Privacy and Security on Cloud Data Storage Using Hybrid Encryption Technique

S. Dhiviyaa[1], B. Lavanya[2], D. Saranya[3]
[2, 3]Dept of BCA & M.Sc SS
[1]Assistant professor, Dept of BCA & M.Sc SS
[1, 2, 3] Sri Krishna arts & Science College, Coimbatore, Tamilnadu

Abstract- *In the modern world of enhancing technologies, cloud network proves as a boon among different network technologies. The cloud environment is about sharing of servers, users and individuals among different resources. Hence it leads to difficulty for providers in ensuring the file security and an easy job for intruders to access, destroy or misuse the personal information of each individual. It is mainly focused as Database-as-a-service (DAAS) which enables data integration and access on a wide and large scale cloud computing services. The paper presents the file security model which uses the concept of hybrid encryption scheme to meet security needs. It suggests a technique to enhance the security of cloud database. This technique provides the flexible multilevel and hybrid security. It uses RSA, Triple DES and Random Number generator algorithms as an encrypting tool.*

Keywords- Hybrid Cryptosystem, Blowfish, SRNN, File Splitting, Cloud Security.

I. INTRODUCTION

Cloud computing is large technology in simple word we say it is a large network which provide all type of facility which are required by the user related to operating system facility, Application software, resources, cloud data storage and some hardware like RAM or memory. Microsoft 2012 designed by Microsoft OS proves as the best example of cloud computing which was hardware dependent. Since The ever-increasing amount of valuable digital data both at home and in business needs to be protected, since its irrevocable loss is unacceptable. Cloud storage services are used to overcome this problem. It provide the ways to store and automatically back up arbitrary data, as well as data sharing between users and synchronization of multiple devices [1]. Cloud computing is a trend in IT where computing and data storage is carried out in data centers. The sharing of resources reduces the cost to individuals'. According to cloud computing services; all users' data are stored on the cloud data storage. So, all the data must undergo encryption process before it is transmitted to the cloud storage.

Although providers of cloud computing services ensure the security and reliability, there are a number of security issues that are created in cloud computing services. In March 2009, security vulnerabilities in even Google Docs led to serious leakage of users' personal information. Google Gmail also appeared a global failure up to 4 hours. A serious outage accident happened in Microsoft's Azure cloud computing platform for about 22 hours.

II.CRYPTOGRAPHIC ALGORITHMS

2.1 3DES

DES was superseded by triple DES (3DES) in November 1998. 3DES is exactly what it is named–it performs 3 iterations of DES encryption on each block. It can do this in a number of ways, but the most common method is the Minus Encrypt-Decrypt-Encrypt (-EDE) method. In –EDE, the block will be encrypted with a 56-bit key. Then a different 56-bit key is used to decrypt the block. On the last pass, a 56-bit key is used to encrypt the data again. This is equivalent to using a 168-bit encryption key. Another method that can be used is Minus Encrypt-Encrypt-Encrypt (-EEE) [2]. This is three successive encryptions using a different 56- bit key. There are several keying methods that 3DES uses. All three keys can be independent of each other, or the first and third keys can be identical, with the second key being unique. All three keys can also be identical, which provides the least security, but is also the fastest to encrypt with. 3DES is still approved for use by US governmental systems, but has been replaced by the advanced encryption standard (AES)

2.2 Random Number Generator

The cryptography mechanism uses lot of random numbers which would be needed for the purpose of creating random Keys. The best a computer can produce is a pseudo-random-sequence generator [3]. A pseudo-random sequence is one that looks random. The sequence's period should be long enough so that a finite sequence of reasonable length—that is, one that is actually used—is not periodic. If it has been needed a billion random bits, don't choose a sequence generator that

repeats after only sixteen thousand bits. These relatively short non periodic subsequences should be as indistinguishable as possible from random sequences.

2.3 RSA

RSA is a public key cryptography algorithm that is being used commonly in the current technologies. It is named after the mathematicians who developed it, Rivest, Shamir, and Adelman. In current trend, RSA is used in hundreds of software products and also it is used for key exchange, encryption of small blocks of data or digital signatures. An encryption block and a key with variable size is used. The key pair is derived from a very large number n, which is the product of two prime numbers chosen according to special rules. Since it was introduced in 1977, RSA has been widely used for establishing secure communication channels and also for authentication purpose i.e., the identity of service provider over insecure communication medium [4]. In the authentication scheme, the server along with its client implements public key authentication. During the authentication it signs the unique message from the client using private key which is called a digital signature.

III. HYBRID CRYPTOSYSTEM SCHEME

Hybrid cryptosystem is used for ensuring that files are secured on cloud. Assumes that the remote server is trusted, so files are encrypted by server and finally encrypted files are stored at the server end.
It is combination of:

- Blowfish or Symmetric Algorithms
- SRNN Algorithms

In this scheme, performance level of Symmetric algorithm is combined with Asymmetric algorithm, whether it has a high security. So Blowfish has best performance. The SRNN used in between of speed and security. In hybrid cryptosystem, first already uploaded files are sliced and each slice is encrypted, then Blowfish key is provide by user. Secondly, each of the n keys are encrypted using SRNN where n is the number of slices.

