

Bibliometric Analysis of Security Concerns in Hybrid Cloud Adoption in Small and Medium-Sized Enterprises SMEs

Zakaria, Alrababah¹ & Jessnor Elmy Binti Mat Jizat^{2*}

¹& ²Faculty of Management and Economics, Universiti Pendidikan Sultan Idris (UPSI), Tanjung Malim, Perak, Malaysia

Email Address:

P2020200@siswa.upsi.edu.my (Zakaria, Alrababah), jessnor@fpe.upsi.edu.my (Jessnor, Elmy Binti Mat Jizat)

*Corresponding author: jessnor@fpe.upsi.edu.my (Jessnor, Elmy Binti Mat Jizat)

To Cite This Article:

Zakaria, A., & Mat Jizat, J. E.. (2024). Bibliometric Analysis of Security Concerns in Hybrid Cloud Adoption in Small and Medium-Sized Enterprises SMEs. *CMU Academy Journal of Management and Business Education*, 3(2), 29–38. <https://doi.org/10.53797/cjmbe.v3i2.4.2024>

Abstract: Hybrid cloud computing is an essential technological innovation that enhances the productivity and efficiency of its adopters. However, security concerns remain a great challenge to its adoption by small and medium-sized enterprises. This bibliometric analysis, therefore, aims to examine the trend of research publications tailored to addressing the security concern of hybrid cloud computing adoption by SMEs. This study identified and screened relevant publications retrieved from the Scopus database. A bibliometric study approach was used to examine publication trends, citations and general impacts. With the aid of Microsoft Excel and VOS viewer, metadata was extracted, analysed and visualised to answer the research questions raised. The findings revealed that research publications on hybrid cloud computing security in SMEs began insignificantly in 2009 through 2014. Significant research attention from scholars began in 2015. It was also found that India, the United States, China and the United Kingdom led the country of affiliation of the top authors on publications related to security topics in hybrid cloud computing adoption by SMEs. This implies that some continents, like Africa and Southern America, are still lagging. These findings will inform scholarly efforts to develop more effective strategies of neutralising security threats facing small and medium-sized enterprises in adopting hybrid cloud computing for their businesses. We equally identified the implications of the findings of this study for stakeholders in the field, including the researchers, SME managers, government and practitioners in the industry.

Keywords: Hybrid cloud computing, SMEs, Security, Bibliometric analysis, cloud computing

1. Introduction

In recent years, the campaign for adopting hybrid cloud solutions has been global and has been increasing among small and medium-sized enterprises (SMEs). Hybrid cloud computing is the blend of the features of the public and private cloud in order to maintain balance between scalability and control by organisations (Majengo & Mbise, 2022; Nyamwesa, 2024). The need for cost-effectiveness in IT infrastructure, as well as flexibility and scalability, drives this. According to (Mwangi et al., 2018), SMEs are currently restructuring their IT cost and embracing IT infrastructure capable of putting them in a vantage position in the business. Hybrid cloud computing enables SMEs to save on the cost of purchasing hardware and software when adopting technology in their enterprise (Gangadhar & Shaikh, 2020b). The world hybrid cloud market as at 2021 was estimated to be \$85 billion, with projections indicating an increase to \$262 billion by 2027 (Vailshery, 2024). Generally, SMEs are mainly known for limited human (multi-tasked) and material resources and informal management (Chaudhary et al., 2023). Despite the innumerable challenges, some SMEs still continue to wax stronger by embracing technological innovations. According to (Gupta et al., 2018), cloud enterprise resource planning (ERP) has been instrumental to SMEs' adoption of the hybrid cloud solution without any need to procure and install IT hardware and software.

The increased advocacy and reliance of SMEs on hybrid cloud infrastructures amidst increasing cyber threats justify the need to understand the extent to which research is conducted to secure adopters. Many organisations do not have absolute trust and confidence in the ability of the cloud service providers to protect their data and privacy (Nyamwesa, 2024)

which usually necessitate the blend of two clouds when adopting it. It is conspicuously observed that small and medium-sized enterprises are particularly vulnerable to cyber threats in their bid to adopt hybrid cloud solutions for their business. This is due to limited expertise, budgets and knowledge of sophisticated security measures and practices (Patil et al., 2023).

