FULLY SECURED MULTI-CLOUD DATA USING SECURE HASH ALGORITHM

Amol L. Deokate
Lecturer,
Sanjivani K.B.P. Polytechnic,
Kopargaon

Vasim Iqbal Memon
HOD
R. C. Patel Polytechnic,
Shirpur

Rahul Ner
Student

Abstract: Multi-*Cloud computing is a fastest growing technology and emerging in the field of Information Technology. As it allows sharing of information and data over a cloud (network). The reason Cloud computing technology gained trust of organization, individuals rapidly was because of its performance, flexibility, availability and low cost among other features. Besides these features, companies are still afraid from binding their business with cloud computing due to the fear of data leakage and data security. The aim and focus of this paper is on the problem of data leakage and data security and data privacy.*

Keywords*:* Availability, Multi-Cloud Security, Confidentiality, Data Leakage, Decryption, Encryption, Integrity

I. Introduction

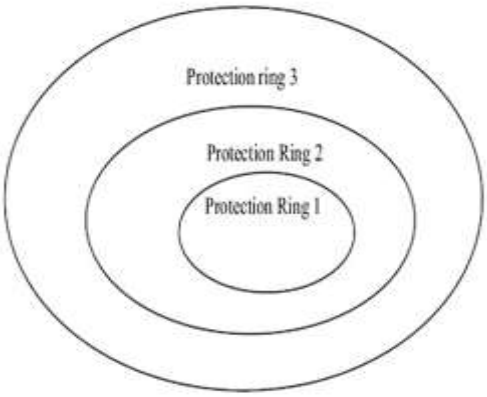
Multi-Cloud computing is a major and fastest growing technology. It also gives access to business organizations and also to use or access different applications, store their information without their accessing their personal files. While considering the power, stability and the security of multi-cloud, one can't ignore the different threats to user's data/file on multi-cloud storage. File access assure in real technique to the file protection due to untrusted cloud servers. In multi-cloud storage system file entrance mechanism is more challenging task. This system in consequence produces redundant copies of similar data/file involves a complete reliable cloud server. Attacks from adverse user are difficult to stop in multi- cloud storage. In proposed system we are implementing the concept of multiple-cloud storage along with enhanced more security using encryption techniques where either storing complete file/data on single multi-cloud system. The system will split the file in different parts then encrypt it and store on different cloud. The data needed to be decrypted and re-arranged that file will be stored in meta-data management server for efficient retrieval of original file .It promotes a system which works in two individual phase. The first phase contain a data encryption and classification which is performed before uploading or storing the data. In this phase, the client may want to encrypt his data prior to uploading. After encryption, data is classified using three parameters namely Confidentiality, Integrity and Availability. With the help of proposed algorithm, criticality rating of the data is calculated. According to the Critical rating, security will be provided. The data is access by the authorized person only. [1][2]

II. Related Work

The main purpose of this project is on the issue of data leakage and data security. It works in two phases. The first phase contains data encryption and classification of data which is performed by the client before storing the data. In this phase, the user may want to encrypt his data prior to uploading.SHA1used for encryption/decryption of user data. After encryption data is classified using three parameters of data security Namely Confidentiality [C], Integrity [I] and Availability [A]. The client must specify the values of these parameters, at the time of storing the data. The value of Confidentiality [C] is reliable on the level of security required for protecting the data. The value of Integrity [I] provides the scale to which the accuracy and reliability of the information stored is required. The value of Availability [A] is reliable on the frequency at which the data/file will be accessed. With the help of proposed algorithm, difficulty in rating of the data is calculated. After the completion of first phase, the second phase contains the data retrieval by the client. Users who want to access their data need to be authenticated user, to avoid data from being leaked. Before accessing the data, the user's identity is verified for authorization. [1]

Phase I: Data Encryption

To uploading the Data/file on cloud, users have an option to encrypt the Data/file for more security user. This allows the user to secure his data/file even further. [1]



Phase I: Data Classification

1. Input: User gives the data as input along with CIA parameters of security levels. User provides the value of CIA parameters. User's data, protection ring, arrays D, C, I, A, S, R of n integer size.

2. Output: Data is classified into three protection rings that are ring 1, ring2, and ring 3. This aids in providing different levels of access to different categories of data. Define data protection ring D [] array of n size. [1]

```
3. For i = 1 to n //Input values of CIA
C[i] – value for i'th data
I[i] – value for i'th data
A[i] – value for i'th data
4. For i=1 to n
/*assume rings 3 and protection levels from 1
To 10 selected manually by client while
Uploading files*/
If (C[i]>6 and I[i]>6) then
Ring level=1 (high)
Else
Calculate new average term CI of both C & I
CI=(C[i] + I[i])/2
Go to step 5
5. For i=1 to n
If (CI>3 and CI<5 and A[i] <5)
Then Ring level 2(Mid)
If (CI>3 and CI<5 and A[i]>5) then
Ring level 3(Low)
If (CI>=1 and CI<=3)
Then Ring level 3(Low)
```

