University of Sindh Journal of Information and Communication Technology
(USJICT)
Volume 2, Issue 1, January 2018

ISSN-E: 2523-1235, ISSN-P: 2521-5582 © Published by University of Sindh, Jamshoro
Website: http://sujo.usindh.edu.pk/index.php/USJICT/

Security of Provider sides in Data Privacy and Data Accessibility Issues in Cloud computing

Taimoor Ahamd, Hala Aslam, Shahzeb Shahzad
Department of CS&IT University of Sargodha Gujranwala campus
Taimoorahmad786@gmail.com, Halaaslam12@gmail.com , professorshahzeb@gmail.com

Abstract: Cloud computing is an approach to share resources under one or more than one leading authority using multiple developments and deployment models such as resources of computational power and storage. Basically, the cloud is a business model, it has grown up in business and various fields of life as well. In spite of its power, it raises numerous security threats including loss of customer important data, data leakage, duplicating, resource pooling etc. As far as security threats are concerned, a wide research has been conducted which show threats with services and deployment models of a cloud. In order to realize these threats, this study is presented to effectively refine the basic security issues under various areas of cloud. This work presents data security threats under the cloud models. The solution is to involve third-party cloud provider in which client send their data to the cloud which is encrypted by third-party. The intention of proposed work is to save the cloud services providers from unauthorized access by blocking the unauthorized users.

Keywords: Cloud Computing, Grid Computing, Security threats, and Access control, Data Accessibility, Data Privacy, Authentication Security and Encryption.

I. INTRODUCTION

Grid computing is a system in which different users are shared their resources to perform a specific task. Different types of errors are created in grid computing such as processing time, user interaction, resource sharing and limited area applications. Furthermore, grid computing has also some limitations like fault tolerance, error detection and scheduling. To minimize these errors and limitations the researchers proposed an emerging technology called cloud computing [1].

In cloud computing, the service providers offer different resources to their end users. These resources are computational power, storage resources, computer resources and software resources. According to "National Institute of Standards and Technology (NIST)", cloud computing is defined as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[2]. Cloud model is made up of five important characteristics (on-demand self-service, broad network access, rapid elasticity, measured services and resource pooling), three service models (software as a service (SaaS), infrastructure as service (IaaS) and platform as a service (PaaS)), and four deployment models (public, private, hybrid and community cloud) [3, 4].

Security can be defined as "The state of being free from danger or threat" [5]. Security is a major element for consumers when they are shifting their data to the cloud. In addition, a number of threats arise for consumers when data is sent to the cloud. These threats are data threats, virtual machine threat, user access threat, infrastructure threat and physical security threat [6]. The proposed work will secure the servers (third party and storage provider server) to access from unauthorized users and blocked users. This study is divided into different sections. Section 2 review the difference between cloud computing and grid computing. Section 3 explain the cloud models. Section 4 define the data threats in cloud computing. Section 5 give the solution. Section 6 has the conclusion.

II. DIFFERENCE BETWEEN CLOUD COMPUTING AND GRID COMPUTING

Table 1: Difference between cloud and grid computing

Technologies	Grid	Cloud
Architecture	Sharing of users resources	Resources provided by the providers
Model	Service Model	Business Model
Access	Limited access of resources	Complete access of required resources

Development of applications	Using executable file	Ready to use application components
Resources availability	Not every time available	Available 24/7

III. MODELS OF CLOUD COMPUTING

There are two models of cloud computing [4, 10]:

A. Deployment Models

This model includes private, public, community and hybrid cloud or model in cloud computing. Normally, private cloud is used by an organization and it is functioned by itself or third party provider, whereas public cloud can be used by more than one organization or general public. The community cloud can be used by a specific community who has same purpose and requirements. The hybrid cloud is a combination of more than one cloud or model, for example, public and private, public and community, private and community etc [4, 10].

B. Delivery Models

The cloud provides different forms of services model like software, platform and infrastructure. Providers delivered costly applications like ERP and CRM to users. These applications run on provider platform that includes languages and libraries. The operating system, database, network bandwidth etc. Comes under infrastructure. There are different types of cloud delivery models [8].

1) Software as a Service (SaaS)

In this model cloud customers have control of utilities that are being delivered by the cloud providers. In SaaS customer do not have control of infrastructure [8].

2) Platform as a Service (PaaS):

In this model cloud customers have control over platforms (tools and software) that is being provided by the cloud providers. Cloud customers can use different types of languages and tools to create their own applications [8].

3) Infrastructure as a Service (IaaS):

In this model cloud customers have complete control over cloud resources that are being provided by cloud providers such as storage, rent processing, network capacity and connectivity [8].

IV. DATA THREAT IN CLOUD COMPUTING

In the cloud, customer faces many security problems and issues while sending their data . So, the data security is the main factor that is decided by enterprise utilities used for cloud computing [9, 10]. Survey of Gartner in 2009 presented that approximately 70% of the respondents in the actual deployment of cloud computing is security and privacy threats [11]. The client faces many threats in the cloud such as data accessibility, data privacy, data confidentiality and data availability threat in the cloud environment.