Security and privacy issues remain a significant obstacle to the smooth adoption of hybrid cloud computing services by SMEs (Alrababah, 2023). Despite relief from not procuring ICT hardware, the need for guaranteed safety by vendors or service providers is still a concern. According to Gupta et al. (2017), cyberthreats become a challenge because sensitive data of the organisation, including financial and customer details, are kept under the company's physical location. The location where this sensitive data is kept may not be totally free from cyber-attacks.

Research activities are generally concentrated on general cloud security and cloud adoption (Gangadhar & Shaikh, 2020a; Jayeola et al., 2022) with uncommon publications in understanding hybrid cloud security, specifically addressing SMEs (Chaudhary et al., 2023). It is, therefore, important to map the research effort in this area using bibliometric analysis. A bibliometric analysis remains a systematic and scientific way to determine the current state of research on hybrid cloud security in SMEs. This type of research enables researchers to understand the trends and emerging themes on how academics and industry have developed to address SME-specific hybrid cloud computing adoption-related challenges. This study aimed to map the scientific research effort in topics related to security in the hybrid cloud computing in the SMEs.

Research questions

The following research questions are raised in this study:

- What is the global trend of publications on hybrid cloud computing security in SMEs?
- What are the most productive journals on research on hybrid cloud computing security on SMEs?
- What are the top 10 countries in publications and citations about security concerns in adopting hybrid cloud computing by SMEs?
- What is the intellectual structure of security concerns and solutions in hybrid cloud computing research?
- What is the trend of themes and emerging topics in hybrid cloud computing security in SMEs?

2. Method

2.1 Data source and search strategy

The SCOPUS is solely used as data source in this study being a n authoritative and dependable research database that is popularly used by researchers around the world. We search the database using abstract, title, and keywords. The search strategy was ("hybrid cloud" OR "cloud computing" OR "cloud" OR "multi-cloud") AND ("security" OR "safety" OR "protection" OR "risk") AND ("concern" OR "issue" OR "challenge" OR "threat") AND ("solution" OR "strategy" OR "approach" OR "measure") AND ("small" OR "medium" OR "SME" OR "enterprise") AND ("adoption" OR "implementation" OR "integration" OR "transition"). Only article available in the Scopus database as of December 21, 2024, when the search was conducted were included. Figure 1 presents the flow of the database search, identification, screening and eligibility.

2.2 Identification of Sources

We adopted the guidelines for conducting systematic reviews popularly known as Preferred Reporting Items for Systematic Reviews and Meta-analyses (PRISMA) (Page et al., 2021; Selçuk, 2019). This guideline enables us to be transparent and explicit about the steps we took in identifying, extracting and reporting used in the bibliometric review see Figure 1.

