IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Review of Computer Engineering Studies
Vol. 9, No. 4, December, 2022, pp. 145-149
Journal homepage: http://iieta.org/journals/rces

Security Issues in Cloud Computing: A Study

Muhammad Hassaan

Department of Computer Science and Information Technology, Virtual University of Pakistan, Lahore 54000, Pakistan

Corresponding Author Email: m.hassaan@vu.edu.pk

https://doi.org/10.18280/rces.090404

Received: 27 November 2022
Accepted: 12 December 2022

Keywords:
cloud computing, services, on-demand computing resources, pay-for-use basis, openness, data security, privacy protection

ABSTRACT

Cloud computing is the study of using remote servers which are hosted on the internet to deliver on-demand computing resources on pay-for-use basis rather than a local server. It provides online services via third party which own the infrastructure. Due to the openness of cloud computing systems, customers have concerns about security point of view in the adoption of the services which they provide. The purpose of this paper is to give a detail regarding to the data security and privacy safety issues in cloud computing systems. A security architecture discussed in this paper to provide security measures. In this architecture it can be seen that every level provides security measures in different ways. Then this paper will also discuss some of the current available solutions. According to the findings of this research, in the designing phase of the applications which are based on cloud, there should be taken security measures to increase the trust level of customers' and organizations.

1. INTRODUCTION

According to IBM, "Cloud computing, often referred to as simply "the cloud," is the delivery of on-demand computing resources-everything from applications to data centers-over the Internet on a pay-for-use basis." [1]. Cloud Computing refers to manipulate, configure and access the applications online. It offers online data storage, infrastructure and application [2, 3]. It is well-known that cloud computing has many potential advantages and plenty of organization packages and facts are migrating to public or hybrid cloud. But concerning a few business-crucial programs, the groups, mainly large organizations, nonetheless would not circulate them to cloud. From the customers' point of view, cloud computing safety concerns, mainly facts protection and privacy safety problems, continue to be the number one inhibitor for adoption of cloud computing offerings. In cloud computing systems, traditional protection problems are still present. This is due to giving the unlimited access to the organizations. Here, the unlimited refer to the extension of boundaries. The main concern of these security issues is of the openness and multi-tenant property which is leading to the remarkable effects on cloud systems security:

(1) As, cloud systems are scalable because these are available at any time and if many people or organizations use these systems for their specific purposes at the same time then no difference occur on the performance of these systems, but still the problem of its data protection remain same because when a large data migrated on the cloud at the same time so it becomes difficult for the system to secure the data at the same time.

(2) According to the provider shipping models of cloud computing, resources cloud point of views primarily based on may be owned with the aid of multiple companies.

(3) Due to the openness in cloud computing systems, it is possible for unauthorized users to access the data of others.

(4) People use cloud computing resources to store big data for quick access in future, but it is possible that due to limited security features a cloud system may not meet the processing of big information.

The main focus of this paper is on data protection that how data can be unsafe in these cloud systems and what safety measures has been taken to safe the data from an illegal or unauthorized organization and what necessary steps should be taken to sort out these kinds of problems to secure the data.

2. RELATED WORK

Cloud security has become the main topic for discussion in both market and academic. Several global conferences have focused on this issue alone, such as the ACM Workshop on Cloud Computing Security, the International Conference on Cloud Security Management, and the most effective European convention at the challenge, Secure Cloud, which had already three editions. Consequently, several scientific contributions have been published not only on conferences proceedings, however also in worldwide journals [4].

3. METHODOLOGY

The paper is organized as follows. Section 4 describes the security issues in cloud computing. Section 5 describes the cloud security fundamentals. Section 6, describes the data security and privacy protection issues in cloud computing. Section 7, what possible solutions for data security are currently available. Section 8 presents the conclusion of the paper.

4. SECURITY ISSUES IN CLOUD COMPUTING

Security issues which come in cloud computing for data security and privacy protection are as follows:

4.1 "Concept of security in cloud computing"

Wikipedia refers cloud computing security as, "the security of data of a customer or an organization from an illegal and unauthorized person, security of data over the network [5]". Here is the point which should be noted that this is deal with the cloud computing security not deal with the software products which are cloud based like anti-virus, anti-spam etc.