In given algorithm the first job of the user is to upload the data on cloud. The proposed framework uses data classification algorithm to classify data on the basis of Confidentiality[C], Integrity [I] and Availability [A]. Here D [] represents data. The user must give the value of C-Confidentiality, I-Integrity and A Availability. After applying proposed formula the value of Criticality Rating (Cr) is calculated. Data is allocated to a protection ring based on the Cr. This encryption technique suggests that internal protection ring is very critical and it requires more security technique to ensure confidentiality. After classification of data/file in above step, three entities are suggested, first one is cloud provider itself, second is organization whose data is stored at multi-cloud and last one is user who request for access of cloud data. As seen above, in the first phase Data is classified into Ring 1, Ring 2, and Ring 3. [1]

FTP Setting Module:

The proposed system, file get scattered at three different location. First location is for the application and the next two more FTP where 2nd and 3rd data/file is store. In proposed system, we design setting page where this will be used by application to upload and download file/data from generated table. Insert into table FTP details. [2]

Upload and Download modules:

Design and develop a web interface to upload and download files/data in multi-cloud storage. The different data/file links are open for uploading. The user can choose the link which we want to upload on cloud. User can upload the file on multi-cloud such as doc file, video, mp3, mp4 etc. Homepage will show list of file uploaded by user from user specific directory. In latest system, we use data list to show data/file list .File class to get folder and file details like file name, file size etc.

 Uploading file by using file uploader control we can let the user choose file which user want to upload.

 Get the sever path by using Server. Map Path () function is used to get path of server directory. [2]

File encryption technique module:

Setting up and configuring different multi-cloud server in order to having storage multi-cloud access. Each clouds its own server. Developing encryption technique like SHA-1 for file encryption before storing the file/data on multi-cloud. In proposed system, we use combination of AES algorithm and SHA-1 algorithm for encrypting and splitting of File. [2]

File splitting and clubbing module:

In latest system, we split the file in different portions then encode and store the file on multi-cloud. Meta data is necessary for decrypting and sending a

file/data that will be stored in Meta data management server. File can combine with another file. [2]

SHA-1:

SHA-1 stands for “Secure Hashing Algorithm”. It is a hashing algorithm designed by the United States National Security Agency (USNSA) developed and published by “NIST”. It is upgraded upon the original SHA-0 and was first SHA-1 is currently the most widely and well known used hash function, although it will soon be replaced by the newer and potentially more safe/secured SHA-2 family of hashing functions. It is currently used in a wide variety of applications, including TLS, SSL, SSH and PGP. SHA1 gives outputs of 160-bit digest of any sized file/data.

SHA1 Algorithm

 Padding

○ Pad the data with a single one followed by zeroes until the final block has 448 bits.

○ Increase the size of the original message as an unsigned 64 bit integer.

 Initialize the 5 hash blocks (h0, h1, h2, h3, h4) to the specific constants specified in the SHA1 standard.

 Hash (for each 512bit Block)

○ Allocate an 80 word array for the message schedule

■ fix the first 16 words to be the 512bit block scatter into 16 words.

■ the rest of the words are generated using the following algorithm word [i-3] XOR word [i-8] XOR word [i-14] XOR word [i-16] then rotated 1 bit to the left.

○ Loop 80 times doing the following

■ Calculate SHA function () and the constant K.

■ e=d

■ d=c

■ c=b (rotated left 30)

■ b=a

■ a = a (rotated left 5) + SHA function () + e + k + word[i]

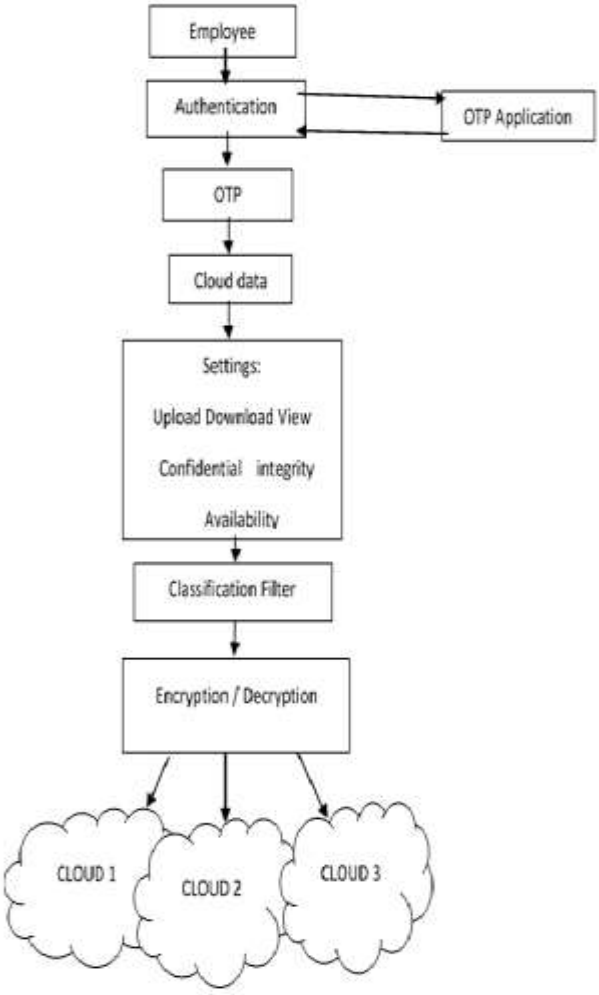
○ Add a, b, c, d and e to the hash output.