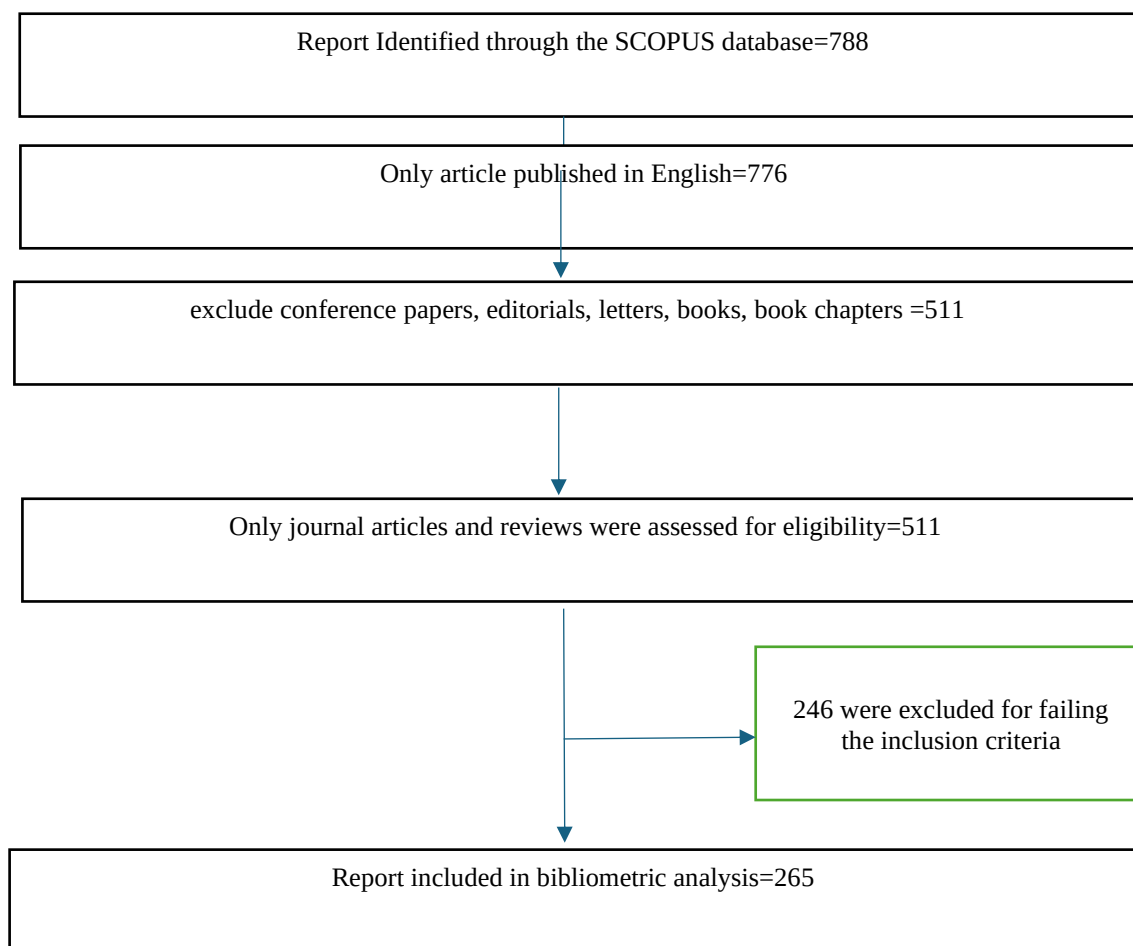


Figure 1. Flow chart of reports related to hybrid cloud computing security in SMEs

Figure 1 presents the flow chart of how we conducted our search to identify relevant literature related to hybrid cloud computing security in SMEs. Based on predetermined inclusion criteria. The inclusion criteria are peer-reviewed journal articles and reviews published in English between 2009 and 2025 in the area of hybrid cloud computing security in SMEs, which are indexed in Scopus. Conversely, the exclusion criteria were articles and reviews published in non-English languages, as well as those published in English before 2009. Also, conference proceedings, books, book chapters, editorials, and letters were excluded. We also excluded articles and reviews unrelated to hybrid cloud computing security in SMEs.

We initially identified 788 from Scopus, after which 265 conference papers, editorials, letters, books, and book chapters were excluded. After the remaining 511 journal articles and reviews were screened for eligibility, 246 were excluded for failing the inclusion criteria. Therefore, only 265 articles and reviews were included in this bibliometric analysis.

2.3 Bibliometric Maps

Bibliometric analysis provides scientific direction (Mitha & Omarsaib, 2024) because it involves rigorous analysis of large amount of scientific data (Donthu et al., 2021). In this study, a VOS viewer tool is used for bibliometric analysis. VOS viewer tool is used because it enables researchers to visualise and generate unambiguous graphs that can be used to understand the relationship among variables in the literature network (You et al., 2024). The tool was used to analyse research distribution on the basis of countries, authors and journals, co-citations of publications, and the clustering of keywords. (McBurney & Novak, 2002).

2.4 Data Analysis

Initially, the whole bibliographic data extracted from the SCOPUS was exported in CSV format. This made it easy for us to screen the data for eligibility and eliminate repetition. The analysis of Co-authorship was employed to determine the collaboration among authors and institutions while citations analysis help us to understand the impact of publications. Also, we used keywords analysis to determine the trend of themes and emerging topics.

3. Results and Discussion

This part presents the descriptive statistics and network analyses of the included publications in this bibliometric analysis.

Table 1. Data Characteristics Using Descriptive Statistics

Description	Results
Time span	2009-2025
Sources (Journal)	194
Documents	265
Average citation per document	34.2
Citations	9,073
References	12578
Keywords	2543
Authors' keywords	951
Index Keywords	1952
Countries	77
Authors	952

Table 1 presents the general overview of the data characteristics related to hybrid cloud computing security studies in SMEs globally. The data covered between 2009 and 2025. Of 265 documents included in this bibliometric analysis, 12,578 references and 2,543 keywords from 952 authors across 77 countries were included. This signifies impactful collaborative contributions in the field. It also suggests that hybrid cloud computing security has interdisciplinary relevance and academic importance.

