Noname manuscript No.
(will be inserted by the editor)

Information Security and Privacy Challenges of Cloud Computing for Government Adoption: A Systematic Review

Ndukwe Ukeje · Jairo Gutierrez · Krassie Petrova

Received: date / Accepted: date

Abstract The advent of new technologies and applications coupled with the COVID-19 pandemic tremendously increased cloud computing adoption in private and public institutions (government) and raised the demand for communication and access to a shared pool of resources and storage capabilities. Governments across the globe are moving to the cloud to improve services, reduce costs, and increase effectiveness and efficiency while fostering innovation and citizen engagement. However, information security and privacy concerns raised in the past remain significant to government adoption and utilisation of cloud computing. The study conducts a systematic literature review (SLR) using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) approach to examine information security and privacy as the fundamental challenges to government intention to adopt cloud computing. This study screened 758 articles and included 33 articles that revealed information security and privacy as critical factors and barriers to adopting cloud computing through a systematic evaluation (PRISMA approach). The combined two factors contributed 70% of the significant gaps to the cloud computing adoption challenges. In contrast, the individual contribution of information security and privacy as a significant gap to the challenges of cloud adoption yielded 9% and 12%, respectively. Furthermore, 9% of the authors recognised the need for a framework to address the challenges but could not attempt to develop the framework. The study contributes to the information security body of knowledge, PRISMA studies and provides direction in proposing strategies and frameworks to tackle information security and privacy challenges as future research.

Keywords Cloud Computing · Information Security · Privacy · Government Cloud adoption · Cloud Challenges · PRISMA

Ndukwe Ukeje
Department of Computer Science and Software Engineering
Auckland University of Technology, New Zealand
E-mail: ndukwe.ukeje@autuni.ac.nz

Jairo Gutierrez
Department of Computer Science and Software Engineering
Auckland University of Technology, New Zealand
E-mail: jairo.gutierrez@aut.ac.nz

Krassie Petrova
Department of Computer Science and Software Engineering
Auckland University of Technology, New Zealand
E-mail: krassie.petrova@aut.ac.nz

1 Introduction

The emergence of new technologies, applications, and the COVID-19 pandemic has tremendously increased cloud computing adoption in both private and public institutions (government) [1] and have raised the demand for advanced communication, access to a shared pool of resources, and for storage capabilities [2]. At the same time, security and privacy remain a concern for the full adoption and utilisation of effective cloud service delivery [3–5]. However, issues of information security and privacy in cloud computing remain and have lingered for quite some time [6]; though researchers have proposed a range of information security and privacy approaches, mechanisms and frameworks [7], there has been a lesser focus on developing a comprehensive information security and privacy framework for government adoption of cloud computing [8].

Governments rely on cloud services for government-to-government (G2G) and government-to-citizen (G2C)

engagement. However, government activities face growing information and privacy risks, which need to be addressed to improve trust in government service delivery. It has been established by Hurwitz and Kirsch [9] that government has stringent security requirements as information and privacy breaches can lead to severe incidents. Notwithstanding the solutions proposed so far, information security and privacy concerns raised in the past remain a significant challenge to government adoption and utilisation of cloud computing [3, 5, 10, 11]. For instance, national health systems that leverage cloud computing technology for effective service delivery are highly concerned with ensuring information security and privacy; the findings of a related study by Keshta and Odeh [12] demonstrate the security and privacy challeneges of handling patient information in the adoption and implementation of electronic health records.

Various scholars operating within different fields of study have recognised the importance of a systematic literature review as a means of identifying the critical dimensions of phenomenon under investigation e.g. [13]. Thus, a systematic review of the extant research can support achieving the research objectives of this study: to identify and examine information security and privacy as critical factors challenging government intention to adopt cloud services. The research question guiding the study can be formulated as "What is the role of information security and privacy in government cloud service adoption?"

PRISMA, as cited by Page et al. [14], refers to minimum evidence-based items for reporting systematic reviews and meta-analyses findings; however, it can also be used to report systematic reviews with objectives. Furthermore, Page et al.[14] and Sohrabi et al.[15] recognised that the PRISMA approach towards a systematic literature review improved the transparency and the scientific merit of the report in systematic review and meta-analysis studies. The researchers adopted PRISMA due to its transparent and consistent approach in identifying potential areas of research and similar work within the areas, and significant knowledge gaps that demand further investigations.

There has been no extensive systematic review using PRISMA in the area of information security and privacy challenges for government adoption of cloud computing. Hence, the study uses the PRISMA approach to systematically review the relevant and explore information security and privacy as the fundamental challenges for government adoption of cloud computing. Information was sourced through a systematic and manual search of available databases to achieve a comprehensive coverage of the literature while maintaining a focus on security and privacy issues in government cloud adoption for service delivery.

The study contributes to the body of knowledge in PRISMA studies. In contrast to related previous work [16–19, 11, 20] that only identified information security and privacy as critical factors that challenge government intention to adopt cloud service, our study provides directions for further research proposing strategies and frameworks to tackle information security and privacy challenges for full government adoption of the cloud for service delivery to citizens. It highlights the need for more research in developing a standard framework that will cut across different country-specific practices of data migration and retention within cloud platforms as also indicated in prior research [21–24].

2 Methods

The study reviewed existing and related literature using the PRISMA approach [13] to determine information security and privacy as the fundamental challenges for government adoption of cloud computing. This encourages more focus on security and privacy issues in government cloud adoption for service delivery. The adoption of PRISMA in this field is novel as it is mainly used by medical and health scholars [13], while the computer and information systems domain widely considers systematic literature review (SLR) in line with the Kitchenham and Charters [25] technique to discover related information from the selected articles [3]. The PRISMA process was followed to identify, evaluate, and perform a systematic review relevant to examine the information security and privacy challenges of cloud-based computing to improve government adoption. The systematic process, according to Page et al. [14], involves defining the review protocol, selecting data sources and search processes, and determining the literature selection criteria.

2.1 Eligibility

The search was limited to English journal articles and conference papers or proceedings published within five (5) years (2019 – 2023). However, other relevant literature beyond the five years is worth referencing and sorting manually if it involves seminal contributions; in other words, the five years is considered a reasonable period to examine the latest research, but a small

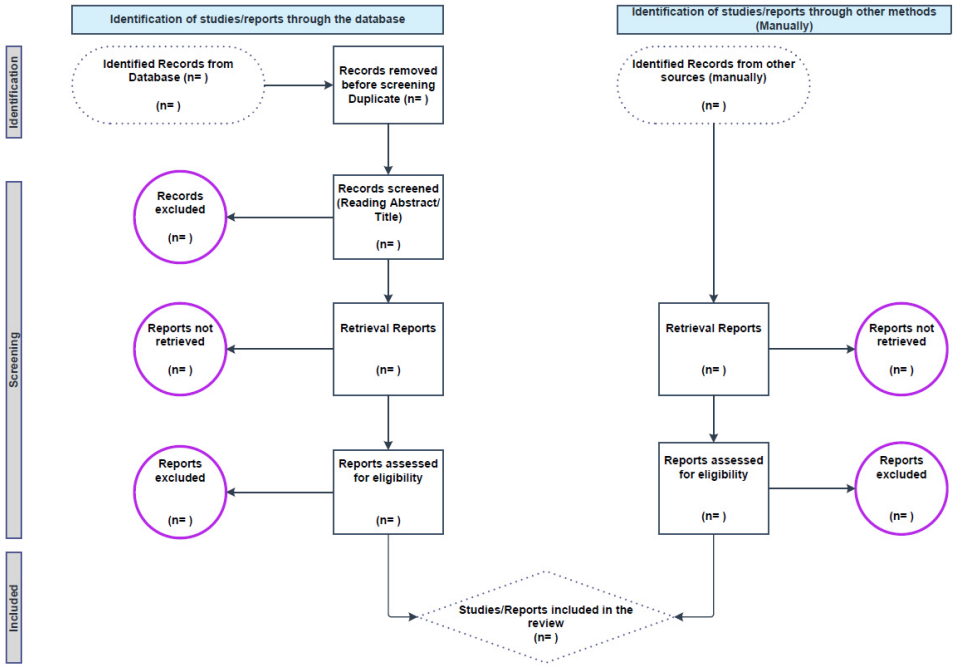

Fig. 1 Adapted PRISMA Flow Diagram for Database and Manual Sorting [26]

number of key papers may also be included. The journal articles and conference papers or proceedings were searched based on related publication titles, subjects, and disciplines that cover information security, data privacy, cloud computing, computer science, and information sciences.

