Data Security in Multi Cloud Computing:A Brief Review

Mrs. Renu Nagendra Shinde, Prof. Mrs. Varsha Khandekar

***Abstract*-cloud computing is an innovative framework for developing, deploying new things. The primary use of cloud is for storage. Traditionally users used to save their data in a hard disk. But they need to carry the hard disk with them all around. The capacity of hard disk failed to match against the tremendous growth of their data. This is the main reason why users decided to use cloud as their primary data storage. In the proposed research work, a secure framework for the cloud providers is demonstrated. Coping with "single cloud" provider became less popular as it introduces the malicious hackers inside the cloud and due to service unavailability many a times. Multi cloud solves this dilemma. Rather than keeping the data with a single cloud provider, multi cloud system encourages users to save their data on many clouds. This avoids having reliance on a single cloud. In the proposed system, secure framework using cloud is build, where we does not rely on a single rather use multiple cloud. We use AES algorithm to encrypt whole data, replicate the data and create a signature using SHA1 algorithm. This provides much better security than the single cloud computing.**

***Index terms*-AES, Cloud Computing, Multi Cloud, Single Cloud, Security, SHA1**

I. INTRODUCTION

Cloud computing is one of the most notable innovation. It relies on shared pools of computing resources. We could use internet as a metaphor to cloud. So in layman's terms cloud computing is internet based computing. Different services are delivered to us using an internet.

Mrs. Renu shinde, department of information technology, Savitribai Phule Pune University, pune, India
Prof. Mrs. Varsha Khandekar, department of information technology, Savitribai Phule Pune University, pune, India

The definition of cloud computing provided by National Institute of Standards and Technology (NIST) [9] says that: "Cloud computing is a model for enabling 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."

Cloud computing comes in different flavors [2]. In the SaaS model developed software is delivered to user. User does not need to configure or maintain the software. The next model is Paas where a platform to form a software is delivered to user. Here for e.g. visual basic is leased to user. This avoids buying of additional platform. The other model is Iaas which forms the basis of above two models. It gives storage, processing, networks needed for an organization

Most fascinating service provided by cloud is storage. Organizations needs to save their tremendous amount of data in cloud. There are many options available in the market that could help an organization to save their data. It is duty of a cloud storage provider to keep this data safe, makes available and keep it accessible all the time.

It is up to an organization which cloud they want to use. Usually they use a services from a single cloud to store and maintain their data. This is called as single cloud computing.

ISSN: 2278 – 1323

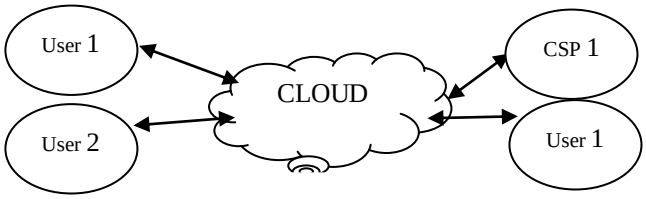

Figure 1: Single Cloud System

The diagram above explains the working of single cloud system. Let us assume that three users store their data on three different service providers. Each customer can retrieve his own data from the CSP who it has a contract with. If a failure occurs at CSP1, due to some internal problems the user 1's data which was stored on CSP1's server will be lost and cannot be retrieved. This is the limitation of a single cloud computing. According to Mohammed A. AlZain, Eric Pardede, Ben Soh, James A. Thom [7] the limitations of a single cloud computing are data integrity, data intrusion and service availability failure. If an organization decided to use a single cloud to store their data in future they might deal with the above listed drawbacks. It is very costly to move from one cloud to the other if earlier cloud is unable to satisfy the needs of an organization.

To avoid these pitfalls associated with a single cloud computing, there is a need to emigrate towards a multi cloud system where we does not keep reliance on a single cloud rather use combination of two or many cloud to distribute and store the data. Figure 2 gives us a brief idea about multi cloud system. When user decides to save his data in it is distributed across two or many clouds. As the data is distributed across the cloud, vendor lock in problem that is associated with a single cloud also minimizes. We does not store entire data on a single cloud. So if hacker hacks a cloud, then he won't have the knowledge of entire data. In future suppose user does not like a service of particular cloud then he could migrate to another cloud. This saves much time and money as compared to single cloud computing.

