Cloud Computing and Data Science
https://ojs.wiserpub.com/index.php/CCDS/

UNIVERSAL WISER PUBLISHER

Research Article

Security Challenges over Cloud Environment from Service Provider Prospective

Wahab Dashti[1], Ahthasham Sajid[2*], Asma Jahangeer[2], Afia Zafar[3]

[1]Department of Information Technology, Faculty of Information and Communication Technology, Balochistan University of Information Technology, Engineering and Management Sciences, Quetta, Baluchistan, Pakistan
[2]Department of Computer Science, Faculty of Information and Communication Technology, Balochistan University of Information Technology, Engineering and Management Sciences, Quetta, Baluchistan, Pakistan
[3]Department of Computer Science, National University of Technology, Islamabad, Pakistan
E-mail: ahthasham.sajid@buitms.edu.pk

Received: 8 March 2020; **Revised:** 16 April 2020; **Accepted:** 27 April 2020

Abstract: Cloud computing becomes very popular and growing rapidly since the last few years, various information technology giants such as Amazon, Google, Microsoft and others speed up their growth in development of cloud computing systems and enhance services for consumers all over the world. Cloud computing provides virtual storage for the clients to avail storage, application, platform and services from their deployed servers over the internet. Various security issues such as: data insecure, data leakage, data availability, attacks; etc. could arise due to poor security policies. This paper discussed in detail security issues in terms of the confidentiality, integrity, and availability (CIA) triangle from a service provider perspective over the services they provide to the end users. By these measurements high security can be achieve in cloud computing. Additionally, to protect confidential data from users on cloud the privacy actions are not updated accordingly. Severally, data backups on cloud cause high security risks. This survey paper analyzes the main security issues which are currently present in the cloud computing and offers best practices to service providers and enterprises hoping to control cloud service.

***Keywords*:** infrastructure as a service (IaaS), software as a service (SaaS), platform as a service (PaaS)

1. Introduction

Computer technology from the start in early 1960 has changed dramatically in terms of development and processing; many modern computing systems are based on mainframe computers that were named in mid of 1960 as they had central processing units. Mainframes were projected as the invention of today's computing system. Today some systems have the same functionality as those of main frame computers but there are some changes such as previously there were large and expensive systems which are now replaced by cheaper and small systems in size. Mainframes and other larger scale machines were developed and used. In short, cloud mutual proficiency is represented in terms of services, management, storage and computation [1]. As clouds have benefits of offering more scale, error tolerant services with more valuable performance. It provides distributed architecture and it centralizes server resources on an accessible platform to provide distributed resources and services. For the development of web services, cloud providers also provide provider's computing resources for example applications, storage and services that required less

DOI: https://doi.org/10.37256/ccds.112020318

management and can be established fast with providers collaboration and enabled in a shared pool of cloud computing network access. Cloud environment offers services in three domains, software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). By these enterprises move towards information technology (IT) solutions which are mandatory to pay for the resources and enterprises may easily meet requirements speedily changing markets if those are always on the leading edge for their customers [2]. Because of the idea of using infrastructure with managing it the cloud computing has become a business necessity. Idea was initially presented in the academic area only. Later it has been rearranged into enterprises as, Microsoft, Google, Amazon, etc. According to the need of enterprises commercial clients rent virtual machines/virtual space. Because of such technology like cloud the users are able to access heavy application as inconsequential portable devices as, personal computers (PCs), personal digital assistants (PDAs) and smart phones. Cloud systems are the latest/ruling trends in the growth of the distributed systems. Controlling the infrastructure of clouds users don't need any knowledge/expertise. Those servers which are being provided by the cloud computing providers are accessed through browsers [3].

2. Related work

There is too many research that has been done which cover security of cloud computing. Few of the researcher presented their work to cover privacy of data that how to secure the data and make the cloud computing reliable for the customers. Other groups of researcher did research on sharing of resources that how securely resources could be shared. This survey paper present work on security issues relates to service provider aspect therefore latest research papers covering this aspect has been addressed in this section and presented in Table 1 below.

