JCSE International Journal of Computer Sciences and Engineering Open Access
Short Communication Volume-2, Issue-8 E-ISSN: 2347-2693

# Secure Cloud Data Sharing Using Key-Aggregate Cryptosystem

Ms.Minimol Mathew[1*], Mrs. Sumathi D.[2], Ms.Ranjima P.[3], Mr.Sivaprakash P.[4]

[1*,2,3,4] Dept of CSE, PPG Institute of Technology

www.ijcseonline.org

Received: 11/07/ 2014 Revised: 22/07/ 2014 Accepted: 12 /08/ 2014 Published: 31 /08/ 2014

***Abstract* -** Cloud computing is used to store and share data by anyone from anywhere in the world. It provides scalable and on demand self services. The cloud data expect maximum security at rest state as well as at transit state. Service providers provide security to the data in the cloud and the data owner also uses some cryptographic techniques for data security. They may use symmetric cryptography or asymmetric cryptography. If the data owner use same cryptographic key for all data files, they cannot share the partial amount of data files. Because of that the owner using the separate encryption/ decryption keys for each file in the cloud. Here to provide security and avoid network burden, the data owner can aggregate all decryption keys into a single key. This aggregate key can decrypt any subset of delegated cipher text blocks.

***Keywords*** – Secure data sharing; TPA; Key aggregate cryptosystem.

## I. INTRODUCTION

Cloud computing is used to provide the services such as sharing software, resources etc. The clouds can be classified as private, public and hybrid. Public cloud allows any client to access data and the private cloud allows only authorized people to access the data. Hybrid cloud is the combination of public and private cloud. It provides scalable and on demand self service. The users of cloud can access the services through networked devices such as desktop computers, laptops, tablets etc. Cloud storage stores the digital data in virtual pools. The physical storage units are managed by cloud service providers.

The cloud data expects more security in its both rest state and transit state. The cloud security is another form of computer security. Because of reputation, the service provider should not inform to data owner about security violation. So the owner uses cryptographic techniques, digital signature, and service from third party auditor.

## II. SECURITY IN CLOUD DATA STORAGE

Cloud storage is used to provide effective data storage and sharing without the burden of local data storage. A cloud service provider provides public and private services. In public service, anyone can access services from anywhere. But in private cloud, only authorized people can access service. Organizations need to provide security to each file, because they use private cloud services.

[1]Service providers have their own authentication methods. They need only one time registration and registrar keeps all signatures. If users want to access the CSP, they first retrieve the signature from registrar and CSP verifies zero knowledge proof. After the successful completion of verification user can access data. But if registrar is not in online user cannot be reach cloud.

To avoid this problem, using simple privacy preserving identity management. In this method, each group of employees has a single signature. A group manager (GM) issues credentials. Any member of group can sign for their group. Here registrar acts as a GM. Certificate consist of group sign and message append to this group sign. They hide some attributes if needed. There are three types of attributes such as sensitive personal information, service specific attributes, irrelevant attributes. Registrar needs to know who are concerned with a selected subset of attributes. There is no need of contacting the registrar before every authentication.

[2] A cloud storage unit consist of cloud user who is stored data and retrieve data from storage unit, the cloud server (CS) managed by cloud service provider (CSP) to provide data storage service. In cloud, there are so many security issues and attacks performed by unauthorized people. Because of their reputation, the service provider decided to hide the data corruption. So we use a third party auditor (TPA) to provide integrity. TPA keeps information about stored data. If any integrity breach happened in data, it informs to user and service provider. TPA has reliable and independent performance. TPA verifies the correctness of cloud data without retrieving the copy of whole data and reduce online burden. TPA cannot derive the stored data by using the collected data to verify integrity. Different users may be delegated to TPA. Individual auditing of these growing task not only increase cost and network burden. To avoid this problem the TPA performs the multiple auditing in batch manner.

To provide the privacy preserving public auditing, the TPA handles different auditing for different users at a time. Individual auditing is inefficient. To given n number of delegations for n number of users, TPA batches these tasks together and performs audit at one time. To achieve this, aggregates n verification equations into one. Batch auditing helps not only implement the auditing simultaneously but also reduce auditing cost. The verification equation holds when all responses are valid. If there is any single response in batch auditing getting invalid that should be fail. The probability of failure is very higher. Practically this need less expensive for the performance of batch auditing. It needs only modular exponentiations and multiplications. When batch auditing fails, recursive binary search approach used to sort the invalid responses from the batch audit.

Most of the organizations are using cryptographic techniques to provide the security. It may be public key encryption or private key encryption. In these methods the key management is an important problem. [3] If the access classes are represented in the hierarchical structure, key management scheme key assign to the class and it distributed to users. User can be access the particular class and its descendant classes. The hash functions are used for a node to derive the keys for descendant classes from its own key. The key efficiency can be measured by time taken to derive the keys for the descendant classes in hierarchy. The best scheme required only bit operations linear in the distance between the nodes. The updates are performed locally, it should not be distribute to the ancestors and descendants of that class.

