IMPLEMENTING DATA SECURITY IN MULTI CLOUD

Ms. Renu Nagendra Shinde
Information Technology
SKNCOE
Pune 41,India
renunikhilp@gmail.com

Prof. Mrs. Varsha Khandekar
Information Technology
SKNCOE
Pune 41, India
Varsha.khandekar@gmail.com

***Abstract*—— 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. This paper focuses on building a secure Transaction Processing System that will ensure both the data availability and secure data processing by replicating the data on two cloud providers in a secure way. The system has client machines who want to store the data on the cloud providers. To provide the maximum availability, our system will replicate the data on three different cloud providers while for ensuring the security by using the security algorithm AES and secret file sharing. To prevent the security risks of data intrusion and data integrity, we will distribute the data into three different cloud providers and we will apply the SHA algorithm on the stored data in the cloud provider. Suppose an intruder attacks one of the cloud provider. We will implement the system in such a way that for the hacker it should be impossible to attack the entire system even if they have one cloud provider's password. By replicating the data on three different cloud providers we reduce the risk of data intrusion.**

Keywords-AES, Cloud Computing, Multi Cloud, Single Cloud, Security

I. INTRODUCTION

One of the prominent services offered by the cloud is storage, where users store their data with the storage providers [7]. Popular storage providers are Amazon s3, Microsoft Sky Drive, Google drive. Since users save their data with the cloud service providers, it becomes the primary duty of the service providers to make their services available all the time with considering the security factor. Traditionally users were storing their data with a single cloud provider. Technology changes faster and thus the cloud world is moving from single cloud to multi cloud.

1.1 Single Cloud Computing

Privacy preservation and data integrity are two of the most critical security issues related to user data [3]. In conventional paradigm, the organizations had the physical possession of their data and hence have an ease of implementing better data security policies. But in case of cloud computing, the data is stored on an autonomous business party that provides data storage as a subscription service. The users have to trust the cloud service provider (SP) with security of their data for a service to depend solely on a particular cloud storage provider has its risks. Even though different cloud storage providers offer nearly identical service commodities, customers can experience vendor lock-in: It can be prohibitively expensive for clients to switch from one provider to another. Storage providers charge clients for inbound and outbound bandwidth and requests as well as for hosting the actual data. A client moving from one provider to another pays for bandwidth twice, in addition to the actual cost of online storage. This doubled cost of moving data leads to a kind of "data inertia"; the more data stored with one provider, the more difficult it becomes to move. This must be taken into consideration by consumers of cloud storage, lest they be locked into less-than-ideal vendors after entrusting them with their data. The resulting vendor lock-in gives storage providers leverage over clients with large amounts of data. These clients are vulnerable to price hikes by vendors, and will not be able to freely move to new and better options when they become available. The quickly evolving cloud storage marketplace makes this concern more real: A customer's best decision now may leave him trapped with an obsolete provider later, held hostage by vendor lock-in. In addition to possible increased costs, vendor lock-in subjects

customers to the possibility of data loss if their provider goes out of business or suffers a catastrophe.

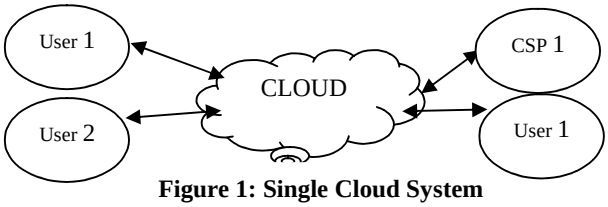


Figure 1: Single Cloud System

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.

2.2 Multi Cloud Computing

Multi-cloud strategy is the concomitant use of two or more cloud services to minimize the risk of widespread data loss or downtime due to a localized component failure in a cloud computing environment. Such a failure can occur in hardware, software, or infrastructure. A multi-cloud strategy can also improve overall enterprise performance by avoiding "vendor lock-in" and using different infrastructures to meet the needs of diverse partners and customers.

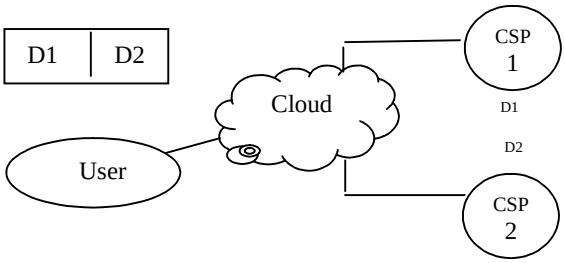


Figure 2: Multi Cloud System

A multi-cloud approach can offer not only the hardware, software and infrastructure redundancy necessary to optimize fault tolerance, but it can also steer traffic from different customer bases or partners through the fastest possible parts of the network. Some clouds are better suited than others for a particular task. For example, a certain cloud might handle large numbers of requests per unit time requiring small data transfers on the average, but a different cloud might perform better for smaller numbers of requests per unit time involving large data transfers on the average. Some organizations use a public cloud to make resources available to consumers over the Internet and a private cloud to provide hosted services to a limited number of people behind a firewall. A third type of cloud, called a hybrid cloud, may also be used to manage miscellaneous internal and external services.

