International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Information Security in Multi-Cloud Environment

Digambar D. Patil[1], Megha Singh[2]

[1]Computer Science & Engineering Department, Central India Institute of Technology, Indore, India

[2]Assistant Professor, Computer Science & Engineering Department, Central India Institute of Technology, Indore, India

Abstract: ***Use of cloud computing is rapidly increases in daily routine where data generates in very large quantity. Actually in small industry cloud gives the better option for storage of large amount data without using extra hardware facility. In large industry it becomes very difficult to always update the hardware as per need for storing the data so they also choose the cloud facility for storage. But problem is that whether the data is secure on cloud storage server or not? In this paper we are concerning about the single cloud security and multi-cloud security and tells the solutions on it. This work will promote the use of multi-cloud environment due to the ability of reducing security risk which affects to the cloud computing user and his/her data.***

Keywords: Cloud computing, Data Integrity, multi-cloud, single cloud, security

1. Introduction

Use of cloud computing is becomes very popular in an industry. Every industry has its own data and database servers. But storing that data on their server is becomes very difficult if data size becomes more. In small industry each time it becomes very costlier to upgrading their hardware capability for frequently storing new data and maintaining that storage becomes difficult. So cloud technology is use and it reduces cost of storage, maintenance. When cloud provider provides cloud facility that time they should mention the privacy and security issues. Use of "single cloud" is becomes less popular due to some problems such as service availability failure and there may be chance of presence of or insertion of malicious thread i.e Insider harmful thread in cloud. Now a day, use of "multi-cloud" or "intercloud" or "cloud-of-clouds" becomes very popular just because of potential problems such as service availability failure in single cloud [1].

This paper is focuses on issues related to the data security in multi-cloud environment. As data stored at third party provider, user wants to their data should be secure. so many people have investigated data or ways for avoiding such a problems for storing the data. In that they found some problems namely authentication of data, integrity of data and service availability by cloud. Proof of data stored on cloud is sometime called as Proof of Retrievability (POR).Such proofs are important in Distributed System, Peer to Peer System, Network file system, database system [2].

Such system frequently checks the data on cloud storage from the modification or misrepresentation of data without intimating the owner of that data. And this information gives idea to the owner about the efficient, frequent, secure and quick verification of data stored on cloud. Just one thing is there owner should take into his/her consideration that server might not be infected with any malicious activity. Otherwise it will give the unreliable and inadvertently corrupted data. So we are developing data integrity scheme which are required for infected servers and unreliable cloud storage.

While accessing the large data which is stored at untrusted cloud storage, it requires the more resources on our local machine with that we may require large bandwidth for accessing that data. For accessing such file becomes very expensive in input/output cost on cloud server. With this it will also consume large bandwidth for transmission of file across the network to the client from the server. The problem is that owner of data may be using the small devices like cell phone or PDA (Personal Device Assist) which having limited CPU power capacity, less battery backup, less bandwidth capacity or communication hence, the need of data integrity proof is required for the above limitation. So scenario should be able to produce a proof without the need to access the whole file on server or retrieve whole file on client. Also it should minimize the local computation and bandwidth consumption at client side. [1],[2]

2. Framework

In cloud computing, there are two types of framework models which are mostly used and they are namely.
1. Delivery Model
2. Deployment Model

2.1 Delivery Model

It consist of three types of models for delivering the cloud service

2.1.1 Software as a Service (SaaS)

It is referred as software available on demand. It is also knowledge as an Application Service Provide (ASP).It provides the efficient access services of cloud to the users. For example Google groups, Gmail. This service mostly used for business applications like HR Management, Enterprise Resource Planning etc.

2.1.2 Platform as a Service (PaaS)

It provides a freedom to the user for application design, development, testing and deployment. With this it also provides an application services such as a database collection i.e. integration of database, security of data. For example Google apps Engine which allows the users to customize their application and give the service to other people.

2.1.3 Infrastructure as a Service (IaaS)

It delivers the virtualization environment as a service. Instead of spending money on purchasing servers, data center, network equipment, software license client can purchase resources as outsourced service. Means client use the third party infrastructure service to for supporting the operations. [3],[4]

2.2 Deployment Model

There are four types of deployment models of clouds and they are-

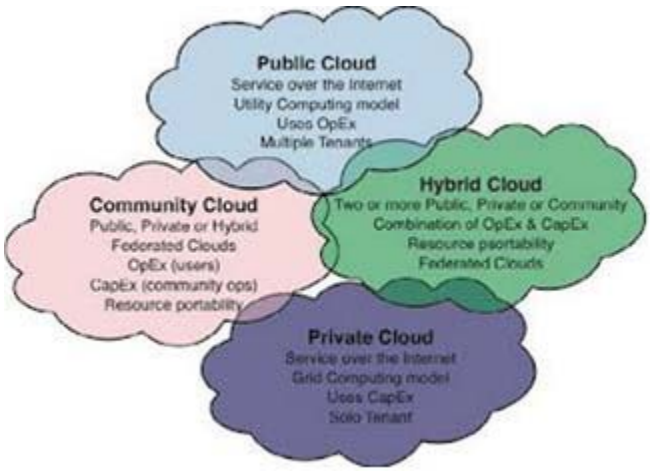

Figure 1: Deployment Model of Clouds

2.2.1 Public Cloud

It is known as external cloud. This service is made available by the service provider through the internet. User may use this service or cloud free or will pay as per his/her usage. The public cloud can be a individual service or collection of services.

