International Journal of Engineering & Technology, 11 (1) (2022) 10-13

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

A Systematic Literature Review on Security Challenges In A Hybrid Cloud Database

Shahad S. Aljehani[1*] **and Norah S. Farooqi**[2]

[1,2] *Umm Al-Qura University, College of Computer and Information Systems, Mecca, 24382, Saudi Arabia*
[*] *Corresponding author E-mail:S44380037@st.uqu.edu.sa*

Abstract

Cloud computing paved the way to many technical facilities for companies to develop their business needs in more effective and efficient manner. Combining private and public cloud into so called Hybrid cloud has made a positive leap in business by allowing applications and data to be shared among enterprises. However, many challenges and issues have arisen when adopting the hybrid cloud to manage, store and process data. The most critical one of these challenges is the security of the adopted Hybrid cloud. This research presented a comprehensive study about the security challenges in the Hybrid cloud computing as well as the suggested solutions. The study used a Systematic Literature Review (SLR) process to collect, review and summarize published articles from IEEE and Springer Nature databases and between 2020 and 2021. As a result, there were 7 eligible articles selected according to the search criteria and fully reviewed. The findings have revealed that there are four main challenges which are Data Security, Access Control, Privacy and Data Leakage and Cyber Attacks. Future studies should be conducted using different databases to have further investigation regarding the security in Hybrid clouds.

Keywords: *Cloud, Hybrid, Security, Systematic Literature Review, Privacy*

1. Introduction

Systematic Literature Review (SLR) is a research method that identifies, evaluates and summarizes the results of previous studies regarding a specific topic or a research question. It is an essential study to push the academic research and knowledge further by understanding the breadth and depth of the current related work and find gaps that need further study [1][4]. There are seven keys that form the basis of SLR which are; Clarity, Integration, Focus, Equality, Accessibility, Coverage and Transparency [4]. To achieve them, researchers must follow the stages of SLR and apply them accurately. Consequently, this research used the SLR method to have a comprehensive study regarding the security challenges and issues that may arise in a hybrid cloud database.

Any large business company concentrates and concerns about processing, storing, managing and securing their data. Handling this on-premise data is convenient if the data has a limited known size. However, in case where huge volumes of data are processed and stored, many challenges may arise in which the business cost increased [2]. Therefore, companies with large data volume are heading for integrating with a Cloud computing solution. This integration helps in increasing the accuracy and speed of data processing as well as improving the performance of the applications[2][3].

Cloud computing is an infrastructure that provides on-demand services as well as offers access to shared resources and applications. It is a form of network-shared services that allows online computing capabilities with high flexibility and compatibility and lower cost [4]. Cloud computing can be divided into four types depending on the type of service that offers including; Public Cloud, which provides services to any user who have an internet connection; Private Cloud, which provides services for a limited number of users or a specific group; Community Cloud, which provides services for two or more communities or groups that have shared tasks or needs; Hybrid Cloud, which is formed by combining at least two types of Cloud services [1][2].

Hybrid cloud is known as a heterogeneous cloud since it has different types and methods of storage, computing and services in a way that increase performance, speed, reduce costs, allow intelligent computing, and provide lightweight applications [7]. However, the implementation of hybrid cloud in the business industry has revealed many issues and risks. One of the most important concerns that have arisen is the security of these clouds and the data that stored in them.

Furthermore, multiple previous studies conducted the SLR process on a Hybrid cloud to investigate the security issues. In 2014, a study [3] investigated 31 articles and discovered that there are numbers of risks from Cloud Providers side as well as Cloud Customer side such as Data Security and Privacy, Technological, Physical Security and Compliance and Audit. While in 2016, researchers in [5] found out that there are three types of challenges in adopting Hybrid cloud based on 120 articles which are; the security risks in the Public could sector, the

