of Individuals' Privacy in Shared COVID-19 Related Data," *SSRN Electronic Journal*, 2020, doi: 10.2139/ssrn.3648430.

[18] C. C. Austin *et al.*, "Fostering global data sharing: highlighting the recommendations of the Research Data Alliance COVID-19 working group," *Wellcome Open Research*, vol. 5, p. 267, Nov. 2020, doi: 10.12688/wellcomeopenres.16378.1.

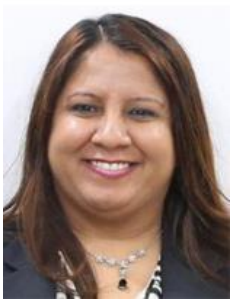
[19] B. de A. Almeida *et al.*, "Preservação da privacidade no enfrentamento da COVID-19: dados pessoais e a pandemia global," *Ciência & Saúde Coletiva*, vol. 25, no. suppl 1, pp. 2487–2492, Jun. 2020, doi: 10.1590/1413-81232020256.1.11792020.

[20] K. Yu, L. Tan, X. Shang, J. Huang, G. Srivastava, and P. Chatterjee, "Efficient and Privacy-Preserving Medical Research Support Platform Against COVID-19: A Blockchain-Based Approach," *IEEE Consumer Electronics Magazine*, vol. 10, no. 2, pp. 111–120, Mar. 2021, doi: 10.1109/MCE.2020.3035520.
[21] W. Houfaf-Khoufaf, G. Touya, and A. Le Guilcher, "Geographically masking addresses to study COVID-19 clusters," *Cartography and Geographic Information Science*, pp. 1–15, Oct. 2021, doi: 10.1080/15230406.2021.1977709.
[22] H. Diddee and B. Kansra, "CrossPriv: User Privacy Preservation Model for Cross-Silo Federated Software," in *Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering*, Dec. 2020, pp. 1370–1372. doi: 10.1145/3324884.3418911.
[23] V. K. M. Pavan Kumar Vadrevu, Sri Krishna Adusumalli, "A hybrid approach for personal differential privacy preservation in homogeneous and heterogeneous health data sharing," *High Technology Letters*, vol. 26, no. 9, pp. 1223–1239, 2020, doi: 10.37896/HTL26.09/1813.
[24] B. Sowmiya, V. S. Abhijith, S. Sudersan, R. Sakthi Jaya Sundar, M. Thangavel, and P. Varalakshmi, "A Survey on Security and Privacy Issues in Contact Tracing Application of Covid-19," *SN Computer Science*, vol. 2, no. 3, p. 136, May 2021, doi: 10.1007/s42979-021-00520-z.
[25] S. K. S. Pavan Kumar Vadrevu, Sri Krishna Adusumalli, Vamsi Krishna Mangalapalli, "A Review on Privacy Preservation Techniques in Surveillance and Health Care Data Publication," *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT)*, vol. 9, no. 5, pp. 356–367, 2021, doi: 10.17577/IJERTCONV9IS05077.
[26] D. Zeinalipour-Yazti and C. Claramunt, "COVID-19 Mobile Contact Tracing Apps (MCTA): A Digital Vaccine or a Privacy Demolition?," in *2020 21st IEEE International Conference on Mobile Data Management (MDM)*, Jun. 2020, pp. 1–4. doi: 10.1109/MDM48529.2020.00020.
[27] H. R. Schmidtke, "Location-aware systems or location-based services: a survey with applications to CoViD-19 contact tracking," *Journal of Reliable Intelligent Environments*, vol. 6, no. 4, pp. 191–214, Dec. 2020, doi: 10.1007/s40860-020-00111-4.
[28] J. Shuja, E. Alanazi, W. Alasmary, and A. Alashaikh, "COVID-19 open source data sets: a comprehensive survey," *Applied Intelligence*, vol. 51, no. 3, pp. 1296–1325, Mar. 2021, doi: 10.1007/s10489-020-01862-6.
[29] E. N. A. . Sihombing, "Legal Securities Against Privacy Data for Covid-19 Patients in Indonesia," *Veteran Law Review*, vol. 4, no. 1, p. 35, Apr. 2021, doi: 10.35586/velrev.v4i1.2618.
[30] V. von Wyl *et al.*, "Drivers of Acceptance of COVID-19 Proximity Tracing Apps in Switzerland: Panel Survey Analysis," *JMIR Public Health and Surveillance*, vol. 7, no. 1, p. e25701, Jan. 2021, doi: 10.2196/25701.
[31] B. M. Zimmermann, A. Fiske, S. McLennan, A. Sierawska, N. Hangel, and A. Buyx, "Motivations and Limits for COVID-19 Policy Compliance in Germany and Switzerland," *International Journal of Health Policy and Management*, Apr. 2021, doi: 10.34172/ijhpm.2021.30.
[32] J. Kim and M.-P. Kwan, "An Examination of People's Privacy Concerns, Perceptions of Social Benefits, and Acceptance of COVID-19 Mitigation Measures That Harness Location Information: A Comparative Study of the U.S. and South Korea," *ISPRS International Journal of Geo-Information*, vol. 10, no. 1, p. 25, Jan. 2021, doi: 10.3390/ijgi10010025.
[33] G. Jung, H. Lee, A. Kim, and U. Lee, "Too Much Information: Assessing Privacy Risks of Contact Trace Data Disclosure on People With COVID-19 in South Korea," *Frontiers in Public Health*, vol. 8, Jun. 2020, doi: 10.3389/fpubh.2020.00305.
[34] V. Shubina, S. Holcer, M. Gould, and E. S. Lohan, "Survey of Decentralized Solutions with Mobile Devices for User Location Tracking, Proximity Detection, and Contact Tracing in the COVID-19 Era," *Data*, vol. 5, no. 4, p. 87, Sep. 2020, doi: 10.3390/data5040087.
[35] S. Altmann *et al.*, "Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Study," *JMIR mHealth and uHealth*, vol. 8, no. 8, p. e19857, Aug. 2020, doi: 10.2196/19857.
[36] M. A. Ferrag, L. Shu, and K.-K. R. Choo, "Fighting COVID-19 and Future Pandemics With the Internet of Things: Security and Privacy Perspectives," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 9, pp. 1477–1499, Sep. 2021, doi: 10.1109/JAS.2021.1004087.
[37] S. Park, G. J. Choi, and H. Ko, "Information Technology–Based Tracing Strategy in Response to COVID-19 in South Korea—Privacy Controversies," *JAMA*, vol. 323, no. 21, p. 2129, Jun. 2020, doi: 10.1001/jama.2020.6602.
[38] Y. He, A. Aliyu, M. Evans, and C. Luo, "Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review," *Journal of Medical Internet Research*, vol. 23, no. 4, p. e21747, Apr. 2021, doi: 10.2196/21747.
[39] J. F. Burnham, "Scopus database: a review," *Biomedical Digital Libraries*, vol. 3, no. 1, p. 1, Dec. 2006, doi: 10.1186/1742-5581-3-1.
[40] A. A. Chadegani *et al.*, "A Comparison between Two Main Academic Literature Collections: Web of Science and Scopus Databases," *Asian Social Science*, vol. 9, no. 5, Apr. 2013, doi: 10.5539/ass.v9n5p18.
[41] W. M. Sweileh, S. W. Al-Jabi, A. S. AbuTaha, S. H. Zyoud, F. M. A. Anayah, and A. F. Sawalha, "Bibliometric analysis of worldwide scientific literature in mobile - health: 2006–2016," *BMC Medical Informatics and Decision Making*, vol. 17, no. 1, p. 72, Dec. 2017, doi: 10.1186/s12911-017-0476-7.
[42] L. Bradford, M. Aboy, and K. Liddell, "COVID-19 contact tracing apps: a stress test for privacy, the GDPR, and data protection regimes," *Journal of Law and the Biosciences*, vol. 7, no. 1, Jul. 2020, doi: 10.1093/jlb/lsaa034.
[43] N. J. van Eck and L. Waltman, "Visualizing Bibliometric Networks," in *Measuring Scholarly Impact*, Cham: Springer International Publishing, 2014, pp. 285–320. doi: 10.1007/978-3-319-10377-8_13.
[44] G. Bansal, F. "Mariam" Zahedi, and D. Gefen, "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems*, vol. 49, no. 2, pp. 138–150, May 2010, doi: 10.1016/j.dss.2010.01.010.
[45] X. Zhao, J. Zuo, G. Wu, and C. Huang, "A bibliometric review of green building research 2000–2016," *Architectural Science Review*, vol. 62, no. 1, pp. 74–88, Jan. 2019, doi: 10.1080/00038628.2018.1485548.
[46] A. S. Ali and Z. F. Zaaba, "A Study on Contact Tracing Apps for Covid-19: Privacy and Security Perspective," *Webology*, vol. 18, no. 1, pp. 341–359, Apr. 2021, doi: 10.14704/WEB/V18I1/WEB18093.

