www.refaad.com

Global Journal of Economics and Business (GJEB)

المجلة العالمية للاقتصاد والأعمال

Journal Homepage: https://www.refaad.com/Journal/Index/2

E-ISSN 2519-9293 | P-ISSN 2519-9285

Vol. 16, Issue 3, 2026, pp. 333 - 343



Bibliometric Review of the Impact of Cloud Computing Usage on Risk

مراجعة بيبلومترية لتأثير استخدام الحوسبة السحابية على المخاطر

Elhaloumi Redouane[1*], Jabraoui Siham[2]

[1] Hassan II University, ENCG –CASABLANCA, LIREIMO, Morocco.

[2] Professor, Hassan II University, ENCG –CASABLANCA, LIREIMO, Morocco.

[*] Corresponding Author: Elhaloumi Redouane (elhaloumi95@gmail.com)

This file is licensed under a
Creative Commons Attribution 4.0 International

Received استلام البحث	Revised مراجعة البحث	Accepted قبول البحث
2026/1/16	2026/2/3	2026/2/22

DOI: https://doi.org/10.31559/GJEB2026.16.3.6

Abstract:

Objectives: This study aims to examine the evolution and intellectual structure of research on the impact of cloud computing on risk, identifying key trends, influential contributors, and emerging thematic priorities over the last decade.

Methods: A bibliometric analysis was performed on 583 articles indexed in the SCOPUS database between 2015 and 2025, focusing on publication trends, citation patterns, collaboration networks, and keyword co-occurrence to identify major research themes and their evolution.

Results: The analysis reveals a steady growth in publications, with cloud security, risk management, and risk assessment emerging as dominant sub-domains. The findings also indicate a growing research emphasis on the relationship between cloud computing services and associated risks.

Conclusions: This study provides a structured overview of the scientific landscape on cloud computing and risk, offering a valuable basis for identifying research gaps and supporting strategic decision-making, while contributing to the guidance of future research directions in this field.

Keywords: *Cloud computing usage; risk; risk management.*

الملخص:

الأهداف: هدفت هذه الدراسة إلى تحليل تطور البنية الفكرية للبحوث العلمية المتعلقة بتأثير الحوسبة السحابية على المخاطر، من خلال تحديد الاتجاهات الرئيسة، والمساهمين الأكثر تأثيرًا، والأولويات الموضوعية الناشئة خلال العقد الأخير.

المنهجية: تم إجراء تحليل ببليومتري على عينة مكوّنة من 583 مقالة علمية مفهرسة في قاعدة بيانات SCOPUS خلال الفترة الممتدة من 2015 إلى 2025، مع التركيز على اتجاهات النشر، وأنماط الاستشهاد، وشبكات التعاون العلمي، وتلازم الكلمات المفتاحية، وذلك بهدف تحديد الموضوعات البحثية الرئيسة وتتبع تطورها.

النتائج: أظهرت نتائج التحليل نموًا مطّردًا في حجم المنشورات العلمية، مع بروز أمن الحوسبة السحابية، وإدارة المخاطر، وتقييم المخاطر بوصفها المجالات الفرعية المهيمنة. كما تشير النتائج إلى تزايد الاهتمام البحثي بالعلاقة بين استخدام خدمات الحوسبة السحابية والمخاطر المرتبطة بها.

الخلاصة: تقدم هذه الدراسة تصورًا منهجيًا ومتكاملًا للمشهد العلمي المتعلق بالحوسبة السحابية والمخاطر، بما يوفّر أساسًا علميًا مهمًا لتحديد الفجوات البحثية ودعم عملية اتخاذ القرار الاستراتيجي، فضلًا عن الإسهام في توجيه مسارات البحث المستقبلية في هذا المجال.

الكلمات المفتاحية: *استخدام الحوسبة السحابية؛ المخاطر؛ إدارة المخاطر.*

Citation

Elhaloumi, R., & Jabraoui, S. (2026). Bibliometric Review of the Impact of Cloud Computing Usage on Risk. *Global Journal of Economics and Business*, 16(3), 333-343. https://doi.org/10.31559/GJEB2026.16.3.6