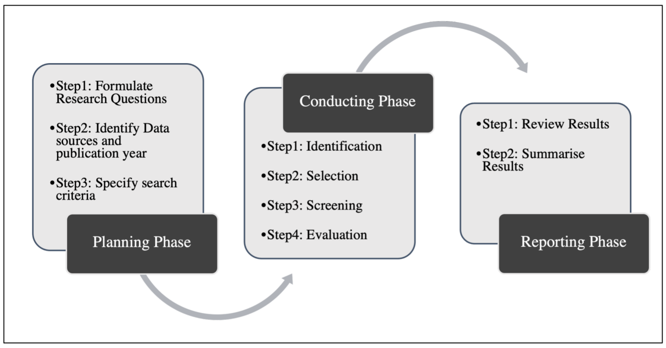
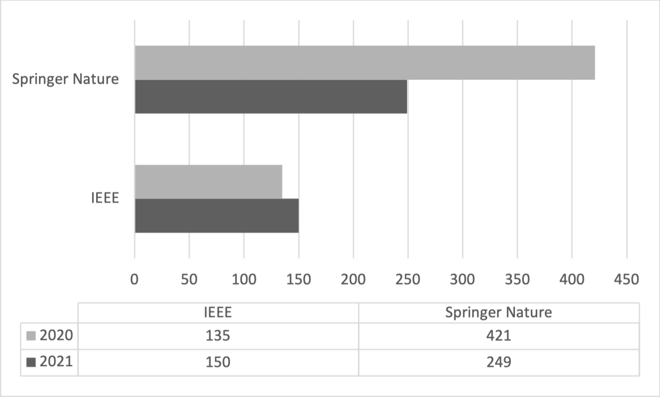

•Step1: Formulate Research Questions
•Step2: Identify Data sources and publication year
•Step3: Specify search criteria
Planning Phase
Conducting Phase
•Step1: Identification
•Step2: Selection
•Step3: Screening
•Step4: Evaluation
•Step1: Review Results
•Step2: Summarise Results
Reporting Phase

Figure 1: Steps Followed for The SLR Process



	IEEE	Springer Nature
■ 2020	135	421
■ 2021	150	249

Figure 2: Number of Publications Across The Years

efficiency issues in the Cloud management, and the complexity of integration. However, these studies were conducted years ago and since the technology evolves rapidly, the need of conducting an SLR process in the field of security of Hybrid cloud is still exist. For that, this study reviewed and analyzed new relevant articles to investigate further in the security challenges of Hybrid cloud and addressed them.
The rest of this paper is organized as follows. Section 2 presents research methodology. Section 3 discusses the results. Section 4 outlines the conclusion and future work.

2. Research Methodology

As stated earlier, this research is conducted using SLR method. The phases of SLR are divided into three main phases, namely, Planning Phase, Conducting Phase and Reporting Phase, each phase has its own steps as shown in figure1 [2][6].

2.1. Planning Phase

The first step in any SLR study is the formulation of research questions. This research was conducted to answer the following questions:
• What are the types of security challenges that appear in adopting Hybrid cloud computing?
• What are the suggested solutions for these challenges?
These questions are clearly and fully answered in Sect 3. The second step is the identification of data sources for this research; which are IEEE and Springer Nature by using Saudi Digital Library (SDL). Most of these articles are from international journals and conferences that were published in 2020 and 2021. The search criteria were determined, which are "Security", "Security Challenges", "Hybrid Cloud" and "Security Challenges in Hybrid Cloud" with the use of "OR" and "AND" identifiers.

2.2. Conducting Phase

This phase consists of three steps, including identification, selection, screening, and evaluation [2]. Thus, it started by selecting the suitable articles. However, since the search results were a lot, the search was narrowed down using specific keywords in the Subject filter which are; "Security" and "Cloud Computing". Based on that, the total number of published articles in 2020 and 2021 was 955 articles (285 in IEEE and 670 in Springer Nature). The results of this step are shown in figure 2.
In the selection step, the titles of the collected articles were reviewed. The article's title that matched the research topic was included, where the one that is not suitable to answer the research question was excluded. This has resulted in 126 of eligible articles. The selected eligible articles entered the screening step where the abstract content and keywords of each study are reviewed. The screening process checks whether these studies are in the boundaries of inclusion criteria (studies that address security issues in Hybrid cloud database). The outcome of this step was 18 suited articles. The articles selected from screening step were fully reviewed in the Evaluation step. Here, evaluating the quality of an article depend on the quality of abstract, introduction, methodology and findings as well as how much the article's idea is relevant to this research topic. Moreover, to avoid bias in evaluating the quality of these articles, all personal information about authors were covered to ensure the research integrity. Finally, the number of studies that pass the Evaluation step is 7. Table 1 shows the outcomes of each

step in the Conducting phase.

