ISSN: 2321-7782 (Online)
Volume 3, Issue 3, March 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Data Security Provision in Multi-Cloud Architecture

Digambar D. Patil[1]
Computer Science & Engineering Department
Central India Institute of Technology, Indore

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

Abstract: ***Utilization of distributed computing is quickly increments in day by day routine where information creates in extensive amount. Really in little industry cloud gives the better alternative for capacity of huge sum information without utilizing additional equipment office. In vast industry it gets to be extremely hard to dependably upgrade the equipment according to requirement for putting away the information so they additionally pick the cloud office for capacity. Anyhow issue is that whether the information is secure on distributed storage server or not?***

In this paper we are worried about the single cloud security and multi-cloud security and tells the arrangements on it. This work will advance the utilization of multi-cloud environment because of the capacity of decreasing security hazard which influences to the distributed computing client and his/her information.

Keywords- Cloud computing, Data Integration, multiple clouds, single cloud, Information security.

I. INTRODUCTION

Utilization of distributed computing is gets to be exceptionally prevalent in an industry. Each industry has its own information and database servers. In any case putting away that information on their server is gets to be exceptionally troublesome if information size gets to be more. In little industry every time it gets to be extremely costlier to redesigning their equipment ability for often putting away new information and keeping up that stockpiling gets to be troublesome. So cloud innovation is utilization and it lessens expense of capacity, upkeep. At the point when cloud supplier gives cloud office that time they ought to specify the security and security issues. Utilization of "single cloud" is gets to be less prevalent because of a few issues, for example, administration accessibility disappointment and there may be risk of vicinity of or insertion of noxious string i.e Insider unsafe string in cloud. Presently a day, utilization of "multi-cloud" or "intercloud" or "billow of-mists" gets to be exceptionally prevalent simply due to potential issues, for example, administration accessibility disappointment in single cloud [1].

This paper is spotlights on issues identified with the information security in multi-cloud environment. As information put away at outsider supplier, client needs to their information ought to be secure. So numerous individuals have explored information or courses for evading such an issues for putting away the information. In that they discovered a few issues in particular verification of information, respectability of information and administration accessibility by cloud. Confirmation of information put away on cloud is at some point called as Proof of Retrievability (POR).Such evidences are vital in Distributed System, Peer to Peer System, Network document framework, database framework [2].

Such framework regularly checks the information on distributed storage from the adjustment or deception of information without implying the holder of that information. Furthermore this data offers thought to the manager about the proficient, successive, secure and speedy check of information put away on cloud. Only one thing is there manager ought to take into his/her thought that server may not be contaminated with any pernicious movement. Else it will give the inconsistent and coincidentally debased information. So we are creating information respectability plan which are needed for contaminated servers and questionable distributed storage.

While getting to the expansive information which is put away at untrusted distributed storage, it requires the more assets on our neighborhood machine with that we may oblige extensive data transmission for getting to that information. For getting to such record gets to be extremely extravagant in information/yield cost on cloud server. With this it will likewise devour expansive data transfer capacity for transmission of document over the system to the customer from the server. The issue is that manager of information may be utilizing the little gadgets like mobile phone or PDA (Personal Device Assist) which having restricted CPU power limit, less battery reinforcement, less transmission capacity limit or correspondence subsequently, the need of information uprightness confirmation is needed for the above confinement. So situation ought to have the capacity to create a proof without the need to get to the entire document on server or recover entire record on customer. Additionally it ought to minimize the neighborhood reckoning and transmission capacity utilization at customer side. [1],[2]

II. FRAME WORK

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 comprise of three sorts of models for conveying the cloud administration

2.1.1 Software as a Service (SaaS)

It is alluded as programming accessible on interest. It is likewise learning as an Application Service Provide (ASP).It gives the proficient access administrations of cloud to the clients. Case in point Google groups, Gmail. This administration generally utilized for business applications like HR Management, Enterprise Resource Planning and so on.

2.1.2 Platform as a Service (PaaS)

It gives an opportunity to the client for application outline, advancement, testing and organization. With this it additionally gives an application administrations, for example, a database accumulation i.e. incorporation of database, security of information. Case in point Google applications Engine which permits the clients to modify their application and give the administration to other individuals.

