European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 03, 2020

Major Security Challenges Ofcloud Computing Technology

Abrar Atif Asghar
King Abdul Aziz University, Jeddah, Saudi Arabia,
E-mail: abrarasghar2013@gmail.com

ABSTRACT
This paper aims to identify the challenges and threats to the information security of cloud computing, which is considered one of the most important technologies in recent decades. Cloud computing provides many virtual services that can be managed and accessed by users through the web and user interfaces. It also enables the users to store their information that can be easily accessed globally. Despite the advantages of cloud computing, there are numerous challenges and threats to the users and service providers that may directly or indirectly affect the cloud computing system as a result affect its information security. Acritical review approach has been adopted as a method to identify the knowledge gaps in the literature. Severalstudiesrelated to the information security challenges of cloud computing have been reviewed and critically evaluated. The critical review approach described in this paper resulted in a set of important information security challenges of cloud computing thatmust betaken into considerationby the users and service providers. Among the most important of these challengesare data encryption, network security, confidentiality, data privacy, malware, Authenticity, databreach, and the challenge of identity and access management.The study recommended the necessity to discover moreinformation security challenges of cloud computing and to take the challenges discussed in this paper into account in order to protect the data and information of the organization and maintain its performance.

Keywords: Cloud computing security - Information security - Challenges of cloud computing- Critical review.

1. INTRODUCTION

In the past decade at the beginning of the emergence of the computer, the computer used to take a large space and needed a whole room to keep it in. Parts were very expensive, and it used to consume a lot of energy compared to modern computers. Nowadays, the drives and expensive electronic parts have been replaced by small and economical parts so that everyone can obtainand benefit from it. Due to the small storage space available in the devices, cloud computing technology has appeared, which gives the users the ability to store a large amount of data and information that can be accessed easily from anywhere [1].Nowadays, cloud computing has become one of the most important technologies which led to an increase in the number of organizations that offer solutions for storing data in the cloud. It enables the users andorganizations to access their data and information easily from anywhere in the worldas

well asallowing the users to expand their data storage spaces as needed.Moreover,cloud computing reduces costs of the organizations, alleviates in managing files through several applications, and shares files with a capacity greater than MB25 by uploading files to the cloud and then sending them via e-mail [2].Despite the advantages of cloud computing,the threats of the information security in cloud computing may directly or indirectly affect the cloud system, which may lead to an imbalance in the security policies, technology, control of data and services in the cloud. These threats may be from anonymoussources that attack filesthrough the network without permission from the cloud administrator or from a program that intercepts messages within the cloud,known as a malicious service agent.Also, there is a type of threat that comes from a trusted source using the cloud, sharing information in the cloud infrastructure, violating cloud usage rights. Also, people can deal with users as employees or third-party agents working in the cloud and carrying out the attack, which is one of the most dangerous types of attacks as they can obtain administrative privileges to access information files inside the cloud. Despite these threats and challenges to the individuals and organizations for the users of cloud computing, there is a lackof Arab studies in the field of information security challenges in cloud computing, and based on the significance and problem of the study, this paper aims to identify the challenges and threats to the information security of cloud computing by reviewing and criticizing previous studies and identifying the knowledge gaps to come up with a comprehensive set of important challenges of cloud computing security.

2. PREVIOUS STUDIES

Previous studies between (2010-2020), have shown the scarcity of Arab studies in the field of information security challenges of cloud computing. Several studies related to the aim of the study have been found andarranged in descending order from newest to oldest. In 2020, Tabrizchi and Rafsanjani [4] study entitled "A Survey onSecurity Challenges in Cloud Computing: Issues, Threats, and Solutions" aimed to identify the challenges, issues, requirements, and weaknesses of cloud computing security. The research highlighted the importance of various components of cloud computing with the focus on information security threats and possible solutions. The study useda quantitative and descriptive survey method. The results of the study summarized that cloud helps organizations to expand and accelerate their business, provides opportunities for cooperation, and stores big data at an affordable cost. The strengths of this studydiscussed future cloud security issueswhich other studies overlooked. Rafsanjani and Tabrizchi [4] study divided information security issues in the cloud into several sections as shown in Table (1):