Table 1. Literature review summary

Year	Paper title	Problem focused	Advantages	Limitations
2020	A survey on security challenges in cloud computing: issues, threats, and solutions [4]	In this survey provides cloud security issues and requirements, identified threats, and known vulnerabilities	Cloud entities such as cloud service provider, the data owner, and cloud user have been addressed	-
2019	eHealth Cloud security challenges: A survey [5]	In this paper cloud computing security issues have been addressed in e-health care domain	In depth study for the researcher who are working in developing e-health care service solution over cloud	No limitations or research gap in the existing e-health care solutions discussed in the paper are highlighted
2018	Cloud computing security challenges & solutions-a survey	Security and privacy issues provided by cloud computing system providers	Security and privacy concerns should be maintained	No reliable privacy
2018	Exploring data security issues and solutions in cloud computing	Explored different data security issues in cloud computing, described different cloud computing models	Privacy and security issues and how to overcome these issues	New deployment and review of security policies and update accordingly
2016	An analysis of the cloud computing security problem	Security and privacy problems, how to fulfill the needs of stack-holders, security management	Making cloud computing security more reliable and review of security and how to make it better	Blocking of hole arise in security management process, detects different stockholders security requirements and map security
2015	Security in cloud computing: Opportunities and challenges	Security and privacy and the challenges in cloud computing	Securing data storage, understanding challenges and overcome of these	Still privacy and security issues are the main challenges of the cloud computing

3. Models of cloud computing

Cloud services are divided into 3 categories.

3.1 *SaaS*

SaaS helps various service providers to use this as a service to deploy and offer different software's over the cloud environment so that user can get easy access to them to install and used them. It is the accountability of SaaS dealer to manage and deploy the information technology infrastructure like, servers, OS software, databases, data center space, cooling, etc., and the full solution is processed as illustrated in Figure 1 below [6].

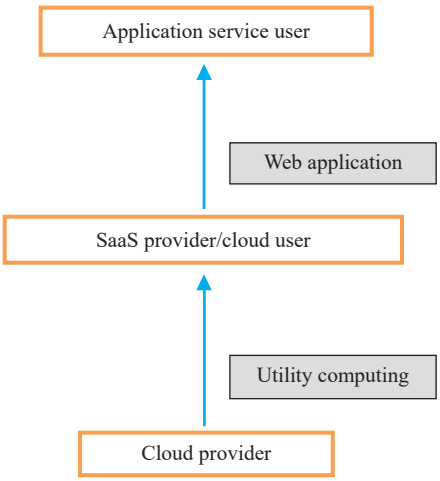

Figure 1. Software as a service

3.2 *PaaS*

PasS is programming environment which offers services to developers and end users where, there is no need to install or download software. Consumers control applications and their arrangements which are deployed but do not accomplish the infrastructure as illustrated in Figure 2 below [6].

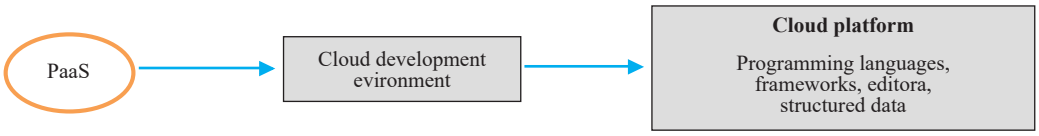

Figure 2. Platform as a service [7]

3.3 *IaaS*

IaaS is sharing of hardware properties which execute services by consuming virtualization technology. Its main intention to offer applications and operating systems easy access to the properties such as, servers, networks and storage. For using the application programming interface (API) for the interaction with the switches, routers, hosts, it deals basic infrastructure on mandate services and ability to add fresh tools in a transparent and simple manner. As the service supplier has the equipment so the provider is the responsible to maintain, house and run it. Clients pay on use basis, as

illustrated in Figure 3 below [6].

