International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 3, Issue 1, January 2016, PP 13-15
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

My Data Security on Cloud Using Key Generator

Lalitha Siva Jyothi Ballada

lalithasivajyothi1973@gmail.com

Cloud Computing trend is rapidly increasing that has a technology connection with Grid Computing, Utility Computing, Distributed Computing. Cloud service providers such

Abstract: *As Amazon IBM, Google's Application, Sales force, Microsoft Azure etc., provide the users in developing applications in cloud environment and to access them from anywhere. Cloud data are stored and accessed in a remote server with the help of services provided by cloud service providers. Providing security is a major concern as the data is transmitted to the remote server over a channel (internet). Before implementing Cloud Computing in an organization, security challenges needs to be addressed first. In this paper, we highlight data related security challenges in cloud based environment and few solutions to overcome.*

Keywords: *Cloud computing; Data security; Data Access.*

1. Introduction

Cloud Computing is the next generation internet based computing system which provides easy and customizable services to the users for accessing or to work with various cloud applications. Cloud Computing provides a way to store and access cloud data from anywhere by connecting the cloud application using internet [1]. By choosing the cloud services the users are able to store their local data in the remote data server [2]. The data stored in remote data center can be accessed or managed through the cloud services provided by the cloud service providers. So the data stored in a remote data center for data processing should be done with utmost care.

Cloud Computing security is the major concern to be addressed nowadays. If security measures are not provided properly for data operations and transmissions then data is at high risk [3]. Since cloud computing provides a facility for a group of users to access the stored data there is a possibility of having high data risk. Strongest security measures are to be implemented by identifying security challenge and solutions to handle these challenges.

The main Advantage of cloud computing is to provide application delivery online without any infrastructure investment and maintenance free service [3]. Other benefit is pay per use of an application. While these were some of the advantages of Cloud Computing, the major threat posed by it is the possible leak and illegal use of data which is a sensitive issue. Though Cloud computing posses some serious threats but the advantages it provides are immense [4].

The main purpose of this paper is to present a possible safe and mechanism to access the databases from cloud. We propose a new software called data access security through key generator software. This software is basically windows console application and this software will make sure that if anybody accesses the database without proper authentication will ask end user to generate the key to access the database and also sends the key to database owner. If somebody other than the database owner is trying to access the database they cannot get this key and they will not perform any actions like data extraction and data updates etc.

2. Security

When multiple organizations share resources there is a risk of data misuse. So, to avoid risk it is necessary to secure data repositories and also the data that involves storage, transit or process. Protection of data is the most important challenges in cloud computing. To enhance the security in cloud computing, it is important to provide authentication, authorization and access control for data stored in cloud. The three main areas in data security are

Confidentiality:- Top vulnerabilities are to be checked to ensure that data is protected from any attacks. So security test has to be done to protect data from malicious user such as Cross-site Scripting, Access Control mechanisms etc..,.

Integrity:- To provide security to the client data, thin clients are used where only few resources are available. Users should not store their personal data such as passwords so that integrity can be assured.

Availability:- Availability is the most important issue in several organizations facing downtime as a major issue. It depends on the agreement between vendor and the client.

3. Locality

In cloud computing, the data is distributed over the number of regions and to find the location of data is difficult. When the data is moved to different geographic locations the laws governing on that data can also change. So there is an issue of compliance and data privacy laws in cloud computing. Customers should know their data location and it is to be intimated by the service provider.

4. Integrity

The system should maintain security such that data can be only modified by the authorized person. In cloud based environment, data integrity must be maintained correctly to avoid the data lost. In general every transactions in cloud computing should follow ACID Properties to preserver data integrity. Most of the web services face lot of problems with the transaction management frequently as it uses HTTP services. HTTP service does not support transaction or guarantee delivery. It can be handled by implementing transaction management in the API itself.

5. Access

Data access mainly refers to the data security policies. In an organization, the employees will be given access to the section of data based on their company security policies. The same data cannot be accessed by the other employee working in the same organization. Various encryption techniques and key management mechanisms are used to ensure that data are shared only with the valid users. The key is distributed only to the authorized parties using various key distribution mechanisms. To secure the data from the unauthorized users the data security policies must be strictly followed. Since access is given through the internet for all cloud users, it is necessary to provide privileged user access. User can use data encryption and protection mechanisms to avoid security risk.