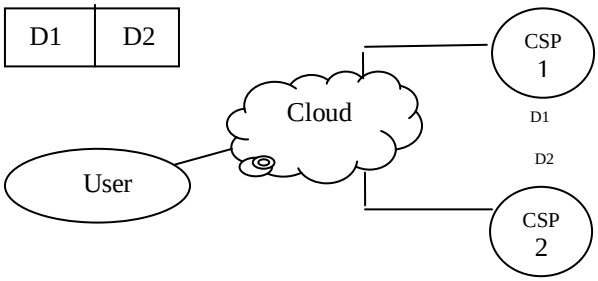

Figure 2: Multi Cloud System

II. RELATED WORK

Bessani, M. Correia, B. Quaresma, F. André and P. Sousa proposed the DepSky dependable and secure storage in a cloud-of-clouds model [1]. The DepSky system addresses the availability and the confidentiality of data in their storage system by using multi-cloud providers. K.D. Bowers, A. Juels and A. Oprea proposed HAIL: A high-availability and integrity layer for cloud storage. HAIL is a distributed cryptographic system that allows a set of servers to prove to a client that a stored file is intact and retrievable. M. A. AlZain, B. Soh and E. Pardede, proposed MCDB: Multi cloud database model. MCDB ensures security and privacy in cloud computing environment and is based on multi-clouds service providers and the secret sharing algorithm [5]. MCDB provides "cloud database" which permit customers with different types of database queries such as aggregation and exact match and range query with the ability to store any different types of data such as video, pictures or documents. H. Abu-Libdeh, L. Princehouse and H. Weather spoon proposed RACS [3]- Redundant Array of Cloud Storage RACS is a cloud storage proxy that transparently stripes data across multiple cloud storage providers. k.rajasekar, c.kamalanathan, delivered RAIN cloud system which has characteristics like rapid elasticity, broad network access, and rapid connectivity within clouds.

.

ISSN: 2278 – 1323

III. PROPOSED SYSTEM

To overcome the failures of single cloud provider system, we are moving towards a multi cloud system, where we do not store client's data on a single cloud but we distribute the data across multiple clouds. Figure 3 gives us a brief idea about our system. This system will guarantee the security on user data as well as the user will get data in a timely manner. The main components of our proposed system are:

- Client (End User)
- Application server (Where application is deploy on IIS server)
- Web server (Central Server implementation of all algorithms)
- Database servers (Cloud Servers)
- Client :

1. Client

Client is the end user in our system; first client will fill all the details on the GUI. These are the users who will use the system. Client will be provided with the options like file uploading, file downloading and file deleting. etc.

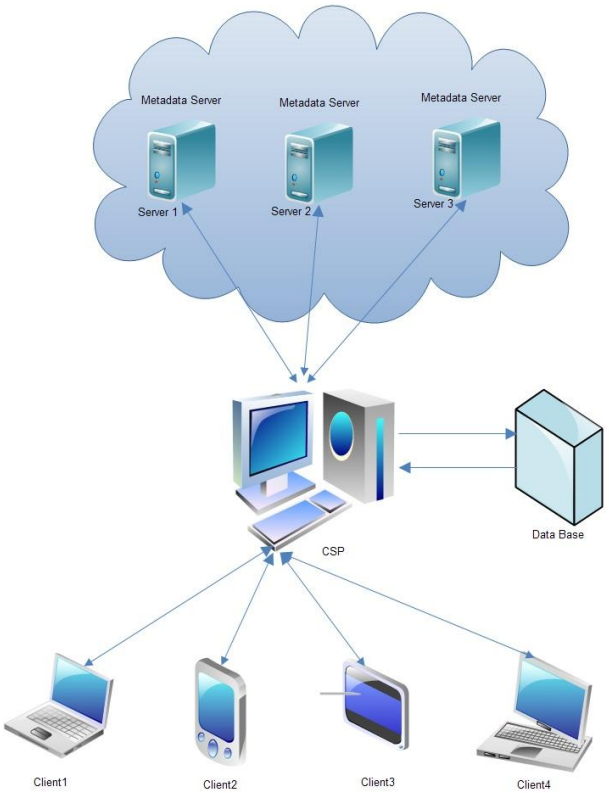

Figure 3: System Architecture

2. Application Server:-

This is a server which is hosting our application with which user interacts and this server then intern interacts with web server.

3. Web server:

This server will host our all web services and will generate the result. It will send the result to application server. This server will interact with database server.

4. Database servers

These are the real database server which will store all the data related to the application. These servers will work as different cloud providers.

Client sends HTTP request to domain server. Domain accept request and send SOAP object to Service provider (Azure ,Amazon, Google etc).Web service which contains Secrete sharing algorithm divide key in no of shadows which are stored on different server X,Y,Z are cloud servers which contains applications. When client request any application after login first secret key is checked after authentication of user application is accessed via HTTP response.

- Upload the Files

When user selects to upload a file, whole file gets encrypted using AES algorithm. Depending upon the number of cloud servers the file gets divided into equal size of parts. Signature of each block is created using SHA1 algorithm. Web services will store these parts on cloud databases. In the proposed framework, we will use backup servers too. So when the block of a whole file gets stored on cloud database same copy will be stored at the backup server too. This helps in data recovery.