1 Introduction

The rise of cloud computing has profoundly transformed corporate IT infrastructures, offering flexible and scalable access to remote IT resources (servers, storage, applications, etc.), while reducing the costs of acquiring and managing hardware infrastructures. Ac-cording to a 2021 O'Reilly study, more than 90% of companies worldwide use cloud ser-vices, reflecting the growing strategic importance of this technology in today's economic and technological environment (Mike Loukides,2021) .However, while cloud computing offers substantial benefits in terms of flexibility, cost reduction and operational efficiency, it also raises significant risk management concerns. Increased reliance on external providers for data and application hosting exposes organizations to new types of risks, including those related to information security, data privacy and regulatory compliance (Hua Tang et al-2016). Outsourcing sensitive data to cloud environments, which are often multi-tenant, can lead to vulnerabilities related to unauthorized access, cybersecurity threats and service failures (Ali et al., 2015).Risk management in cloud computing has been a widely studied topic, with proposals for risk assessment models aimed at better understanding and controlling the dangers inherent in the use of this technology (Mouna and Rabai-2017). However, risk management approaches must evolve in line with the dynamic nature and heteroge-neity of cloud environments. For example, a model based on risk assessment (Xuan Zhang et al, 2023) allows vulnerabilities to be identified and prioritized more effectively, but requires close integration with the company's IT security strategies. Despite growing attention to these issues, there remains a lack of consensus on the best way to assess and reduce risks in cloud computing. Numerous studies (Srijita Basu, 2018) point to the importance of adopting risk mitigation strategies, such as cryptography, access management and continuous monitoring of cloud infrastructures. However, these strategies must be tailored to the specific characteristics of each organization and the particularities of each cloud provider. However, this transition to cloud-based environments also raises major concerns in terms of risk management. Indeed, the outsourcing of sensitive data and access to remote services increase vulnerabilities related to information security, data confidentiality and regulatory compliance (BADER ALOUFFI et al., 2021). While the cloud offers substantial advantages in terms of flexibility, cost and scalability, it also introduces new types of risks, particularly those related to access management, cyber threats and service failures (Yara Alghofaili et al, 2021).Furthermore, the impact of cloud computing on organizational risks is complex and multifaceted. Some studies highlight the risks inherent in adopting the cloud, while others highlight how effective management of cloud infrastructure can reduce certain types of risks. However, despite growing recognition of these issues, there is still a lack of consensus on the precise assessment of these risks in the context of cloud computing use (Maniah et al,2022). The bibliometric review presented here aims to explore this issue by analyzing scientific publications that address the impact of cloud computing on risks, in order to identify trends, gaps and developments in the existing literature. The objective of this study is to provide an overview of previous research, highlighting the methodologies used, the main results obtained and the practical implications for businesses. By conducting a bibliometric analysis, we also hope to provide a framework for future research on this crucial topic, particularly at a time when cloud computing is becoming a pillar of modern business technology strategies (Umar Yusuf Dayyabu.2022) .In such a complex field, it is essential to map scientific knowledge in order to identify major trends, key players and gaps in research. Although several previous bibliometric analyses have already studied this subject (Umar Yusuf Dayyabu.2022) (Zakaria, A et al.2024) (Meshari F et al .2024) , they fail to cover one essential aspect: previous work does not explore the notion of downstream risk associated with the use of cloud computing. The majority of these studies are limited to analyzing the determining factors of its use, focusing mainly on security and confidentiality issues, without examining other dimensions of risk or assessment methods that would clarify the real impact of cloud use on risk (Mohammad Masudur Rahman et al.2018) (Annunziata, G et al.2024). This study aims to fill these gaps by answering three fundamental ques-tions:1) Which publications and scientific journals dominate the field of research on the use of cloud computing services and risk, both in terms of impact and major contributions? 2)How do researchers, institutions and existing work analyse the impact of cloud computing use on different dimensions of risk, including risk level, risk maturity, risk management and risk assessment methods? 3) What emerging sub-themes provide a better understanding of the role of risk as an explanatory or mediating mechanism in the relationship between the use of cloud computing and various organisational dynamics? To answer these questions, a comprehensive bibliometric analysis was conducted, combining data from leading scientific databases with visualization tools. This method-ology makes it possible to quantify the impact of publications, identify thematic groups and track the chronological evolution of concepts. Section 2 details the methodological framework, Section 3 presents the results, including citation maps and co-author net-works,

and Section 4 discusses the main conclusions. This research provides an up-to-date overview of a rapidly evolving field and aims to inform researchers, decision- makers and practitioners about strategies for better understanding and managing the risk associated with cloud computing.

2 Method

This research aims to shed light on current topics and anticipate future trends in the field of cloud computing use and its implications for risk. To achieve these objectives (Naveen Donthu et al,2021), a rigorous methodology was adopted, as illustrated in Figure 1.

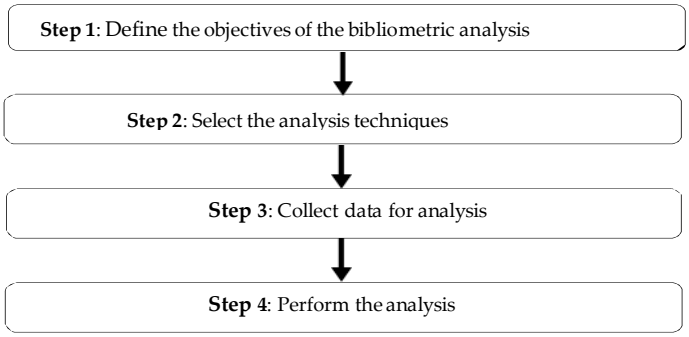
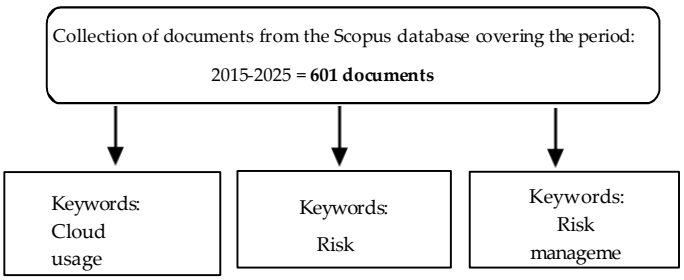


Figure 1: The bibliometric analysis procedure.

