ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

Truly Secured Multi-Cloud Data Using Advanced Encryption Standard (AES)

Shubham Aher [1], Salman Shaikh[2], Arsalaan Merchant[3], Krishna Palav[4]

Student, Dept. of I.T., Guru Gobind Singh Polytechnic, Nashik, Maharashtra, India

ABSTRACT: 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 security and data privacy.

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

I. Introduction

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 developing 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. [1][2]

II. Related work

The main purpose of this project is on the issue of data security. It works in two phases. The first phase contains data encryption which takes place automatically when client storing the data. In this phase, the user may want to encrypt his data prior to uploading.AES standard used for encryption/decryption of user data. 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 upload the Data/file. Encryption and file splitting takes place automatically. This allows the user to secure his data/file even further. [1]

A. *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]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

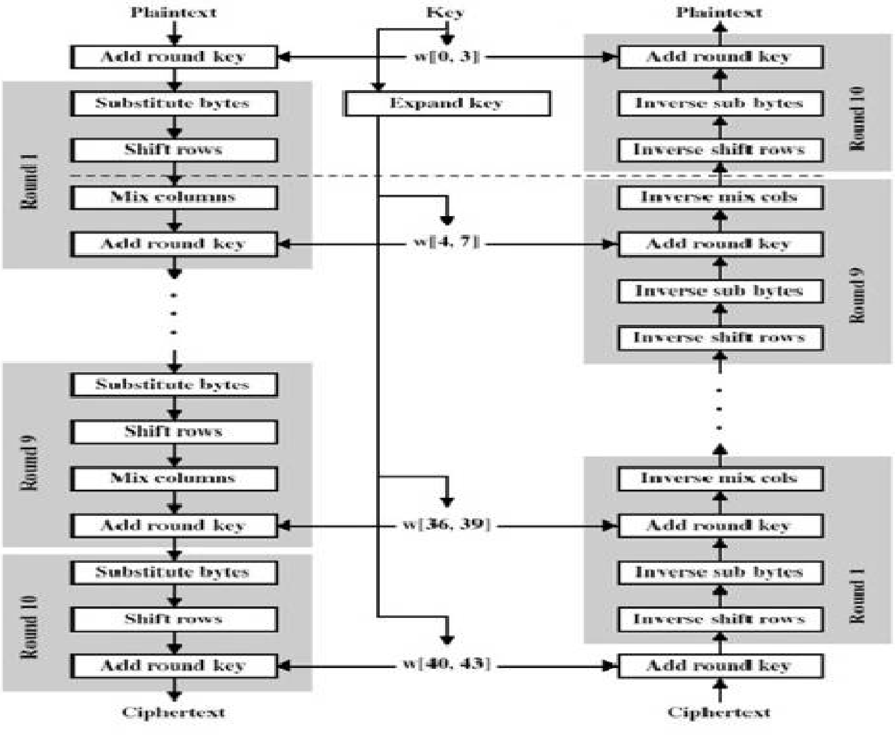
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

B. *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 AES for file encryption before storing the file/data on multi-cloud. In proposed system, we used, AES is a symmetric block cipher. This means that it uses the same key
For both encryption and decryption and splitting of File.

C. *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]

Advanced Encryption Standard (AES):
AES stands for "Advanced Encryption Standard".AES is a symmetric block cipher. This means that it uses the same key for both encryption and decryption.AES standard states that the algorithm can only accept a block size of 128 bits and a choice of three keys - 128, 192, 256 bits. Depending on which version is used, the name of the standard is modified to AES-128, AES-192 or AES-256 respectively. [3]



(a) Encryption (b) Decryption

Fig: Overall structure of the AES algorithm. [3]

Inner Workings of a Round:
The algorithm begins with an Add round keystage followed by 9 rounds of four stages and a tenth round of three stages. This applies for both encryption and decryption with the exception that each stage of a round the decryption algorithm is the inverse of itscounterpart in the encryption algorithm. The four stages are as follows:
1. Substitute bytes
2. Shift rows

3. Mix Columns
4. Add Round Key

The tenth round simply leaves out the Mix Columnsstage. The first nine rounds of the decryption algorithm consist of the following:
1. Inverse Shift rows
2. Inverse Substitute bytes
3. Inverse Add Round Key
4. Inverse Mix Columns [3]

Phase II: Data Access:
When user want to download his file he login in his account then select a file which he wants to download and then click on download button decryption takes place automatically parts of file download from different cloud and combine with each other.

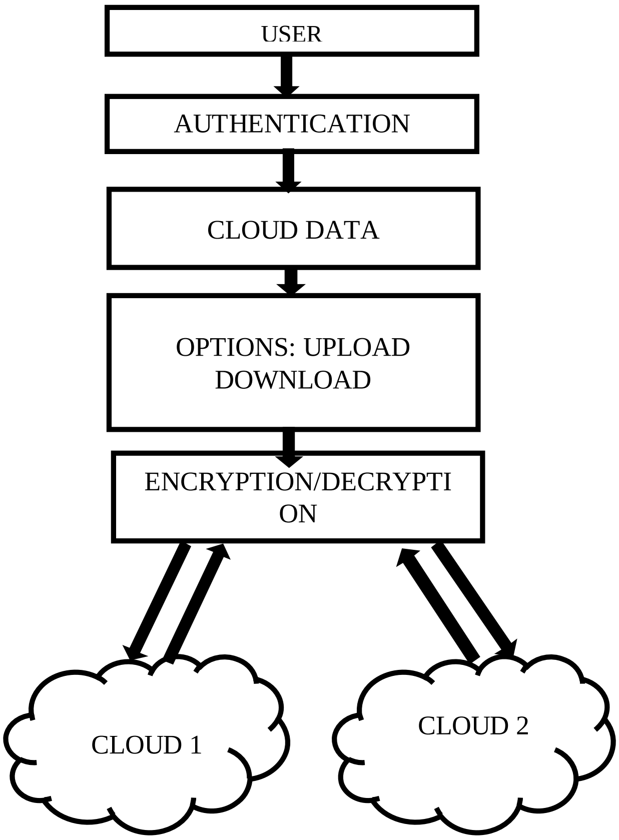


Fig: Overall working process project

III. Conclusion and Future Work

Customers usually raise data security concerns related to:

- Better Security
- Regulatory Compliance
- Flexible deployment provision
- Dealing with Complexity

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.

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]Chapter 7 the AES Algorithm pdf book

[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 KazarImplementation of Cloud Computing Approach Based on Mobile Agents International Journal of Computer and Information Technology

[6] Varsha AlangarCloud 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

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