The search records and references were organised using Excel and Endnote applications. The articles were downloaded and read to ascertain their relevance to the study. However, a further review of several valuable works of literature identified significant gaps to support the research objectives in examining information security and privacy challenges that affect government cloud adoption.

2.2 Information Sources

The systematic process identifies the keywords and phrases comprised of information security and privacy in cloud computing, challenges of cloud computing, barriers to government cloud adoption, and information security and cloud computing, among others. The keywords are selected to ensure that we do not miss out on some critical articles relevant to the research. The search keywords were combined with Boolean operators to identify results relevant to the study. The search based on the PRISMA statement of purpose shown in Fig. 1 [26] was presented as follows:

- TITLE-ABS-KEY (information AND security AND privacy AND in AND cloud AND computing) AND PUBYEAR ¿ 2019 AND PUBYEAR ¡ 2023 AND (LIMIT-TO (SRCTYPE,"j") OR LIMIT-TO (SRCTYPE,"p")) AND (LIMIT-TO (PUBSTAGE,"final")) AND (LIMIT-TO (SUBJAREA,"COMP")) AND (LIMIT-TO (DOCTYPE,"re") OR LIMIT-TO (DOCTYPE,"cr")) AND (LIMIT-TO (LANGUAGE,"English"))

- TITLE-ABS-KEY (challenges AND of AND cloud AND computing) AND PUBYEAR ¿ 2018 AND PUBYEAR ¡ 2024 AND (LIMIT-TO (LANGUAGE , "English")) AND (LIMIT-TO (PUBSTAGE , "final")) AND (LIMIT-TO (SRCTYPE , "j") OR LIMIT-TO (SRCTYPE , "p")) AND (LIMIT-TO (SUBJAREA , "COMP")) AND (LIMIT-TO (DOCTYPE , "re") OR LIMIT-TO (DOCTYPE , "cr")) AND (LIMIT-TO (EXACTKEYWORD , "Cloud Computing") OR LIMIT-TO (EXACTKEYWORD , "Cloud Services") OR LIMIT-TO (EXACTKEYWORD , "Cloud Security") OR LIMIT-TO (EXACTKEYWORD , "Challenges") OR LIMIT-TO (EXACTKEYWORD , "Literature Reviews") OR LIMIT-TO (EXACTKEYWORD , "Metadata") OR LIMIT-TO (EXACTKEYWORD , "Cloud-based") OR LIMIT-TO (EXACTKEYWORD , "Cloud Computing Services") OR LIMIT-TO (EXACTKEYWORD , "Security Challenges") OR LIMIT-TO (EXACTKEY-

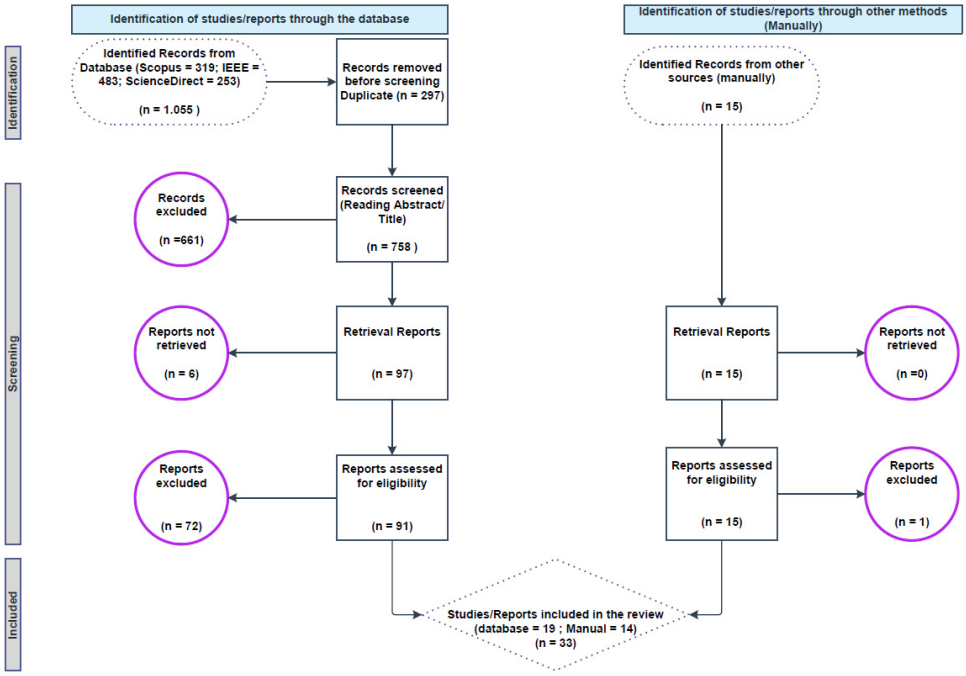

Fig. 2 Adapted PRISMA Flow Diagram Showing the Results of the Database and the Manual Search in this Study

WORD , "Cloud Data Security") OR LIMIT-TO (EXACTKEYWORD , "Security And Privacy") OR LIMIT-TO (EXACTKEYWORD , "Data Privacy"))

- TITLE-ABS-KEY (barriers AND to AND government AND cloud AND adoption) AND PUBYEAR ¿ 2009 AND PUBYEAR ¡ 2023 AND (LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ar") OR LIMIT-TO (DOCTYPE , "ch"))

- TITLE-ABS-KEY (information AND security AND cloud AND computing) AND PUBYEAR ¿ 2019 AND PUBYEAR ¡ 2023 AND (LIMIT-TO (PUBSTAGE,"final")) AND (LIMIT-TO (SUBJAREA,"COMP")) AND (LIMIT-TO (DOCTYPE,"ar") OR LIMIT-TO (DOCTYPE,"cp") OR LIMIT-TO (DOCTYPE,"ch")) AND (LIMIT-TO (EXACTSRCTITLE,"IEEE Transactions On Cloud Computing")) AND (LIMIT-TO (LANGUAGE,"English")) AND (LIMIT-TO (EXACTKEYWORD,"Cloud Computing"))

2.2.1 Search

The process was carried out through various databases (Scopus, IEEE, ScienceDirect) and manually sourced information with a title and keywords through Google Scholar and other related search engines. The databases are considered because of their wider coverage in technology, engineering, computer sciences, etc. The search was carried out separately on various selected databases based on the titles, abstract, and keywords with the following phrases, information security and privacy in cloud computing; challenges of cloud computing; barriers to government cloud adoption; information security and cloud computing. The manual process included searching through Google Scholar and other sources with the specific title of the relevant publications.