The methodological approach begins with the definition of research objectives. Data collection was carried out using the SCOPUS database, renowned for its extensive coverage of peer-reviewed scientific publications. Once the data had been extracted, it was pre-processed to ensure its quality and relevance for bibliometric analysis. This process included cleaning metadata, removing duplicates and harmonizing information on authors and institutional affiliations. The study focuses on three main dimensions. The first is co- authorship analysis, which identifies collaborations between researchers and between countries. The second is citation analysis, which examines the links between publications and scientific journals. The third dimension is the analysis of co-occurrence and thematic clustering, which highlights the conceptual structure of the field under study. These analyses are complemented by the mapping of thematic trends and the examination of the evolution of research topics, thus providing a de-tailed view of the dynamics and emerging trends in the field of cloud computing use and its impact on risk. The VOSviewer tool was used to visualize and help interpret the results. It pro-vides an interactive interface for examining research dynamics through interactive graphics, in- depth analysis and exploration of collaboration and citation networks. The bibliographic data selected for this study focuses exclusively on articles directly related to the issue of cloud computing use and its impact on risk. It comes from fields such as information systems, risk management, business and management, information security, risk management and multidisciplinary sciences. This selection ensures relevant and comprehensive coverage of scientific output relating to the risk issues associated with cloud computing services. The search query used in the Scopus database is formulated as follows: TITLE-ABS-KEY = (("cloud computing" OR "cloud ser-vices" OR "cloud adoption" OR " cloud usage ") AND ("risk" OR "risk management" OR "cybersecurity risk" OR "risk assessment" OR "privacy risk" OR "security risk" OR "data security" OR "information security")).In order to ensure that the time frame covered is representative of recent developments in the field, the analysis period was limited to the last 10 years (2015–2025). The data was collected in 2025. This approach identified 718 peer-reviewed scientific publications, which were selected for in-depth bibliometric analysis. These methodological steps ensure the robustness and reliability of the results obtained, thereby contributing to a better under-standing of the dynamics of research into the use of cloud computing services and its impact on risk.



Search criteria applied:

- Inclusion of publications in English.
- Exclusion of publications outside the period 2015-2025.
- Selection of relevant fields and categories in the Scopus database, such as computer science, business, management and accounting, and multidisciplinary sciences.
- Construction of semantic relationships using the Boolean operators "OR" and "AND" to combine terms related to cloud computing and risk.

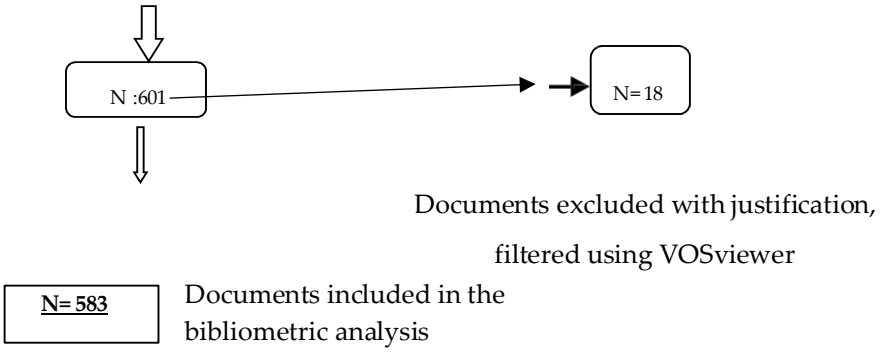


Figure 2: Methodological diagram of the structure of the bibliometric review.

3 Results

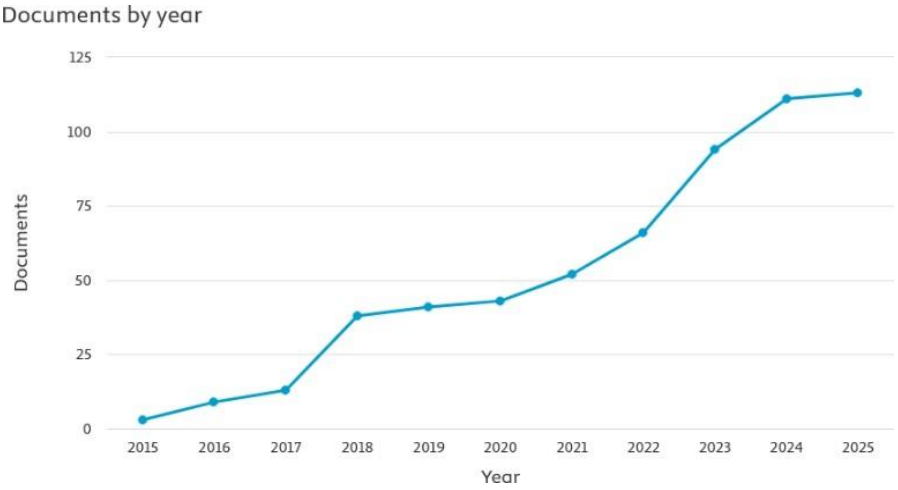
3.1 Database

Table 1: Key data information

Description	Results
Period	2015-2025
Documents	583
Annual growth rate (%)	27.34
Average age of documents (in years)	7.5
Average citations per document	30.43
Author's keywords (DE)	1609
Authors	1503
Co-authors per document	3.14
Percentage of co-authors international	46.74%