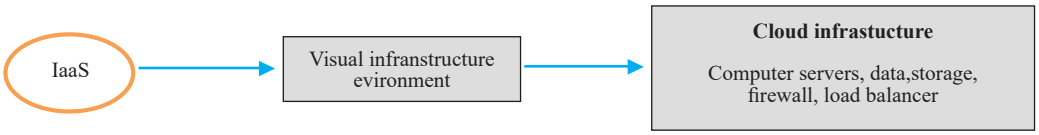

Figure 3. IaaS reference [7]

4. Cloud deployment models

4.1 *Private cloud*

Private cloud is used by the enterprises or any other third party at on-premises/off-premises and it is more secured and expensive if it is linked to public cloud. An extra safety rules, legal requirements/bandwidth restrictions are not contained by private cloud where these can be presented in public cloud. In the private cloud the control of infrastructure and security updates is upgraded by cloud service consumers and by suppliers as the user's networks and access used are limited. The example of private cloud is Eucalyptus systems [8, 9].

4.2 *Public cloud*

A public cloud is an infrastructure which Private cloud is used by the enterprises or any other third party at on-premises/off-premises and it is more secured and expensive if it is linked to public cloud. An extra safety rules, legal requirements/bandwidth restrictions are not contained by private cloud where these can be presented in public cloud. In the private cloud the control of infrastructure and security updates is upgraded by cloud service consumers and by suppliers as the user's networks and access used is limited. The example of private cloud is Eucalyptus systems [8, 9]. Is provided to numerous users and skilled by outsiders that are third party and occurs away the corporations firewall. Too many initiatives may work at the same time on an infrastructure which is provided and also users can vigorously supply resources. Such clouds are completely accommodated and managed by the supplier and all the accountabilities like installation, provisioning, management and maintenance. Individual charges are for the resources which are used by the users. In this infrastructure users have limited control so, for the public clouds security and controlling compliance are not continually a decent fit. There are no access restraints, no authorization and no authentication techniques in public cloud. Google and Amazon refer an access control to their customers. For example, Google App Engine, Microsoft Azure, and public cloud [10-12].

4.3 *Hybrid cloud*

It is a mixture of more than one cloud placement model which are connected in such a manner that data transmission occurs between models and no disturbance happens. These clouds are produced by initiative and the division of management accountabilities would be between the cloud provider and enterprise. In hybrid cloud an enterprise can shape the aims and essentials of services. Well-developed this cloud can be trustful to provide safe services as getting purchasers payments and also to those which are secondary to the enterprise. The big weakness to this cloud is the complication of creating and controlling as solution. Service areas which are taken from other bases must be gained and provisioned such as those are initiated from a solo locality and interaction among private and public components that may build operation even more complex. Linked clouds by typical technology that delivers transportability of data and applications amongst combing clouds are private, public or community. For example: Amazon Web Services [12-14].

4.4 *Community cloud*

That collective infrastructure by numerous enterprises for a sharing basis and maybe it is accomplished by them or

by any other third party provision supplier and hardly presented cloud model. Such clouds are established on a contract associated enterprises such as, educational organizations, shopping malls and banking. A cloud environment which being managed accordingly to this model may occur nearby or remotely. For Example: Facebook [12, 15].

5. Privacy security services

Cloud facilities are those applications which are consecutively wherever in the cloud computing infrastructure by the core net or internet. For the operators, data are kept in which place or where services are provided without any knowledge [8]. Providers are allowed to cultivate, organize, and route applications that can simply propagate in the performance, scalability and hardly failure chances in reliability. The weakness to gain these possessions of the clouds is storing identifiable private data to the further sideways of the internet and gain facility from third parties. So, the result in cloud computing security issues [10]. The question arises here is only what kind of security is useful for the users? This paper targeted privacy issues that could be possible in the case of SAS, IAS and PAS. Availability, confidentiality, data integrity, control and audit are considered key milestones that would lead toward achieving good safety level. Yes! There are some cloud systems which may attain these five collected now days [12].