- **RQ1: What is the global trend of publications on hybrid cloud computing security in SMEs?**



Figure 2. Published Data from 2009 to 2025

Figure 2 provides the global trend of research publications on hybrid cloud computing security in SMEs. The visual representation indicates that the initial research at its early stage in 2009 was sparse, with limited and insignificant scholarly attention from 2009 to 2012. In 2024 and 2023, hybrid cloud computing security in SMEs recorded 43 and 32 publications, respectively, which was the highest. However, this field of study recorded fewer publications in 2011 and 2012, with 3 and 6 publications, respectively, suggesting that the topic was less explored during the period. A significant increase in the research output begins in 2015 with 19 publications. The momentum of continuous growth was maintained in 2019 and 2020, recording 23 and 25 publications respectively. This steady rise in the research output indicates a significant evolving contribution in the research area.

- **RQ2: What are the most productive journals on research on hybrid cloud computing security on SMEs?**

Table 2. The most productive journals on research on hybrid cloud computing security on SMEs

S/N	Journal	TC	SJR	Quartile
1	IEEE Access	145	0.96	Q1
2	International Journal of Information Management	79	5.78	Q1
3	Sensors	66	0.79	Q1
4	Future generation Computer System	58	1.95	Q1
5	Sustainability	49	0.67	Q1
6	Journal of enterprise information management	45	1.65	Q1
7	Communication of the ACM	44	2.96	Q1
8	Decision support system	40	2.21	Q1
9	IEEE transactions on nuclear science	38	0.54	Q2
10	Procedia computer science	35	0.51	N/A

Note: TC= Total citations; SJR= SCimago journal ranking; Q= Quartiles

Table 2 revealed the analysis of journal productivity and impact. The most prominent journal that published research on hybrid cloud computing security is IEEE Access, with a total citation of 145 and a SCimago journal rank of 0.96. more importantly, the International Journal of Information Management, with 79 citations, has the highest SJR score of 5.78, showing its reputation for publishing high impact studied. All the top 10 journals belong to Quartile 1 except IEEE transactions on nuclear science (Q2) and Procedia computer science which has not yet been assigned any quartile ranking. These finding indicate that Q1 journals dominate the dissemination of impactful studies of hybrid cloud computing security in SMEs globally.

- **RQ3: What are the top 10 countries in publications and citations about security concerns in adopting hybrid cloud computing by SMEs?**

Table 3. Top 10 countries in publications and citations about security concerns in adopting hybrid cloud computing by SMEs

S/N	Country	Publications	Citations
1	India	59	1649
2	United State	35	993
3	China	33	1492
4	United Kingdom	21	770
5	Australia	18	670
6	Saudi Arabia	13	92
7	Italy	12	733
8	Canada	12	368
9	Malaysia	10	174
10	Spain	9	623

Table 3 presents the global distribution of research activity among scholars on security concerns and solutions in hybrid cloud computing adoption by small and medium-sized enterprises (SMEs). The outcome reveals that India has the highest research output of 59 publications and 1,649 citations indicating a robust influence. China follows with 33 publications and 1, 492 citations, reflecting a strong research influence in the field. Following the same trend, the United States of America is with the third largest output of 35 publications and 993 citations. The United Kingdom and Australia also demonstrated significant research impact, with 770 and 670 citations respectively despite their fewer publications (21 and 18) respectively. Similarly, Spain and Italy demonstrated high citations of 623 and 733 form just 9 and 12 research output respectively. There is also moderate level of research activity with however less impacts in terms of citations from other countries including Canada (12 publications, 368 citations), Saudi Arabia Canada (13 publications, 92 citations), and Malaysia Canada (10 publications, 174 citations), this presupposes that countries like India and China from Asian continent and the United States are playing the leading role in advancing research on hybrid cloud computing security for SMEs, while also emphasising the impactful contributions of countries with fewer publications but higher citation impact.