A. BlowFish Algorithm

In this method, use the amalgamation of two Mechanisms to process.

They are:

1. Splitting File Mechanism
2. Merging File Mechanism

It is symmetric type of block cipher, it uses Fiestal network, which consists 16 rounds, it takes encryption and decryption functional designs to perform iteration. The block size is 64- bits; the size can be different in measuring the length of Blowfish [5].

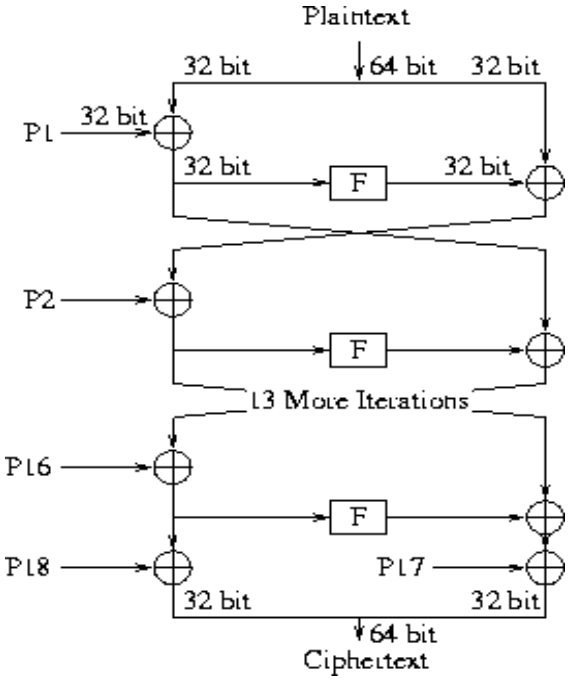

Fig 1. Blowfish Algorithm

B. SRNN algorithm

It is second type of algorithm which is used in Hybrid scheme. It is same as RSA algorithm, with some improvement. In this algorithm, which extremely contains a huge number of two prime factors, which is similar to RSA is used. In addition, pair of keys is used from two short range natural numbers. So, this helps to progress the refuge in cryptosystem. SRNN algorithm is used for communication between user and cloud servers in secure and strong.

IV. PHASES OF HYBRID CRYPTOSYSTEM

The hybrid cryptosystem used to maintain security of the files has two phases:

- Encryption Phase
- Decryption Phase

A. Encryption Method or Encryption Phase

Encryption works end, then Based on user specification, the file should be encrypted and then it will be sliced into n slices. All the files sliced are encrypted using Blowfish key method, which is given by the user for each and

every slice of file.Again, the key undergoes for an encryption using SRNN public key.

Once the encryption is completed, then encrypted files are slices with the corresponding encrypted keys.

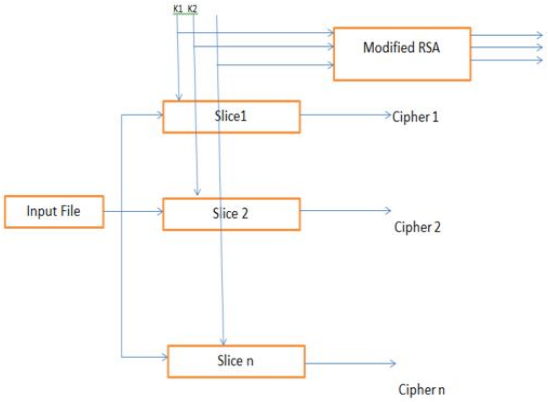

Fig 2. Encryption Phase
Ki - BlowFish Key, Eki – Encrypted BlowFish Key

In encryption method, files should be split up into slices and it could be combined by decryption method.

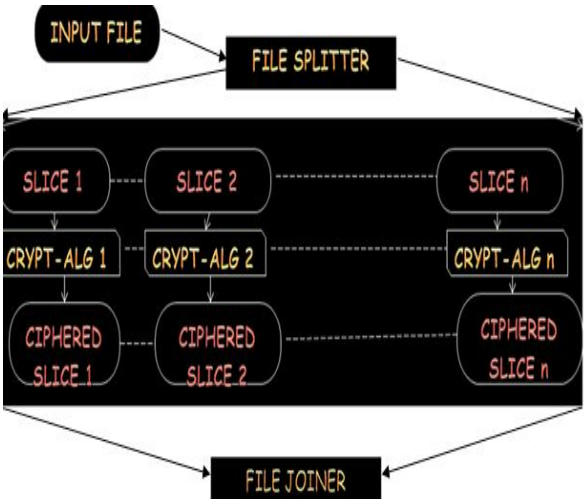

Fig 3. File Splitting and Merging Mechanism

B. Decryption Method or Decryption Phase

At the end of decryption phase,

There are 'n' numbers of SRNN private keys are given by the user.

Based on the amount of slices (n) created in the encryption method, Blowfish type key is used to decrypted at the server side using the SRNN private key specific to the slice.