5.1 *Availability*

It means to guarantee users may operate cloud systems anywhere and anytime. Cloud computing systems as being web-based enable operators to get entree to the system from wherever. Cloud systems should be separated all the time when operators want to access. There are two policies such as; redundancy and strengthening are fundamentally applied to improve the accessibility of the cloud system and applications which are accommodated on it [8]. Too many cloud system dealers offer infrastructure and stages of cloud which are centered on virtual machines that are used by the cloud system as infrastructure. VMware, Microsoft hypervisor and Xen are hypervisors that are carried by virtual lab management application. Other than this S3, EC2 (Amazon web service) are based on virtual machine (VM). And the virtual machine (Xen) has the capacity to provide separate memory, central processing unit (CPU), storage, machine virtualization and so on [10]. These all are available on the boundless number of service systems. This is the main motive that cloud facility providers are in a position to split resources, CPU cycles, and storage. This is the main reason virtual machines are the fundamental components to provide hosting to such services. Even the VMs consumes the ability to deliver on mandatory facilities in term of user's supply necessity for huge quantity of operators. These can be used for on-premises system and can be upgraded at any time by the user. Other side, the cloud system retailers depend on VM to link service personal computers (PCs) servers composed and to get them access and health system [13]. Recently infrastructures and platforms are provided by the cloud system vendors which are based virtual machine (Amazon, Skytap) that delivers the capacity to chunk and filter traffic established on the internet protocol (IP) address and port which is only to protect the systems. But as to be known accommodation is not correspondent for controlling net safety in most of initiatives [12, 26].

5.2 *Confidentiality*

Confidentiality means privacy of the secret data of the users in the cloud systems. The basic issue in the cloud systems for the operators. As we know that currently cloud system that is being delivered are public networks and systems are not protected to more attacks if these are compared to those, hosted in private data centers. To gain more users the confidentiality of users' data is the main requirement which will attract them the most. As there are for two fundamental methods which are physical separation and cryptography to get such secrecy but these are roughly implemented by the cloud computer retailers. So it's known that cloud systems are delivering data and services that are transmitted through networks which public. Because of such users are unable to get physical isolation. Physical and virtual layers are separated by deploying firewall and by packet clean. Such as, CohesiveFT reliefs virtual private network (VPN) cubed for IT infrastructure to afford safety edge however, it is privileged a solo cloud, multiple clouds or mixture cloud data center. If Amazon EC2 database is used to deploy a secure database and provide VPN and Firewall. If a Vertica database occurrence is stored by the Amazon EC2 than operators are provided complete root

entree through which operators will be able to make the system secured [13]. Due to which they will be able to choose to generate VPN among their initiative operators and Vertica for the cloud order and manage firewall to outdoor world. And there is another choice which can improve the confidentiality that is encrypted storage [17]. For example, when the data are encrypted before stored in the cloud will be more protected than unencrypted data in the limited data midpoint. A healthcare company TC3 successfully used this method to entree to thoughtful records of patient and healthcare privileges while moving health insurance portability and accountability act (HIPAA) compliant application [11, 14].

5.3 *Data integrity*

Say that all the information integrity should be reserved in the cloud system. For example, data must not be modified by illegal operators or lost. As records are the fundamental to provide cloud computing service likewise Data as a Service. It is the basic task to make data integrity. As, huge data process capability is provided by cloud computing systems [10]. For the data integrity which is related through data storing in cloud computing system are as follows, at first of recent development of hard disk drives are their ability increases are not capable to speed with data growth. Vendors are required to add up a populated hard drive to speed up data which is stored in the cloud. It might successively provide the result of the great likelihood of node disaster, data corruption, and disk letdown or data loss to. Secondly, their capacity of solid state disks is being bigger and bigger but these are not being enhanced to be faster while data access. Here this paper introduces Zetta system briefly which is delivered by Zetta that mostly focus on the data honesty for the cloud facilities which have related idea to redundant array of independent disks (RAID) systems. Zetta offers systems for storage service which are on mandatory mostly allowing for on data integrity. Data integrity state which at great measure and over extended ages of the period the system will not be corrupt or lost data. For the principal data accommodating facility, the Zetta implements RAINs 6 in Zetta system which mostly considers on the integrity of data [15]. As RAIN 6 is known for the reason that it has almost same implementation to RAIDs 6 and both consider ability the integrity of data almost. As RAIN6 is not just capable understanding high-definition (HD) disaster and bit faults but even to improve from node letdown and faults for any reasons. Due to data placement in terms of node the property of data integrity is gained. So, N + 3 implementation is used by Zetta system when compared to a RAID system that is said that it had the capability to accept three instantaneous disasters like, a 3 failure of disks or three whole nodes failure in a specified line. 8 + 3 is the standard encoding for Zetta system and in 8 pieces of primary data which are prearranged into 11 chunks that are more spread across 11 self-determining storing nodes where respectively of them comprises terminated network links. Due to such node level processing Zetta gets ability to offer data with great integrity. For integrity of data testing the commonly used technique is the digital signature. So data reliability is essential for cloud system which is to be gained by procedures like, digital signature. RAID liked approaches and others [12, 15].