- **RQ4: What is the intellectual structure of security concerns and solutions in hybrid cloud computing research?**

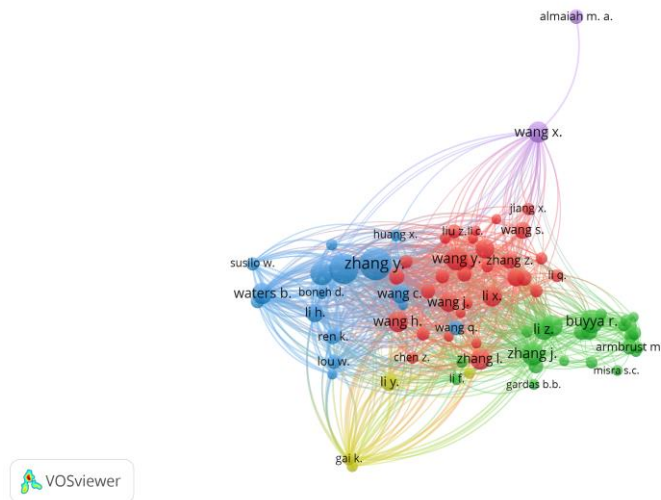


Figure 3. Co-citation analysis of the cited authors

Figure 3 provides a visual representation of the co-citation analysis of the intellectual structure of security concerns and solutions in hybrid cloud computing research. Of 23945 authors, 78 meet the minimum threshold of 20 citations. It also identified the influential cited authors and thematic structure within the field. Authors like Zhang Y and Wang X have high co-citation frequencies, signifying their influence and foundational contributions. Meanwhile, Almajah, M.A is relatively isolated, indicating an emerging research area in hybrid cloud computing security with limited overlap with broader themes

Table 4. Co-authorship network based on countries

S/N	Country	Documents	Citations	Total links strength
1	United States	35	993	23
2	India	59	1649	18
3	China	33	1492	17
4	Australia	18	670	16
5	Canada	12	368	14
6	Saudi Arabia	13	92	14
7	South Korea	9	309	10
8	United Kingdom	21	770	10
9	Pakistan	6	225	9
10	Egypt	7	60	6
11	Taiwan	7	204	5
12	Italy	12	733	4
13	Malaysia	10	174	4
14	Spain	9	623	4
15	Germany	9	175	3
16	Greece	7	110	3
17	Iraq	8	155	3

continued

18	Netherland	5	61	2
19	Jordan	5	101	1

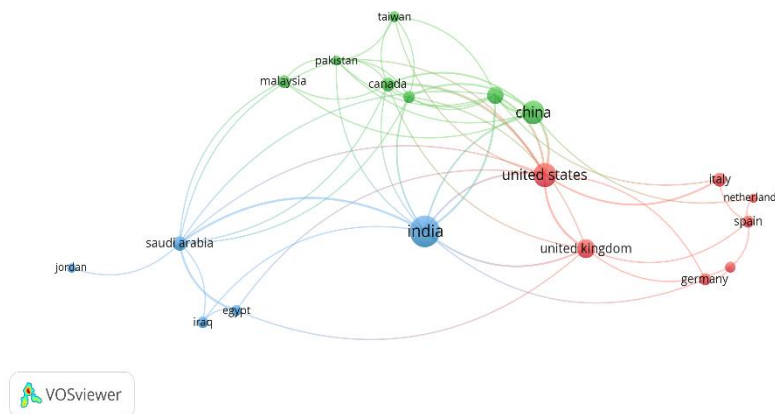


Figure 4. Co-authorship network based on countries

Of the 77 countries in the data under review, only 19 countries have co-authorship in at least five documents, as shown in Figure 4. When there is more co-authorship based on countries, more solutions will be produced for SMEs to address their security concerns in hybrid cloud computing adoption for their businesses. The US, India, the United Kingdom, China and Australia top the list of countries with the highest co-authorship links. This presupposes that more intercontinental co-authorship on hybrid cloud solution security related topics globally.



Figure 5. Co-authorship network based on authors

Figure 5 revealed the overlay visualisation of co-authorship of research related to hybrid cloud computing adoption in SMEs on topics related to security concerns and solutions. Of the 952 authors, only 6 meet the collaboration threshold in at least three documents globally. For each of the 6 authors, the total strength of co-authorship with other authors was calculated with Gupta, Shivam and Misra Subhas C having 3 links each, while Zhang and Zheng had 2 each. This implies that more effort is needed in co-authorship of topics related to hybrid cloud computing security in SMEs.