6. Confidentiality

Data is stored on remote servers by the cloud users and content such as data, videos etc.., can be stored with the single or multi cloud providers. When data is stored in the remote server, data confidentiality is one of the important requirements. To maintain confidentiality data understanding and its classification, users should be aware of which data is stored in cloud and its accessibility.

7. Breaches

Data Breaches is another important security issue to be concentrated in cloud. Since large data from various users are stored in the cloud, there is a possibility of malicious user entering the cloud such that the entire cloud environment is prone to a high value attack. A breach can occur due to various accidental transmission issues or due to insider attack.

8. Segregation

One the major characteristics of cloud computing is multi-tenancy. Since multi-tenancy allows to store data by multiple users on cloud servers there is a possibility of data intrusion. By injecting a client code or by using any application, data can be intruded. So there is a necessity to store data separately from the remaining customer's data.

Vulnerabilities with data segregation can be detected or found out using the tests such as SQL injection aws, Data validation and insecure storage**.**

9. Storage

The data stored in virtual machines have many issues one such issue is reliability of data storage. Virtual machines needs to be stored in a physical infrastructure which may cause security risk.

10. Data Center Operation

In case of data transfer bottlenecks and disaster, organizations using cloud computing applications needs to protect the user's data without any loss. If data is not managed properly, then there is an issue of data storage and data access. In case of disaster, the cloud providers are responsible for the loss of data.

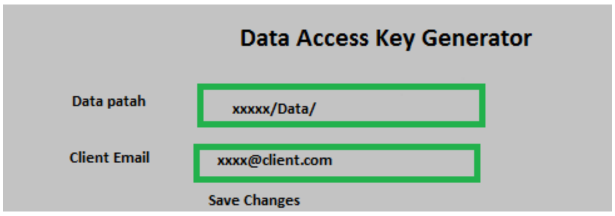
In case of data transfer bottlenecks and disaster, organizations using cloud computing applications needs to protect the user's data without any loss. If data is not managed properly, then there is an issue of data storage and data access. In case of disaster, the cloud providers are responsible for the loss of data.

11. How Key Generatot Software Will Help In Secure The Client Databases

When client signup the agreement with cloud services client can request to install the key generator software where client data is hosted and no service providers will say no to install this software because they need the more and more business.

Step1: After install the key generator software on the cloud machine. This application will start watching

Users who are accessing the client data and make log of the activities and sends email to database owner.



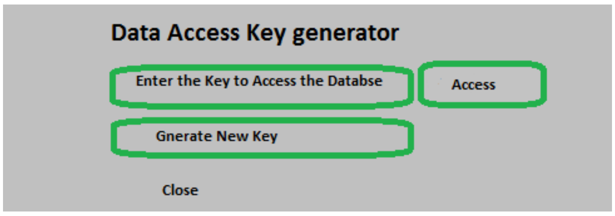
Data Access Key Generator

Data patah: xxxxx/Data/

Client Email: xxxx@client.com

There are so many ways to access the databases. The first and routine way is access the data from the application. This is more secured because after user authentication they can login into the site and they access the data. In this case also key generator software will keep track of the users and their activities.

The second way is access the data without any authorization. In this case key generator will ask the key to open the database else they can generate the key using this software to access the database.



Data Access Key generator

Enter the Key to Access the Databse

This software can be used for any cloud services to protect the client database.

References

[1] L.M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner. A break in the clouds: towards a cloud definition, in: ACM SIGCOMM Computer Communication Review, 2008.p.50-55.

[2] M.B. Mollah, K.R. Islam, and S.S. Islam. Next generation of computing through cloud computing technology, in: 2012 25th IEEE Canadian Conference on Electrical Computer Engineering (CCECE), May 2012.p.1-6.

[3] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou. Achieving secure, scalable and fine-grained data access control in cloud computing, in: IN-FOCOM, 2010 Proceedings IEEE, 2010.p.1-9.