5.4 *Control*

Control means to have authority to use the system, applications, its infrastructure and records in the cloud system. As the distributed calculation on many large measure datasets crossways vast numbers of computer nodes are always contained by cloud systems. All the users of the internet have the ability to pay his/her specific record control to the cloud that can be used further on the internet. For example, Google search web pages, the Amazon book store etc. are clicked by users that might be operated to provide directed advertisement. In the upcoming maybe healthcare applications will be able to use someone's deoxyribonucleic acid (DNA) sequence to progress personalized drugs and further therapeutic treatments with these particular records are stored in the cloud. Cloud systems operators may get several fears to their records. For instance, a medical patient is willing to take part in a healthcare study or not [12]. At the beginning he/she may be worried about the uncaring or malicious use of his/her information and therefore, results in the experience of his/her records. Later, he/she may think that if all calculations are done suitably and safely. So that, the study results itself may drip thoughtful material about his/her personal info. As such thoughtful specific records increases serious privacy and security worries if distributed computation are accomplished in the cloud system. To control the spread calculation in cloud systems over single records is basic in necessity. In cloud computing, decentralized information flow control is integrated by Airavat and also differential privacy to offer complicated secrecy and safety control in computation for individual records in the MapReduce outline. DIFC is used by Airavat for the confirmation that if the system is unrestricted from illegal storage entrée [14]. For example, this controls Mappers to

not drip the records over leaky network links or to not permit the intermediary result data in leaky local files. Because of multiple reliable early mappers and reducers, Airavat is capable to bring out secret conserving calculations in MapReduce outline which allows the operators to add their own mappers. As preliminary mapper need to be reliable because it states the data representation and it also affords a sample of input records to permit numerous queries to be collected in comparable that decreases the quantity of noise which is required to gain variance secrecy. As powerful and flexible computation platform is created by it and it guarantees to provide differential privacy. So however, control of data access efficiently and effectively in such system and determine the activities of the facilities which are accommodated on cloud systems would surely improve safekeeping systems [18].

5.5 *Audit*

Audit states that to check the cloud system if something has happened. Extra layer (Auditability) could be added above visualized OS which is accommodated on VM to facilitate that what ensued in the system. As it is capable of watching entire access duration so, it is considerable more protected than the one which is assembled into applications or to software themselves [19].

For such scenarios, 3 main points should be audited:

Events: The state alterations and many other influences that realized the system accessibility.

Logs: Proper logs should be maintained related to all service providers operator with their respective applications and users details.

Maintaining proper logs and activities under cloud environment would help to monitor specific issues even.

Monitoring: New feature strengthens the developers of cloud computing that to an emphasis on delivering visualized aptitudes rather than exact hardware that is to be given. As it is known that in technique perspective these have proficiency in auditing entire cloud system. There is other related concern which is the laws of every nation which require cloud computing suppliers to recall user records and copyrighted documents inside the national boundaries that is responsible to make the audit ability surely in the regulation problem viewpoint [14, 16, 18].

Table 2. Security responsibility comparison (cloud providers, customers and shared)

Types of security	IaaS	SaaS	PaaS
Data security	Customer responsibility	Customer responsibility	Customer responsibility
Application security	Customer responsibility	Customer responsibility	Shared responsibility
Platform security	Customer responsibility	Shared responsibility	Provider responsibility
Infrastructure security	Shared responsibility	Provider responsibility	Provider responsibility
Physical security	Provider responsibility	Provider responsibility	Provider responsibility