- **RQ5: What is the trend of themes and emerging topics in hybrid cloud computing security in SMEs?**

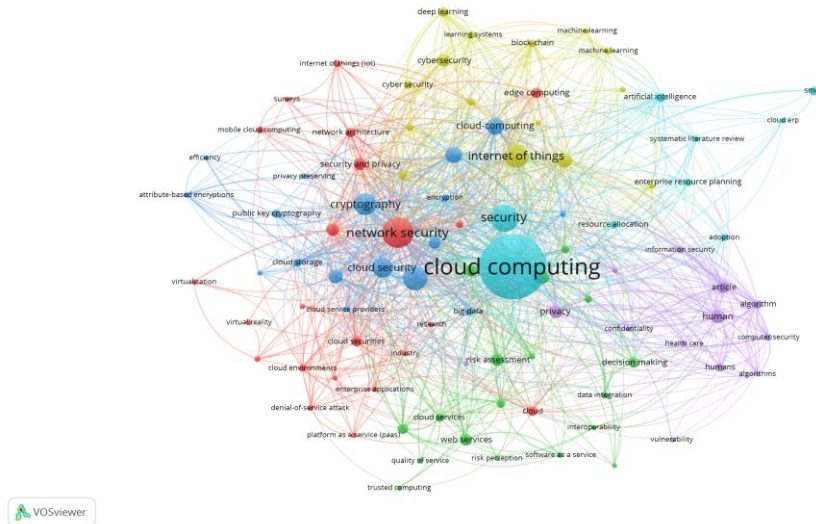


Figure 6. Co-occurrence of all Keywords on security concerns in hybrid cloud adoption in SMEs

Figure 6 presents the overlay visualisation of all keywords used in research publications on security concerns in hybrid cloud adoption in SMEs. The prominent and the most central keyword in the studies in this area is cloud computing. Similarly, close keywords like network security, security, cryptography, and compliance emphasise the important role of compliance and security in fostering a hitch-free adoption of the hybrid cloud computing by the SMEs. Of all 2453 keywords, only 94 meet the threshold of minimum number of occurrences of keyword.

Furthermore, the appearance of keywords internet of things, data storage, and data privacy underscores the importance of data protection in the adoption of the hybrid cloud services and infrastructures by the SMEs.

4. Discussion

This study aims to unravel the complex nature of research on hybrid cloud computing security in SMEs. The bibliometric analysis revealed that the trend of global research publications on hybrid cloud computing security in SMEs began with insignificant scholarly attention at the early stage between 2009 and 2014. No research output on cloud computing before 2008 on Scopus data base (Gonçalves et al., 2023). The highest publications got noticed around 2020, 2023 2024 when the world have learned from the COVID-19 pandemic. The increase in the adoption of cloud computing by organisations, including the SMEs, is one of the gains of the pandemic. This also instil that consciousness in the researchers of the need to research topics related to security mater in the hybrid computing.

The study also examined the most productive journals on research on hybrid cloud computing security for SMEs. It was found that the theme of security in hybrid cloud computing has been attracting the interest of different journals. However, IEEE Access has the highest citations, though it ranked behind the International Journal of Information Management. This finding aligns Gonçalves et al. (2023) who also found that cloud computing has been gaining attention in the business field since 2008. This means that as the world is experiencing technological advancement, so also there is increasing attention from academic scholars in research the implications of technology to businesses.

This study has also found the most productive countries of affiliations of the researchers of the included publications. It was found that India from the Asia continent is one of the most productive countries, while the United States followed suit. The report revealed that Asia-Pacific has the highest SMEs in the world, with 328 million out of the estimate 358 million SMEs all over the world as of 2023 (Dyvik, 2024). However, according to the World Crime Index (WCI), China is the country with the third highest rate of cybercrime (27.86%) globally (Bruce et al., 2024).

Another finding of this bibliometric analysis revealed that despite the fact that there was a growing research interest in hybrid cloud computing security in SMEs, the authors' productivity was relatively low. It is interesting to mention that authors including Gupta, Shivam, Misra Subhas C, Zhang, and Zheng have 3 links each, which is the highest. All the mentioned authors are from far- Asia. This could be possibly linked to the presence of the highest number of SMEs in the region.

