Enabling Security to Multi-cloud through cryptographic Techniques

P. Sabitha
Research Scholar, O.U.
Hyderabad, Telangana.

Dr. V.B. Narasimha
Assistant Professor, O.U.

Abstract

The cloud computing is considered to be the architecture of the information and technology of the upcoming generation. The use of this cloud computing, which provides benefits like cost efficiency and accessibility of data has been increasing speedily in various organization. The major disadvantages with this cloud computing is associated with security issues like, privacy, integrity and confidentiality of the data, this private data is managed by the third parties whom we cannot trust. We have identified this potential security problem and difficulties in the accessibility of the data while the earlier works ensure remote data integrity. It seriously lacks the security of the data. Hence, the aim here is to ensure privacy and protect integrity and confidentiality of the data and access.

This paper in particular tries to archive privacy, integrity, confidentiality of data stored in the cloud and moving towards Multi-cloud which is a recent origin. We tried to provide security by adopting cryptographic techniques, where we focus on Elliptical curve and Diffie Hellman key exchange protocol for encryption and decryption of Multi-cloud.

Keywords: Integrity, privacy, Confidentality, cryptography

1. Introduction

Cloud computing is an on-demand service that has obtained mass appeal in corporate database. Cloud computing enables companies to consume computer resources like virtual machine (VM), storage, as a utility and maintain the infrastructure [1]. Cloud computing can provide low-cost, high –quality, flexible and scalable services to users [2]. Cloud computing services are infrastructure as a services(IaaS), platform as a services(PaaS), and software as a service(SaaS) to users. Cloud computing can be private cloud, public cloud, and hybrid cloud. Single clouds are more vulnerable to failure of services unavailability and malicious insiders. Many organization adopted to multi-cloud for reducing the failure of services. Multi-cloud is the combination of public, private or managed clouds including service providers [4]. Multi-cloud data system enhances data sharing and greatly helps to the users.

Cloud data storage is used for storage of data which offers an on-demand data services [5]. The main use of data storage is to ensure the integrity of data which are written by user once. Data storage is semi-trusted cloud service providers (CSP) that maintain and operate the outsourced data [6]. Cloud storage may suffer from single point failure and vendor lock-in. Hence, securing the cloud is an important role in cloud environment [7]. The data file and remote data centers have to be given extra security from third party intruders [8]. The existing methods ensured data integrity with availability. The files are available for the other authenticated in the file system[9]. The key exchanges are numeric and it can be easily predicted [10].

1.2 Need of multi-cloud

There is no doubt that Multi-cloud is going to be the future of IT. It provides various benefits when compared to single cloud. Unlike single cloud which provides limited resources and various security issues, Multi-cloud is a “space” with which all resource such as application ,services storage, software, infrastructure etc. can be shared, it provides various benefits to the users by avoids vender Lock-ins, Power of choice,flexability,realibilty and cost and performance optimization. But security is one of the key issues in the cloud world. Majorly trust is the important factors in the cloud. The security issues in the cloud are Integrity, privacy, Confidentiality.

2. Literature Review

Cong Wang., *et al*.,[13] utilized public key based homomorphic authenticator with random masking to achieve privacy-preserving public cloud data auditing system. This method introduced Third Party Auditor (TPA) audit the cloud data storage without demand the local copy of data and no vulnerabilities toward user's privacy data. This method guaranteed that TPA was unable to learn any knowledge about the data content in cloud storage. The disadvantage of this storage method was lack of multiple auditing tasks in a batch manner performed by TDA.

Qian Wang., *et al*.,[14] constructed classic Merkle Hash Tree for blog tag authentication and explored technique called bilinear aggregate signature. The proposed method provided simultaneous public audit ability by bilinear aggregate signature. Data dynamics for remote data integrity check in cloud computing was achieved by existing proof of storage models by manipulating the classic Merkle Hash Tree. The proposed scheme was highly efficient and provably secure. The major disadvantage of the proposed scheme was private keys were not verified by public audit ability. System efficiency was greatly affected by large communication overhead.

Rashmi Jogdand., *et al*.,[15] ensured data integrity with public verifiability and availability. The verifiability method achieved public verifiability by manipulating classic Merkle Hash Tree in multi-cloud. This method assured data availability by adopting DepSky System model for multi-clouds. This multi-cloud storage made file access by transmitting the link as one time download for other users. The files were available for the other authentic users in the file system. The disadvantage was redundancy of the distributed chunks over several servers on the cloud was very high.