3.2 Annual growth in scientific publications

The trend in research publications on the impact of cloud computing on risk shows steady growth in recent years, with an average annual rate of 27.34%. A sharp increase was observed between 2022 and 2025, reflecting a growing interest in studying the risks associated with the adoption and use of cloud computing services. Recent trends suggest a growing focus on risk management and security in this area.



3.3 Documents per year according to sources

This analysis examines the annual evolution of the number of publications from major scientific sources on the use of cloud computing and its implications.in terms of risk. For a maximum of ten major journals on Fig. 2. Methodological diagram of the structure of the bibliometric review conferences, the number of documents published each year is compared, making it possible to identify the most prolific sources and periods of intensified scientific production. This comparison highlights the dynamics of publication within the field studied and helps to identify the most influential channels of dissemination in the literature on cloud computing and risk.

Table (2). Documents per year for the ten most prolific sources

Scientific sources	Number of articles	(2015- 2020)	(2020- 2025)	Cite Score Tracker
IEEE Access	121	51	70	8.4 in 2025
Sensors	48	0	48	8.5 in 2025
Journal of Cloud Computing	35	11	24	13 in 2025
Applied Sciences (Switzerland)	26	1	25	5.6 in 2025
Sustainability (Switzerland)	26	3	23	8.3 in 2025
International Journal of Advanced Computer Science and Applications	24	7	17	3.1 in 2025
Computers, Materials and Continua	19	2	17	5.9 in 2025
Electronics (Switzerland)	18	1	17	6.4 in 2025
Information (Switzerland)	10	4	6	7.2 in 2025
Future Internet	8	3	5	8.8 in 2025

The table highlights different dynamics in scientific output and academic impact between the periods 2015–2020 and 2020–2025. The journal Sensors stands out with a sharp increase in publications only during the period 2020–2025, whereas its output was zero or virtually non-existent during the previous period, reflecting recent scientific interest in this source. Furthermore, the analysis of academic impact shows that the Journal of Cloud Computing has a high CiteScoreTracker of 13 in 2025, indicating significant scientific influence despite variable changes in the number of publications. It also reveals that journals such as Sensors and Future Internet maintain a high academic impact, while others have a more moderate influence. Overall, these results highlight different dynamics between journals, combining growth, stability or decline in scientific output, in line with their visibility and academic impact.

3.4 Scientific documents by affiliation

This analysis compares the number of documents produced by up to ten of the most active institutional affiliations in the field of cloud computing and risk. It identifies the universities, research centers and organizations that contribute the most, highlighting the concentration of scientific output, the dominant players and the research dynamics within the most influential institutions.

Table 3: Documents per year for the ten most prolific sources

Affiliation	Country	Number of articles
King Saud University	Saudi Arabia	12
Vellore Institute of Technology	India	9
Princess Nourah Bint Abdulrahman University	Saudi Arabia	8
Taif University	Saudi Arabia	8
University of Jeddah	Saudi Arabia	8
Chinese Academy of Sciences	China	8
King Abdulaziz University	Saudi Arabia	8
Universiti Kebangsaan Malaysia	Malaysia	7
Ministry of Education of the People's Republic of China	China	7
King Faisal University	Saudi Arabia	6

The table highlights a high concentration of scientific publications on the impact of cloud computing on risk within institutions in Saudi Arabia, which largely dominate production with several universities among the most productive, particularly King Saud University. This predominance reflects the country's significant investment in scientific research and sustained institutional momentum. Furthermore, the contribution of Asian institutions such as those in India, China and Malaysia reflects regional collaboration and scientific influence, although their publication volumes remain lower than those of Saudi institutions. Overall, the distribution observed reflects both a geographical concentration of research and institutional diversity, suggesting a scientific landscape structured around strong national hubs while remaining open to international contributions.

