Analysis on Securing Methods in Multi Cloud

M. Sasikala
Assistant Professor
KG College of Arts and Science, Coimbatore, India.

Abstract- *Cloud computing is most popular because of its most important feature data sharing with multiple users which giving humongous advantage to the user. [1] Data sharing is the top priority among the organization which leads them to share 74% with customers and 64% with suppliers. By more number of users contributes in Cloud through which it is economically and timely more effective. The growth of Cloud in the recent decade to till date is rapid. From the invention of sharing idea of data the problem of securing data is also challenging factor which come across in this environment. This paper deals with how to secure data in cloud computing using multi computing.*

Keywords- Security, Multi-Cloud Computing

I. INTRODUCTION

At present globally from an individual person to big multinational organization is very keen in sharing data and getting their own productivity through the cloud. Social media platforms and giant cloud providers are big earning people in this form of business. When it comes to sharing the data, then the cloud business model have to ensure the following criteria for the proper process attaining.

- Confidential in data providing
- User revoking properly
- Providing good scalability and efficiency

Cloud Computing is giving huge privileges to the users to access the data, this feature is most vigorous to the attackers and malicious users for mishandling the data and its growing as big threat to organization market. This leads to following types of attacks in the cloud environment

[1]Different Types of Attacks on the Cloud Computing:-

- XML Signature Wrapping Attacks
- Cross site scripting attacks
- Flooding Attack Problem
- Denial-of-Service Attacks
- Law Enforcement Requests
- Data Stealing Problem
-

[1]Expectations and Cause of Malicious User:-

- Stealing the high priority data
- Creating problems by duplicating data
- Helping hackers to use the space
- For the sake of proving intelligence
- By Curiosity doing this work

Traditionally the way of providing security in cloud is encryption and decryption of data with proper keys. In recent times all the key managing process are broken down and it's questioning the trust of data security in cloud. To overcome the data violation a concept multi cloud with different techniques are discussed below.

II. MULTI CLOUD COMPUTING

Multi cloud is collection of several cloud infrastructures to form a service pattern for providing needs to the users. [2] An example of Multi Cloud architecture is DepSky architecture fig (1). DepSky model contains clients and a cloud of several cloud storage providers. The storage providers perform the task issued by clients.

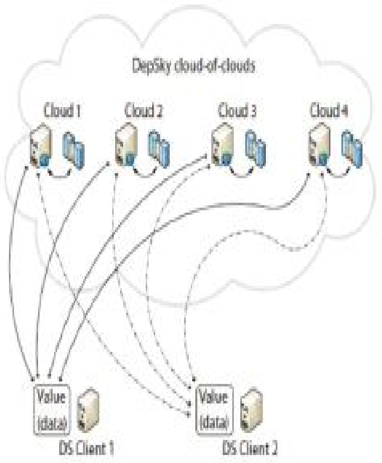

Fig (1):- DepSky Architecture

[3] A multi-cloud system is also known as cloud-to-cloud or mashup clouds, which is a distributed system where data have a certain degree of redundancy and replicated among different clouds owned by different vendors. Several reasons are there for moving to multi cloud in which its ability to provide both public and private data in different clouds. It's

giving organization workers to concentrate on private cloud for securing data rather on public cloud. Also it's provides the cloud to be part in different part of world.

In this pattern data are in different parts which makes its secured, even then there are threats to this architecture. In this paper we are seeing several techniques and enhancing methods for providing security for data.

III. SECRET SHARING ALGORITHM

[2] Data can be compromised or lost in the cloud. Hence securing the data is a vital process in the cloud environment. Therefore to secure the data in multi-cloud, Shamir proposed to store the data in more than one cloud and encrypt the same in the cloud before it transferred and saved.

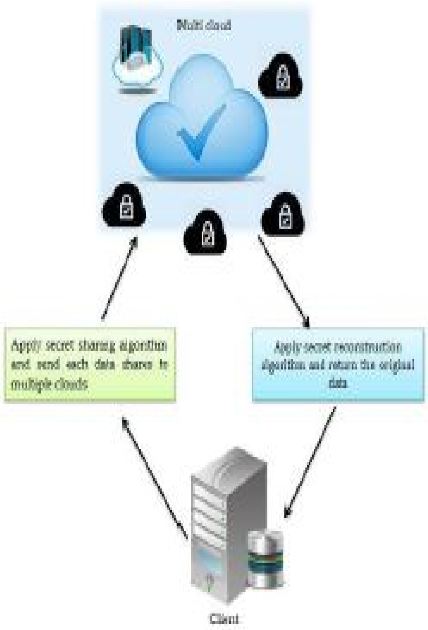
Multi cloud
Apply secret sharing algorithm and send each data shares to multiple clouds
Apply secret reconstruction algorithm and return the original data
Client

Fig (2):- Block Diagram of Sharing Algorithm

MATHEMATICAL DEFINITION:

The goal of the algorithm is to divide the data **DATA** into **n** pieces (DATA1, DATA2, DATA3, DATA4 …..DATAn) so that,

1. Retrieving any **k** or more **DATAi** pieces makes **DATA** easily computable.
2. Retrieving any **k-1** or fewer DATAi pieces leaves **DATA** thoroughly undetermined.