2.2.2 Study Selection

The articles from different databases were last sorted on 21/05/2023 and exported as text files and Microsoft Excel spreadsheets based on affiliations with the subjects, titles, authors, year, source, and abstract. The exported documents were first screened by reading the title and abstract to ascertain their relevancy to the study, afterword the article was downloaded for further reading. The inclusion and exclusion screening strategies were identified as 1 – Accepted for further review after going through the title and abstract, 2 – maybe accepted for further review after going through the title and abstract, and 0 – rejected for further review. Further screening selection process was conducted with the endnote to remove the duplicate and ascertain the actual number of relevant papers included and excluded from the study. The authors independently read the articles to determine relevant papers to be included, and any disagreement on inclusion was discussed to achieve consensus.

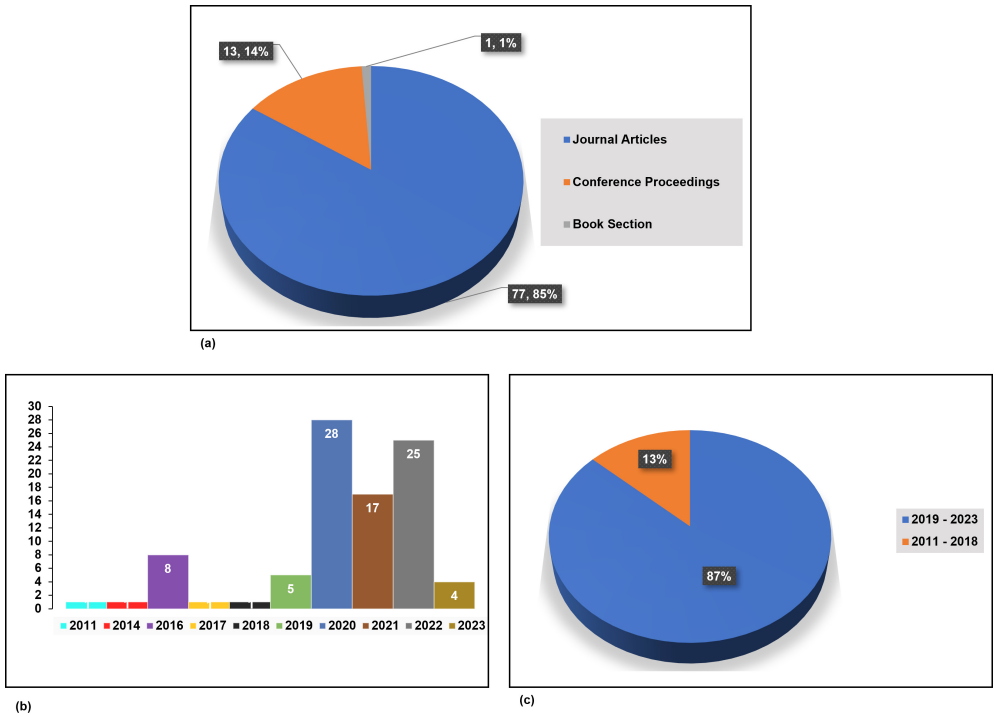

Fig. 3 Distribution of Publications (from Database Search) Screened for Eligibility

The study adapted the PRISMA flow diagram in Fig. 1 for systematic reviews [26]; the flowchart depicts records identified through digital and manual database search sources.

3 Results/Findings

The findings from the PRISMA review in Fig. 2 show that the initial database search from the three different selected databases (IEEE, ScienceDirect, and Scopus) yielded 1,055 research papers (IEEE: 483; ScienceDirect: 253; Scopus: 319). Before the subsequent initial screening, a total of 264 research articles were removed individually because of duplicates across databases (IEEE: 176; ScienceDirect: 67; Scopus: 21); further 33 articles were removed when the results from the three databases were combined. In total, 297 duplicated research articles were removed. Thus, the adjusted number of records to be reviewed was 758 articles. After the initial screening, 661 articles records were excluded because the articles did not match the literature selection criteria for the study. The remaining 97 research articles were sorted for retrieval; however, 6 articles were excluded as not retrievable. Therefore, 91 research articles were retrieved, reviewed, and assessed for eligibility. After this second screening stage of the literature review, 72 articles were excluded due to irrelevancy and for not being applicable to the study. Thus, the search of the three selected databases yielded 19 articles that were found eligible for inclusion in the study review sample.

The study identified 15 more research articles through the manual method. These articles were included because their respective contribution was considered seminal; 14 were found eligible while 1 was excluded as it was a duplicate of an article identified through the database search.

The search process ended with a total 33 research articles to be included in the review, as shown in Fig. 2 and Table 1; out of the 33 eligible articles, 19 were found through the database search, while 14 more articles were found through the manual search. The review articles were last sorted on 21/05/2023.

3.1 Syntheses of the Results

As a result of the database search, 91 documents were retrieved (out of the 97 found eligible to be included in the review). The distribution of the 91 retrieved documents according to reference type was as follows: 77 (85%) were journal articles, while the remaining 14 publications were published as papers in conference proceedings (13, or 14%), or as book chapters (1, or 1%) (Fig. 3). This distribution confirmed the relevance of the eligibility criteria: most of the relevant publica-

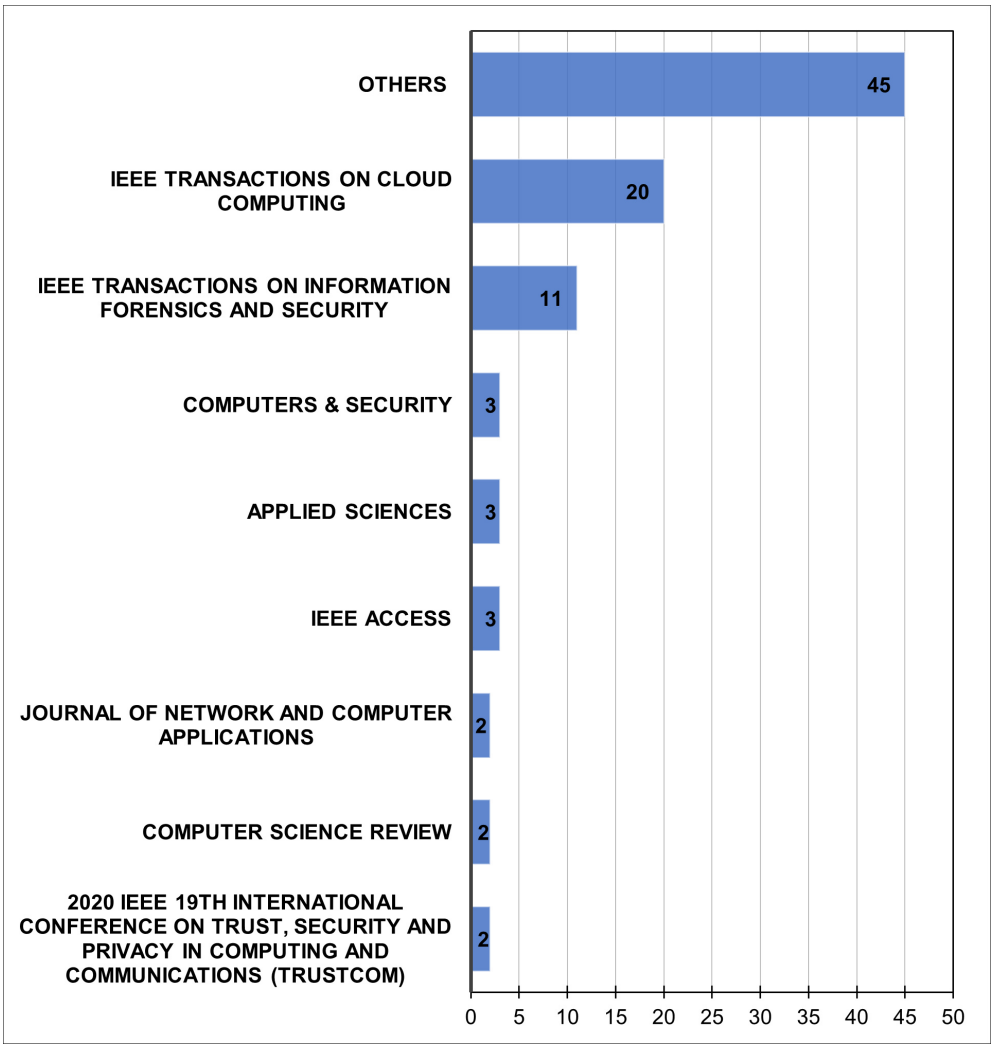

Fig. 4 Distribution of Articles Screened for Eligibility by Publication (Database Search)