Table 1
Challenges to the information security of cloud computing form Rafsanjani and Tabrizchi[4]study

Cloud computing challenges	
Security policies	Service and agreements
	Client management issue
	Antecedent trust

User-oriented Security	Authentication
	Authorization
	Identity and access management
Data storage	Data warehouse
	CIA tired
	Malware
	Meta data
Application	Operating systems
	Front end/ back end
	Application vulnerabilities
Network	Instruction prevention system
	Intrusion detection system
	Firewalls

In 2020 Mondal, Goswami, and Nath [5] published a study entitled "Cloud Computing Security Issues and Challenges: A Review Study". The study aimed to review studies related to the security challenges of cloud computing such as trust, authenticity, confidentiality, encryption, and others. The importance of the study lies in an attempt to provide security in the cloud environment, and to examine the findings of the studies reviewed on this topic. The method used in the study was the qualitative and critical review approach. The most important findings of the study were the need to strengthen the cloud computing service, enhancing theencrypted data, and solving information security issues. So, that no untrusted source can access it. Among the strengths of this study werethe findings tables that summarized and comparedthe previous studies in terms of the year of publication, the title, the names of the authors, and a simple explanation for each study. Through reviewing Mondal, Goswami, and Nath [5], information security challenges in cloud computing have been extracted as shown in Table (2):

Table 2
Challenges to the information security of cloud computing form Nath, Goswami and Modal [5] study

Cloud computing challenges
Trust
Confidentiality problem
Authenticity
Encryption
Key management
Data splitting

In 2019 Ahmad's study [6] was published entitled “A brief review: Security issues in Cloud Computing and their solutions” The study aimed to identify the information security issues related to data privacy and the factors that have an impact on the cloud computing system. The significance of the study was combining the challenges and threats facinginformation

security in cloud computing. The study used the qualitative approach and provided some solutions in data encryption and electronic signature. However,it was noted that the study did not cover the topic and the scientific sources sufficiently and did not discuss it in a scientific critical way. The research can be developed in addition to some scientific sources from well-known databases and the use of a scientific research method that enriches the study better. Through reviewing Ahmad's study [6], information security challenges in cloud computing have been extracted as shown in Table (3):

Table 3
Challenges to the information security of cloud computing form Ahmad [6] study

Cloud computing challenges
Database
Operating system
Network
Load balancing
Concurrency control
Virtualization
Transaction management
Resources management
Memory management
Outsourcing
Multitenancy
Service level agreements
Heterogeneity
Server breakdown
Backup
Data redundancy

In the same year 2019, Bhajantri and Mujawar [3] presented a study entitled "A survey of Cloud Computing Security Challenges, issues, and theircountermeasures". The study aimed to discover various challenges and threats related to cloud computingsecurity including infrastructure and level of data. It discussed the ways of how to mitigate or avoid various information security issues. The study applied aquantitative and descriptive survey method. Itprovided some solutionsin terms of encrypting and dividing the data into several sensitive data parts. As for the weaknesses of the study, it did not address various previous models of cloud computing challenges, and the researcher did not highlight the importance of the study clearly. The study can be enhanced by reviewing other studies that are not covered as well as discussing and analyzingthe updated models. Through reviewing the study of Mujawar and Bhajantri [3], the information security challenges in cloud computing have been extracted as shown in Table (4):

Table 4
Challenges to the information security of cloud computing form Mujawar and Bhajantri[3] study

Cloud computing challenges
Data security
Non-compliance with regulatory mandates
Loss of control
Expertise
Compromised accounts or insider threats
Disaster management
Infrastructure security
Data security
Identity and access management