Another way to provide security is digital signature. Digital signatures are used to provide integrity. [4] Aggregate signatures are related to multi signatures. An aggregate signature scheme is a digital signature which supports aggregation. Given n signatures on n distinct messages from n distinct users, it is possible to aggregate all these signatures into a single short signature. This single signature will convince the verifier to verify the n number of original messages. Many real-world applications involve signatures which are many different messages generated by many different users. Aggregate key schemes use encryption signature methods. In this method the sender signs on a message and encrypts that using third parties public key. Receiver verifies the message that encrypted message is whether valid or not.

Let us consider N number of users and each member has a signing key pair of public key and secret key. Each user produces a signature on messages. Then aggregate these keys into a single aggregate key by aggregate party. The aggregate party has the public keys for the messages but not any private keys. The length of aggregate signature is similar to the length of single signature. Suppose sender wants to show receiver that the signed a message, but does not want receiver to possess the signature of that message. Sender can achieve this by encrypting the signature using the public key of a trusted third party, and sending this to receiver along with a proof that given a valid encryption of signature. Receiver can verify that sender has signed the message, but cannot deduce any information about that signature. If data owner is unable or unwilling to reveal their signature, user can ask the third party to reveal owner's signature.

In many situations the data owner provides the separate access control to each user. In this time they need multi cryptographic keys. [5] Because of the need of different cryptographic keys owner should be generate some scheme to provide correct key to each user. This scheme should be at low cost. If there are N keys are provided to the users these keys are related to each other. The keys are generated from a single key is known as master key. Each master key space consists of $2^N$-1 when providing N number of keys. Development of master key system is based on modular exponentiation. The weakness of master key system affects the whole cryptographic keys.

To avoid attacks in master key, factors of master key must be kept in secret otherwise discard when it is no need of expansion. To keep information about master key, create a committee. The committee members only know about the details of master key. But any one does not have complete knowledge to derive the master key.

The data owner should send the message with a key, if the data owner wants to share the data which are encrypted by a cryptographic key. But if data owner have different blocks of data and owner needs to partially share the data to user, they can be using the separate cipher text keys. But these key's secure storing and transformation is difficult. And the keys must generate from some common scheme. To overcome these problems, use the master key scheme with key aggregation [6]. Secret keys for each cipher text can be derived from the master key. Each cipher text has an identity number known as class. And aggregate cipher text keys into single key. And send messages with aggregate key and set of identity number of each cipher text to user. The size of aggregate key is similar to the size of cipher text key. User decrypts this message by using the aggregate key. If the cipher text identity number is not present in the identity number set given by the sender, the decryption fail.

| Ref Number | Security Method | Signature | Master Key | Aggregate Key |
|---|---|---|---|---|
| [1] | Group signature | Yes | No | No |
| [2] | Batch auditing by TPA | - | No | - |
| [3] | Hierarchical key structure | No | No | Yes |
| [4] | Signed message with public key encryption | Yes | No | YES |

| | | | | |
|---|---|---|---|---|
| [5] | Encryption with master key | No | Yes | No |
| [6] | Encryption with master key and Decrypt with aggregate key | No | Yes | Yes |

**Table1**. Comparison between different cloud data security methods

## III. CONCLUSION

We have so many methods to provide the data security in cloud such as using TPA, digital signature, encryption/decryption methods etc. In encryption methods, the key management and transformation is difficult. To overcome these problems we have to use the master key to generate the number of keys for different blocks of data and aggregate key to transfer the group of cipher text keys. The size of aggregate key is same as that of cipher text keys. It will reduce the network burden during key transformation.

## IV. REFERENCE

[1] S.S.M. Chow, Y.J. He, L.C.K. Hui, and S.-M. Yiu, "SPICE- SimplePrivacy-Preserving Identity-Management for Cloud Environment," Proc. 10th Int'l Conf. Applied Cryptography and Network Security (ACNS), vol. 7341, pp. 526-543, 2012.

[2] C. Wang, S.S.M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362-375, Feb. 2013.

[3] F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," Proc. Information Security and Cryptology (Inscrypt '07), vol. 4990, pp. 384-398, 2007.

[4] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," Proc. 22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '03), pp. 416-432, 2003.

[5] G.C. Chick and S.E. Tavares, "Flexible Access Control with Master Keys," Proc. Advances in Cryptology (CRYPTO '89), vol. 435, pp. 316-322, 1989.

[6] Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage," in *Parallel And Distributed Systems*, VOL. 25, NO. 2, pp. 468-477, 2014

[7] Thamil kumaran V.C , Chithra Mol C.R , Sai Prasath, "An Impact of Implementing Various Cryptographic Techniques Efficiently in a Public Centric Cloud", Vol 4, Issue 4, 83-86

[8] Jaydip Sen, "Security and Privacy Issues in cloud computing", Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA

[9] Bharat Bhargava, Anya Kim,YounSun Cho "Research in Cloud Security and Privacy"

[10] http://en.wikipedia.org/wiki/Cloud_computing.

[11] L. Hardesty, Secure Computers Aren't so Secure. MIT press, http://www.physorg.com/ news176107396.html, 2009.

[12] B. Wang, S.S.M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security- Mediator," Proc. IEEE 33rd Int'l Conf. Distributed Computing Systems (ICDCS), 2013.

[13]http://en.wikipedia.org/wiki/Cloud_computing_security