2.2.2 Private Cloud

It is also known as internal cloud or on-premise cloud. It provides the limited access to its user and resources which are belonging to that particular organization. That is it manages the data within the organization without the taking care of network bandwidth. So that's why security, privacy will be maintained.

2.2.3 Hybrid Cloud

It is the combination of public cloud and private cloud. It is also known as multiple cloud system. It gives the facility to the enterprise for managing the workload in private cloud but suppose workload increases and it asking for the public cloud for computing the resources then it gives the authority for public cloud.[4],[5],[6]

2.2.4 Community Cloud

It is the cloud which is managed by group of organizations for achieving the common objective. In this type of cloud mostly common resources are shared within the organizations.

3. Data Security Issues in Cloud

There are three types of major issues in data cloud security namely Availability, Confidentiality, Integrity known as AIC triad. [3]

- **Availability:** It is the proof that data will be available to user worldwide irrespective of location. It is handled by network security, authentication and fault tolerance.
- **Integrity:** It is the proof that data receive is same as the data sent and it is not modified in between the transfer. Integrity is a copyright of data. It is handled by Firewalls and intrusion detection
- **Confidentiality:** It is the avoidance of unauthorized access of user. It is handled by authentication services, DES, Security protocols like Kerberos.

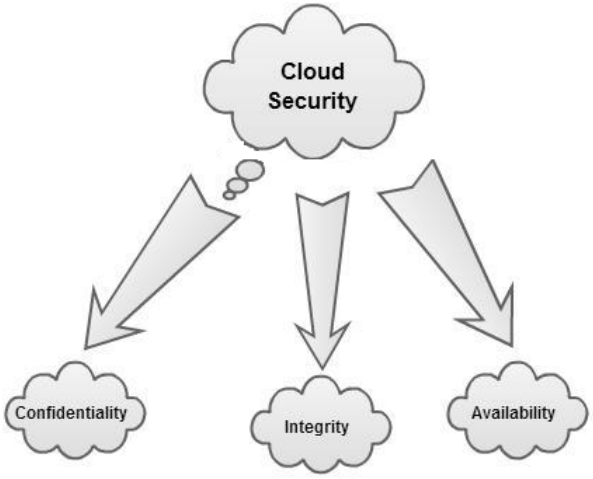

Figure 2: The AIC triad

4. Problem Formulation

In cloud computing technology, many policy issues are there which include issues of security, privacy, reliability, integrity, service availability etc. But out of that the most serious issue is security and how cloud provider solves that issue? Generally cloud has many types of users such as general user, enterprise user, cloud administrator etc. For general user security point of view is different, or enterprise user security point of view is different and for cloud administrator it is different. So for all of these users security issue is most important.

5. Proposed Work

In this paper we are concern about data security in cloud. So we are using the AES algorithm for securing the data and MD5 algorithm for creating the encryption key.

- **AES (Advanced Encryption Standard) algorithm:**

It is based on substitution permutation concept. It is faster algorithm than DES (Data Encryption Standard) algorithm and triple DES .In AES key size is of 128 bits, 192 bits, 256 bits. Key size of AES algorithm specifies the number of transformation rounds conducted on plain text for getting AES cipher text.

The number of repetition cycle perform as follows-

- 10 cycles for 128 bit key.

- 12 cycles for 192 bit key.
- 14 cycles for 256 bit key.

Description of Algorithm:
Algorithm work in 4 steps:

1) Key Expansion

Round keys are derived from cipher keys and AES requires the 128 bit round key for each round.

2) Initial Round

1) Add Round key- Using bitwise operation each block of data is attached with one block of round key.

