Two Tier Security Scheme under Cloud Computing

Ms. Shivani Harne[1] Ms. Nikita Tayade[2] Ms. Ruhi Bobade[3] Mr. Vivek Chavhan[4]
Prof. N .A. Deshmukh[5]
[5]Professor
[1,2,3,4,5]Department of Computer Science & Engineering
[1,2,3,4,5]PRMIT&R, Badnera, Amravati, Maharashtra, India

Abstract— Cloud computing is rising as a powerful computing tool. The security aspect plays crucial role in cloud, as the decision of shifting to cloud from customer's perspective mainly depends upon privacy of the data and the other benefits they would attain by shifting on cloud storage. The overall emphasis of this project is to conquer security issues in the existing system. We propose a secure cloud-based storage system that stores the data in the cloud efficiently by storing it on multiple cloud instead of storing it on single cloud. It enhances the security of data stored on the cloud.

Key words: AES

I. INTRODUCTION

The word "cloud" often refers to the Internet and more precisely to some datacenter full of servers that is connected to the Internet. However, the term "cloud computing" is a form of internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is an internet based computing which enables sharing of services. It is widely developed technology used in IT industries to provide services like resources, rapid resource elasticity, network access control and platform as per user require. In cloud computing the user data is centralized to the cloud. The user can access the cloud services within the help of mobile devices and internet connection.[1] .With the increasing information that we humans access, the storage requirements to accumulate that information keeps on increasing, it may be a collection of documents, files, movie, software or some songs, the data requirements keeps on increasing day by day. Here it is more important that how we access the big data whether it is for the personal use or professional use. People either prefer using hard drives or even sometimes prefer using compact disks as well, but with the advancement in technology everyone wants access to data on the go, without having the need to carry physical hardware and hence cloud storage requirements fall into place. [6]Cloud storage means storing data online so that we can access it from any place. Nowadays the growth of cloud computing environment is encouraging many organizations to migrate their IT infrastructure to function completely or moderately in the cloud. Though the cloud guarantees a more secure and dependable environment to their clients, the uprightness of information in the cloud might still be a issue of great concern, because of the presence of human blunders. Thus it is a need to take a time from user's side to check the integrity of the data. [2] One of the most huge and normal elements of these system is to increase the security of data stored in cloud. There is a threat of data stolen, misused or theft, as consumers have no control over cloud.

In order to increase the security, the two tier security scheme protects data or file by splitting it into several blocks and storing it into different cloud server positions. Each splited file block is encrypted before it is stored on various locations. That file is kept to be adequate of self-auditing. In case of malicious attack, attacker will not able to retrieve entire file since it is splited & stored on different locations.

Cloud computing has several advantages. People can run their apps and store data remotely. They can have access to data at any time, from anywhere, reduced IT cost and scaling of applications based on traffic from zero to many.

A. Objectives

- To develop a cloud based web application which manages uploaded documents with security.
- To implement AES algorithm for document encryption.
- To develop a multi cloud server for document storage to increase security of data.
- To implement document splitting scheme for security.

II. RELATED WORK

Public auditing scheme allows decrypted sample blocks to external auditor which are in linear combination form. ZHANG Wei [3] describe a new method, which is called as the bit split bit combination data privacy protection method for the data privacy protection which is not depend on the encryption keys performance. To achieve the privacy of data protection for users, the original data broken up by bit split method and uploaded to multiple cloud storages. When users would like to access the original data, they can access by downloading the broken data from the several cloud data storages and access the data only after the suitable bit combination process is completed. To protect the user data privacy without encryption keys management and efficiently reduces the time required for the data privacy protection.

Further Alexandru Butoi, Nicolae Tomai proposed the protocol which is based on a secret sharing scheme [4] in which data is split in best possible chunks, whereas each and every chunk transports a smallest amount of informational content which is relative to the whole informational content of the sets of the data.