3.5. Author profiles: publication volume and h-index

Table (4). Distribution of publications by affiliation and institutional location

Authors	Number of articles	Country	H-index
Afantitis, Antreas	4	Cyprus	40
Lynch, Iseult	4	UK	84
Melagraki, Georgia	4	Greece	39
Tsoumanis, Andreas C.	4	Cyprus	14
Alshammari, Salah Telaihan	3	Saudi Arabia	4
Georgiou, Dimitra	3	Greece	4
Latip, Rohaya Binti	3	Malaysia	16
Li, Qingfu	3	China	25
Maple, Carsten R.	3	UK	46
Papadiamantis, Anastasios G.	3	Greece	18

The table shows a breakdown of scientific publications on the impact of cloud computing on risks, based on the authors' affiliation and country. There is geographical diversity, with researchers affiliated with institutions in Cyprus, the United Kingdom, Greece, Malaysia, Saudi Arabia and China. The most prolific authors, such as Afantitis, Antreas and Melaqargi, Georgia, have published four articles, while others, such as Iseult Lynch, stand out with a high H- index of 84, reflecting the significant impact of her work in analyzing the risks associated with cloud computing. This table highlights strong international collaboration, with a notable concentration of expertise in the United Kingdom and Greece. The H-index highlights authors who have made a substantial and lasting contribution to research on the risks associated with security, privacy and cloud service management.

3.6 Geographical distribution of scientific publications (2015-2025).

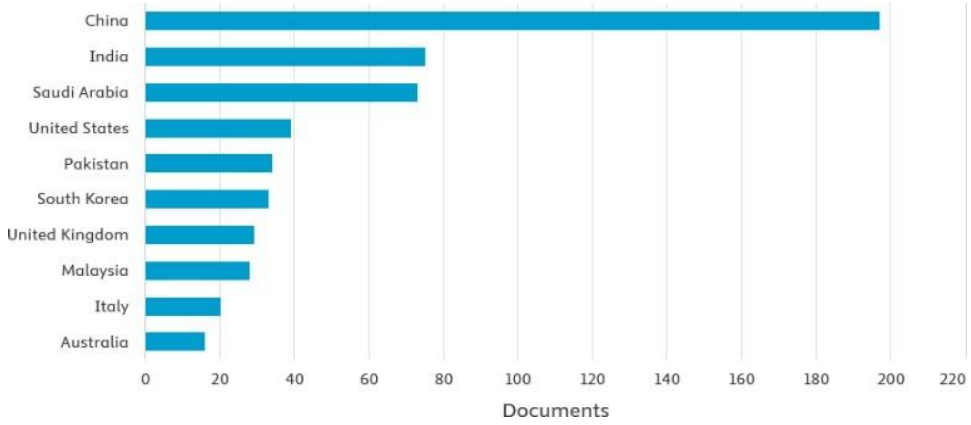


Figure 4: Geographical distribution of scientific publications over the period 2015–2025

Analysis of the geographical distribution of scientific publications over the period 2015–2025 highlights a marked concentration of academic output in a limited number of countries. China stands out as the main contributor, with a volume of publications significantly higher than that of other nations, reflecting a sustained commitment to scientific and technological research. It is followed by India and Saudi Arabia, whose levels of production, although more modest, reflect the emergence of new research hubs, particularly around issues related to digital transformation and risk management. The United States occupies an intermediate position, reflecting a significant but relatively less dominant participation in this specific field. Other countries, such as Pakistan, South Korea, the United Kingdom, Malaysia, Italy and Australia, have smaller volumes but nevertheless demonstrate a constant scientific interest, often supported by international collaboration. Overall, this distribution confirms that scientific output remains largely driven by a few major players, while highlighting a gradual spread of research activity to geographically and economically diverse regions.

3.7 Analysis of publications by scientific field: Top seven sectors

Analysis of the distribution of publications by subject area identifies the scientific fields that mainly structure research on the use of cloud computing and its impact on risk. By examining the seven most represented fields, this section highlights the major trends in the literature, particularly around security, risk management, organizational performance and digital transformation. This thematic mapping thus provides an overview of disciplinary contributions and sheds light on the areas that currently dominate the scientific debate.

Table 5: Main thematic areas of publications

Area of scientific study	Documents	Percentage
Computer Science	563	64
Materials Science	170	19
Environmental Science	40	5
Business, Management and Accounting	37	4
Social Sciences	36	4
Decision Sciences	20	2
Economics, Econometrics and Finance	9	1

The table shows the distribution of scientific publications by field of study, with a marked dominance of computer science (64%), followed by materials science (19%) and environmental science (5%). In the context of research on the impact of cloud computing on risk, computer science is the main basis for the analysis of technological risks, particularly those related to system security, data management and cloud infrastructures. However, the field of Business, Management and Accounting, although representing a smaller proportion of publications (4%), plays a central role in understanding cloud computing from a management science perspective, with an emphasis on the organizational, strategic, financial and regulatory risks associated with its adoption by businesses.%), plays a central role in understanding cloud computing from a management science perspective, focusing on the organizational, strategic, financial and regulatory risks associated with its adoption by businesses. Other fields, such as social sciences, economics and environmental sciences, provide additional insights that enable a comprehensive and multidimensional analysis of the risks associated with cloud computing.