4.2 "Security issues associated with the cloud"

In cloud computing, there are many security issues which can be divided into many ranges. According to Gartner [6], when customers buy the cloud services, they have many questions and they ask from the vendors about particular safety concerns. Some of main concerns are: "what will be in user access?", "where their data will reside?", "how data will be segregated?", "in case if data has been lost then will it be easily recoverable?", "how much it will be reliable?" etc. Forrester Research Inc. evaluated privacy services of big organizations which provide cloud services to the customers, such as Amazon, Google etc. to evaluate that what kind of security measures they provide and in case of data usage by unauthorized person, what is their legal stance [7]. Cloud Security Alliance (CSA) is on the mission to gather security solutions and they are trying to find out the solutions by discussions i.e., individual or grouped. So that, best practices can be find out for current and future use of cloud computing services to ensure the quality of its safety measures [8, 9]. Subashini and Kavitha [10], they have done complete research on the security issues provided by cloud computing systems to ensure that the models through which they provide services to users are reliable or not and what is their way to provide services to the users and where difficulties come. Also, according to some researchers [11], they also evaluated the security issues which come in using cloud computing services. They described that what issues come related to the architecture of cloud computing, its properties and its stakeholders. Similarly, some other researchers [12] believed that due to the openness of cloud computing services and its multi-tenant behavior also leads to the security issues.

5. CLOUD SECURITY FUNDAMENTALS

Three fundamental features make up a secure cloud computing architecture: secrecy, integrity, and availability. Your efforts to plan a more secure cloud deployment will be guided by an understanding of each capability.

5.1 Secrecy

The ability to keep information hidden and unreadable from those who shouldn't have access to it, such attackers or employees inside an organization without the necessary access level, is known as confidentiality. Privacy and trust are additional examples of confidentiality, or when a company promises to handle consumer data in confidence.

5.2 Integrity

Integrity refers to the notion that the systems and applications are precisely what you anticipate them to be and behave exactly how you anticipate. Losses may result if a system or programme has been exploited to generate an unknown, unexpected, or false output.

5.3 Availability

The third capability, availability, is typically given the least thought by cloud architects. The term "availability" refers to DoS assaults. Perhaps an attacker can't access your data or alter it. However, if an attacker manages to render systems unavailable to you or your clients, you will be unable to do operations that are crucial to running your company.

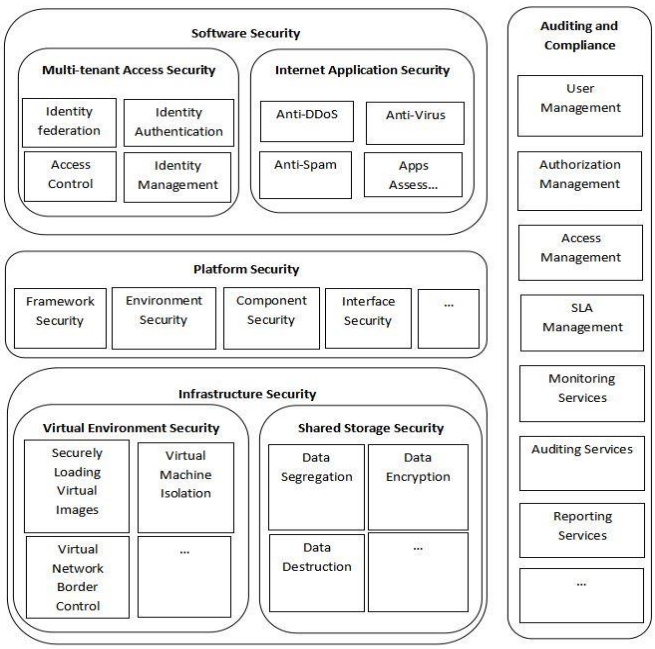

Figure 1. Security architecture of cloud computing

The security architecture of cloud computing can be seen in Figure 1. The term "cloud security architecture" refers to all the hardware and software used in cloud platforms to safeguard data, workloads, and systems. When creating blueprints and designs for cloud platforms, a strategy for cloud security architecture should be developed and integrated from the ground up. Too frequently, cloud architects will put their full attention on performance first and try to add security later. In this architecture it can be seen that every level provides security measures in different ways.