Table 1: Number of Articles in Each Step of The Conducting Phase

Source of Database	Identification (of search criteria)	Selection (of titles)	Screening (of abstract and keyword)	Evaluation (selected for full review)
IEEE	285	106	11	6
Springer Nature	670	20	7	1
Total	955	126	18	7

2.3. Reporting Phase

Only 7 articles that passed the SLR phases and were approved to be fully investigated to answer the research questions. These studies are reviewed and discussed in Sect.3.

3. Results and discussion

The final number of eligible articles was 7 that were related to security issues and solutions in Hybrid clouds. These selected articles were reviewed and analyzed to extract the necessary data and answer the research questions. Table 2 provides a summary of the details of these articles.

Table 2: Analysis Results of Selected Articles

Ref.	Source of Database	Year of publication	Hybrid Cloud	Security Challenge	Security Solution	Business Area
[13]	Springer Nature	2020	✓	✓	✓	General
[7]	IEEE	2020	✓	✓	×	E-health
[8]	IEEE	2020	✓	✓	✓	IoT Environment
[9]	IEEE	2020	✓	✓	✓	General
[10]	IEEE	2021	✓	✓	✓	Govermental
[12]	IEEE	2020	✓	✓	✓	General
[11]	IEEE	2021	✓	✓	✓	Economic

The research results are categorized based on the types of security concerns that were extracted from these articles. Such concerns are as follows:

3.1. Data Security

As a general view, securing data in a Hybrid cloud can be a complex objective due to the nature of cloud availability and lack of trust [7][8]. For that, the researchers in [8] presented a highly secure framework for IoT-Hybrid systems. The model encrypts sensitive data using Rivest cipher 6 (RC6) and Fiestel encryption algorithms while nonsensitive data is encrypted using Advanced Encryption Standard (AES) encryption.

3.2. Access Control

Based on the studies in [9] and [13], Hybrid clouds have a complexity in managing an effective access control over the data. Also, retrieving, storing and accessing data from the cloud database need to be more secure. This can be solved using Dynamic Spatial Role Based Access Control Algorithm [13], a machine learning algorithm helps in restricting the access of user data. While researchers in [9] used another method called Proxy Re-Encryption (PRE) scheme in which a description mechanism is used to specify the factors of access control with XML.

3.3. Privacy and Data Leakage

One of the most crucial concerns of adopting Hybrid clouds is the privacy and confidentiality of stored data, especially when building governmental [10], commercial [12] or economic [11] clouds. In order to gain more data privacy and protection and prevent data leakage, Hybrid clouds must support encryption as well as authentication methods. In [12], researchers proposed an encryption technique called Attribute based Encryption Scheme with Dynamic Attributes Supporting (ABE-DAS) to prevent data leakage and enhance the privacy in commercial clouds. Furthermore, the authors in [10] used another encryption method to prevent leakage of governmental documents and provide privacy and protection over the cloud which is Top-k ciphertext. Such method combines different key technologies such as homomorphic matrix encryption method and the vector space model. On the other hand, the study in [11] presented a security model that uses two different authentication techniques to protect data from unauthenticated users.

3.4. Cyber Attacks

Any organization that uses on-demand services may face the threats of cyber and malicious attacks [7][11]. These threats are associated with the implementation of Hybrid clouds such as Crypto-jacking and Hijacking of Accounts. The area needs more study to overcome these cyber issues.

Table 3 presents the key points of the reviewed articles and security challenges. These challenges raised concern about the effectiveness of implementing Hybrid cloud and whether there is another more secure and better solution regarding the security of the clouds. Nevertheless, the technology evolves at a rapid pace and the issues of the past become the growth of the present. It is necessary to know and explore the scientific gaps so that future studies can focus on them.