This study has also found some emerging keywords that are central to hybrid cloud computing security in SMEs. Keywords like security, privacy and adoption indicate persistent concern of issues of unauthorized access and data protection. This also presuppose that the hybrid cloud computing is an off shoot of cloud computing, and the more reason

why the central keyword is cloud computing. As such, whatever measure is taken to address security concerns in the cloud computing could be extended to the hybrid cloud computing.

5. Limitations

The included publications on hybrid cloud computing security in SMEs were limited to those indexed in Scopus from January 2009 to January 2025. We relied solely on the SCOPUS database because it is known for indexing high-quality studies. Subsequent bibliometric studies can explore other databases like Web of Science and Dimensions. Another limitation is that we used documents published in English from the examined Scopus database. This limitation is because other non-English documents may produce a more comprehensive overview of publications on hybrid cloud computing security in SMEs. However, considering the objective of this study, which is to produce global research interest on the subject, documents published in English have been considered to provide the needed data to achieve the objective.

6. Conclusion

This bibliometric study analysed the progression of hybrid cloud computing tailored to security concerns in its adoption by SMEs between 2009 and 2025. We X-ray research activity and productivity in terms of citation performance, emerging research themes and the most influential countries and authors within the years under review. We found that 265 publications from 952 authors affiliated to 77 countries yielded 9,073 citations. The findings of this bibliometric analysis will enable researchers to identify the leading researchers, journals, countries, collaborations and citations worldwide.

7. Implications

The findings of this bibliometric analysis have implications for stakeholders in the field, including researchers, SME managers, government officials, and practitioners in the industry. First and foremost, the outcomes of this bibliometric analysis of research trends and impact provide the much-needed roadmap to guide future research endeavours. It alerts researchers from regions with low research output to finetune their research direction and collaborate where and when necessary. In addition, researchers will be able to examine the emerging themes of hybrid cloud computing and the role of artificial intelligence (AI) in achieving virile security when SMEs are adopting hybrid cloud solutions in their enterprises. Secondly, the result of this study implies the need for industry practitioners to re-strategise and redirect their cybersecurity solutions. Vendors and service providers will be able to develop a product that addresses an SMEs-specific security solution and is cost-effective, having identified limited resources and experts as remote causes of the security concerns.

Furthermore, the findings of this study implies that policymakers need to make tailored guidelines, and organised training programmes that will assist SMEs to comply with the security measures that are cost-effective. In addition, government and private sectors need to for a synergy in fighting cybercrime, create awareness about cybersecurity and instill the spirit of resiliency in the SMEs. SME managers can now give preference to investment to data protection, compliance, and advanced security technologies using AI. By so doing, SMEs can enhance their cybersecurity and ensure cost-efficiency. Another implication is that the finding of this bibliometric analysis offers insight into the existing and emerging security challenges for SME managers.

Acknowledgment

The Chief Editors, Managing Editors, and anonymous reviewers deserve the authors' sincere gratitude and admiration for their insightful remarks, advice, and constructive criticism.

References

- Alrababah, Z. (2023). Barriers to cloud computing adoption among SMEs in the middle east: a systematic review. *Journal of Theoretical and Applied Information Technology*, 101(17), 6853–6865.
- Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLoS ONE*, 19(4), e0297312. <https://doi.org/10.1371/journal.pone.0297312>
- Chaudhary, S., Gkioulos, V., & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness. *Computer Science Review*, 50(830929), 100592. <https://doi.org/10.1016/j.cosrev.2023.100592>
- Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: an overview and guidelines. *Journal of Business Research*, 133(133), 285–296. <https://doi.org/10.1016/j.jbusres.2021.04.070>.