tions were journal articles and conference papers. Significantly, the yearly distribution of the articles screened indicated that the majority of the retrieved articles were relatively published recently, between 2019 and 2023 (87%) (Fig. 3). From the manual search, the 14 retrieved screened articles were from different individual publications, and none were from the same publisher; 13 (93%) out of the 14 articles were journal articles, while 1 (7%) was a book.

The distribution of articles screened for eligibility based on publication outlets (Fig. 4) shows the number of articles from different journals. IEEE (Transactions on Cloud Computing and Transactions on Information Forensics and Security) had the highest number of peer-reviewed articles (31), followed by six journals with 2 or more articles sourced from each one of them. The articles classified as 'Other' in Fig. 4 were each published in a different journal or conference proceedings (for details on the publications, see Table 2 in Appendix).

The review sample included 33 articles, of which 19 were sourced through the database search while 14 were manually sourced. Fig. 5a shows the distribution of the articles to be included in the review according to the year of publication. The distribution of the included reviewed articles by reference type in Fig. 5c shows 82% (27) journal articles, 12% (4) papers in conference proceedings, and 6% (2) book sections; this distribution re-confirms that relevance of the research eligibility criteria. Furthermore, the percentage distribution of the articles by year in Fig. 5b shows that 70% of the included articles fall within the review eligibility criteria for 2019 to 2023. However, the remaining 30% of relevant literature sources were published between 2010 and 2018, i.e., beyond the five-year period originally stipulated. These articles were found worth referencing and were included in the review due to the significance

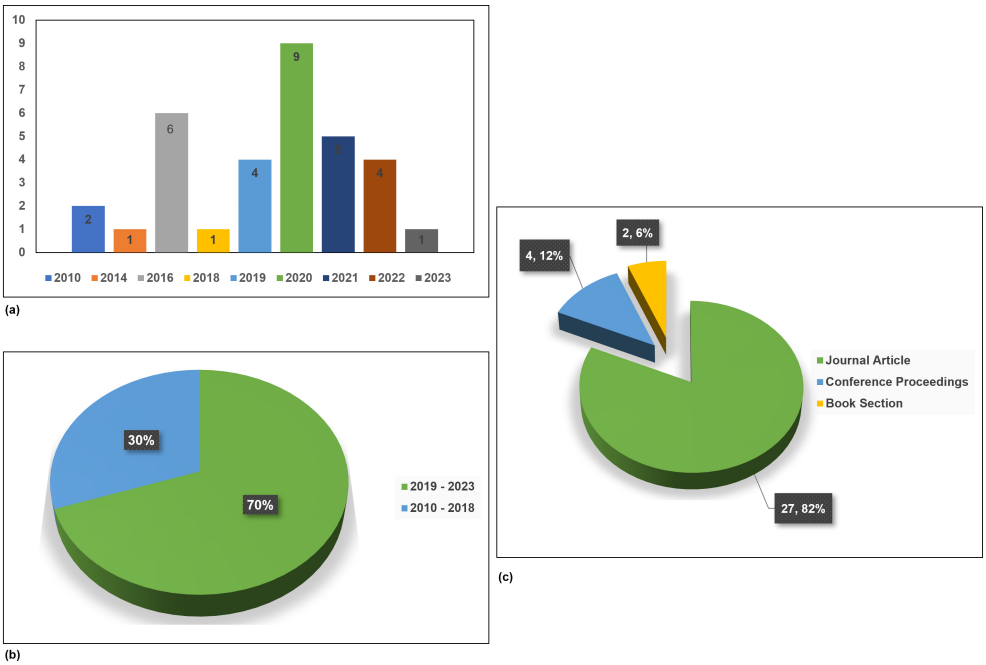

Fig. 5 Distribution of Included Articles

of their contributions. The distribution of the articles to be reviewed by publication shows that articles were sourced from a wide range of publication outlets (Table 3 in Appendix).

The results of the review of the 33 articles in the review sample indicated that in most studies, information security and privacy were identified jointly as critical, challenging factors for cloud service adoption. In contrast, only in a few studies information security and privacy were considered as two separate factors that deterred governments from fully adopting cloud computing for service delivery. This is evident in Fig. 6; the grouping of the two critical factors, information security and privacy, yielded the highest percentage 70% (27) of the distribution, while the individual representation of information security and privacy yielded 9% (2) and 12% (4), respectively. However, it is surprising that privacy delivered more in terms of the critical, challenging factor than information security; this could be because of growing identity theft threats affecting various government and corporate institutions [27].

4 Discussion

We conducted a thorough systematic review to identify and examine information security and privacy as critical factors that challenge governments' intention to adopt cloud services. To achieve the objective, we adopted the PRISMA methodology due to its transparent and consistent approach in identifying potential areas for investigation, similar work within the areas, and significant knowledge gaps that demand further investigation. Our results, as synthesised in Table 1, showed that information security and privacy were identified as significant issues that challenged the government's intention to adopt cloud computing to deliver services to its citizens effectively but without developing an appropriate governance framework. The results in Fig. 7 shows the distribution of 'significance gaps' in the reviewed articles included in the study. The representation of a significance gap margin of 1 in the line graph indicates that the authors have acknowledged one or two of the significant factors shown in Fig. 6 as a challenge to government adoption of cloud for service delivery. Some authors acknowledged the lack of framework as a challenging factor and encouraged the development of a framework to mitigate the challenges. The zero (0) margin in the line graph (Fig. 7) indicates the point where the authors did not acknowledge one or two of the significant challenging factors.

These results imply that in the literature, information security and privacy are identified as a critical challenge that deters government intention to adopt cloud services. These findings align with the earlier work [16–19, 28, 11, 20], that considers information security and privacy as a significance obstacle to cloud service adoption within government organisations and proposes strategies and frameworks to tackle information security and