2.1.3 Infrastructure as a Service (IaaS)

It conveys the virtualization environment as an administration. As opposed to burning through cash on obtaining servers, server farm, system gear, programming permit customer can buy assets as outsourced administration. Implies customer utilize the outsider foundation administration to for supporting the operations. [3],[4]

2.2 Deployment Model-

Followings are four types of deployment models of clouds-

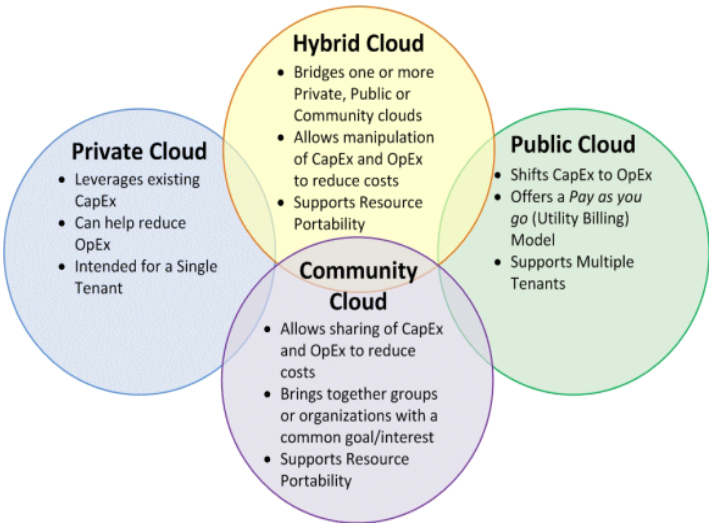

Fig: 1 Deployment Model of Clouds

2.2.1 Public Cloud:

It is known as outside cloud. This administration is made accessible by the administration supplier through the web. Client may utilize this administration or cloud free or will pay according to his/her use. People in general cloud can be an individual administration or gathering of administrations.

2.2.2 Private Cloud:

It is otherwise called inner cloud or on-reason cloud. It gives the constrained access to its client and assets which are fitting in with that specific association. That is it oversees the information inside the association without the dealing with system data transfer capacity. So that is the reason security, protection will be kept up.

2.2.3 Hybrid Cloud:

It is the mix of open cloud and private cloud. It is otherwise called various cloud system. It gives the office to the venture for dealing with the workload in private cloud however assume workload increments and it requesting the open cloud for processing the assets then it gives the power for open cloud.[4],[5],[6].

2.2.4 Community Cloud:

It is the cloud which is overseen by gathering of associations for accomplishing the basic target. In this sort of cloud basically normal assets are imparted inside the associations..

III. INFORMATION SECURITY ISSUES IN CLOUD

There are three sorts of real issues in information cloud security AIC triad [3].

Availability: It is the evidence that information will be accessible to client overall independent of area. It is taken care of by system security, verification and adaptation to non-critical failure.

Integrity: It is the verification that information get is same as the information sent and it is not altered in the middle of the exchange. Respectability is a copyright of information. It is taken care of by Firewalls and interruption identification.

Confidentiality: It is the shirking of unapproved access of client. It is taken care of by verification administrations, DES, Security conventions like Kerberos.

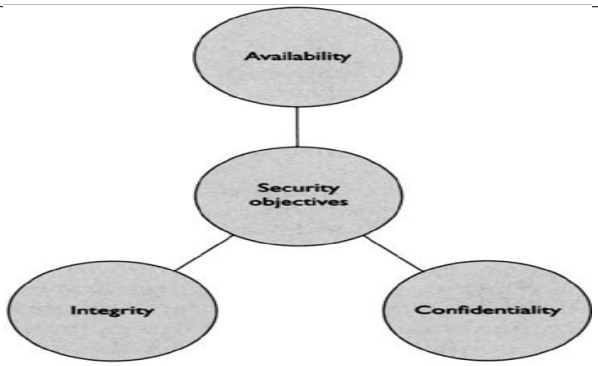

Fig: 2 The AIC traid

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.

IV. METHODOLOGY

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.