The above scheme is known as **threshold(k, n).** if **k=n,** then all pieces are available for reconstruction of DATA.

The objective of Adi Shamir's secret sharing algorithm algorithm is that, k points are enough to define a polynomial of degree k-1.[1] Example, 2 points are sufficient to define a line.

Choose an approximate **k-1** coefficients **c0**, **c1, c2, c3….ck-1** in **H**, and let **c0 = S**, where **S** is the Secret data which is going to be stored in cloud. Build the polynomial **H(z) = c0 + c1z1 + c2 z2+……+ck-1zk-1**. Then **n** points are defined, for example set **i=1,2….n** to retrieve **(i, H(i))** . A pair is formed with input to the polynomial and output.

Given any subset of k of these pairs, using interpolation the coefficients of the polynomial can be found and the constant term **a0** is the secret.

The secret is divided into pieces by considering an approximate degree polynomial

H(z) = c0 + c1z1 + c2 z2+……+ck-1zk-1

In which **c0 = S, S1 = H(1), S2 = H(2),…………, Sn = H(n)** and represent each share as a point

(zi, G(zi) = yi)

The secret sharing algorithm has a dynamic foundation which provides good platform for services and also it's overcomes the disadvantages of single cloud.

IV. MULTI-CLOUDS DATABASE MODEL

Multi Cloud database model ensured privacy using service providers and secret sharing algorithm. In this technique its permits customers to access with different types of database queries which avoid the malicious user inside the cloud. Database management system take care connection between service providers and clients by this dbms requesting a separate query for each service provider Fig (3).

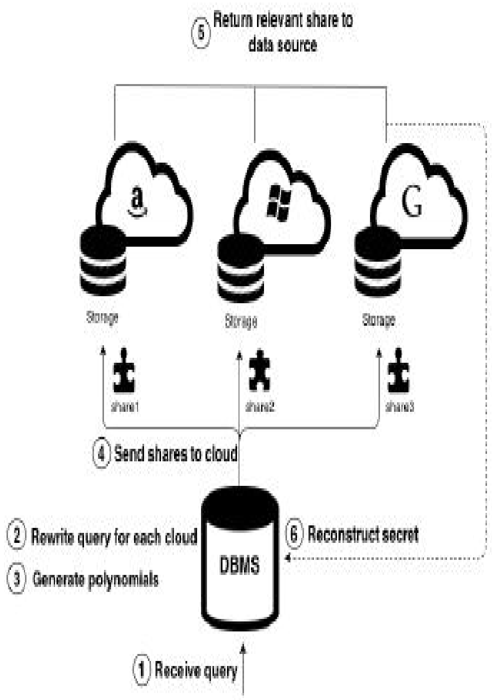

Fig (3):- Multi-Clouds DB Data workflow

Multi Cloud database model proven to be secured and it's consists of superior encryption techniques due to their biggest limitation and its overcome the security issue of single cloud.

V. USDSMC FRAMEWORK

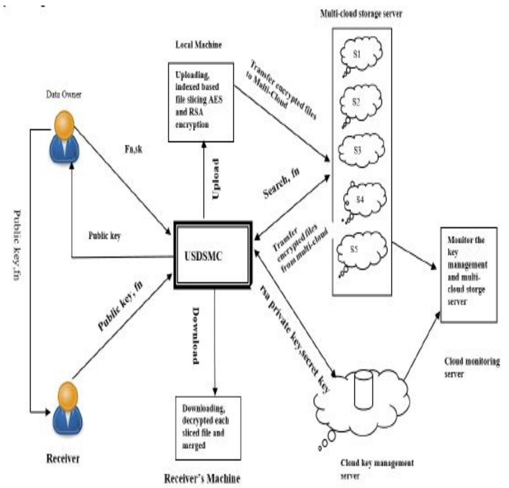
Multi-cloud storage server
Local Machine
Uploading, indexed based file slicing AES and RSA encryption
Transfer encrypted files to Multi-Cloud
Data Owner
Fn,sk
Upload
Search, fn
S1
S2
S3
S4
S5
Public key
USDSMC
Transfer encrypted files from multi-cloud
Monitor the key management and multi-cloud storge server
Public key ,fn
Public key, fn
Download
rsa private key,secret key
Cloud monitoring server
Receiver
Downloading, decrypted each sliced file and merged
Receiver's Machine
Cloud key management server