The Popli and Gagandeep [7] study appeared in 2019 titled “A Survey onCloud Security Issues and Challenges” aimed at introducing the concept of cloud computing, reviewing several cloud models for information security challenges, and explaining how to maintain confidentiality and integrity in the cloud. The study highlighted the types of cloud computing in terms of structure, service providers, and the models and features that benefit the readers. The studyapplied the qualitative approach and reviewed some other methods from the previous studies. The strengths of this study wereprovidingsome solutions forthe information securityvulnerabilities of cloud computing. It was recommended the need forproviding more solutions to cover all aspects of information security in the cloud and conductingmore research on information security issues in the cloud that affect data confidentiality and integrity.Further research topics were recommended to be studiesincluding the risk of hacking while transferring data from users to service providers, methods of securing cloud storage from attack, the threat of impersonation of untrusted individuals, and threats to breach data sharing points between multiple users. Through reviewing the study of Popli and Gagandeep [7], the information security challenges in cloud computing were extracted as shown in Table (5):

Table 5
Challenges to the information security of cloud computing form Popli and Gagandeep [7] study

Cloud computing challenges
Networks
Virtual machine
Storage attacks
Applications

In 2019 the Rizwan and Zubair study [8] was published. Entitled "Basic Security Challenges in Cloud Computing", which aimed to discover the continuous developments in cloud computing, shed light on the challenges and information security, and discuss some solutions.

The importance of this study was on determining the need to use cloud computing and learning about the structure and types of the cloud. The qualitative approach was adopted as a method. The study found that the greater the degree of security in the cloud, the higher the performance of the cloud network, so the cloud service provider should try to use information security technologies to increase the security feature in the cloud. The weaknesses of this study were that little information and references were provided. The work can be developed by using a survey or experimental scientific approach that provides more information on this topic. Through reviewing the study of Rizwan and Zubair [8], information security challenges in cloud computing have been extracted as shown in Table (6):

Table 6
Challenges to the information security of cloud computing form Rizwan and Zubair[8] study

Cloud computing challenges
Data breach
Malware injection
Insecure APLs
DDoS attacks
System vulnerabilities
Phishing attack
Unawareness

In 2018, Zakaria [9] presented a study entitled "The Future of Library and Information Profession in the Cloud Computing Environment, Requirements and Challenges". The study aimed to explore the various challenges that libraries face in using cloud computing and the services and requirements provided by the cloud. The importance of this research was to clarify the future of the library and information profession in light of cloud services and advanced technologies. The study used the qualitative approach and content analysis method. Among the most important findings of the study is the necessity to stimulate the use of cloud computing by spreading awareness and developing the technical skills of workers. Thestudy recommended the need of conducting research and feasibility studies for the transformation of libraries into cloud computing in light of the library's needs and beneficiaries' concerns. This study can be enhanced by conducting more research in other librariesusing the qualitative and quantitative approachesin order to explore the efficiency in the case of applying clouding computing. Through reviewing Zakaria's study [9], information security challenges in cloud computing have been extracted as shown in Table (7):

Table 7
Challenges to the information security of cloud computing form Zakaria[9] study

Cloud computing challenges
Legal challenges
Technical challenges and connection speed
Professional challenges

In 2017, Chatterjee and Singh [1] presented a study titled "Cloud security Issues and Challenges: A Survey"The study aimed to identify the key features of cloud computing and its challenges as well as providing some solutions for solving these challenges. This study has covered various key subjects related to cloud computing such as cloud components, cloud technologies, cloud security, and the threats and attacks the cloud computing faces. The study used the quantitative survey and critical review method. Among the results of the study was developing a model including the security issues in cloud computing. One of the main strengths of this study was reviewingand analyzingnumerousstudies related to information security in a critical scientific reviewfor the periods between 2010 to 2017. Through reviewing the study of Chatterjee and Singh [1], information security challenges in cloud computing have been extracted as shown in Table (8):

Table 8
Challenges to the information security of cloud computing form Chatterjee and Singh [1] study

Cloud security issues	
Data storage and computing security issues	Data storage issue
	Un-trusted computing
	Data and service availability
	Cryptography
	Cloud data recycling
	Malware
Virtualization security issues	VMs image management
	Virtual machine monitor
	Network virtualization
	Mobility
	Issues in virtual machine
	Malware
Internet and services related security issues	Advanced repeated threats and venomous outsiders
	Internet protocols
	Web services
	Web technologies
	Services availability
Network security issues	Mobile platforms