AES pseudocode:

Constants:

int Nb = 4;

int Nr = 10, 12, or 14;

Inputs:

array in of 4*Nb bytes

array out of 4*Nb bytes

array w of 4*Nb*(Nr+1) bytes

Internal work array:

state, 2-dim array of 4*Nb bytes, 4 rows and Nb cols

Algorithm:


```
void Cipher(byte[] in, byte[] out, byte[] w)
{
byte[][] state = new byte[4][Nb];
state = in;
AddRoundKey(state, w, 0, Nb - 1);
for (int round = 1; round < Nr; round++)
{
SubBytes(state);  ShiftRows(state);  MixColumns(state);  AddRoundKey(state, w, round*Nb, (round+1)*Nb - 1);
}
SubBytes(state);
ShiftRows(state); // see Section 5 below
AddRoundKey(state, w, Nr*Nb, (Nr+1)*Nb - 1);
out = state;
}
```

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***

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.

   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**

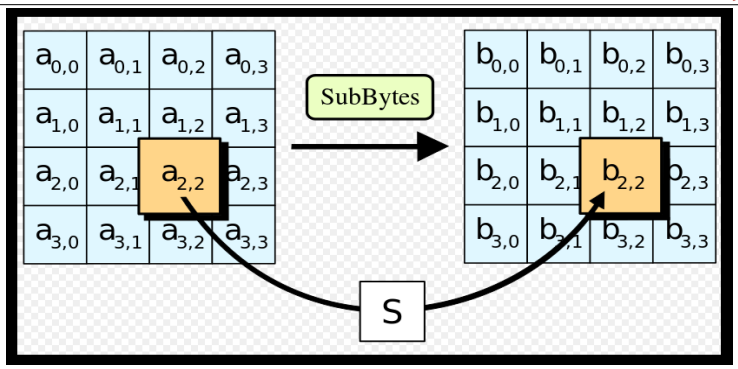

Fig: 3 Sub Bytes

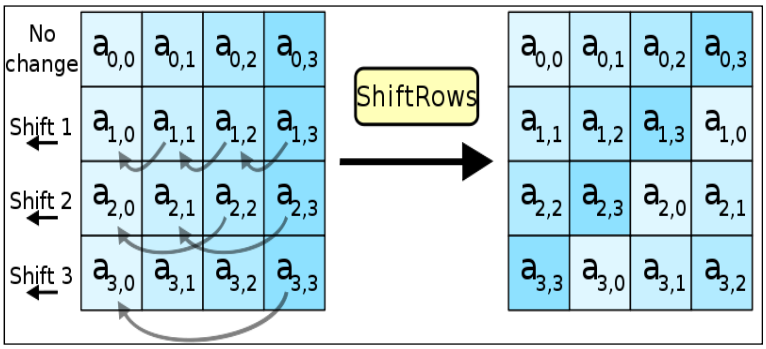

Fig: 4 Shift Rows

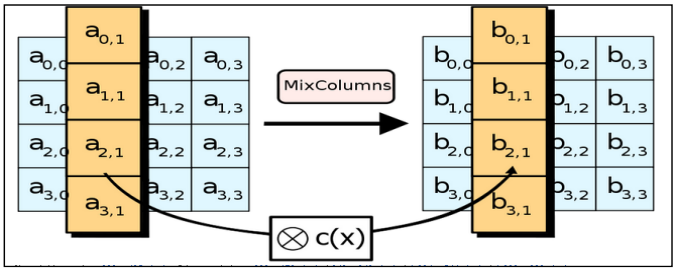

Fig: 5 Mix Columns

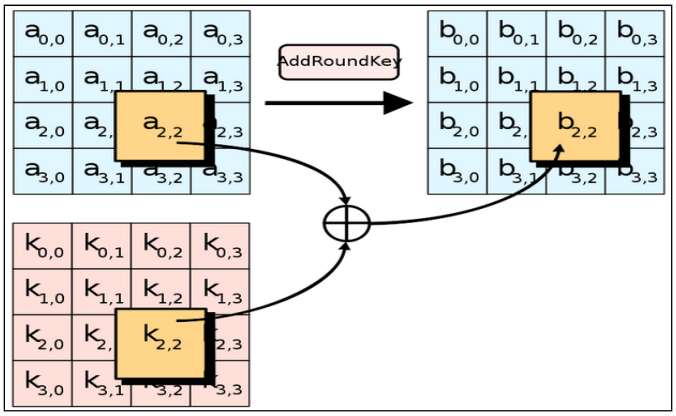

Fig: 6 Add Round Key

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.