A. Data accessibility threat:

Data accessibility can be defined as “An access control system (ACS) is a type of security that manages and controls who or what is allowed entrance to a system, environment or facility. It identifies entities that have access to a controlled device or facility based on the validity of their credentials.”[12]. In simple words, data accessibility is to make a connection with the database where the customer store their data. The access to data is not provided to everyone because of data security issues, data can be hacked or attacker can change and leak the private data of customers. To avoid these issues, the access granted only to interrelated persons that are directly connected with a specific domain. The trustworthy persons who have to authenticate approval from the upper management to access the data and system for communication. The system requires some specific credentials from users who have authenticated with the rights after this they will request and access the data.

Access to data plays an important role in the field of cloud computing because a person/company wants to save their data where the person can access data anytime or anywhere. Users prefer online access and services that are available 24/7.

1) Data Accessibility Issues:

According to the cloud policies, customer data are stored in different locations but clients are not familiar with the exact location of data.

Many scholars discussed data accessibility issues. Valuable data can be access by a user or third party. They can read, write, and modify the data [8, 14]. For example in a company, information is shared only with authorized users [10]. We cannot ignore the data security issues such as if an unauthorized user attack on the private data then they can modify data and leak the personal data of an organization [11]. In the cloud, clients access data and services using the internet that will create a risk for users. A user can implement access rights with its own policies [13].

Mostly, researchers only discussed client level data accessibility. In cloud computing, the providers have rights to access the client’s private data. Most of the cloud providers have stored customer data through encryption standards. Unauthorized providers know the encryption standards and technique that they are using for their customers. Through this, they can damage customer data [14].

B. Data Privacy

Data privacy is known as information privacy. It can be defined as “data privacy, is the necessity to preserve and protect any personal information, collected by any organization, from being accessed by a third party. It is a part of Information Technology that helps an individual or an organization determines what data within a system can be shared with others and which should be restricted” [15]. In simple words, data privacy is justifying data that is saved in the cloud. Therefore, data privacy term is used specifically for the protection of data from illegal folks that occurs due to hacking. These days everything is possible when we are talking about the digital world where any obstacle is not taking more time.

Data privacy is essential when we are discussing the security of data. It is important for an organization to apply some security checks while accessing any data from cloud [15].

1) Data Privacy Issues

In cloud computing data privacy is the primary focus for a service provider. Cloud Suppliers tell that data is secured at their locations. Different researchers talk about data privacy issues. Their concepts are “Top vulnerabilities are to be checked to ensure that data is protected from any attacks”[16]. Sensitive and non-sensitive data that comes from an authorized host can create threats with virtual co-tenancy [13, 17]. Attackers get access to confidential data and moving towards data breaches. A researcher has revealed malicious attacks through unauthorized operators by targeting the IP address and physical server [4, 8].

From the prior discussion, the data privacy issues arise in proposed work. When a user sends their data to the cloud, they expect that their data can be secure and confidential. Sometimes cloud data can be breached and altered by the attacker. The consumers faced disaster at the time of data retrievals due to these issues. It is needed to provide solutions that give complete privacy to users. If a hacker, provider and admin access the data. The accessed data couldn’t be understandable to them. There are also need to secure the third party and storage server from unauthorized access.

V. SOLUTION

In previous research, cloud providers use only one encryption standard at a time to encrypt the user data. The main issue in earlier research is that the cloud administrator knows how to encrypt the data and have a chance to get the access of customer data that harm the cloud users.

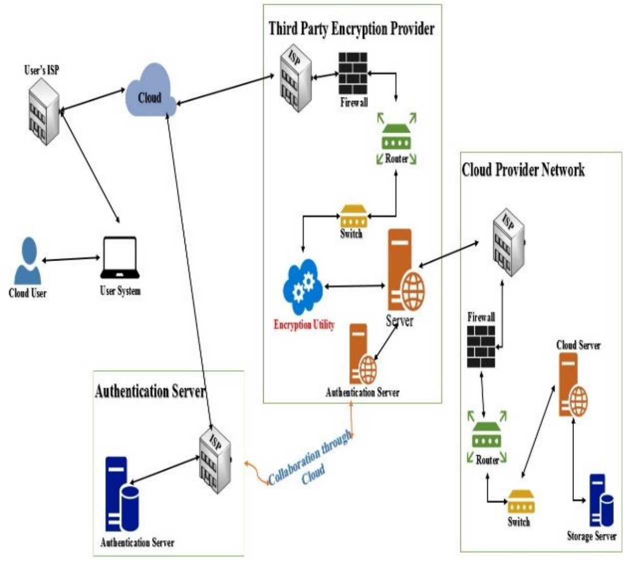

Figure 1: Referenced architecture

In Figure 1 the user sends their data to the cloud. Firstly, it toward the third-party whose responsibility to encrypt the user data using encryption utility (which has more than one encryption standards and customers have their own choice to choose the standard and encrypt their data using his desired key). After this, the encrypted data is sent to the cloud provider's side and if a cloud provider admin accesses the data of a customer. The admin will only see the customer's data that is not understandable for them [18].