6. DATA SECURITY AND PRIVACY PROTECTION ISSUES

The concept related to protection of data and privacy in cloud computing is same as we have in the safety of our real-life data. So, due to the openness of the cloud system customers have many concerns related to the protection of their data. Everyone has different idea related to the data privacy which may or may not be different from others. They want to secure their data according to their requirements. So, these requirements can be varying from person to person, because everyone has different perspectives. According to the Organization for Economic Cooperation and Development (OECD) [13] is that, "everyone has different perspectives related to their data privacy, which may be differ from person to person".

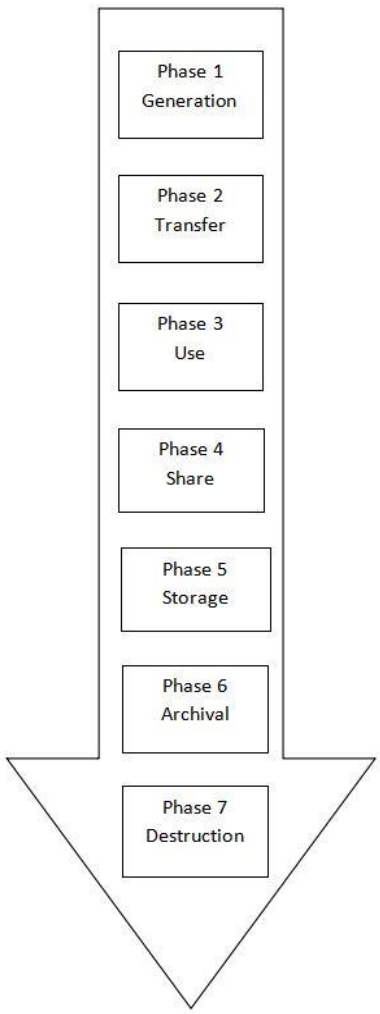

Figure 2. Life cycle of data

So, in the life cycle of data many issues related to the data privacy can be seen in each phase of the cycle.

Life Cycle of Data

Life Cycle of Data presents the technique of data from the technology to its destruction. It consists on seven different phases, which can be seen in Figure 2.

6.1 Generation phase

The generation of data is involved within the information possession. Traditionally, we can see that data is managed by users or corporations own and manage the data but when we talk about to refer data on the cloud so it should be thought that how data ownership can be maintained.

6.2 Transfer phase

It is not require encrypting the data for transmission within the boundaries of an organization. For the integrity and confidentiality of data in transmission over the boundaries of an organization, it should be ensured that data is out of access from any illegal or unauthorized person. Here, the integrity of data must be ensured because only the encryption of data cannot be enough. So, it ought to make sure that delivery protocols provide each confidentiality and integrity. There is need to ensure that integrity and confidentiality of data transmission is not only in cloud storage and organization storage but also in the services which are provided by cloud.

6.3 Use phase

It can be seen that; data is to be transfer on the cloud system due to its vast range of storage capacity. So that data can be used in future. But due to security point of views, sometimes data encryption is feasible or sometimes it is not feasible. Because in indexing and querying it leads to many problems. Here is the point which should be noted that why this occur because the applications which are cloud based used data which is generally not encrypted. This is not only for the cloud systems but this is also in the traditional systems. Generally, the data which they transfer is not encrypted. As, it can be seen above again and again cloud systems are multi-tenant. This is because; the applications which are cloud based processed the data, which is stored with others data. So, the un-encrypted data is really a serious data security threat.

6.4 Share phase

This phase has an importance in sense of security of data while sharing from one part to another. Because a person who have his own data and he can share it a single person. But on the other side person cannot ensure that the data which he has shared with one person is not shared with any other. So, this issue remains same for data owners that, “is there any restriction on third party to use their data or not?”. So, it should be ensuring in the designing phase of the applications which are based on cloud that the data which is owned by any private owner should not be used by any other illegal or unauthorized third party. This becomes the cause of destroying the trust level of customers and organizations from the system.