Kan Yang and Xiaohua Jia..,[11] designed an auditing framework for data storage in cloud computing. This framework extended to support data dynamic operations and batch auditing for both multiple owners and multiple clouds without using trusted organizer. This method was very efficient, less communication cost and less computation cost and improved the auditing performance. The disadvantage was auditing framework in cloud tends to occupy more memory space.

Kan Yang and Xiaohua Jia...,[12] developed a revocable data access control scheme by multi-authority Ciphertext-Policy Attribute-Based Encryption (CP-ABE) for multi-cloud storage systems. The attribute revocation method achieved both forward security and backward security in cloud system. The revocation method proved that the scheme was highly secured in random oracle model. The multi-authority CP-ABE technique was applied on remote storage systems. The disadvantage of the CP-ABE was storage overhead, especially when the number of ciphertext was large in cloud storage system.

3. Objectives

To provide a decision model, that provides a better security by distributing the data over multiple cloud to the users of the cloud computing.

- To preserve Privacy to the valuable resources, stored in multi-cloud.
- To provide Integrity and Confidentiality to the data, stored in multi-cloud.
- To save the time in Encryption and Decryption technique.

4. Problem Definition

Security plays a major role in the cloud computing environment, Even if the service providers of the cloud computing can offer benefits to the users. The cloud services will get effected by the issues related to internet security, as the cloud services have been built over internet. As a result there arise various security issues like Privacy, Data integrity and Confidentiality to the valuable resources that were stored within cloud, which form the basis of the cloud computing security.

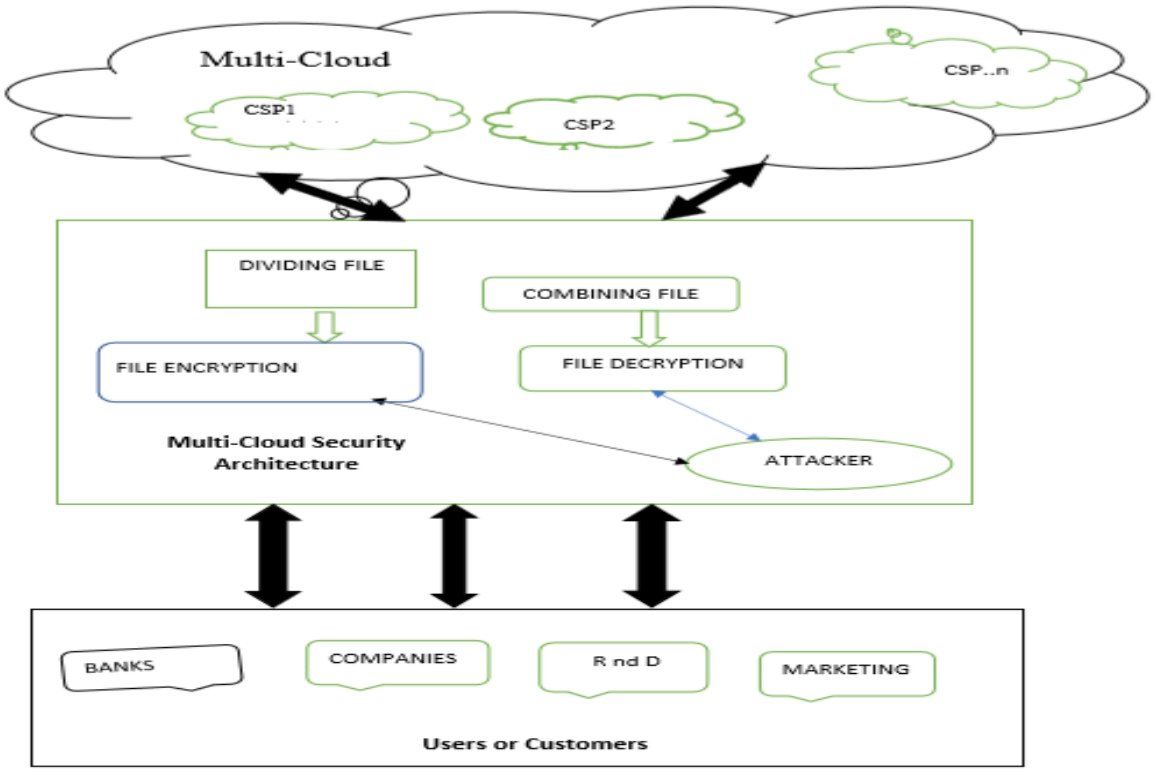
In order to overcome these major problems and make the service accessible, we need to design such a technique to the users with which they avail the services without any distortions. Thus, we can address the problem definition as the concern towards providing three security factors i.e. Privacy, Data integrity and Confidentiality that particularly affect the cloud.