Fig (4):- USDSMC Framework

[5] The figure 4 provides the architecture of the hybrid cryptosystem. According to the architecture, data owner transmits the file and the secret key via the framework interface. The file is uploaded to the USDSMC by the framework and indexed based slicing and encryption consequently performed on the files before being transferred to the multi-cloud storage server. Furthermore, the secret key is also encrypted using the RSA key and a portion of the key transmitted to the owner and cloud database server. The decryption phase also involves a number of processes. For instance, upon receiving the necessary credentials from the owner, the filename and the public key are transmitted using the untrusted or semi-trusted channel. The file name is searched and the private keys used to decrypt the sliced files to the receiver's computer.

The USDSMC framework act as a middleware or web API to connect with Multi-cloud server. The following are the operations or process performed by the framework when the file gets uploaded or downloaded.

a) File Uploading: File gets uploaded in the owner's local machine.
b) Indexed Based File Slicing: File gets sliced based on the number of storage service providers. All the sliced file sizes are constant.
c) RSA Encryption: Owner's a secret key gets encrypted and as a result, framework sends the public key to the owner and another part to the cloud database server.
d) AES Encryption: Each part of the sliced file is encrypted and sent to the multi-cloud storage server. It uses 8-bit secret key to reducing the round trip process while performing encryption which in turn increase the efficiency of the proposed algorithm.
e). File Downloading: Once the receiver enters the public key and file name via framework interface it searches the file name and downloads all the parts in the receiver's machine.
f) File Merging: Once the file parts are received merging process will result to give a required file. All the processes get monitored at the provider's end.

USDSMC framework overcome the problems of malicious files, threats while sharing data and also it offers solution in designing safe, dependable and efficient architecture in Multi-Cloud storage.

VI. MULTI AGENT SYSTEM (MAS) AND DATA ENCODING TECHNIQUE

[6] Using Multi Agent system (MAS) and Data Encoding technique they are combined together to give a new mechanism which provides security in both data transmission and storage place also. Clients' file can be divided into any number of parts and stored in n number of clouds. There are two main modules, one is the user module and the second is the TPA module. In user module, user can login and upload

files, admin will register the users, encrypt the file and divided into 3 parts and store each part redundantly in n/3 number of clouds. Alerts are sent to the actual user when his data is undergone to any try of tampering in the cloud storage. The diagrammatic representation of this technique.

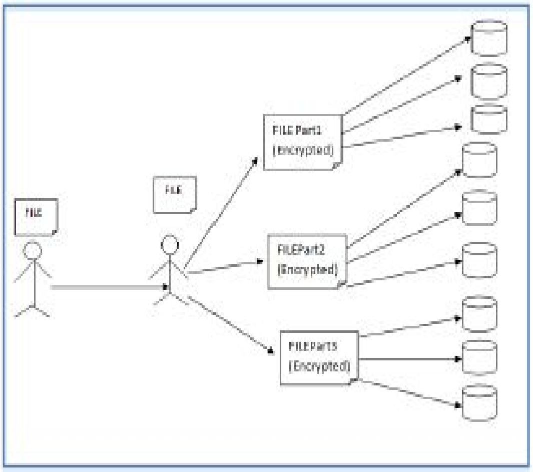

Fig (5.a):- Uploading the files part into multiple cloud storage .

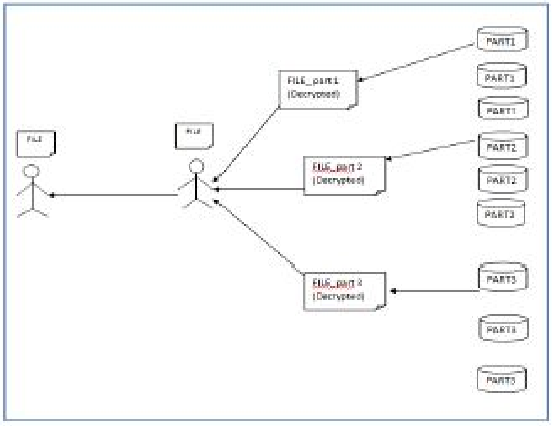

Fig (5.b):- Reconstructing the file by collecting the file parts stored in different cloud storages.