3) Rounds

a) Sub bytes - Each byte is replace with another byte.
b) Shift Rows- Cyclically last three rows are shifted.
c) Mix Columns- Combining four byte of each column.
d) Add Round Key

4) Final Rounds

a) Sub bytes
b) Shift Rows
c) **Add Round Key**

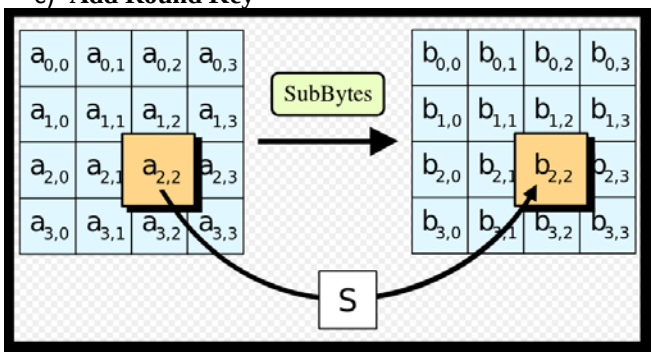

Figure 3: Sub Bytes

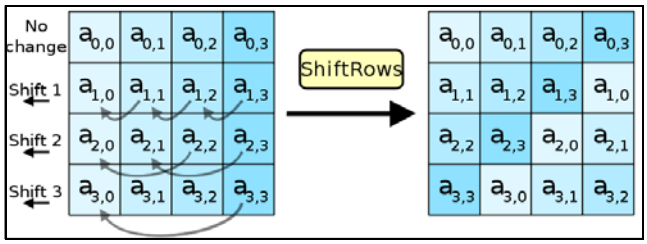

Figure 4: Shift Rows

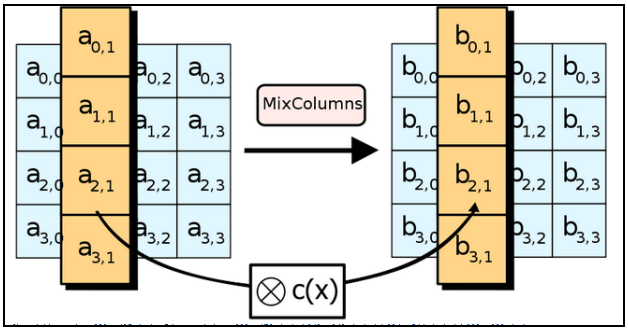

Figure 5: Mix Columns

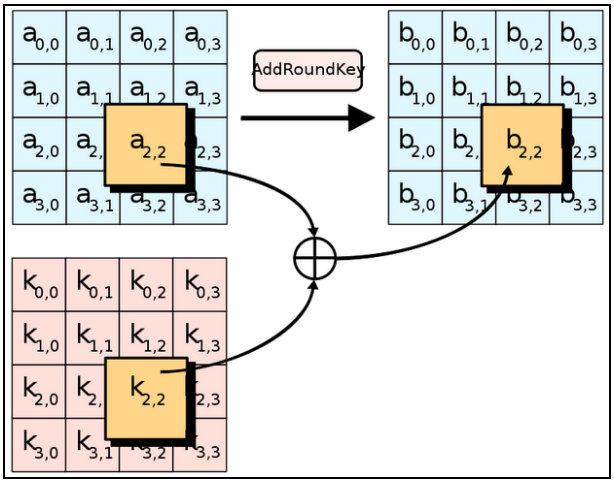

Figure 6: Add Round Key

MD5- (Message-Digest algorithm 5), a mostly known as cryptographic hash function with a 128-bit hash value, it processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks . the message is padded so that its length is divisible by 512.

This algorithm takes an input a message of undefined length but produces the 128 bit, which is generally less than the length of the input message. The MD5 algorithm is designed for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA ,DES, Triple DES, AES. This algorithm is mostly fast on 32 bit machines.

6. Conclusion

So now a day most of the organizations are using cloud servers or cloud databases for storing their databases. In this paper we are just trying to minimize the hackers attack from losing the private data from the server. There are many algorithms in the world out of that we are using AES and MD5 algorithms. AES having so many advantages so AES gives the better performance with MD5 algorithm.

References

[1] Mohammed A. AlZain, Eric Pardede, Ben Soh , James A. Thom “Cloud Computing Security: From Single to Multi-Clouds”,cloud computing , HICSS’12,Proc.45th Hawaii International Conference on System Sciences ,2012,pp 5490-5499
[2] Sravan Kumar R, Ashutosh Saxena, “Data Integrity Proof in Cloud Storage”, COMSNETS’11, Proc.Bangalore 3rd International Conference on Communications Systems and Networks,2011
[3] Tirthani, Neha, and R. Ganesan. "Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography.", International Association for Cryptologic Research, 20140121/049
[4] Mohit Marwaha, Rajeev Bedi ,”Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing”, IJCSI,Vol.10,Jan.2013

[5] Mandeep Kaur,Manish Mahajan, "Using encryption Algorithms to enhance the Data Security in Cloud Computing", IJCCTS,Vol.01,Jan.2013
[6] K.S.Suresh, K.V.Prasad, "Security issues and Security algorithms in Cloud Computing",IJARCSSE,Vol.02,Oct.2012.
[7] Nesrine Kaaniche, Maryline Laurent, "A Secure Client side Dedplication Scheme in Cloud Storage Environment", New Technologies, Mobility and Security (NTMS), 2014 6th International Conference at Dubai ,2014,pp 1-7