5. Proposed system

The major concern of the cloud computing in the present scenario is the security of the valuable resources, information, data that stored on the cloud. One of the top priority concerns with the storage is privacy, integrity and confidentiality at the un-trusted servers. There is always a risk with the third party with whom we share our private data. Cloud providers should address these issues of privacy, integrity and confidentiality as a matter of high and urgent priority. The cloud computing brings about many issues of challenging designs, which have a great influence on the security and accessibility of the overall system.

In order to solve these problems many schemes were projected under different systems and models. Various design techniques provide the way to overcome some of these risks. There is no single technique which provides solution to all these problems at a time. The proposed solution focuses simultaneously on the three major issues viz., privacy, integrity and confidentiality of the valuable data, stored in the clouds. The proposed solution is designed with certain assumptions to develop the proposed system model as follows.

5.1 Multi cloud Security Architecture



5.2 Architectural Modules

Data Owner - A cloud user named data owner share or upload the file by using the framework interface in addition with Private key and number of file parts to slice the file.

***File Sepa*ration**-The framework divides the file and stored in the cloud provider**.**

File Encryption -Each part of the blocks of file gets encrypted by the framework and gets stored in the multi-cloud storage

Multi-cloud storage-It consists of many storage servers .Encrypted file parts are stored securely.

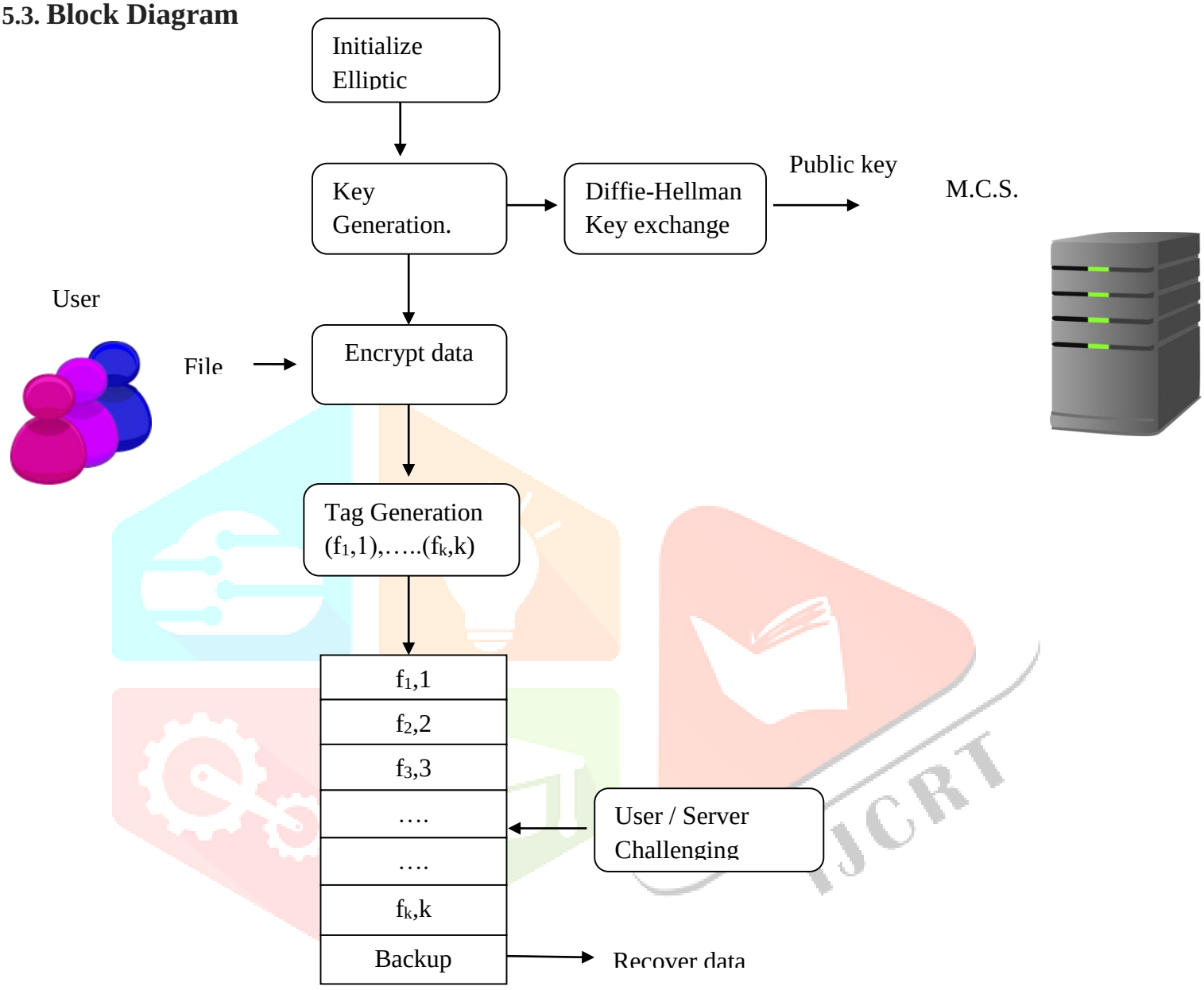
Client- The receiver gets the necessary details from the data owner to download the file