Dr.J.Suganthi Ananthi J Archana Proposed a public auditing privacy preserving system for solving the issues related with privacy using Aggregate Signatures [5] on shared data to build authenticators which are homomorphic. It enables public verifier to be able to correct the shared data integrity without retrieving the whole data which may identify each signer on data blocks and kept them private from public verifier.

III. PROPOSED MODEL

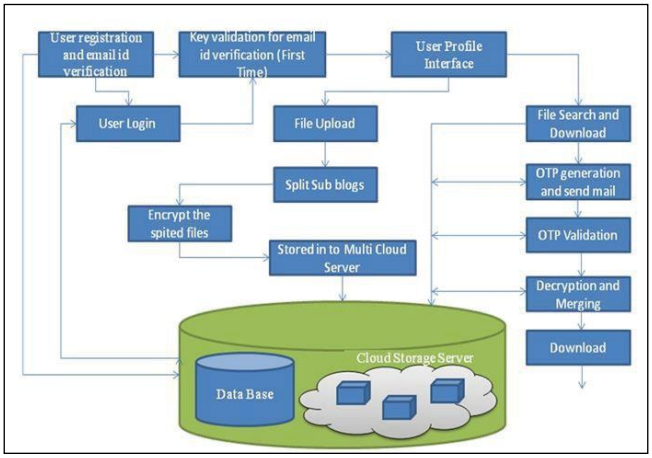

Fig. 1: System Architecture Design

The two tier security scheme provides scattered method with data in the cloud. User can enroll and login into their space. When the user register, email id verification is done. Once the registration process is complete user can login into the application. User profile is created where they have an option to upload and share the data from cloud space. Here we are accessing the two tier idea for putting data into the cloud. The first tier protection is the data or file is splited into several blocks and it is stored into different cloud server positions. In second tier protection each splited file block is encrypted before it is stored on various locations. The shared users can access and make changes in the file on cloud with file owner's acceptance. That file is kept to be adequate of self auditing. Afterwards client required to login and process the file. User can find and download the data, by using security key. The system can allow downloading of data from cloud once the authentication is successful by decrypting and rearrange the splitted blocks from cloud.

The proposed model of this project as shown in the figure 1.1 consists of four main phases as follows,

1) Secret key generation
2) File uploading process
3) Mail alert process
4) File downloading process

AES algorithm is used for file encryption. If user want to download a file then the user need to login the application. If valid user, they have privilege to access our application. If entered file name is available on server it will download page. You have to click download button, and enter the required secret key to download the file. Without secret key it is not possible to download. If owner share the key to user, that user can download file which is stored in encrypted format, it will be decrypted using AES algorithm once user enters the secret key. In case of malicious attack, attacker will not able to retrieve entire file since it is splited & stored on different locations.

A. *Encryption*

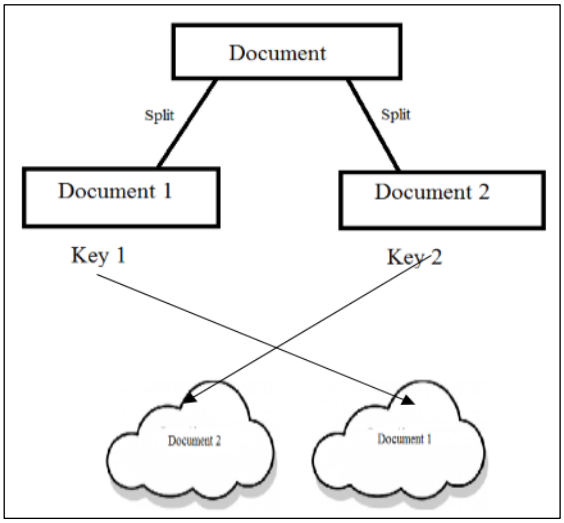

Fig. 2: Encryption Process

When the document is uploaded it is divided into 2 parts. Seperate keys are generated for each part. Each individual part is encrypted using AES algorithm. Each individual part is transferred to two separate cloud. The information about each individual part is stored in database.