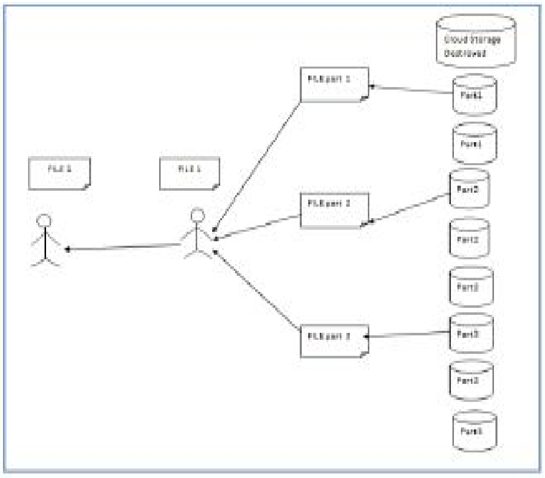

Fig (5.c):- Redundancy feature when cloud storage containing the file part is destroyed

This technique allows the user to work with greater functionality to upload or download file from any place and from any computer to his account using multi cloud architecture.

VII. AES ALGORITHM

AES (Advanced Encryption Standard) is a symmetric encryption technique. The algorithm was proposed by two Belgian cryptographers Joan Daemen and Vincent Rijmen. AES was designed to be effective in both hardware and software; AES is block cipher which supports a block length of 128 bits and key lengths of 128, 192, and 256 bits. AES algorithm operates on a 4×4 column-major order matrix of bytes, called as the state.

Algorithm:

1. Key Expansion—round keys are obtained from the cipher key using Rijndael's key schedule. AES needs
a separate 128-bit round key block for each round plus one more.
2. Initial Round and AddRoundKey—each byte of the state is merged with a block of the round key using bitwise xor.
3. Rounds Sub Bytes—the non-linear substitution step in which each byte is returned with another using a lookup table. Shift Rows—a transposition step in which the last three rows of the state are moved cyclically a definite number of steps. Mix Columns—a mixing operation which performs on the columns of the state, merging the four bytes in each column. AddRoundKey
4. Final Round (no Mix Columns) Sub Bytes Then Shift Rows And AddRoundKey.

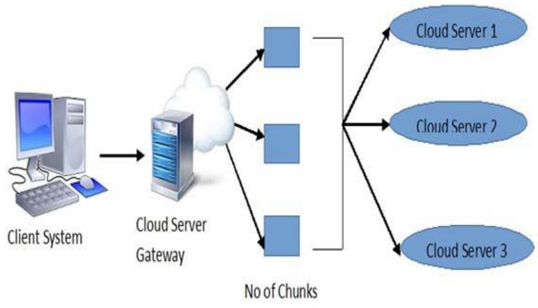

Fig (6):- Framework of AES Algorithm

The architecture of proposed system involves three different modules like client module, cloud server gateway module and cloud storage module. In first module client will create the file which is to be stored on cloud server gateway. Cloud server will divide this file into number of chunks which is to be encrypted using AES symmetric key algorithm. Rather storing complete file on single cloud system will split the file in different chunks then encrypt it and store it on different cloud and the Meta data required for decrypting and rearranging a file will be stored in metadata management server.

VIII. CONCLUSION

In this paper it's discussed the various techniques available in multi cloud environment to provide the security and privacy for data. All this process ensuring the customer need and satisfaction for sharing data and receive the higher productivity for their responsive work.

REFERENCES

[1] Secure Data Sharing in the Cloud by Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo

[2] Securing Multi-Cloud using Secret Sharing Algorithm M.Muhila, U.Hemanth Krishnaa, R.Kishore Kumara, E. A. Mary Anitaa*M. Muhil et al. / Procedia Computer Science 50 (2015) 421 – 426*

[3] On Securing Multi-Clouds: Survey on Advances and Current Challenges Tara Salman

[4] Multi-Clouds Database: A New Model to Provide Security in Cloud Computing by Ion Morozan ion.morozan@gmail.com, Vrije Universiteit, Amsterdam, The Netherlands.

[5] Secure and Reliable Unstructured Data Sharing in Multi-Cloud Storage using the Hybrid Crypto System Dr.K.Subramanian1, F.Leo John2*. IJCSNS International Journal of Computer Science and Network Security, VOL.17 No.6, June 2017

[6] Efficient Encryption Scheme for Small Arbitrary Length Domains, by Dr. S.Vidhya International for Research in Applied Science and Engineering Technology (IJRASET) Vol.6, Issue 1, Jan 2018.

[7] Design and Implementation of a Secure Multi-Cloud Data Storage Using Encryption by Prof. M. Ben Swarup, Chukkala Varaha Sampath Pothabathula Srikanth International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 5, May 2014

[8] Enhanced Security for Multi Cloud Storage using AES Algorithm by Namita N. Pathak 1, Prof. Meghana Nagori 2 Namita N. Pathak et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (6) , 2015, 5313-5315