- Download the Files

In this phase, we use a special approach to access a file, we manage in application access control facility to all users. When any user uploads the file he can give the access to all users which is registered on the system, which is the link file. When user give the request to server

ISSN: 2278 – 1323

for download the file, the central server collect all data blocks from cloud servers, and decrypt the whole data using AES algorithm, if all servers gives the complete response then it will collect in single file and give the response to end user.

- Delete the Files

Here in this module we make session key authentication for every user. When user deletes the file it will first check the session value with database values and secret keys. If both are same then file will be deleted otherwise it will not grant to users.

IV. MATHEMATICAL MODEL

1] Identify the Users
U= {u1, u2, u3….}
Where 'U' is main set of Users like u1, u2, u3…

2] Identify the Set of file data Uploaded by user
F= {f1, f2, f3….}
Where 'F' is set of uploaded files like f1, f2, f3…

3] Identify the Set of Files Downloaded by user
D= {d1, d2, d3….}
Where 'D' is set of downloaded files like d1, d2, d3…

4] Identify the Set of Hash
H= {h1, h2, h3, h4}
Where 'S' is set of hashh1, h2, h3, h4.

5] Identify Servers (Servers)
S = {s1, s2, s3, s4….}
Where S is main set of servers

6] Identify the set of file data blocks
B= {b1, b2, b3, b4}
Where 'B' is set of file datablocks b1, b2, b3, b4.

7] Identify set of request for files.
R= {r1, r2, r3….}
Where 'R' is set of request for verification r1, r2, r3…

8] Identify Set of modified block.
M= {m1, m2, m3, m4}
Where 'M' is set of modified blocks m1, m2, m3, m4.

9] Identify Set of Proof.
P= {p1, p2, p3….}
Where 'P' is set of proof required for proof verificationp1, p2, p3…

10] Identify Set of Keys
K= {k1, K2, k3….}
Where 'K' is set of secrete key required for encryption and decryption K1, K2, k3…

V. CONCLUSION

This research paper focuses on implementing security in multi cloud. We cannot trust a single cloud provider because we store all the valuable data into it. To overcome this we support multi cloud system, where user's data is more securely saved. We have used AES and SHA1 which forms a very secure system. In addition we have also used backup servers. So even if data from main server gets lost, we could get it from the backup server. The future scope of this project is to make the hacker's job tougher by using combination of other encryption algorithm.

Acknowledgment

I would like to thank my guide prof. Varsha Khandekar. Her guidance made this work to be complete. I would also like to thank my family who gave me all the support that I needed.

REFERENCES

[1] Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, June 2011,*"DepSky: dependable and secure storage in a cloud-of-clouds"*, EuroSys'11:Proc. 6thConf. On Computer systems, pp. 31-46

[2] C. Cachin, R. Haas and M. Vukolic, June 2010, *"Dependable storage in the Intercloud"*, Research Report RZ, 378..

[3] H. Abu-Libdeh, L. Princehouse and H. Weather spoon, 2010,*"RACS: a case for cloud storage diversity"*, SoCC'10:Proc. 1st ACM symposium on Cloud computing, pp. 229-240.

[4] K.D. Bowers, A. Juels and A. Oprea, 2009, *"HAIL: A high-availability and integrity layer for cloud storage"*, CCS'09: Proc. 16th ACM Conf. on Computer and communications security, pp. 187-198

[5] K.rajasekar, c.kamalanathan, June 2012," Towards of secured cost-effective multi-cloud storage in cloud computing" Undergraduate Academic Research Journal (UARJ), ISSN : 2278 – 1129, Volume-1, Issue-2. Autonomic and Secure Computing (DASC), IEEE, Sydney, pp. 784-791.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[6] M. A. AlZain, B. Soh and E. Pardede, 2011 April"MCDB: Using Multi-clouds to Ensure Security in Cloud Computing", Proceedings of the 2011 Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC), IEEE, Sydney, Australia

ISSN: 2278 – 1323

[7] Mohammed A. AlZain,Eric Pardede,Ben Soh, James A. Thom, may 2013"A Survey on Data Security Issues in Cloud Computing: From Single to Multi-Clouds", journal of software,vol.8,no.5

[8] Subashini S, Kavitha V, Jan 2011 "A survey on Security issues in service delivery models of Cloud Computing", J Netw Compute Appl 34(1):1–11

[9] National Institute of Standards and Technology - Computer Security Resource Center - www.csrc.nist.gov

Mrs Renu Shinde,currently pursuing her master in engeeniring in the department of information technology from Smt. Kashibai Navale College of Engineering, Wadgoan Bk., Pune-41, Maharashtra- India.

Prof. Mrs Varsha Khandekar working in Smt. Kashibai Navale College of Engineering, Wadgoan Bk. She has over 10 years of working experience.

ISSN: 2278 – 1323