- Dyvik, E. H. (2024). *Number of SMEs worldwide 2000-2023 by region*. Statista. <https://www.statista.com/statistics/1261598/global-smes-by-region/#:~:text=There were estimated to be,the most SMEs was Asia>.
- Gangadhar, V. R., & Shaikh, A. (2020a). Research outlook on cloud computing adoption in small and computing adoption in small and medium enterprises (SMEs) across globe. *International Journal of Management*, 11(12), 2307–2318. <https://doi.org/10.34218/IJM.11.12.2020.218>
- Gangadhar, V. R., & Shaikh, A. (2020b). Small and Medium Enterprises and Cloud Technology – Challenges and Opportunities during COVID19. *International Research Journal on Advanced Science Hub*, 02(12s), 32–38. <https://doi.org/10.47392/irjash.2020.257>
- Gonçalves, C. A., Messias, C. O. de S., Soares, J. L., & Peixoto, M. M. da C. L. (2023). Adoption of Cloud Computing in the organizations: a bibliometric analysis of this technology within a digital transformation context. *Revista de Administração Da UFSM*, 16(3), e1. <https://doi.org/10.5902/1983465975326>
- Gupta, S., Misra, S. C., Kock, N., & Roubaud, D. (2018). Organizational , technological and extrinsic factors in the implementation of cloud ERP in SMEs. *Journal of Organizational Change Management*, 31(1), 83–102. <https://doi.org/10.1108/JOCM-06-2017-0230>
- Gupta, S., Misra, S. C., & Singh, A. (2017). Identification of challenges and their ranking in the implementation of cloud ERP A comparative study for SMEs and large organizations. *International Journal of Quality & Reliability Management*, 34(7), 1056–1072. <https://doi.org/10.1108/IJQRM-09-2015-0133>
- Jayeola, O., Sidek, S., Rahman, A. A., & Hu, J. (2022). Cloud Computing Adoption in Small and Medium Enterprises (SMEs): A Systematic Literature Review and Directions for Future Research. *International Journal of Business and Society*, 23(1), 226–243. <https://doi.org/10.33736/ijbs.4610.2022>
- Majengo, R., & Mbise, M. (2022). Determinants of Software-as-a-Service Adoption by Small and Medium Enterprises in Tanzania. *The African Journal of Information Systems*, 14(1), 2.
- McBurney, M. ., & Novak, P. . (2002). What is bibliometrics and why you care? *IEEE International Professional Communication Conference*, 108–114. <https://doi.org/http://doi.org/10.1109/ipcc.2002.1049094>
- Mitha, S. B., & Omarsaib, M. (2024). Emerging technologies and higher education libraries: a bibliometric analysis of the global literature. *Library Hi Tech*. <https://doi.org/10.1108/LHT-02-2024-0105>
- Mwangi, I. K., Okeyo, G. O., & Kimwele, M. W. (2018). A Hybrid Framework for Cloud Computing Adoption for Small and Medium Size Enterprises. *International Journal of Science and Applied Information Technology*, 7(4), 1–6. <https://doi.org/10.30534/ijisait/2018/01742018>
- Nyamwesa, A. (2024). Cloud Computing Technology Adoption: Challenges for SMEs, A Case of Selected SMEs in Tanzania. *International Journal of Advanced Business Studies*, 3(2), 1–12. <https://doi.org/10.59857/ijabs.3118>
- Page, M. J., Mckenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-wilson, E., Mcdonald, S., ... Moher, D. (2021). The PRISMA 2020 statement : an updated guideline for reporting systematic reviews. *Systematic Reviews*, 10(89), 1–11.
- Patil, P. P., Bhambure, R., Salunke, A., Bhujade, N., & Dhadve, S. (2023). Cybersecurity for MSMEs in India : “ Analysis of Cyber-Attacks and Implementation of Suitable Security Framework .” *International Journal of Advanced Research in Science, Communication and Technology*, 3(1), 35–38. <https://doi.org/10.48175/IJAR SCT-7831>
- Selçuk, A. A. (2019). A Guide for Systematic Reviews : PRISMA. *Turk Arch Otorhinolaryngol*, 57(1), 57–58. <https://doi.org/10.5152/tao.2019.4058>
- Vailshery, L. S. (2024). *Hybrid cloud market size worldwide 2021-2027*. Statista. <https://www.statista.com/statistics/1232355/hybrid-cloud-market-size/#:~:text=In 2021%2C the global hybrid,HPE%2C AWS%2C and IBM>.
- You, C., Awang, S. R., & Wu, Y. (2024). Bibliometric analysis of global research trends on higher education leadership development using Scopus database from 2013–2023. *Discover Sustainability*, 5(1). <https://doi.org/10.1007/s43621-024-00432-x>