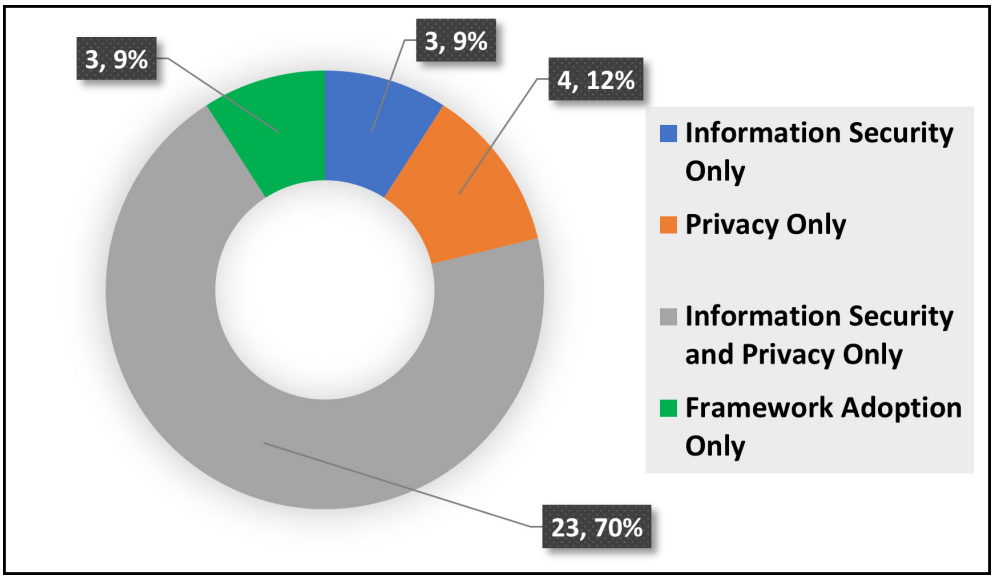

Fig. 6 Distribution of Challenging Factors

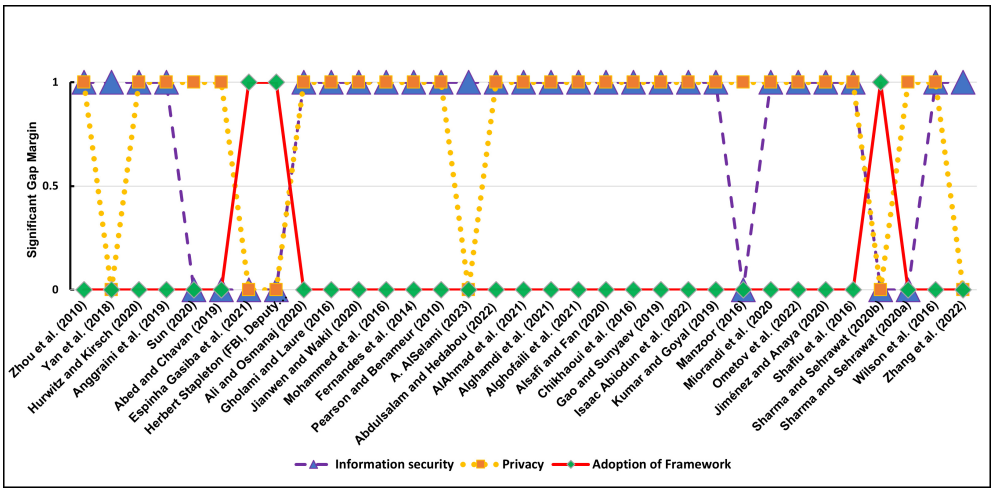

Fig. 7 Distribution of Significance Gaps (by Authorship)

privacy challenges as future research.

Our analysis shows evidence of an overlap between information security and privacy, as combining the two factors contributed to 70% (23) of the significant factors in the cloud computing adoption challenges, as shown in Fig. 6. At the same time, the individual contribution of information security and privacy as a significant factor to the challenges of cloud adoption yielded 9% (3) and 12% (4), respectively. Furthermore, 9% (3) of the authors recognise the need for a framework to address those challenges but did not attempt to develop a framework. Furthermore, in some instances, researchers identify information security and privacy as distinct disciplines, while others consider them as overlapping. Therefore, it is essential to recognise that government cannot deploy effective privacy strategies or frameworks without a solid information security foundation [29]. The investigation shows significant corroboration with works that capture iinformation security and privacy together and observe them as two apparent factors that deter the government from fully adopting cloud computing for service delivery, further recognising the need for a framework to mitigate those challenges (see Fig. 6 and Table 1).

These findings undermine the previous work such as the suggestion in the study by [18] that there is a need to create a system of 'Health-specific Cloud' for the government health sector without considering the cost-effectiveness and data distribution, retention, and migration when cloud-specific approach is adopted differ-

ently in health sectors. However, our findings are consistent and corroborated with the suggestions to adopt an adaptive mechanism [16] and to develop a holistic cloud service framework and strategies that cover every sector of government [17,1,23]. In contrast to previous related studies [16–19,11,20] that only identify information security and privacy as critical factors that challenge government intention to adopt cloud service, our study provides further direction in proposing strategies and frameworks to tackle information security and privacy challenges for government full adoption of the cloud for service delivery to citizens. This study also highlights the need for more research in the area of developing a standard framework that will cut across different country-specific data migration and retention practices within cloud platforms, as supported by various literature [21–24].

The use of the PRISMA approach for the systematic literature review could be a limitation as it may be more suitable for work done by medical and health scholars [13]; however, it has demonstrated its relevance in our study in identifying potential research areas and similar work within the areas, including areas requiring further research. Future research applying different systematic literature review approaches could reconfirm the findings of this study. The researchers see this as a gap that needs to be addressed to contribute to the security aspect of government policy initiatives for protecting government information and citizen privacy while utilising the cloud for service delivery.

5 Conclusion

Government cloud services' information security and privacy challenges can not only be solved technically; other approaches such as standardisation, frameworks, laws, and regulations are required to prevent and mitigate security threats and achieve a resilient and secure cloud environment. Due to the dynamic nature of cloud computing technology, researchers, academia, industry, and government need to continuously collaborate to secure a cloud computing environment.

The study conducted a systematic literature review using a PRISMA approach to examine information security and privacy as the fundamental challenges for government adoption of cloud computing and synthesise the relevant findings. The review provided a systematic evaluation with results encouraging more focus on security and privacy issues in government cloud adoption. The findings of the study confirmed security and privacy as critical factors and barriers to adopting cloud computing services. However, only a few researchers have suggested implementing and adopting frameworks to address those challenges and encourage the government's intention to adopt cloud computing for service delivery to its citizens. The researchers see this as a gap that needs to be addressed to contribute to the security aspect of government policy initiatives for protecting government information and citizen privacy while utilising the cloud for service delivery.

Furthermore, the researchers believe that the study contributes to the body of knowledge and improve the adoption of PRISMA in conducting a systematic literature review. The study also contributes to the exploration of framework adoption to encourage mitigation of cloud security risks and privacy challenges while inspiring citizen participation and government intention to adopt the cloud for effective service delivery.

6 Further Study

The government cloud governance structures exist with question marks because of their limited ability to identify and manage risks associated with cloud environments. Therefore, any government adopting the cloud should proceed cautiously because an appropriate governance structure is required, without which cloud implementation will probably have undesirable consequences for the government. Hence, a continuation of this study may be conducting a survey to examine the information security and privacy challenges and explore the development of a framework to mitigate gaps in government adoption of cloud for service delivery and to address cross-border management of citizen information and privacy challenges to data retention, storage, and transfer between countries.

Statements and Declarations

The authors have no competing interests to declare that are directly or indirectly related to the content of this article.

Research Data Policy and Data Availability Statements

All data supporting the findings and the analysis of this study are available within the paper and its Supplementary Information files.