6. Other security issues in cloud computing

6.1 *Virtual machine security*

As it states that virtualization is the main mechanisms of cloud. All the virtual machines are dynamic. It mean that can be returned to the previous state, restarted and paused. Certifying that the foremost task of virtualization is that dissimilar occurrences which are being run on the same physical machine are separated from one alternative. These can be seamlessly moved and duplicated amongst physical attendants. Such dynamic nature and probable for virtual machine stretch create it tough to gain and preserve reliable safety. As vulnerabilities/configuration inaccuracies maybe accidently transmitted. There are two sorts of virtualization in cloud computing. Full virtualization and Para virtualization. Whole architecture replication occurs virtually in full virtualization. In Para virtualization, a operating

system (OS) is determined that it may be able to operate alongside with other OS. Extraction of physical resources which were used by the various virtual machines is done by a software layer virtual machine monitor. It also offers virtual processor and those other visualized versions of devices which are, input/output (I/O) devices, storage, memory, so on. In popular virtual machine monitor many bugs were found which allowed for absconding from VM. Due to vulnerability in the Microsoft virtual system and Microsoft virtual server might permit guest OS operator to execute a program on the host or any other guest OS. Vulnerability in Xen is to be demoralized by the super user of a guest domain to run random instructions. Another concern arises which is the control of superintendent on host and guest OS. Recent VM monitors don't deal perfect separation, due to which would be root protected, means there should not be privilege within the visualized guest environment licenses intrusion with the host system [20].

6.2 *Network security*

Attacks over network level security could be categorized in term of server attacks; distributed denial-of-service (DDoS), network level attacks; sniffing packets during transmission, client level security in the case of services provided over the network in cloud also suffers from confidentiality, authentication attacks [21]. Applications launch sniffer attacks which can internment packets rolling in net and when the files which are to be transported through such packets are not encoded then it can be read and dynamic information travelling across the net can be traced/caught. As a sniffer code, which is through network interface card (NIC) assurances which the data/traffic allied to different systems on the net gets noted too. It is gained by hiring NIC in promiscuous mode and all the records can be tracked in promiscuous mode travelling on the same network. Address resolution protocol and round trip time that are used to determine sniffing systems which are being operated on a network through malicious sniffing detection platform. Internet protocol address problems have been a vast network security worry when used again [22]. If the user is connected to network through an IP address will move out of that network, then his IP address will be given to a new user. Due lag of time between change of internet protocol address in a domain name server will be sometimes risky for security as to clear that address in domain name server crashes. As that is known that old internet protocol address is allotted to a new user and still the chances of regaining files by other users is not insignificant as the address is yet exists in the domain name server cashes and when data are being fitted to an operator may become reachable to some other operator violating the secrecy of the main operator [23].

7. Conclusion

Cloud computing converted very popular and growing very fast. Its emerging continuously and many initiatives are taken in order to provide services. Thus, security issues implement tough obstacle for consumers' implementation of Cloud systems and Cloud services. We perceived security fears presented by an amount of Cloud computing system providers in this paper. Yet, those fears are not satisfactory. Proper security policies should be maintained in the Cloud environment to achieve the 5 goals (i.e. availability, confidentiality, data integrity, control and audit) as well as privacy acts should be altered to facilitate users and providers in the Cloud literature. A key issue related to security that can be considered as a threat is those cloud service providers have to share resources between their customers, so to achieve a satisfactory security level they should update their security policies based on their customer profiles. This survey highlighted in start different cloud computing models which could be deployed followed by security issues related to cloud computing, out of those research challenges security related to securing data is the most key objective that should be accomplished under each deployed model. Securing network access to provide virtual access under cloud computing is another fundamental concern in cloud computing. This survey paper highlighted all those security issues and the work cut out for the improvement so far.

Future work

In future still there are possibilities for the improvement of securing data and access in cloud computing so therefore proposing new techniques algorithms and protocol could enhance security.

Conflict of interest

The authors declare there is no conflict of interest.

References

[1] Aljawarneh S, Radhakrishna V, Kumar PV, Janaki V. A similarity measure for temporal pattern discovery in time series data generated by IoT. In: *2016 International Conference on Engineering & MIS (ICEMIS)*. Agadir, Morocco: IEEE; 2016. p.1-4.