With the help of Blowfish keys is mostly used to decrypt, file should be sliced and it is stored at server in decrypted type [6].

Then the slices which are decrypted are merged into a single file. The scenario of decryption phase

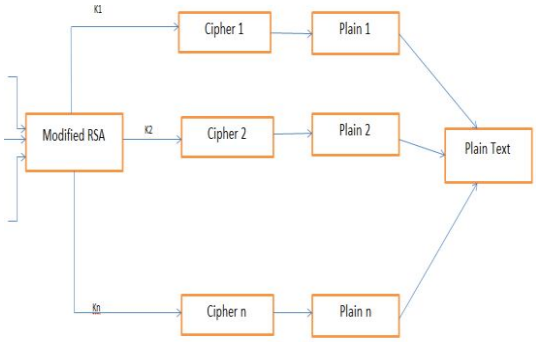

Fig 4. Decryption Phase

V. SECURITY ARCHITECTURE OF CLOUD MODEL IN PROPOSED SYSTEM

In clouds file security, hybrid cryptosystem is developed and used. In cloud server, which is mainly concentrate on misusing or unauthorized data accessed by intruder or data leak out or other security problem, the data should be encrypted first and then stored on server side.
It can be classify into three phases:

- Registration Phase
- Uploading Phase
- Downloading Phase

Open Nebula is a tool to integrate with different environment, which executes all the process in the frontend of a program. In this, VM needed information or data should be given by cluster nodes. All the clusters connected with front end by physical networks.

A. Registration Phase:

In this phase, clients have to upload a file, viewing a file, changing anything in a file from the cloud server. Whenever request should be given by a client, first it moves on to front node which assigns a VM on cluster. It can handle Maximum number of loads in a request. All the encrypted file type and blowfish and SRNN mechanism are used in VM.

B. Uploading Phase:

In this phase, upload a data in cloud server various steps have to follow by user.

- The client send a request to server (i.e.) front node for authenticate to access.
- After getting authentication rights, the front end, sends the IP number (address) of client to VM against which user was registered.
- The uploaded files are sending by the client, which goes to registered server (VM).
- File should be encrypting by hybrid cryptosystem mechanism.
- Now files are divided into slices.
- Blowfish mechanism is used to encrypting the data (slices) and stored these data in VM data store.
- SRNN mechanism sends these file to the appropriate user and deleted these from server. So authenticated user can view this uploaded file.

C. Downloading Phase:

Some steps are used to download the files. They are

- The client send a request to server (i.e.) front node for authenticate to access.
- After getting authentication rights, the front end, sends IP address of that client to VM against which user was registered.
- The upload the files by client n SRNN private keys used for corresponding n slices.
- It is used to decrypting the encrypted Blowfish keys and the encrypted slices are decrypted by Blowfish keys.
- Then decrypted files are combined to generate original file.
- The decrypted file is downloaded and viewed by client.

VI.BENEFITS OF PROPOSED MODEL

This system provides all the security facility to the client data on cloud server. Blowfish mechanism is used for encrypting the file into slices with minimum time and maximizes throughput for encrypt and decrypt the files from other symmetric algorithms. Security is higher than RSA by SRNN mechanism. The idea of splitting and merging the data concept in cloud is mainly for data security. It makes the remote server more secure, helps the cloud providers to fetch more details from trust of their users.

The various benefits are as summarized:

- Cryptography is used to facilitate authorization of user for accessing each file.
- Secure encryption system is used for file information preserving system on cloud is satisfied.
- The file splitting and merging makes the model impracticable to get attacked.

VII. CONCLUSION

This technique is used to increase the security problem in cloud using hybrid security algorithms using the symmetric key. One difficultly is key secure and accessible by authorize user. Mainly focused on cloud data storage not about travelling of data among user by secure channel. The Encryption Algorithm applicability provides the flexibility. Even the user does not select any encryption

REFERENCES

[1] Data Security and Privacy in Cloud Storage using Hybrid Symmetric Encryption Algorithm Dr. L. Arockiam1, S. Monikandan2 International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 8, August 2013

[2] Data Security and Privacy Protection Issues in Cloud Computing. 2012 International Conference on Computer Science and electronics engineering.

[3] International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 842 ISSN 2229-5518 IJSER © 2013 Survey on Various Techniques for Data Storage Security in Cloud Computing Jahnvi S. Kapadia.

[4] Volume 3, Issue 3, March 2013 ISSN: 2277 128X International Journal of Advanced Research in computer Science and Software Engineering Security in Data Storage and Transmission in Cloud Computing Pradnyesh Bhisikar #1, Prof. Amit Sahu *2

[5] Ramgovind S, Eloff MM, Smith E ,"The Management of Security in Cloud Computing", School of Computing, University of South Africa, Pretoria, South Africa ©2010 IEEE.

[6] Alok Tripathi, Abhinav Mishra," Cloud Computing Security Considerations", IT Division, DOEACC Society, Gorakhpur Centre Gorakhpur, India, 2010, IEEE.