MD5 Algorithm Description:

MD5 processes a great variable-length message straight into a fixed-length output involving 128 bits. Ones input message will be broken up directly into chunks associated with 512-bit blocks; your own message will be padded so the idea is their length is usually divisible through 512. Your current ingredient filling works in the same way follows: first a great solitary bit, 1, can be appended towards the end of any message. It is followed by just as numerous zeros just like are forced to bring ones length of a message up to help 64 bits fewer than an multiple of 512. your current remaining bits usually are stuffed up using a 64-bit integer representing the length of a original message.

The main MD5 algorithm functions in a good 128-bit state, divided directly into four 32-bit words, denoted A, B, C in addition to D. They are initialized to certain fixed constants. Your own main algorithm and then works from each 512-bit message block within turn, each block modifying your state. ones processing of your message block incorporates four similar stages, termed rounds; each round can be written involving 16 similar operations Based on the non-linear perform F, modular addition, as well as left rotation.

V. Results And Discussion

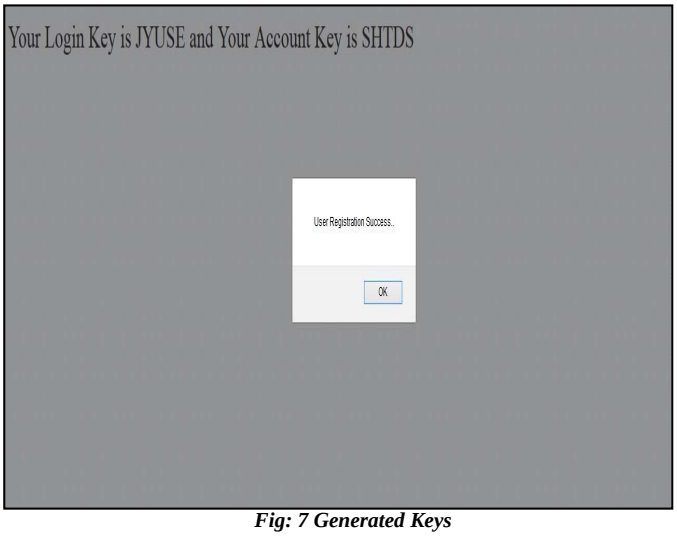

Fig: 7 Generated Keys

On successful registration two keys are generated Login key and Secret key. Using these keys we can cross the threshold of the system. Then home page will open. Where we can upload, download and delete the files. Also we can share our own file on the cloud and give access to particular user. Fig 10 demonstrates file uploading on cloud.