Table 3: Summary of The Key Points of The Security Articles

Ref.	Data Security	Access Control	Privacy	Data Leakage	Cyber Attacks
[13]	✓	✓	✓		
[7]	✓		✓		✓
[8]	✓		✓		
[9]	✓	✓	✓		
[10]	✓		✓	✓	
[12]	✓		✓	✓	
[11]	✓		✓	✓	✓

4. Conclusion

Hybrid Cloud is an advanced solution for enterprises and companies that deal with large volume of data and need to provide on-demand services and applications. However, moving toward the cloud computing technology has raised concerns regarding the security of the systems. In order to gather evidences about the security level in a hybrid cloud, this research conducted a systematic literature review to collect and review published articles about security challenges in Hybrid cloud. The selected articles were gathered from two different databases namely; IEEE and Springer Nature and published in 2020 or 2021. Based on the search criteria, 955 articles were selected to enter the phases of SLR process and only 7 of them considered to be related and relevant to the research topic. After reviewing and analyzing them, the results showed that there are several concerns about security, such as access control, data leakage and cyberattacks. Some of the reviewed studies suggested various solutions, all of them are based on different encryption, authentication and cryptography techniques. To cover the limitations of this research, future studies can investigate other articles from another databases.

References

[1] Maniah, B. Soewito, F. Lumban Gaol and E. Ab- durachman, “A systematic literature Review: Risk analy- sis in cloud migration”, *Journal of King Saud University - Computer and Information Sciences*, 2021

[2] J. Gong and N. Navimipour, “An in-depth and system- atic literature review on the blockchain-based approaches for cloud computing”, *Cluster Computing*, 2021.

[3] Latif R., Abbas H., Assar S., Ali Q., ”Cloud Computing Risk Assessment: A Systematic Literature Re- view”, *Park J., Stojmenovic I., Choi M., Xhafa F. (eds) Future Information Technology.*,Lecture Notes in Electri- cal Engineering, 2014, vol 276. Springer, Berlin, Heidelberg.

[4] Pittway, L.” Systematic literature reviews”, *Thorpe, R. Holt, R. The SAGE dictionary of qual- itative management research.*, 2008.

[5] Khan, Siffat Ullah Ullah, Naeem., ”Challenges in the Adoption of Hybrid Cloud: An Exploratory Study us- ing Systematic Literature Review.” *The Journal of Engineering*, 2016.

[6] Sabir, Fatima Palma, Francis Rasool, Ghulam Guéhéneuc, Yann-Gaël Moha, Naouel, “A systematic literature review on the detection of smells and their evolu- tion in object-oriented and service-oriented systems”, *Soft- ware: Practice and Experience*, 2018

[7] M. Joshi, N. Tewari and S. K. Budhani, “Security Chal- lenges in Implementing a Secured Hybrid Cloud Model for e- Health Services”, *2020 9th International Conference System Modeling and Advancement in Research Trends (SMART)*, 2020, pp. 3-7.

[8] Atiewi, Saleh, Amer A. Al-Rahayfeh, Muder Almiani, Salman Yussof, Omar Alfandi, Ahed Abugabah and Yaser Jararweh, ”Scalable and Secure Big Data IoT System Based on Multifactor Authentication and Lightweight Cryptogra- phy.”, *IEEE Access 8* , 2020

[9] Z. Lian, M. Su, A. Fu, H. Wang and C. Zhou, ” Proxy Re-Encryption Scheme For Complicated Access Control Factors Description in Hybrid Cloud”, *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1-6.

[10] L. Yong, L. Hefei, S. Xiujuan, Y. Bin and W. Kun, ”Keyword Semantic Extended Top-k Ciphertext Retrieval Scheme Over Hybrid Government Cloud Environment” *IEEE Access*, vol. 9, pp. 155249-155259, 2021.

[11] A. Dutta, R. Bose, S. K. Chakraborty, S. Roy and H. Mondal, “Data Security Mechanism for Green Cloud”, *021 Innovations in Energy Management and Renewable Resources(52042)*, 2021, pp. 1-4

[12] Rd, R.Dhanapal., “An Attribute Based En- cryption Scheme with Dynamic Attributes Supporting in the Hybrid Clouds”, *Proceedings of the Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 2020

[13] Praveena, D., Rangarajan, ”A machine learning application for reducing the security risks in hybrid cloud networks”, *Multimed Tools Appl 79, 5161–5173*, 2020