	Circumference security
Access control issues	Physical access
	User credentials
	Entity authentication
	Authorization
	Management of user identity
	Anonymization
Software security issues	Platform and frameworks
	User frontend
Trust management issues	Cloud to cloud trust
	Human aspect
	Reputation
	Trust on the auditability reports
	Anonymization
Compliance and legal aspects	Forensics
	Acts
	Legal problems
	Incorrect resource usage metering
	Governance

In 2015, Mahmoud's study [2] entitled "Uses of Cloud Storage in Libraries and Information Center and Information Security". This study aimed to identify the uses, advantages, and disadvantages of cloud storage in libraries and information centers, as well asidentifyingthe challenges facing information security. The study divided the challenges of information security into two parts: the challenges that face the cloud storage service providers, and the challenges that face the users of the cloud storage service. The study used a descriptive and analytical approach.Among the results of the study was that the users do not need the technical expertise to manage the cloud. It was also recommended in increasing scientific research in the field of cloud storage and the necessity of activating the cloud storage service in all institutions, particularly libraries and information centers. It also recommended that data should be secured during using cloud storage.Among the strengths of Mahmoud's [2] the study has covered cloud computing from many different aspects, such as the advantages and disadvantages of cloud computing and itstypes. The study can be developed by conducting a survey and questionnaire for service providers and users in order totorecognize their impressions and how information security can be developed in cloud computing. One of the weaknesses of this study was that it focused only on cloud storage in the library and information environment and overlooked other environments. Through reviewing Mahmoud's study [2], several challenges to information security in cloud computing and cloud storage were extracted as shown in Table (9):

Table 9
Challenges to the information security of cloud computing form Mahmoud[2] study

Cloud computing challenges
Server breakdown
Security and privacy
Loss of control

In the same year 2015, Kaur [10] undertook a study entitled "Cloud Computing Security Issues and its Solutions: A Review". The study aimed to identify the challenge of information security in cloud computing and the techniques that overcome the data privacy issues. The study also has explored some cloud security issues and the challenges that face the cloud service provider. The importance of this study was on identifying the image steganography technique to overcome data security issues. The method used in the study was the qualitative approach and critical review. The most prominent finding of the study was that most of the companies that provide cloud service, such as Amazon, Google, etc. face the challenges of information security. One of the strengths of this study wasprovidingseveralsolutions in terms of encryption and image steganography, and to ascertain the agreement of the service provider and what degree of security it provides to the user. The Kaur study [10] covered a number of components that could affect the security of cloud computing, including cloud network, databases, operating systems, information memory management, and control management.

Among the information security challenges facing the cloud is controlling access to illegal data, and the challenge of data integrity, which includes data integrity, as human errors may occur when entering data or errors occur when transferring data from one computer to another, such as a hard disk failure. In addition to the challenge of data loss and data theft, as it is a big problem that can face banking, commercial transactions, and research and development. As for the privacy challenge, the users and service provider needstoensure security, especially if external servers are using. There is a challenge of losing and tampering with personal information, so the user must ensure that his account has not been subjected to any changes that have not occurred before him. And finally, challenging the problem of the security level in the server, which is the link between the service provider and the user. Through a review of the Kaur study [10], the information security challenges in cloud computing were extracted as shown in Table (10):

Table 10
Challenges to the information security of cloud computing form Kaur[10] study

Cloud computing challenges
Data access
Data integrity
Data loss
Data theft

Privacy issues
User level issues
Security issue in provider level

In 2012, a study by Zissis and Lekkas [11] appeared entitled "Addressing Cloud Computing Security Issues". This study aimed to assess the information security requirements in the cloud as well as an attempt to provide a solution to eliminating threats to the cloud. The study divided the information security challenges and threats in the cloud into three sections according to the service level, the level of software as a service (SAS), the level of Platform as a Service (PAS), infrastructure as a service (IAS) and finally the physical datacenter. Among the most important results of the study was that a cryptographic solution was proposed to ensure the integrity of information and the confidentiality of data and communications. One of the strengths of the study was that it addressed variousnew important challenges and threats and covered all aspects of cloud computing challenges. Through reviewing the study of Zissis and Lekkas [11], information security challenges in cloud computing have been extracted as shown in Table (11):