Now there is a danger to get unauthenticated or unauthorized access to provider servers. The solution to this problem is when an irrelevant person wants to access the admin system. It needs some credentials to log in. If credentials are authenticated then system send 6 digits code on admin's phone. Admin has to convey the generated code to the system for performing their functionalities on the system. If the code is not authenticated then the server will be also shut down for that admin.

If the credentials are unauthenticated twice then the system show non-running state for that user. At the same time, it blocks the IP address as well and put him on the block list.

VI. CONCLUSION

Cloud computing is an emerging technology in nowadays that provides a great number of benefits, but it also contains many security challenges. The main purpose of a cloud is to store and manage the user data securely. When talking about cloud system, it consists of development and deployment models which a provider provides to their customers. In this paper, the proposed work discussed the security of third-party cloud and cloud storage providers. They count the number of logins attempt. If the login attempts exceeded to defined value than the system will go to un-running state for that user.

VII. REFERENCES

[1] "Grid vs CLoud Computing," 2017. [Online]. Available: http://www.brighthub.com/environment/green-computing/articles/68785.aspx.

[2] F. Lui *et al.*, "NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology," *NIST Spec. Publ. 500-292*, 2011.

[3] "What is SPI model (SaaS, PaaS, IaaS)? - Definition from WhatIs.com." [Online]. Available: http://searchcloudcomputing.techtarget.com/definition/SPI-model. [Accessed: 10-Aug-2017].

[4] B. Kaur, "Cloud Computing and Security Issues : A Survey Barinder Kaur," vol. 3, no. 2, pp. 168–171, 2015.

[5] "security - definition of security in English | Oxford Dictionaries." [Online]. Available: https://en.oxforddictionaries.com/definition/security. [Accessed: 10-Aug-2017].

[6] X. P. Xu, J. H. Yan, and L. Liu, "The Research on Cloud Computing Data Security Mechanism," *Adv. Mater. Res.*, vol. 846–847, no. 3, pp. 1595–1599, 2013.

[7] A. Hossain, B. Hossain, and S. Uddin, "Researched on Security Challenges with Possible Solution Strategies in Cloud Computing," vol. 5, no. 2, pp. 31–39, 2016.

[8] S. H. Rathi, "Efficient And Secure Privacy Preserving Data Storage and Auditability In Cloud Assisted Mobile Health Data," no. February, 2015.

[9] M. Ahmed and M. Ashraf Hossain, "Cloud Computing and Security Issues in the Cloud," *Int. J. Netw. Secur. Its Appl.*, vol. 6, no. 1, pp. 25–36, 2014.

[10] R. Velumadhava Rao and K. Selvamani, "Data security challenges and its solutions in cloud computing," *Procedia Comput. Sci.*, vol. 48, no. C, pp. 204–209, 2015.

[11] M. D. H. Parekh, "An Analysis of Security Challenges in Cloud Computing," *IJACSA) Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 1, pp. 38–46, 2013.

[12] "What is an Access Control System (ACS)? - Definition from Techopedia." [Online]. Available:https://www.techopedia.com/definition/29707/access-control-system-acs. [Accessed: 17-Dec-2017].

[13] R. Padhy, M. Patra, and S. Satapathy, "Cloud Computing: Security Issues and Research Challenges," *... Inf. Technol. Secur. ...*, vol. 1, no. 2, pp. 136–146, 2011.

[14] "Top Data Privacy Issues To Scare You In 2016 - InformationWeek." [Online]. Available:http://www.informationweek.com/strategic-cio/security-and-risk-strategy/top-data-privacy-issues-to-scare-you-in-2016/a/d-id/1323752. [Accessed: 11-Aug-2017].

[15] "Data Privacy - Definition &amp; Types of Data." [Online]. Available: https://www.cleverism.com/lexicon/data-privacy/. [Accessed: 12-May-2017].

[16] R. V. Rao and K. Selvamani, "ScienceDirect Data Security Challenges and Its Solutions in Cloud Computing," *Procedia - Procedia Comput. Sci.*, vol. 48, pp. 204–209, 2015.

[17] B. S. Al-Attab and H. S. Fadewar, "Security Issues and Challenges in Cloud Computing," *Int. J. Emerg. Sci. Eng.*, vol. 2, no. 7, pp. 22–26, 2014.

[18] Taimoor Ahmad,Hala Aslam and Shahzeb Shahzad, "Data privacy and Data Accessibilty issues in Cloud Enviornment"