6.5 Storage phase

To ensure the data confidentiality and integrity is to encrypt the data, this is the common answer when we talk about the

data confidentiality and data integrity. Everyone has different idea related to the data privacy which may or may not be different from others. They want to secure their data according to their requirements. So, these requirements can be varied from person to person, because everyone has different perspectives. So, according to the storage point of view in cloud system, we deal with the huge data to store and this is understood that we use cloud systems to store and manage a huge data because it is also providing a big storage according to the customer or organization needs. So, organizations generate patterns in storage to ensure the security of their data from an illegal or unauthorized person. Here is an issue, which is that in early stages when a customer uses the storage of cloud systems, they are not confident related to the protection of their data. They entrust the system that is there data is safe here or not. Because, the main problem in cloud systems security is due to its openness, which becomes the cause of uncertainty related to the safety of data. Additionally, we can also see that cloud systems are easily available at everywhere to store and manipulate the data. The main thing is that we require a continuous connection to perform our tasks on the cloud system. In such case, if we lost our data from the cloud, "so is it will provide the backup?" also force the customer or an organization to think about that.

6.6 Archival phase

As everyone knows that, word archive referred as "to store the data". Similarly, in the life cycle of data a phase comes, which is referred as archival phase. In this phase, it has to be decided that where the data will be stored. As, the data security concern is the main issue of every customer and organization. So, where the data should be resides and what patterns or encryption methods should be followed to secure the data from unauthorized people have to decide in this phase of life cycle of data referred as "archival phase".

6.7 Destruction phase

At the end, this phase comes which is referred as "destruction phase". In this phase, data has to be destroyed if it has not required more. So, every copy of the data item has to be removed from the organization. As data is archived, so this activity has to done from an archive. So, in this phase it has to be ensured that data destruction has to be done properly or not.

7. CURRENTLY AVAILABLE SOLUTIONS FOR DATA SAFETY AND TO PROTECT THE PRIVACY

An encryption scheme which has developed by IBM processed the data without decryption [14]. As we have discussed above that, it can be seen that, data is to be transfer on the cloud system due to its vast range of storage capacity. So that data can be used in future. But due to security point of views, sometimes data encryption is feasible or sometimes it is not feasible. Because in indexing and querying it leads to many problems. Here is the point which should be noted that why this occur because the applications which are cloud based used data which is generally not encrypted. So, in this case this encryption scheme is very precious. A system referred as "airavat" [15] is a machine which prevents privacy leakage from unauthorized people. As, everyone has different idea related to the data privacy which may or may not be different from others. They want to secure their data according to their requirements. So, these requirements can be varied from person to person, because everyone has different perspectives. So, in this case, this system is very useful. The Organization for the Advancement of Structured Information Standards (OASIS) Key Management Interoperability Protocol (KMIP) is trying to resolve such troubles [16]". As, cloud systems are scalable because these are available at any time and if many people or organizations use these systems for their specific purposes at the same time then no difference occur on the performance of these systems, but still the problem of its data protection remain same because when a large data migrated on the cloud at the same time so it becomes difficult for the system to secure the data at the same time. As, the data is dynamic in cloud storage, conventional facts integrity answers are no longer suitable. NEC Labs' provable records integrity (PDI) answer can guide public facts integrity verification and some researchers proposed mathematical solutions to ensure the integrity of data dynamically which are saved inside the cloud [17, 18]. Similarly, some researchers proposed privacy management tools regarding to the privacy of data storage to assist the users that how they can prevent their sensitive data from illegal persons within a cloud [19]. Similarly, some researchers discuss the technologies with their proposed solutions i.e. graph anonymization, data pre-processing techniques etc. [20]. The Information Architecture (IA) agent can discover the users who are getting access to data and the forms of data they use [21]. So, this is also a safety measure which can prevent data from unauthorized people.

8. CONCLUSION

After analyzing the security concerns related to data protection, we know that, "Cloud Computing refers to manipulate, configure and access the applications online. It offers online data storage, infrastructure and application" but on the other side it also has security concerns as discussed above. According to the analysis it is too much difficult to fulfill the all requirements of a customer or an organization related to their safety point of views regarding to cloud systems for data security. This is because, openness of these systems become the main problem here which cannot omit. But on the other side, there should be taken necessary steps to satisfy the customers to ensure them that their data is in secure place. As some current solutions are available in this regard and they should be considered to enhance the safety of the data. So, in the designing phase of the applications which are based on cloud, there should be taken security measures to increase the trust level of customers' and organizations.