Table 11

Challenges to the information security of cloud computing form Zissis and Lekkas[11] study

Cloud computing challenges
Trust
Integrity
Privacy
Protection of information
Access control
Network protection
Software security
Hardware security

Finally, in 2010 Yang and Chen [12] published a study entitled “Cloud Computing Research and Security Issues”. This study aimed to provide an overviewof the cloud computing service and its types, as well as discussing the information security issues in cloud computing. Among the most important findings of the study was the use of data encryption and the development of legal policies to protect the users as a solution for the information security issues in cloud computing. The study stated that the ability to store big data will be provided in the near future by cloud computing. Among the weaknesses of this study was that it did not discuss the issues of cloud computing comprehensively and did not show how the data was collected, in addition, the methodology used in the study and the mechanism of data collection were not explained. Through reviewing Yang and Chen’s study [12], information security challenges in cloud computing have been extracted as shown in Table (12):

Table 12
Challenges to the information security of cloud computing form Yang and Chen[12] study

Cloud computing challenges
Trust
Privacy
Reliability
Legal issues
Long-term viability

3. METHOD

This study adopts the critical review approach, which aims to review therelated studies and related literature that are closer or more related to the study, analyze and critique the literature. It also aims to identify the knowledge gaps looking at the similarities and differences - strengths and weaknesses - contradictions concerning the methodology, study tools, study hypotheses, etc. The critical scientific review approach can also be used in evaluating the quality of the research, discussing ideas and hypotheses, developing current models, or producing new models [13]. This research relied on the secondary data for the data collectionwhich refers to the data that has already been collected and analyzed by somebody else. The data was collected from scientific journals including Since Direct, IEEE, and the Saudi Digital Library. The latest studies in relation to the information security challenges in cloud computing have been collected and reviewed for the past ten years for the periods between (2010-2020).

4. RESULTS AND DISCUSSION

Through discussing and analyzing the previous studies, all studies have emphasized the importance of cloud computing securityand the need to increase scientific research in the field of cloud computingand secure data while using cloud computing. Cloud computing could benefit organizations to accelerate business and enables easy access to cloud computing from any region. Some studies have aimed to identify the challenges and threats to the security of cloud computing information, such as the Kaur study [10], the Zakaria study [9], the study of Singh and Chatterjee [1]. However, it has been found that there isstill no comprehensive studiesthat have covered all the challenges and threats to the security of cloud computing information. Other studies have attempted to offer some solutions to the information securitychallengesrather thanfocusing only on discovering thechallenges and threats to the security of cloud computing information such as the studies of Ahmad [6], Bhajantri and Mujawar [3], Rizwan and Zubair [8], Tabrizchi and Rafsanjani [4]. It has been found that the majority of the previous studies relied on the secondary data for the data collection, which used the qualitative methodcritical review approach such as Kaur study [10], Zakaria [9] study, Singh and Chatterjee study [1], Ahmad [6] study, and finally Mondal, Goswami, and Nath study [5]]. While other studies used the quantitative and descriptive survey method, such as the study of Bhajantri and Mujawar [3], the study of Rizwan and Zubair [8], the study of Tabrizchi and [4] Rafsanjani, the study of Mahmoud [2], and the

study of Popli and Gagandeep [7]. Through the analysis of the previous studies, the researcher has summarized the most important challenges to cloud computing security as shown in Table (13). It was found that the most frequent challenges to cloud computing security were: the challenge of data encryption, network security, data security followed by the trust challenge, security policies, data breach,identity and access managementand then the challenge ofconfidentialityand malwarechallenges.