## BIOGRAPHIES OF AUTHORS

**Auwal Shehu Ali** received a Bachelor of Science (Second Class Hons.) in Computer Science (Hons.) from Bayero University Kano, Nigeria, and a master's degree in Computer Science from Bayero University Kano, Nigeria. He is pursuing a PhD in Computer Science with Universiti Sains Malaysia (USM), Malaysia. He is also a lecturer with the Department of Computer Sciences, Bayero University Kano, Nigeria. His research interest includes security and privacy policy, cyber security, information security, privacy enhancing technology (PET), deferential privacy, machine learning (ML), and NLP. He can be contacted at email: asali.cs@buk.edu.ng.

**Zarul Fitri Zaaba** was born in Kuala Lumpur, Malaysia, in 1981. He received his BSc in Information Technology from the Universiti Utara Malaysia in 2003, an MSc in Information Security from the Royal Holloway University of London in 2007, and a PhD from the University of Plymouth, the United Kingdom, in 2014. He is currently a Senior Lecturer at the School of Computer Sciences, Universiti Sains Malaysia (USM). Before joining USM, he had worked for a few years with the government and semi-government sectors. He specialises in security management, data privacy, web security, and the human aspects of security. He is also actively involved in Science, Technology, Engineering & Mathematics (STEM) education and has been appointed a Master Trainer in computational thinking. He can be contacted at email: zarulfitri@usm.my.



**Manmeet Mahinderjit Singh** is an Associate Professor born in Perak, Malaysia, in 1978. She received her BSc and MSc in Computer Sciences from the Universiti Sains Malaysia and a PhD from the University of Queensland Australia. Her research interests focus on computer and data security trusted models and systems and cyber-crime. She is also actively involved in Science, Technology, Engineering & Mathematics (STEM) education and has been appointed a Master Trainer in computational thinking. She can be contacted at email: manmeet@usm.my.