[2] Ahmad N. Cloud computing: Technology, security issues and solutions. In: *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*. Abha, Saudi Arabia: IEEE; 2017. p.30-35.

[3] Gupta BB, Yamaguchi S, Agrawal DP. Advances in security and privacy of multimedia big data in mobile and cloud computing. *Multimedia Tools and Applications*. 2018; 77(7): 9203-9208.

[4] Tabrizchi H, Kuchaki Rafsanjani M. A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*. 2020; 76: 9493-9532.

[5] Al-Issa Y, Ottom MA, Tamrawi A. EHealth cloud security challenges: A survey. *Journal of Healthcare Engineering*. 2019; 2019: 7516035.

[6] Basu S, Bardhan A, Gupta K, Saha P, Pal M, Bose M. Cloud computing security challenges & solutions-a survey. In: *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*. Las Vegas, NV, USA: IEEE; 2018. p.347-356.

[7] Davies A. *Top 10 Cloud Services Providers*. Available from: https://www.devteam.space/blog/top-10-cloud-computing-services-providers/ [Accessed 14 April 2020].

[8] Wan J, Lin K, Zeng D, Li J, Xiang Y, Liao X, et al. *Cloud Computing, Security, Privacy in New Computing Environments*. Cham: Springer; 2018.

[9] Feng DG, Zhang M, Zhang Y, Xu Z. Study on cloud computing security. *Journal of Software*. 2011; 22(1): 71-83.

[10] Chen D, Zhao H. Data security and privacy protection issues in cloud computing. In: *2012 International Conference on Computer Science and Electronics Engineering*. Hangzhou, China: IEEE; 2012. p.647-651.

[11] Behl A. Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation. In: *2011 World Congress on Information and Communication Technologies*. Mumbai, India: IEEE; 2011. p.217-222.

[12] Kajal N, Ikram N, Prachi. Security threats in cloud computing. In: *International Conference on Computing, Communication & Automation*. Greater Noida, India: IEEE; 2015. p.691-694.

[13] Padhy RP, Patra MR, Satapathy SC. Cloud computing: security issues and research challenges. *International Journal of Computer Science and Information Technology & Security (IJCSITS)*. 2011; 1: 136-146.

[14] Zhou M, Zhang R, Xie W, Qian W, Zhou A. Security and privacy in cloud computing: A survey. In: *2010 Sixth International Conference on Semantics, Knowledge and Grids*. Beijing, China: IEEE; 2010. p.105-112.

[15] Liu W. Research on cloud computing security problem and strategy. In: *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*. Yichang, China: IEEE; 2012. p.1216-1219.

[16] Wang C, Wang Q, Ren K, Lou W. Privacy-preserving public auditing for data storage security in cloud computing. In: *2010 Proceedings IEEE INFOCOM*. San Diego, CA, USA: IEEE; 2010. p.1-9.

[17] Shaikh FB, Haider S. Security threats in cloud computing. In *2011 International Conference for Internet Technology and Secured Transactions*. Abu Dhabi; 2011. p.214-219.

[18] Yi S, Qin Z, Li Q. Security and privacy issues of fog computing: A survey. In: *International Conference on Wireless Algorithms, Systems, and Applications*. Cham: Springer; 2015. p.685-695.

[19] Gampala V, Inuganti S, Muppidi S. Data security in cloud computing with elliptic curve cryptography. *International Journal of Soft Computing and Engineering (IJSCE)*. 2012; 2(3): 138-141.

[20] Zissis D, Lekkas D. Addressing cloud computing security issues. *Future Generation Computer Systems*. 2012; 28(3): 583-592.

[21] Feng DG, Min Z, Yan Z, Zhen X. Study on cloud computing security. *Journal of Software*. 2011; 22(1): 71-83.

[22] Chen Y, Paxson V, Katz RH. *What's New About Cloud Computing Security?* University of California, Berkeley Report No. UCB/EECS-2010-5 January 20, 2010.

[23] Wu H, Ding Y, Winer C, Yao L. Network security for virtual machine in cloud computing. In: *5th International Conference on Computer Sciences and Convergence Information Technology*. Seoul: IEEE; 2010. p.18-21.