Table 13

Challenges to the information security of cloud computing

challenges	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
Trust	√	√		√	√						√	√
Confidentiality problem				√	√		√			√	√	
Encryption	√		√		√	√				√	√	√
Data splitting					√	√						
Security policies	√		√	√		√	√			√		
Data storage	√			√								
Software security				√				√			√	
Network security	√		√	√		√	√	√			√	
Service and agreements	√			√								
Client management issue				√								
Authentication	√			√								
Authorization	√			√								
Identity and access management	√			√		√				√	√	√
Data warehouse				√		√						
CIA tired				√								
Meta data				√								
Malware	√		√	√			√	√				
Operating system				√		√						
Insecure APLs	√			√				√				
Data breach	√		√	√			√	√		√		
Intrusion detection system				√								
Firewalls				√								
Unawareness								√				
Data security		√	√							√		
Loss of control		√	√							√		
Expertise			√						√			

Disaster management			√									
Infrastructure security			√									
Data security		√	√		√	√				√	√	√
Identity and access management			√			√				√		
load balancing						√						
Virtualization						√						
Transaction management						√						
Memory management						√						
Heterogeneity						√						
Server breakdown		√				√						√
Backup						√						
Legal challenges	√								√			√
Technical challenges and connection speed									√			
Reputation	√											
Data integrity										√	√	
Software security issues											√	