Table 1 Literature Review Gaps and Significance

Reference Author	Information Security	Privacy	Governance Framework for Cloud Adoption	Significance Gaps
Zhou et al. [30]	✓	✓	*	Identified security and privacy as the significant barriers to cloud computing adoption but did not propose measures to encourage government adoption.
Yan et al. [24]	✓	*	*	Confirmed security is the biggest obstacle to adopting cloud computing without consideration for privacy or an acknowledged framework to encourage government cloud service adoption.
Hurwitz and Kirsch [9]	✓	✓	*	Confirmed that the government requires stringent security measures as the breach of its information and privacy could cause incidents.
Anggraini et al. [8]	✓	✓	*	Confirmed less research into information security and privacy challenges associated with government cloud adoption and service delivery has been done.
Sun [31]	*	✓	*	Structural characteristics of the cloud computing environment led to Cloud Service providers (CSPs) disclosing customers' privacy in the transmission, processing, and storage process in its outsourcing service model.
Abed and Chavan [32]	*	✓	*	Identified data privacy as a significant challenge in cloud computing for multinational corporations but could not consider the government. Also, buttress that there are no common laws to protect data across borders as institutional and regulatory constraints and governance differ across countries.
Espinha Gasiba et al [1]	*	*	✓	Confirms the need to develop a framework to improve awareness of vulnerabilities in cloud infrastructures. However, it should have considered other areas that cover a holistic framework for government adoption of cloud services.
Herbert Stapleton (FBI, Deputy Assistant Director) in Verizon [33]	*	*	✓	Acknowledged adopting an interwoven framework to protect government cloud computing as critical infrastructure.
Mohammed et al. [11], Ali and Osmanaj [34], Gholami and Laure [35], Jianwen and Wakil [36]	✓	✓	*	Attributed security and privacy as significant reasons that influenced the adoption of cloud computing.
Fernandes et al. [37], Pearson and Benameur [38]	✓	✓	*	The success of cloud computing relies on a clear understanding of security and privacy risks in cloud computing.
AlSelami [39]	✓	*	*	Acknowledged security (DDoS) as a critical factor to why organisations prefer not to move to cloud services but rather utilise their own standalone devices to keep critical information.
Abdulsalam and Hedabou [16]	✓	✓	*	Highlights cloud privacy protection and data security as the primary challenges to cloud service model adoption. Further, it envisaged cloud computing to be prone to security and privacy without the practical adoption of adaptive mechanisms for user experience.

✓ Denotes identification of the factor included as a gap. *Denotes identification of the factor not included as a gap.

Table 1 Literature Review Gaps and Significance (Continued)

Reference Author	Information Security	Privacy	Governance Framework for Cloud Adoption	Significance Gaps
AlAhmad et al. [40]	✓	✓	*	Reveal that the existing mobile cloud computing model could not address all security issues and that disregarding any of the mobile cloud computing issues will result in the exposure of data security, privacy, and integrity, which affect cloud data centres.
Alghamdi et al [21]	✓	✓	*	The research measured the architectural requirements to overcome common technical cloud barriers identified as data security and privacy, which poses challenges that require strategic effort to address - of which appropriate guidelines and practices, as highly ranked by the survey, will be required. It supports the need for an adequate strategic framework to address the challenges.
Alghofaili et al. [41]	✓	✓	*	Reviewed the security issues in cloud computing infrastructure and identified data security and privacy as the significant challenges to adopting cloud computing.
Alsafi and Fan [17]	✓	✓	*	The study found the most common challenges to cloud adoption in SMEs of the Saudi Arabian Government as security, privacy, and others. Further, they identified that addressing such barriers will help the Saudi government and SMEs develop effective strategies for adopting cloud computing.
Chikhaoui et al. [18]	✓	✓	*	Information security and privacy still need to be improved despite potential gains from eHealth services' cloud computing. The study identified security and privacy as key challenges to fully adopting cloud computing in the Saudi healthcare sector. They further highlighted the need for a specific framework for security management in cloud computing for the health sector.
Gao and Sunyaev [19]	✓	✓	*	Reviewed data/information collected from patients as context matters requiring protection as it remains individual (patients) property. It highlighted concerns about the patient's data/information as security, privacy, and interoperability. It suggested the need to further investigate Cloud computing adoption in the healthcare sector (government) by relying on specific that challenges patients' data/information.
Isaac Abiodun et al. [42]	✓	✓	*	The survey acknowledged security and privacy issues in the industry as the reason for the gradual acceptance of cloud computing. Further, reveal that assurances on the security of provenance information from cloud services are crucial to the key areas that can give cloud forensic investigators a mechanism to gather investigatory provenance evidence. In the plan, he proposed a project mechanism that will focus on cross-border infrastructure privacy protection to address increasing concerns about the security of personal data in the cloud.

✓ Denotes identification of the factor included as a gap. *Denotes identification of the factor not included as a gap.

Table 1 Literature Review Gaps and Significance (Continued)

Reference Author	Information Security	Privacy	Governance Framework for Cloud Adoption	Significance Gaps
Kumar and Goyal [43]	✓	✓	*	The study explained the inhibition of widespread adoption of cloud-enabled services as the associated security and privacy challenges, which required further exploration. It further suggested future research in implementing and developing self-adaptive security countermeasures to cater to the cloud environment's changing landscape of threats and dynamism. The study considers the security threats dynamism existing within the government landscape to address the challenges to government adoption of cloud services.
Manzoor [22]	*	✓	*	Arguably agree that data privacy and regulatory issues are the barriers to government adoption of cloud services and implementation. He recommended the implementation of the governance framework for cloud implementation at all levels, which needs to be addressed.
Miorandi et al. [44]	✓	✓	*	The survey highlighted data security and privacy as key barriers to adopting innovative IT solutions like cloud computing. It proposes a machine-readable approach (sticky policy) to improve users' data control to ensure confidentiality.
Ometov et al. [45]; Jiménez and Anaya [41]	✓	✓	*	The survey considered security and privacy as the primary setbacks limiting organisations from adopting cloud computing. However, it believes that technology (IDS and encryption) can be deployed to mitigate some of the issues. Still, more research must be done due to the need for more standardisation to address new techniques and mechanisms.
Shafiu et al. [20]	✓	✓	*	The study observed two significant barriers to adopting cloud computing service (IaaS) in public sector organisations: security and privacy, which override cost savings as the most perceived driver identified. However, the study is limited to a single government agency and could not recommend possible solutions to address the gaps; instead, more work could be done to confirm existing drivers and barriers to aid the decision-making process in similar contexts.
Sharma and Sehrawat [23]	*	*	✓	The study identified and examined the barriers to cloud computing adoption in the manufacturing sector in India using SWOT factors. The finding demonstrated the lack of government policy standards as one of the most critical factors influencing the adoption decision in government. The findings support the researcher's need to develop a framework to address the challenges and encourage government cloud adoption for service delivery.

✓ Denotes identification of the factor included as a gap. *Denotes identification of the factor not included as a gap.

Table 1 Literature Review Gaps and Significance (Continued)

Reference Author	Information Security	Privacy	Governance Framework for Cloud Adoption	Significance Gaps
Sharma and Sehrawat [46]	*	✓	*	The research investigated the determinants influencing cloud computing adoption decisions in the healthcare sector. The study identified security, amongst others, as the critical drawback to adopting cloud computing in the sector. Further, highlight that proper policies and framework through legislation can improve the adoption of cloud services.
Wilson et al. [47]	✓	✓	*	The study identified the security of cloud services and data privacy as barriers to cloud adoption among small and medium enterprises in Tamil Nadu.
Zhang et al. [48]	✓	*	*	In reference to the survey, the research paper identified cloud security as a challenge to power grid operators and utilities' hesitant adoption of cloud technology. The security challenges are identified as shared responsibilities between the power users and the cloud service providers, and such responsibilities depend on the cloud service model in existence.

✓ Denotes identification of the factor included as a gap. ∗Denotes identification of the factor not included as a gap.