3.8 Keyword analysis

According to Ivan Župič, M.Sc and Tomaž Čater (Meshari F. Alhayan,2024) (Dragoș M. Obreja, 2024) (Zupic,Iet al, 2015), the conceptual structure highlights the underlying organization and relationships between the concepts used in the literature on the use of cloud computing and its impact on risk. It illustrates how the central concepts in the field are linked to each other through semantic or theoretical associations. A co- occurrence network analysis was therefore conducted to examine the patterns of joint occurrence of terms or keywords in this literature, revealing their implicit links and interconnections. The analysis focused on the co-occurrence structure of the most frequently used keywords in all the publications studied. Figure 4 presents these keywords, with the size of the nodes proportional to their frequency. The co-occurrence network thus provides a detailed and nuanced representation of the thematic landscape related to cloud computing and the associated risks. Each node, sized according to the frequency of a keyword, reflects the preponderance of certain concepts, while the connecting lines, whose thickness varies, indicate the strength of the associations between terms. Major keywords such as "cloud Computing, information security, risk assessment", "privacy" and "cybersecurity" appear as central nodes, highlighting their essential role in structuring scientific discourse. The coloring of the clusters also makes it possible to identify distinct but interrelated thematic groupings, highlighting sub-domains such as security, information security, risk analysis and assessment, confidentiality, and also governance and performance.

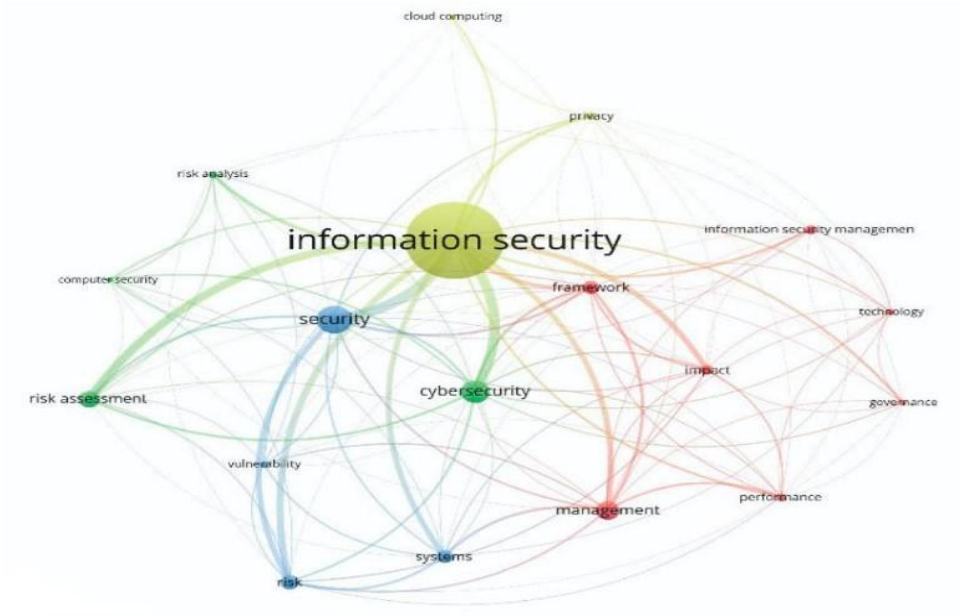


Figure 5: Co-occurrence network of authors' keywords

Analysis of the keyword co-occurrence network highlights the main directions of scientific research on cloud computing and its implications for risk management. At the heart of the network, the term "information security" occupies a central and dominant position, indicating that information security is the main prism through which the impact of cloud computing on risk is studied. This centrality reflects the strategic importance attached to data protection, confidentiality and information integrity in cloud environments. Although the term 'cloud computing' appears more peripherally in the network, it remains closely connected to key concepts such as 'privacy', 'risk analysis' and 'information security management'. This configuration suggests that cloud computing is primarily addressed as an amplifier of existing risks rather than as an isolated concept. Research therefore focuses on assessing the risks associated with outsourcing IT resources, sharing infrastructure and dependence on cloud service providers. The network also reveals a strong association between cloud computing and the concepts of cybersecurity, vulnerability, risk assessment and computer security, highlighting the growing importance of cyber threats in cloud environments. These links reflect a major concern for the identification, analysis and mitigation of cloud-specific vulnerabilities, including risks related to cyberattacks, security breaches, and data loss. Thus, risk management in the cloud relies heavily on enhanced cybersecurity strategies and methodological risk assessment frameworks. Furthermore, the presence of clusters related to "management ", "governance", "framework" and "performance" shows that the impact of cloud computing on risk is also being studied from an organizational and strategic perspective. The cloud is not only perceived as a source of technical risks, but also as a lever for organizational transformation requiring

appropriate governance mechanisms. Organizations are seeking to reconcile the benefits of the cloud – such as flexibility, cost reduction and improved performance – with the control of operational, legal and strategic risks. Moreover, the interconnection between the concepts of 'systems', 'technology' and 'innovation' suggests that cloud computing is seen as a catalyst for innovation, while introducing new systemic risks. This duality highlights a constant trade-off between "technology" and "innovation" suggests that cloud computing is seen as a catalyst for innovation, while introducing new systemic risks. This duality highlights a constant trade-off between technological opportunities and increased risk exposure, reinforcing the need for integrated risk management approaches in cloud environments. Finally, the overall analysis of the keyword network shows a shift in research towards an increasingly interdisciplinary approach, combining information security, cybersecurity, risk management and organizational performance. This convergence highlights that the impact of cloud computing on risk cannot be understood in a fragmented way, but requires a comprehensive vision that integrates technical, organizational and strategic dimensions. Academic work therefore tends to propose more comprehensive risk management frameworks to support organizations in the secure and effective adoption of cloud computing.