File Decryption- The receiver submit the file name and private key through the framework which in turn searches the file name in all the available storage locations and decrypts the matched file parts.

File Merging- The decrypted file parts are merged to give the whole information to the receiver.

Attacker –Recovers modified file to provide integrity of data

5.3. Block Diagram



we are using cryptographic technique for providing security to Multi-cloud. In the above block diagram ECC curve generates the public key, Private key is a random number. Then the file is divided into blocks and encrypted, when user request for the file, then file is been decrypted by entering the credential for accessing the file. Diffie-Hellman key exchange protocol is employed, which is a method of securely exchanging cryptographic keys over a multiple cloud. For the purpose of reliable and unpredictable generation of keys the elliptic curve model is utilized. The implementation can explained into four phases.

- Initialization phase
- Data Storage phase
- Challenging Phase
- Recovery Phase

5.3.1. Initialization phase

Step 1: Elliptic curve domain parameters (p,a,b,G,n,h) are determined initially to build the cryptography system. From the domain parameters, an elliptic curve will be generated.

Step 2: User will be delegated with private key and public key in the key generation phase. In elliptic curve, a random point is selected for the private key generation for the user. Generated private key is represented as d_i.

Step 3: User generate public key which is represented by Q can be derived from the generator point of curve and the private key as follows

$Q = d_A * G$ …, where G is generator point of curve.

Step 4: In order to attain a secure key transmission with the help of Diffie Hellman Key Exchange, user will share their public keys to the server by satisfying the following condition

$d_A Q_S = d_S Q_A$ ……, where d_A, d_S are the private keys of user and server.

- Q_A,Q_S are the public keys of user and server

5.3.2. Data Storage phase:

Step 1: When a user sends a file to the data storage, the files are converted into number of blocks which is in the form of metadata.

Step 2: The blocks of data can be converted into a number of blocks by using tag generation. The length of tag generation will be based on number of multi-clouds available.

Step 3: Blocks will be stored in mult-icloud storage according to the number of corresponding tag generation.

5.3.3. Challenging Phase:

Step 1: When user/server monitor any modification happened in the stored blocks of data without user authentication it will send a challenge.

Step 2: For a received challenge, the storage will generate a proof messages and forward it to user/server.

Step 3: The proof message is verified from the user/ server side for any modification in data. If any of the block modifications happened without user authentication, then it will recover the lost data.