References

1. Espinha Gasiba, T., Andrei-Cristian, I., Lechner, U., and Pinto-Albuquerque, M., Raising Security Awareness of Cloud Deployments using Infrastructure as Code through CyberSecurity Challenges, The 16th International Conference on Availability, Reliability and Security, 1-8 (2021) https://doi.org/10.1145/3465481.3470030
2. Alhomdy, S., et al., The role of cloud computing technology: A savior to fight the lockdown in COVID 19 crisis, the benefits, characteristics and applications, International Journal of Intelligent Networks, 2, 166-174, (2021) https://doi.org/10.1016/j.ijin.2021.08.001
3. Al Hadwer, A., et al., A Systematic Review of Organizational Factors Impacting Cloud-based Technology Adoption Using Technology-Organization-Environment Framework, Internet of Things, 15, 100407, (2021) https://doi.org/10.1016/j.iot.2021.100407
4. Salem, M.M. and G.-H. Hwang, Critical Factors Influencing Adoption of Cloud Computing for Government Organizations in Yemen, The Journal of Distribution Science, 14 (11), 37-47, (2016) https://doi.org/10.15722/jds.14.11.201611.37
5. Nugraha, Y. and A. Martin, Towards a framework for trustworthy data security level agreement in cloud procurement, Computers and Security, 106, 102266, (2021) https://doi.org/10.1016/j.cose.2021.102266
6. Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L., and Leaf, D, NIST cloud computing reference architecture, NIST special publication, 500, 1-28, (2011) https://doi.org/10.1016/j.cose.2021.102266
7. Alonso, J., M. Escalante, and L. Orue-Echevarria, Transformational Cloud Government (TCG): Transforming Public Administrations with a Cloud of Public Services, Procedia Computer Science, 97, 43-52, (2016) https://doi.org/10.1016/j.procs.2016.08.279
8. Anggraini, N., Binariswanto, and N. Legowo, Cloud Computing Adoption Strategic Planning Using ROCCA and TOGAF 9.2: A Study in Government Agency, Procedia Computer Science, 161, 1316-1324, (2019) https://doi.org/10.1016/j.procs.2019.11.247
9. Hurwitz, J.S. and D. Kirsch, Cloud computing for dummies, John Wiley and Sons, (2020)
10. Liu, Y., Sun, Y. L., Ryoo, J., Rizvi, S., and Vasilakos, A. V., A survey of security and privacy challenges in cloud computing: solutions and future directions, Journal of Computing Science and Engineering, 9(3), 119-133, (2015) https://doi.org/10.5626/JCSE.2015.9.3.119
11. Mohammed, F., O. Ibrahim, and N. Ithnin, Factors influencing cloud computing adoption for e-government implementation in developing countries, Journal of Systems and Information Technology, 18(3), 297-327, (2016) https://doi.org/10.1108/JSIT-01-2016-0001
12. Keshta, I. and A. Odeh, Security and privacy of electronic health records: Concerns and challenges, Egyptian Informatics Journal, 22(2), 177-183, (2021) https://doi.org/10.1016/j.eij.2020.07.003
13. Pahlevan-Sharif, S., P. Mura, and S.N.R. Wijesinghe, A systematic review of systematic reviews in tourism. Journal of Hospitality and Tourism Management, 39, 158-165 (2019) https://doi.org/10.1016/j.jhtm.2019.04.001
14. Page, M. J., Moher, D., 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., . . . McKenzie, J. E., PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews, BMJ, 372, n160, (2021) https://doi.org/10.1136/bmj.n160
15. Sohrabi, C., Franchi, T., Mathew, G., Kerwan, A., Nicola, M., Griffin, M., Agha, M., and Agha, R., PRISMA 2020 statement: What's new and

the importance of reporting guidelines. International Journal of Surgery, 88, 105918, (2021) https://doi.org/https://doi.org/10.1016/j.ijsu.2021.105918
16. Abdulsalam, Y. S., and Hedabou, M., Security and Privacy in Cloud Computing: Technical Review, Future Internet, 14(1), 11 (2022) https://doi.org/10.3390/fi14010011
17. Alsafi, T., and Fan, I. S., Cloud Computing Adoption Barriers Faced by Saudi Manufacturing SMEs, 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 1- 6 (2020)
18. Chikhaoui, E., Sarabdeen, J., and Parveen, R., Privacy and security issues in the use of clouds in e-health in the Kingdom of Saudi Arabia, Proceedings of the 28th International Business Information Management Association Conference - Vision 2020: Innovation Management, Development Sustainability, and Competitive Economic Growth, (2016)
19. Gao, F., and Sunyaev, A., Context matters: A review of the determinant factors in the decision to adopt cloud computing in healthcare, International Journal of Information Management, 48, 120-138 (2019) https://doi.org/10.1016/j.ijinfomgt.2019.02.002
20. Shafiu, I., Wang, W. Y. C., and Singh, H., Drivers and barriers in the decision to adopt IaaS: A public sector case study, International Journal of Business Information Systems, 21(2), 249-267 (2016) https://doi.org/10.1504/IJBIS.2016.074257
21. Alghamdi, B., Potter, L. E., and Drew, S., Validation of architectural requirements for tackling cloud computing barriers: Cloud provider perspective, Procedia Computer Science, 181, 477-486 (2021)
22. Manzoor, A., Cloud Computing Applications in the Public Sector, In Cloud Computing Technologies for Connected Government, 215-246 (2016). https://doi.org/10.4018/978-1-4666-8629-8.ch009
23. Sharma, M., and Sehrawat, R., Quantifying SWOT analysis for cloud adoption using FAHP-DEMATEL approach: evidence from the manufacturing sector, Journal of Enterprise Information Management, 33(5), 1111-1152 (2020) https://doi.org/10.1108/JEIM-09-2019-0276
24. Yan, L., Hao, X., Cheng, Z., and Zhou, R., Cloud Computing Security and Privacy, Proceedings of the 3rd International Conference on Big Data and Computing, Shenzhen, China., 119-123 (2018)-https://doi.org/10.1145/3220199.3220217
25. Kitchenham, B. and S. Charters, Guidelines for performing systematic literature reviews in software engineering, Technical report, ver. 2.3 ebse technical report. ebse (2007)
26. 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., and Brennan, S. E., The PRISMA 2020 statement: an updated guideline for reporting systematic reviews, International journal of surgery, 88, 105906, (2021)
27. Burnes, D., DeLiema, M., and Langton, L., Risk and protective factors of identity theft victimization in the United States. Prev Med Rep, 17, 101058 (2020) https://doi.org/10.1016/j.pmedr.2020.101058
28. Jiménez, S. D. O., and Anaya, E. A., A Survey on Information Security in Cloud Computing, Computacion y Sistemas, 24(2), 819-833 (2020) https://doi.org/10.13053/CyS-24-2-3119
29. Force, J.T. and T. Initiative, Security and privacy controls for federal information systems and organizations, NIST Special Publication, 8-13, (2013)
30. Zhou, Minqi and Zhang, Rong and Xie, Wei and Qian, Weining and Zhou, Aoying, Security and Privacy in Cloud Computing: A Survey, 2010 Sixth International Conference on Semantics, Knowledge and Grids., 105-112 (2010)
31. Sun, P.. Security and privacy protection in cloud computing: Discussions and challenges. Journal of Network and Computer Applications, 160, 102642 (2020)
32. Abed, Y. and M. Chavan, The Challenges of Institutional Distance: Data Privacy Issues in Cloud Computing, Science, Technology and Society. 24(1), 161-181 (2019) https://doi.org/10.1177/0971721818806088
33. Verizon, Verizon 2021 Data Breach Investigations Report, Verizon 2021DBIR Master's Guide, (2021)
34. Ali, O., and Osmanaj, V., The role of government regulations in the adoption of cloud computing: A case study of local government, Computer Law and Security Review, 36, 105396 (2020) https://doi.org/10.1016/j.clsr.2020.105396
35. Gholami, A., and Laure, E., Security and privacy of sensitive data in cloud computing: a survey of recent developments, arXiv preprint arXiv:1601.01498 (2016)
36. Jianwen, C., and Wakil, K., A model for evaluating the vital factors affecting cloud computing adoption, Kybernetes, 49(10), 2475-2492 (2020) https://doi.org/10.1108/K-06-2019-0434
37. Fernandes, D. A. B., Soares, L. F. B., Gomes, J. V., Freire, M. M., and Inácio, P. R. M., Security issues in cloud environments: A survey. International Journal of Information Security, 13(2), 113-170 (2014) https://doi.org/10.1007/s10207-013-0208-7
38. Pearson, S., and Benameur, A., Privacy, Security and Trust Issues Arising from Cloud Computing, 2010 IEEE Second International Conference on Cloud Computing Technology and Science, 693-702 (2010)
39. AlSelami, F. A., Major Cloud Computing Security Challenges with Innovative Approaches. Tehnicki Glasnik, 17(1), 141-145 (2023) https://doi.org/10.31803/tg-20220826124655
40. AlAhmad, A. S., Kahtan, H., Alzoubi, Y. I., Ali, O., and Jaradat, A., Mobile cloud computing models security issues: A systematic review, Journal of Network and Computer Applications, 190, Article 103152 (2021) https://doi.org/10.1016/j.jnca.2021.103152
41. Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M. A., and Al-Rimy, B. A. S., Secure cloud infrastructure: A survey on issues, current solutions, and open challenges, Applied Sciences (Switzerland), 11(19), Article 9005 (2021) https://doi.org/10.3390/app11199005
42. Isaac Abiodun, O., Alawida, M., Esther Omolara, A., and Alabdulatif, A., Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey, Journal of King Saud University - Computer and Information Sciences, 34(10), 10217-10245 (2022) https://doi.org/10.1016/j.jksuci.2022.10.018
43. Kumar, R., and Goyal, R., On cloud security requirements, threats, vulnerabilities and countermeasures: A survey, Computer Science Review, 33, 1-48 (2019) https://doi.org/10.1016/j.cosrev.2019.05.002
44. Miorandi, D., Rizzardi, A., Sicari, S., and Coen-Porisini, A., Sticky Policies: A Survey, IEEE Transactions on Knowledge and Data Engineering, 32(12), 2481-2499. (2020) https://doi.org/10.1109/TKDE.2019.2936353