4 Discussion

This study adopts a bibliometric approach, based on co- author networks, keyword co-occurrence and thematic clustering, in order to identify three major trends concerning the impact of cloud computing on risk. Firstly, a global phenomenon emerges: (1) the growing use of cloud computing as a lever to reduce certain types of operational risk and improve the resilience of information systems (Thomas Welsh et al, 2020), (2) the examination of the socio-economic implications of the risks associated with cloud adoption in emerging economies (including concerns about data security and governance in these contexts) (Ukeje,N et al,2024), and (3) the emergence of interdisciplinary links between risk management, information security, confidentiality and cybersecurity, which require an integrated approach to assess and mitigate these risks (Najat Tissir et al,2021). Despite notable progress in assessing the risks associated with cloud computing and the technological solutions proposed for managing them, significant gaps remain, particularly with regard to risks related to data governance, privacy protection, and risk management in multi-cloud or hybrid environments. These issues are particularly pronounced in regions with low digital development, where security infrastructures are often inadequate. The results highlight the need to strengthen the integration of security, transparency and regulatory principles in the adoption of cloud computing in order to respond more effectively to the emerging risks of the 21st century (Said El Kafhali et al,2021).Investments in cloud computing technologies are a key sector in corporate innovation strategies, with major implications for IT risk management, system flexibility and competitiveness. Understanding the academic landscape regarding the impact of cloud computing on risk is essential for informed strategic decisions and effective risk management (Annunziata, G et al,2024) (Alonso, J et al,2023) (Chen, X. et al,2022). This review demonstrates that the impacts of cloud computing on risk are strongly influenced by specific technological and organizational contexts. Further research is needed to better understand disparities in cloud usage, spillover effects related to data security, and the risks associated with increased dependence on cloud service providers (Marston, S. R. et al,2021).Furthermore, it is imperative that policymakers and businesses adopt a more targeted and sustainable approach to cloud computing integration, ensuring better regulation of data security practices and promoting greater resilience to digital risks. Only then can cloud computing truly fulfil its role as a catalyst for growth while limiting the associated risks (Mine Omurgonulsen,2021). However, as with any research, our study has certain methodological limitations. On the one hand, the analysis is based on data from a limited number of databases, which may not capture all publications from emerging or non-English-speaking countries. Secondly, the study focuses on specific topics, which may overlook certain broader aspects of risk management in the cloud environment (Mongeon, P et al ,2016) (Naveen Donthu et al,2021) (Zupic, I et al,2015).

5 Conclusions

Finally, although empirical and contextual studies play a fundamental role in advancing knowledge, they often remain limited in their ability to capture the full complexity and multidimensional dynamics characterizing this field. The predominance of narrowly focused case studies or context-specific analyses may restrict the generalizability of findings and overlook broader structural, technological, and organizational interactions. These limitations highlight the need for more integrative research approaches that combine empirical evidence with theoretical frameworks, longitudinal perspectives, and cross-contextual comparisons. Such approaches

would enable a deeper and more comprehensive understanding of the evolution of the phenomenon, its underlying mechanisms, and its long-term implications. Adopting broader and more holistic analytical perspectives is therefore essential to advance the maturity of the field and to support more informed academic and managerial decision-making.

5.1 Recommendations

- **Assessment of cloud models**: Evaluate the risk levels associated with public, private, and hybrid cloud models, considering the sensitivity of patient data and the criticality of healthcare services.
- **Security and risk management**: Implement measures such as encryption, authentication, and access control to mitigate the risks of data leakage or loss.
- **Emerging technologies**: Examine how innovations like edge computing, serverless architectures, and artificial intelligence can reduce vulnerabilities and strengthen the security of cloud systems.
- **Cloud adoption in Moroccan public healthcare**: Deploy cloud solutions within a clear risk management framework to ensure the confidentiality, integrity, and availability of patient data.
- **Proactive approach**: Anticipate emerging risks associated with the evolution of cloud computing and establish robust governance mechanisms to protect sensitive information over the long term.

5.2 Acknowledgments

At the conclusion of this research work, I would like to express my gratitude to all those who supported me during the preparation of this thesis. First and foremost, I wish to thank my thesis supervisor, Professor JABRAOUI SIHAM, for her guidance, support, and encouragement. I am especially grateful for the trust she placed in me and for allowing me the freedom to shape my work according to my own understanding of the real world. I would also like to thank the entire team of the REFAAD journal for their commitment, follow-up, and encouragement regarding my two published scientific works—the first being a systematic review and the second a bibliometric study. Finally, I sincerely thank all members of my family for standing by my side from the moment I decided to undertake this thesis project, and for their unwavering support and encouragement.