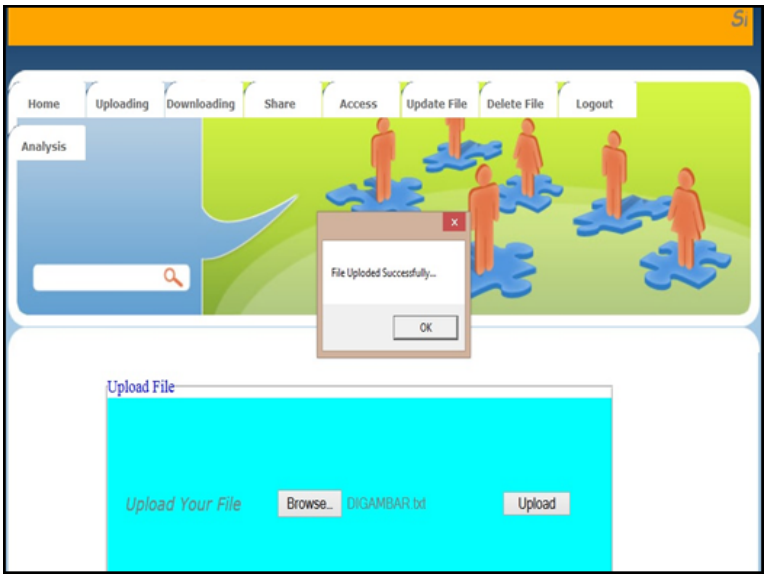

Fig: 8 File Uploaded on cloud

DATABASE RESULTS

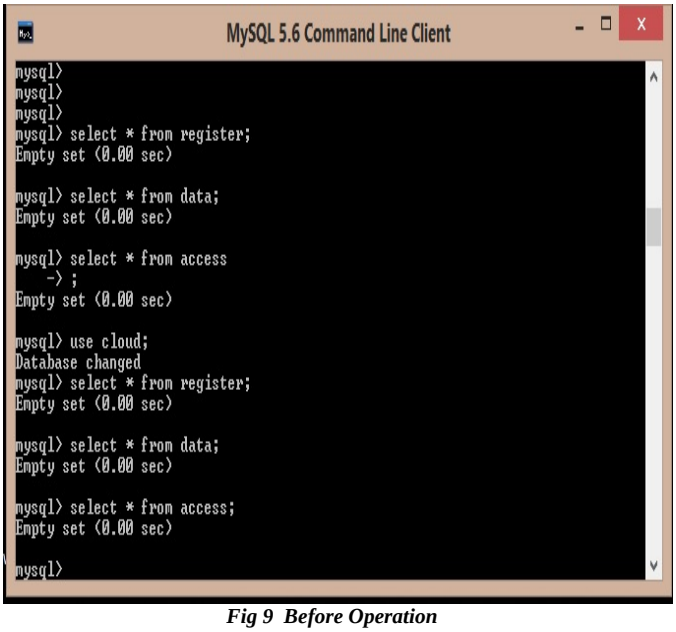

Fig 9 Before Operation

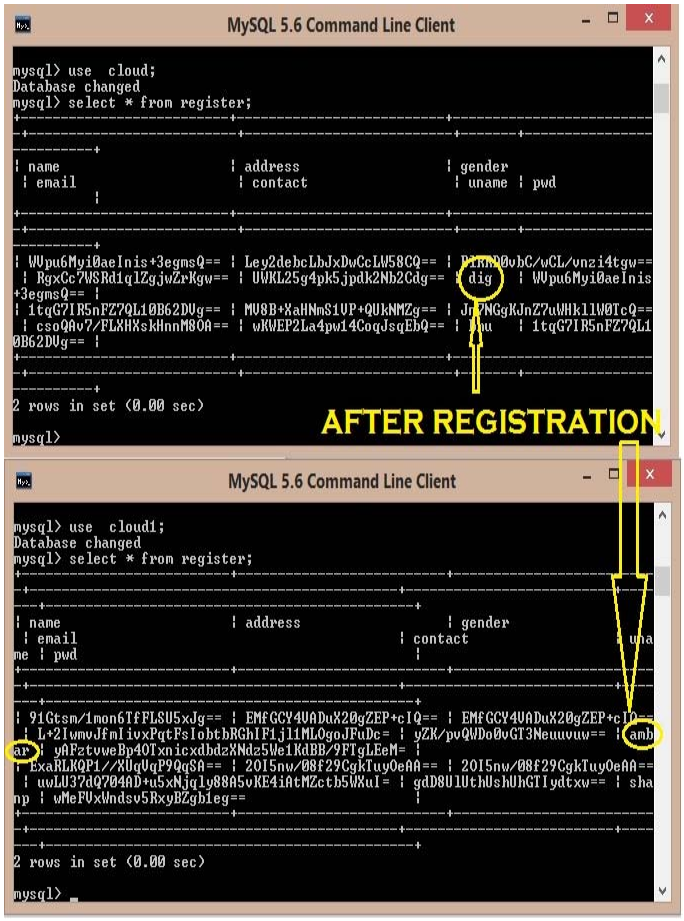

Fig 10 After Operation

In database results we can see that before operation database is empty but after registration the username is divided into chunks and stored on two different clouds. Above Fig 15 demonstrates this by marking notations.

VI. CONCLUSION

So now a day's a large portion of the associations are utilizing cloud servers or cloud databases for putting away their databases. In this paper we are simply attempting to minimize the programmer's assault from losing the private information from the server. There are numerous calculations on the planet out of that we are utilizing AES and MD5 calculations. AES having such a large number of points of interest so AES gives the better execution with MD5 calculation.

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 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