5.3.4. Recovery Phase:

In this phase, the client or owner checks the integrity of file blocks by selecting the subset of those blocks. The data integrity verification is done by data owner by challenging the cloud provider itself. The attacker step stores multiple user processes and transactions into the storage. The abstract information about the cloud hacking is recorded in the cloud storage . The user processes and administrator process transactions are indicated in this phase, attacker phase includes Modifying file, deleting file, and Uploading file operations. This provides integrity, privacy and Confidentiality and secure distribution of data sharing in multi-cloud

6. Conclusion

Cloud security is still a major issue in cloud computing environment, although the use of it is rapidly increasing. The clients do not want to lose or tampered their private information. Impact, the loss of services accessibility has caused many problems for a large number of clients in the recent times. In this particular situation, the multi-cloud plays a vital role in providing solutions to this problems by protecting privacy and providing integrity and confidentiality to the data, since the data is stored in multiple cloud servers, any number of contends can simultaneous request for the

services and can easily avail them without any distortion. The proposed solutions will integrate these goals and intactness can be checked without the intervention of the third party. Our technique is deliberately design to meet these three important goals with efficiency.

7. Reference

[1] Subramanian, K., and F. Leo John. "Dynamic Data Slicing in Multi Cloud Storage Using Cryptographic Technique." *Computing and Communication Technologies (WCCCT), 2017 World Congress on*. IEEE, 2017.

[2] Mehta, Shital, and Gaurang Panchal., "File distribution preparation with file retrieval and error recovery in cloud environment", *International Conference on Information and Communication Technology for Intelligent Systems*. Springer, Cham, 2017.

[3] M. A. AlZain, E. Pardede, B. Soh, and J.A. Thom, "Cloud computing security: from single to multi-clouds" , In *System Science (HICSS), 45th Hawaii International Conference on* IEEE, pp. 5490-5499, 2012.

[4] Yang, Kan, and Xiaohua Jia., "Attributed-based access control for multi-authority systems in cloud storage", *Distributed Computing Systems (ICDCS), IEEE 32nd International Conference on*., 2012.

[5] Wu, Xianglong, Rui Jiang, and Bharat Bhargava., "On the security of data access control for multiauthority cloud storage systems", *IEEE Transactions on Services Computing* vol. 10, no. 2, pp. 258-272, 2017.

[6] Agarkhed, Jayashree, and R. Ashalatha. "An efficient auditing scheme for data storage security in cloud", *Circuit, Power and Computing Technologies (ICCPCT), International Conference on*. IEEE, 2017.

[7] J. K. Liu, K. Liang, W. Susilo, J. Liu, and Y. Xiang, "Two-factor data security protection mechanism for cloud storage system", *IEEE Transactions on Computers*, vol. 65, no. 6, pp. 1992-2004, 2016.

[8] K. M. Abbasi, I. ul Haq, A.K. Malik, and T.A. Khan, "Data security in cloud as a service for access control among multilevel users", In *Communication Technologies (ComTech), International Conference on* IEEE pp. 168-173, 2017.

[9] R. M. Jogdand, R. H. Goudar, G. B. Sayed, and P.B. Dhamanekar., "Enabling public verifiability and availability for secure data storage in cloud computing", *Evolving Systems*, vol.6, no. 1, pp. 55-65, 2015.

[10] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage" , *IEEE transactions on computers*, vol. 62, no. 2 , pp. 362-375, 2013.

[11] Yang Kan, and Xiaohua Jia.,"An efficient and secure dynamic auditing protocol for data storage in cloud computing", *IEEE transactions on parallel and distributed systems*,vol. 24, no.9, pp. 1717-1726, 2013.

[12] Yang Kan, and Xiaohua Jia., "Expressive, efficient, and revocable data access control for multi-authority cloud storage", *IEEE transactions on parallel and distributed system*, vol. 25, no. 7, pp. 1735-1744, 2014.

[13] C. Wang, Q. Wang, K. Ren, and W. Lou.,"Privacy-preserving public auditing for data storage security in cloud computing", In *Infocom, proceedings IEEE* . pp.1-9, 2010.

[14]Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li.., "Enabling public auditability and data dynamics for storage security in cloud computing", *IEEE transactions on parallel and distributed systems*, vol. 22, no. 5, pp. 847-859, 2011.

[15] R.M. Jogdand., R.H. Goudar, G.B. Sayed, and P.B. Dhamanekar., "Enabling public verifiability and availability for secure data storage in cloud computing", *Evolving Systems*, vol. 6, no. 1, pp. 55-65, 2015.