 Output the concatenation (h0, h1, h2, h3, h4) which is the data digest. [2]

Phase II: Data Access:

The Fig. below gives an overview of the first step of the second phase in which the Methodology for accessing the data.

Now if a user want to access the data, if it belongs to protection of ring 1, it require authentication with "OTP" sent on Users Mobile, if the data belongs to protection of ring 2 then user have to Authenticate with Graphical Password, if the data belongs to protection of ring 3, then it just needs the user to re-enter the password. Now suppose the user login itself for accessing data or information, the Client Software will provide Username, Password Multi-Dimensional Password for Authentication as well as gives the OTP Generation on the Users Mobile to provide more security to our data. [1]



When user sends request along with username and password to access the data to multi-cloud provider, the multi-cloud provider first checks the user’s mobile number, then it generates the OTP and sends it on the Users Mobile.

Then, the user must enter the "OTP" received for authentication, and after authentication access to the data will be provided.

- A Random String is generated using the user data as follows:
- This String is converted to 160-bit SHA-1 hash function.
- This 160-bit (20 bytes) Hash is scattered into 4 groups of 5 byte each.
- The first byte of each group is XO Red to get first byte of OTP.
  Similarly the remaining bytes of OTP are Generated, as shown below.
- The XO Red String ABCDE is converted to Hexadecimal and Sent to User's Mobile as an OTP. Once the user enters the OTP it verifies it with the OTP generated and then allow access to the data. Generally the OTP should be valid for a limited period of time say 10 minutes. [1]

Download:

Get the file name selected by user read 1st part of file(means file a) from user specific directory and get A and also FTP detail from user get from user name and FTP password user in textbox connect B FTP download 2nd part from FTP. Download file function, we get part B and repeat above process we will get C or part C. we combine 2nd (B) and 3rd (C) part we will get X, then combine i.e. 1st part with X. Finally we have club file in Byte buffer and save this buffer to memory Stream.

Acknowledgment

I would like to show my sincere gratitude towards my project guide Ms. H.P Patil, Lecturer, Guru 3Gobind Singh Polytechnic, Nashik for her valuable guidance and encouragement.

We are grateful to the Guru Gobind Singh Polytechnic, Nashik for taking initiative to start the international journal IJTS.

III. Future Work

Customers usually raise data security concerns related to:

- Better Security
- Regulatory Compliance
- Flexible deployment provision
- Dealing with Complexity
- Key Management in case of encryption

There is a strong industry agreement that secure and parallel with regulatory compliance, is the first 99obstacle to adoption of cloud computing [10]. Underlining these concerns is the need to build trust an organization can outsource its storage or its compute resources, but confidentiality cannot be outsourced.

At the same time, companies are attracted to multi-cloud computing for its various advantages such as flexibility, elasticity and the easy economic model. Multi-Cloud customers can brings up servers and storage in short time and they expect a safety solution to provide the high level of automation and management. [1]

IV. Conclusion

This technique provides a new way to authenticate and as well as providing an optional Encryption Framework. Because of classification data security is more increases. The data availability is provided by overcoming many existing problems like data leakage, user managed encryption keys etc. It also provides more flexibility, capability and reliability to overcome the problems faced by today's complex and diverse networks.

References

[1] Sagar Tirodkar1, Yazad Baldawala1, Sagar Ulane1, Ashok Jori1 3-Dimensional Security in
Cloud Computing International Journal of Computer Trends and Technology (IJCTT) – volume 9 number 5– Mar 2014

[2] Nisha D. Dable, 2Nitin Mishra Enhanced File Security using Encryption and Splitting technique over Multi-cloud Environment International Journal on Advanced Computer Theory and Engineering (IJACTE)

[3] Venkata Narasimha Inukollu1, Sailaja Arsi1 and Srinivasa Rao Ravuri3 SECURITY ISSUES ASSOCIATED WITH BIG DATA IN CLOUD COMPUTING International Journal of Network Security & Its Applications (IJNSA), Vol.6, No.3, May 2014
DOI: 10.5121/ijnsa.2014.6304 45

[4] Sasikumar Gurumurthy, T. Niranjan Babu, G. Siva Shankar an Approach for Security and Privacy Enhancing by Making Use of Distinct Clouds International Journal of Soft Computing and Engineering (IJSCE)
ISSN: 2231-2307, Volume-4, Issue-2, May 2014

[5] Alwesabi Ali, Almutewekel Abdullah Okba Kazar Implementation of Cloud Computing Approach Based on Mobile Agents International Journal of Computer and Information Technology

[6] Varsha Alangar Cloud Computing Security and Encryption Volume 1, Issue 5, October 2013 International Journal of Advance Research in Computer Science and Management Studies

[7] Prasad Adireddi Data Access Control using Cryptographic techniques in Cloud Computing environment International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 5, May - 2014