6 References

Alghofaili, Y.; Albattah, A.; Alrajeh, N.; Rassam, M.A.; Al-rimy, B.A.S. (2021). Secure Cloud Infrastructure: A Survey on Issues, *Current Solutions, and Open Challenges. Appl. Sci.* 11, 9005. [DOI]

Alhayan, M. F., & Abuhassna, H. (2024). A Comprehensive Bibliometric Analysis of Cybersecurity Trends on Cloud Computing. *International Journal of Academic Research in Business and Social Sciences,* 14 (1). [DOI]

Alonso, J., Orue-Echevarria, L., Casola, V. et al. (2023). Understanding the challenges and novel architectural models of multi-cloud native applications – a systematic literature review. J Cloud Comp 12, 6. [DOI]

Alouffi, B., et al. (2017). A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies. *IEEE Access.* [DOI]

Annunziata, G., Sheykina, A., Palomba, F., De Lucia, A., Catolino, G., & Ferrucci, F. (2024). *Security Risk Assessment on Cloud: A Systematic Mapping Study*. In 28th International Conference on Evaluation and Assessment in Software Engineering (EASE 2024), 18-21 June 2024, Salerno, Italy. ACM, New York, NY, USA 10 Pages. [DOI]

Chen, X. et al. (2022). Estimating the impact of cloud computing on firm performance: An empirical investigation of listed firms. *Information &Amp; Management,* 59(3), 103603. [DOI]

Dayyabu, U. Y., Uppin, C., & Greenwood, J. (2020). A Bibliometric Analysis of Cloud Security Research. *International Journal of Computer Engineering and Technology,* 11(4), 14-30. http://iaeme.com/Home/issue/IJCET?Volume=11&Issue=4

Donthu, N. et al. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research,* 133, 285–296. [DOI]

Dragoș M., et al. (2024). Mapping the conceptual structure of innovation in artificial intelligence research: A bibliometric analysis and systematic literature review. *Journal of Innovation amp; Knowledge*, 9(1), 100465. [DOI]

El Kafhali, S. et al. (2021). Security Threats, Defence Mechanisms, Challenges, and Future Directions in Cloud Computing. *Archives of Computational Methods in Engineering,* 29(1), 223–246. [DOI]

Jouini, M., & Ben Arfa Rabai, L. (2017). A Security Risk Management Model for Cloud Computing Systems: Infrastructure as a Service. *Security, Privacy, and Anonymity in Computation, Communication, and Storage,* 594–608. [DOI]

Loukides, M. (2021). *The Cloud in 2021: Adoption Continues*. O'REILLY Report.

Maniah, et al. (2022). A systematic literature Review: Risk analysis in cloud migration-2022-Journal of King Saud University. *Computer and Information Sciences,* 34, 3111–3120. [DOI]

Marston, S. R. et al., (April 2021). *Cloud computing*- The business perspective. *Decision Support Systems,* 51(1), 176-189. [DOI]

Mazhar Ali. (2015). Security in Cloud Computing: Opportunities and Challenges. [DOI]

Mongeon, P., & Paul-Hus, A. (2016). The journal coverage of Web of Science and Scopus: a comparative analysis. *Scientometrics,* 106, 213–228. [DOI]

Omurgonulsen, M. (2021). Cloud Computing: A Systematic Literature Review and Future Agenda. *Journal of Global Information Management*, 29 (6). [DOI]

Pan, Jun Sun. (2019). Privacy Protection and Data Security in Cloud Computing: A Survey, Challenges, and Solutions. *Digital Object Identifier.*

Rahman, M. M. et al. (2018). A Model of Factors Influencing Cloud Computing Adoption Among Faculty Members and Students of Higher Educational Institutions of Bangladesh. IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS), 1-5. [DOI]

Tang, H. (2016). A Research for Cloud Computing Security Risk Assessment. *The Open Cybernetics & Systemics Journal,* 10, 210-217.

Tinankoria, D., & Babak Bashari, R. (). Cloud Computing: A review of the Concepts and Deployment Models. *International Journal of Information Technology and Computer Science(IJITCS),* 9 (6), 50-58, 2017.

Tissir, N. et al. (2021). Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal. *Journal of Reliable Intelligent Environments,* [DOI]

Ukeje, N., Gutierrez, J., & Petrova, K. (2024). Information security and privacy challenges of cloud computing for government adoption: a systematic review. *Int. J. Inf. Secur.* 23, 1459–1475. [DOI]

Welsh, T., & Benkhelifa, E. (2020). On Resilience in Cloud Computing: A Survey of Techniques across the Cloud Domain. *ACM Comput. Surv.* 53(3), Article 59, 36 pages. [DOI]

Workshop and Conference (CCWC), Las Vegas, NV, USA, 2018, pp. 347-356.

Xuan Zhang et al. (2023). Information Security Risk Management Framework for the Cloud Computing Environments. 2010 *10th IEEE International Conference on Computer and Information Technology,* 1328–1334. [DOI]

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. [DOI]

Zupic, I., & Čater, T. (2015). Bibliometric Methods in Management and Organisation. *Organisational Research Methods,* 18(3), 429-472. [DOI]