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.

.

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 important data on a single cloud but we distribute the data across multiple clouds. 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

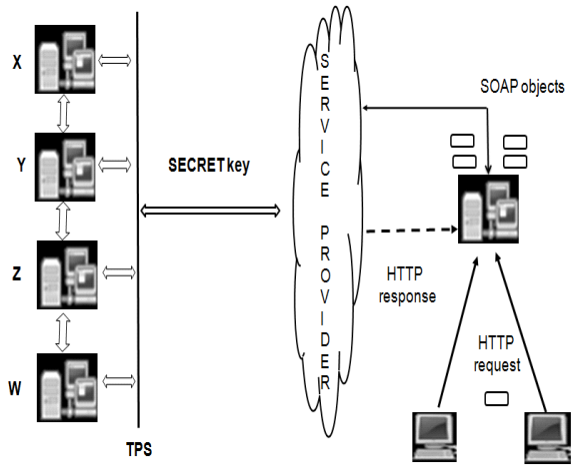


Figure 3: System Architecture

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

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 etc.

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 via TPS (Transaction process System).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**

In proposed approach, there are three main steps to save a file. Firstly, make a hash value at the client; secondly, it convert into different blogs on cloud servers; thirdly, save the file. Given architecture shows the procedures for storing a file. Firstly, users select the files or folders which are going to be uploaded and saved by using our application. The application use the AES algorithm to calculate the secrete key value. Central server will split the given file into number of blocks depending on how much cloud servers are there, then encrypt all the data using AES algorithm and store on different cloud servers using TPS algorithm.

- **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 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 modifiedblocks 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 decryptionk1, k2, k3…

11] Identify the Algorithm as Algo.

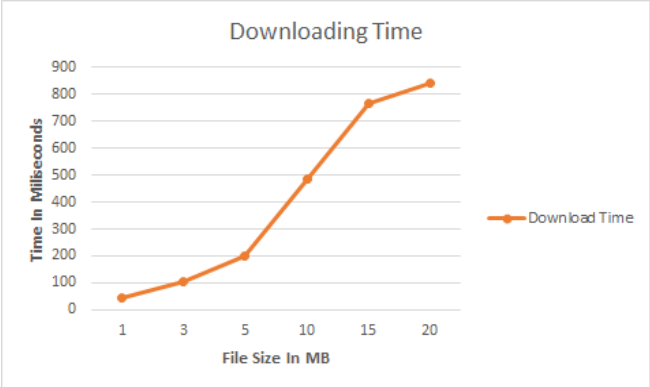
Algo= {Set of algorithms}

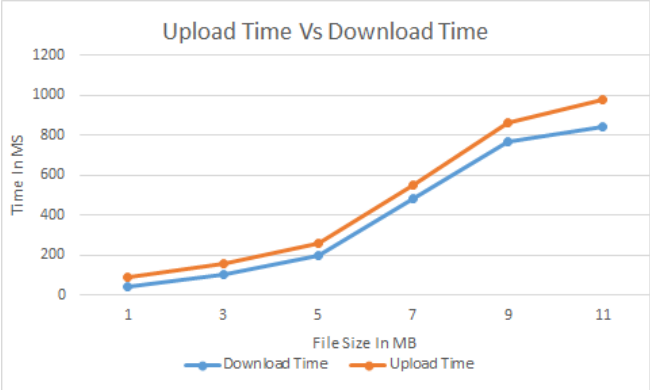
Algo = {al1, al2, al3,al4……}

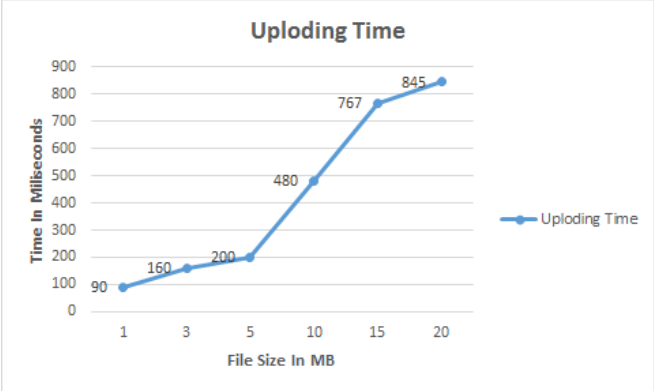
Where 'Algo' is the main set of algorithms al1,al2,al3…..

i.e {VerifyData,DataAvailability}

V. TENTATIVE RESULTS







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

[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