45. Ometov, A., Molua, O. L., Komarov, M., and Nurmi, J., A Survey of Security in Cloud, Edge, and Fog Computing, Sensors, 22(3), 927 (2022) https://www.mdpi.com/1424-8220/22/3/927
46. Sharma, M., and Sehrawat, R., A hybrid multi-criteria decision-making method for cloud adoption: Evidence from the healthcare sector, Technology in Society, 61, Article 101258 (2020) https://doi.org/10.1016/j.techsoc.2020.101258
47. Wilson, B. M. R., Khazaei, B., and Hirsch, L., Enablers and Barriers of Cloud Adoption among Small and Medium Enterprises in Tamil Nadu, Proceedings - 2015 IEEE International Conference on Cloud Computing in Emerging Markets, CCEM 2015, 140-145 (2015) doi: 10.1109/CCEM.2015.21
48. Zhang, S., Pandey, A., Luo, X., Powell, M., Banerji, R., Fan, L., Parchure, A., and Luzcando, E., Practical Adoption of Cloud Computing in Power Systems - Drivers, Challenges, Guidance, and Real-World Use Cases, IEEE Transactions on Smart Grid, 13(3), 2390-2411 (2022) https://doi.org/10.1109/TSG.2022.3148978

Appendices

Table 2 Distribution of Screened Articles for Eligibility by Journal Publications

Article Publications	Screened Articles
Tehnički glasnik	1
Future Internet	1
Computers	1
IEEE Access	3
IEEE Transactions on Information Forensics and Security	11
CLOSER 2016 - Proceedings of the 6th International Conference on Cloud Computing and Services Science	1
Verizon 2021DBIR Master's Guide	1
2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)	2
AMCIS 2017 - America's Conference on Information Systems: A Tradition of Innovation	1
ACM Computing Surveys	1
Advances in Engineering Software	1
Applied Sciences	3
Arabian Journal for Science and Engineering	1
Archives of Computational Methods in Engineering	1
Artif Intell Med	1
Cloud Computing Technologies for Connected Government	1
Comput Intell Neurosci	1
Computación y Sistemas	1
Computer Law & Security Review	1
Computer Science Review	2
Computer Standards & Interfaces	1
Computers & Security	3
Electronics	1
Frontiers in Computer Science	1
IEEE Internet of Things Journal	1
IEEE Transactions on Cloud Computing	20
IEEE Transactions on Knowledge and Data Engineering	1
IEEE Transactions on Smart Grid	1
International Journal of Advanced Science and Technology	1
International Journal of Advanced Technology and Engineering Exploration	1
International Journal of Business Information Systems	1
International Journal of Information Management	1
International Journal of Web Information Systems	1
Internet of Things	1
Journal of Enterprise Information Management	1
Journal of Grid Computing	1
Journal of Information Security and Applications	1
Journal of Information Systems Engineering and Management	1
Journal of King Saud University - Computer and Information Sciences	1
Journal of Network and Computer Applications	2
Journal of Physics: Conference Series	1
Library Hi Tech	1
Procedia Computer Science	1
Proceedings - 2015 IEEE International Conference on Cloud Computing in Emerging Markets, CCEM 2015	1
Proceedings - IEEE Military Communications Conference MILCOM	1
Proceedings of the 11th Australian Information Security Management Conference, ISM 2013	1
Proceedings of the 28th International Business Information Management Association Conference - Vision 2020: Innovation Management, Development	1
Proceedings of the Confluence 2020 - 10th International Conference on Cloud Computing, Data Science and Engineering	1
Scientific Programming	1
Sensors (Basel)	1
SIGMIS-CPR 2016 - Proceedings of the 2016 ACM SIGMIS Conference on Computers and People Research	1
Technology in Society	1
Wireless Personal Communications	1

Table 3 Distribution of Included Articles to the Review by Publications

Article Publications	Screened Articles
Tehnički glasnik	1
Future Internet	1
Journal of Network and Computer Applications	1
Procedia Computer Science	1
Applied Sciences	1
Journal of Information Systems Engineering and Management	1
Proceedings of the 28th International Business Information Management Association Conference - Vision 2020: Innovation Management, Development Sustainability, and Competitive Economic Growth	1
2021DBIR Master's Guide	1
International Journal of Information Management	1
Journal of King Saud University - Computer and Information Sciences	1
Computer Science Review	1
Cloud Computing Technologies for Connected Government	1
Sensors (Basel)	1
Computación y Sistemas	1
International Journal of Business Information Systems	1
Journal of Enterprise Information Management	1
Technology in Society	1
Proceedings - 2015 IEEE International Conference on Cloud Computing in Emerging Markets, CCEM 2015	1
IEEE Transactions on Smart Grid	1
IEEE Transactions on Knowledge and Data Engineering	1
Science, Technology and Society	1
Computer Law & Security Review	1
Procedia Computer Science	1
The 16th International Conference on Availability, Reliability and Security	1
International Journal of Information Security	1
arXiv preprint arXiv:1601.01498	1
John Wiley & Sons	1
Kybernetes	1
ACM	1
Journal of Systems and Information Technology	1
2010 IEEE Second International Conference on Cloud Computing Technology and Science	1
Journal of Network and Computer Applications	1
2010 Sixth International Conference on Semantics, Knowledge and Grids	1