REFERENCES

[1] Cloud computing: A complete guide|IBM. https://www.ibm.com/cloud/learn/cloud-computing, accessed on Sep. 25, 2022.

[2] Jadeja, Y., Modi, K. (2012). Cloud computing-concepts, architecture and challenges. In: 2012 international conference on computing, electronics and electrical technologies (ICCEET) IEEE, pp: 877-880. https://doi.org/10.1109/ICCEET.2012.6203873

[3] Zhang, Q., Cheng, L., Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. Journal of Internet Services and Applications, 1: 7-18. https://doi.org/10.1007/s13174-010-0007-6

[4] Fernandes, D.A., Soares, L.F., Gomes, J.V., Freire, M. M., Inácio, P.R. (2015). Security issues in cloud environments: a survey. International Journal of Information Security, 13: 113-170. https://doi.org/10.1007/s10207-013-0208-7

[5] Cloud computing security. https://en.wikipedia.org/wiki/Cloud_computing_security, accessed on Oct. 16, 2022.

[6] Gartner: Seven cloud-computing security risks|InfoWorld. https://www.infoworld.com/article/2652198/gartner--seven-cloud-computing-security-risks.html, accessed on Oct. 20, 2022.

[7] Cloud Security Front and Center. https://go.forrester.com/blogs/09-11-18-cloud_security_front_and_center/, accessed on Oct. 25, 2022.

[8] Cloud Security Alliance– Wikipedia. https://en.wikipedia.org/wiki/Cloud_Security_Alliance, accessed on Nov. 1, 2022.

[9] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing. https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/csaguide.v3.0.pdf, accessed on Nov. 4, 2022.

[10] Subashini, S., Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1): 1-11. https://doi.org/10.1016/j.jnca.2010.07.006

[11] Almorsy, M., Grundy, J., Müller, I. (2016). An analysis of the cloud computing security problem. arXiv preprint arXiv:1609.01107.

[12] Chen, Y., Paxson, V., Katz, R.H. (2010). What's new about cloud computing security? University of California, Berkeley Report No. UCB/EECS-2010-5 January 20, 2010.

[13] IBM Discovers Encryption Scheme That Could Improve Cloud Security, Spam Filtering, https://www.eweek.com/security/ibm-discovers-encryption-scheme-that-could-improve-cloud-security-spam-filtering, accessed on Dec. 10, 2022.

[14] Roy, I., Setty, S.T., Kilzer, A., Shmatikov, V., Witchel, E. (2010). Airavat: security and privacy for mapreduce. In NSDI, 10: 297-312.

[15] OASIS Key Management Interoperability Protocol (KMIP) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=kmip, accessed on Dec. 11, 2022.

[16] Zeng, K. (2008). Publicly verifiable remote data integrity. In: Chen LQ, Ryan MD, Wang GL, eds. LNCS 5308. Birmingham: Springer-Verlag, 419-434.

[17] Wang, C., Wang, Q., Ren, K., Lou, W.J. (2009). Ensuring Data Storage Security in Cloud Computing. In Proceedings of the 17thInternational Workshop on Quality of Point of view, 1-9.

[18] Bo Bowers, K.D., Juels, A., Oprea, A. (2009). Proofs of retrievability: Theory and implementation. In Proceedings of the 2009 ACM workshop on Cloud Computing Security, 43-54. https://doi.org/10.1145/1655008.1655015

[19] Muntés-Mulero, V., Nin, J. (2009). Privacy and anonymization for very large datasets. In Proceedings of the 18th ACM conference on Information and knowledge management, pp. 2117-2118. https://doi.org/10.1145/1645953.1646333

[20] Gajanayake, R., Iannella, R., Sahama, T. (2011). Sharing with care: An information accountability perspective. IEEE Internet Computing, 15(4): 31-38. https://doi.org/10.1109/MIC.2011.51

[21] Kissel, R., Scholl, M., Skolochenko, S., Li, X. (2011). Guidelines for Media Sanitization. NIST Special Publication 800-88. http://dx.doi.org/10.6028/NIST.SP.800-88r1