B. *Decryption*

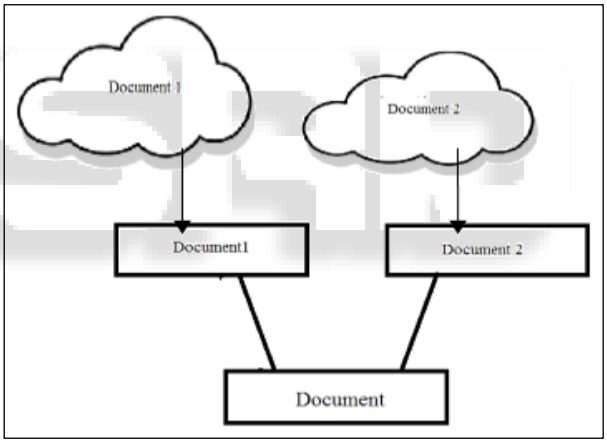

Fig. 3: Decryption Process

To decrypt the document the key of the document is specified and key verification is done. The various parts of document is fetched from various servers. The various parts of document is merged into single document and the complete document is delivered.

1) Key generation:

Key generation is used to generate unique key for every file blocks. When user upload any file on cloud server, system will generate one unique key K using following algorithm.

K=Docid+Docname|0+Date|day+S|@+time|hr

The file will be converted into byte[] array. Then the system will select any random no between 2- 5. The system will divide the byte[] array into N parts as byte1[], byte2[], ….byteN[]. To encrypt file parts, system will generate N secrete keys randomly using following algorithm

– Keys will be combined with K to generate final keys
  - K1=merge K and k1
  - Eg. K=A3jd@12 and k1=He49 then k1=AH3ej4d9@12

- The various parts of bytes will be encrypted using AES algorithm
- The parts will be transferred to other servers randomly

The sequence to parts will be stored in db.

IV. ADVANTAGES

- Scalability: The suggested model uses various tools and techniques that make the cloud-based framework more scalable in comparison with related works. Using a client-based user authentication has decreased the dependency of this process to cloud-based operations considerably and by this decrease, the process of authentication will be more scalable
- Security: By using various tools and techniques during authentication and also data protection processes, security of the suggested model has been improved.
- Efficiency: The process of authentication in the suggested model has been more efficient by establishing logical and reasonable communications between various agents during the process of authentication.

V. CONCLUSION

Two tier security scheme manages the uploading of document with security. The multi cloud servers for document storage increase the security of data the shared users can access and make changes in the file on cloud with file owner's acceptance. In case of malicious attack, attacker will not able to retrieve entire file since it is splited & stored on different locations.

REFERENCES

[1] M.S.Shashi Dhara, "Privacy Preserving Third Party Auditing In Multi Cloud Storage Environment.", IEEE International Conference on Cloud Computing in Emerging Markets (CCEM),pp.1-6,2014.
[2] Juels and B. S. Kaliski Jr, "Pors: Proofs of retrievability for large files," in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 584–597.
[3] ZHANG Wei and SUN Xinwei, "Data Privacy Protection Using Multiple Cloud Storages". International Conference on Mechatronic Sciences, Electrical Engineering and Computer (MEC) Dec 20-22,2013 pp 1768 - 1772. 121C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.
[4] Reza Curtmola and Osama Khan, "MR-PDP: Multiple-Replica Provable Data Possession," Comm. ACM, vol. 14, no. 1, 2011.
[5] M.Pardeshi,Deepali Borade, "Enhancing Data Dynamics and Storage security for Cloud Computing using Merkle Hash Tree and AES Algorithms",International Journal of Computer Applications; Vol. 98, p1 ,Jul 2014.
[6] Syam Kumar P,Subramanian R, "An Efficient and Secure Protocol for Ensuring Data Storage Security in Cloud Computing", International Journal of Computer Science Issues (IJCSI); Vol. 8 Issue 6, p261, Nov2011.