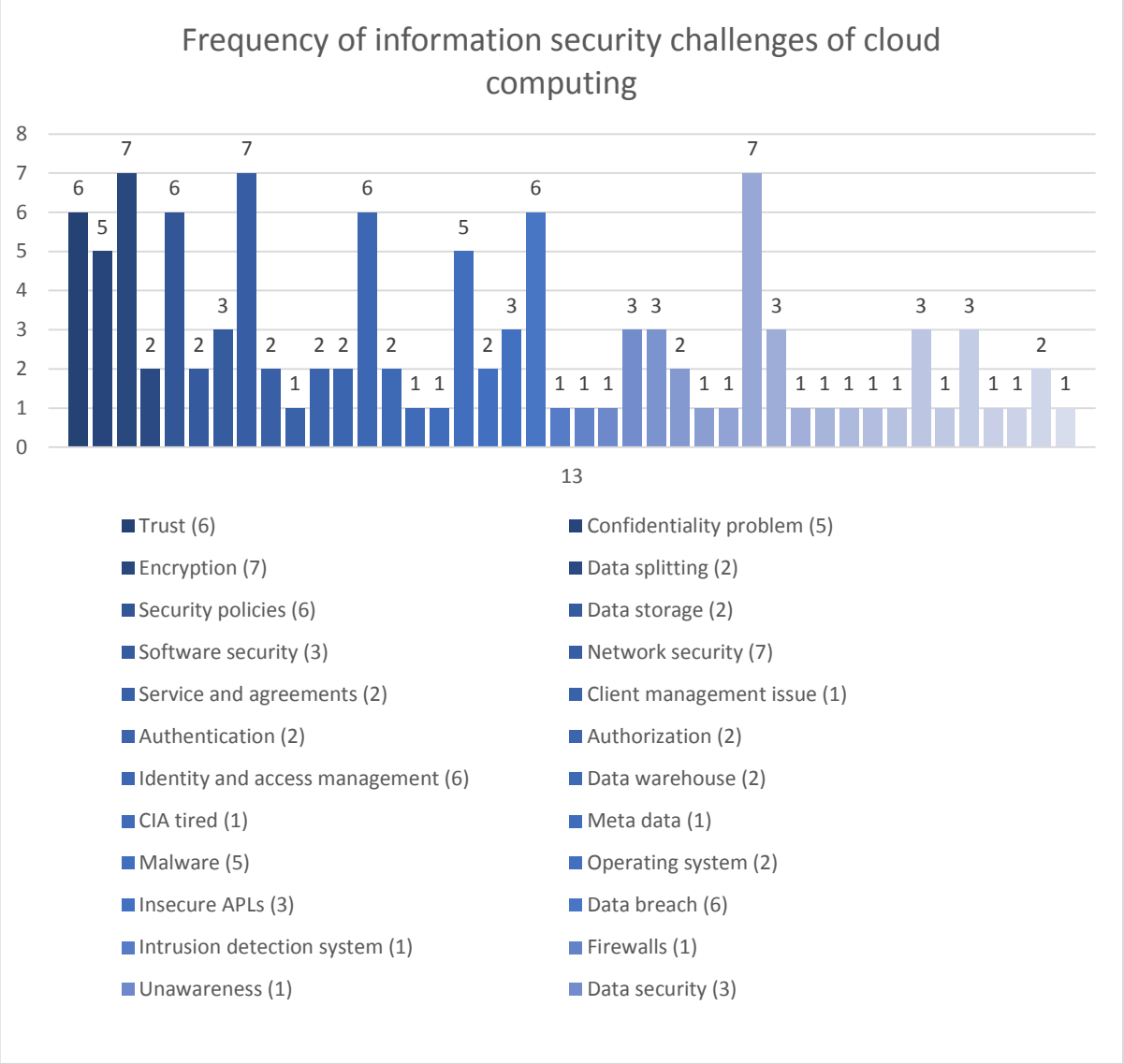

Figure 1 information security challenges of cloud computing

5. CONCLUSIONS

Cloud services have become part of the life of organizations, which gives tremendous opportunities to accelerate business and increase their ability to expand rapidly and provide many advantages that help organizations to raise their performance such as speed in dealing, reducing costs, storage space, and easy access to files. Despite the advantages of cloud computing, numerous issues still exist, such as the challenges and threats to the security of cloud computing informationdiscussed in this paper. The researcher has concluded a set of important challenges that must be taken into consideration by the cloud computing users and service providers in order to avoid falling into any of these challenges. It is recommended tomaintain Information security and provide safe user interfaces, and design a standard security system in which maintenance, support, confidentiality, credibility, and identity verifications are available for people who are used to gain access to files, in addition to using strong passwords that contain letters, symbols, and numbers.Due to the development of cloud technologies, challenges will last to emerge of various kinds, thus, the researcher recommends discovering and classifying other challenges and threats facing the cloud of various types, knowledge of their causes and how to avoid and deal with them, as well as providing possible solutions to preserve the information of individuals and organizations. With the emergence of modern technologies such as smart cities,the Internet of Things, and the big data that must be stored, it is imperative to recognize how to deal with the challenges and threats facing cloud computing in the correct mannerand reduce them to the maximum extent possible.

6. REFERENCES

[1] A. Singh and K. Chatterjee, 'Cloud security issues and challenges : A survey', vol. 79, no. November 2016, pp. 88–115, 2017.

[2] M. Mahmoud, 'Uses of Cloud Storage in Libraries and Information Center and Information Security'. 2015.

[3] L. B. Bhajantri and T. Mujawar., 'A Survey of Cloud Computing Security Challenges , Issues and their Countermeasures', pp. 376–380, 2019.

[4] H. Tabrizchi and M. K. Rafsanjani, *A survey on security challenges in cloud computing: issues, threats, and solutions*, vol. 76, no. 12. Springer US, 2020.

[5] A. Mondal, G. R, and N. S, 'Cloud computing security issues & challenges : A Review', pp. 20–24, 2020.

[6] I. Ahmed, 'A brief review : security issues in cloud computing and their solutions', vol. 17, no. 6, pp. 2812–2818, 2019.

[7] M. Popli, 'A Survey on Cloud Security Issues and Challenges', pp. 230–235, 2019.

[8] S. Rizwan and M. Zubair, 'Basic Security Challenges in Cloud Computing', pp. 13–16, 2019.

[9] M. Zakaria, 'The Future of Library and Information Profession in the Cloud Computing Environment, Requirements and Challenges', no. 5, pp. 4–31, 2018.

[10] R. Kaur and J. Kaur, 'Cloud Computing Security Issues and its Solution : A Review', pp. 1198–1200, 2015.

[11] D. Zissis and D. Lekkas, 'Addressing cloud computing security issues', *Futur. Gener. Comput. Syst.*, vol. 28, no. 3, pp. 583–592, 2012.

[12] J. Yang and Z. Chen, 'Cloud computing research and security issues', *2010 Int. Conf. Comput. Intell. Softw. Eng. CiSE 2010*, pp. 1–3, 2010.

[13] M. J. Grant and A. Booth, 'A typology of reviews: An analysis of 14 review types and associated methodologies', *Health Info. Libr. J.*, vol. 26, no. 2, pp. 91–108, 2009.