Development of Novel Encryption for Secured Data Sharing

T. Dhivya Bharathi[1], Dr. S. Sivananaithaperumal[2], V. S. Krithikaa venket[3]

P.G.Scholar,Department of I.T.,Dr.Sivanthi Aditanar College of Engineering,TamilNadu,India
Assistant Professor,Department of I.T.,Dr.Sivanthi aditanar College of Engineering,TamilNadu,India
P.G.Scholar,Department of I.T.,Dr.Sivanthi Aditanar College of Engineering,TamilNadu,India

Abstract**—** *In cloud storage the data sharing is important one. Key-aggregate cryptosystem produce constant size cipher text . That is very efficient delegation rights of decryption for any set of cipher text are possible. Any set of secret keys can be aggregated and make them as single key, which groups all the key by making it a aggregate key. This aggregate key can be sent to the others for decryption of cipher text set and remaining .Encrypted files outside the set are remains confidential. Cloud storage could provide secured data sharing.*

Keywords**— Cloud storage, key aggregate cryptosystem, secret key, encryption, decryption**.

I. INTRODUCTION

Cloud storage is used for storing the multiple data and it is storing the data off-site to the physical storage. It maintained by third party. The third party responsible for keeping data available and accessible. Instead of storing data and any other information to any other local storage, we store the data to remote storage because it is accessible at anytime.

Data sharing is one of the major activity in cloud storage, because an user can access the data from anywhere and multiple user can share their data from one to another.

Cryptography technique contain two major ways.

1. Symmetric key encryption
2. Asymmetric key encryption

1. Symmetric key encryption is nothing but single key is used for encryption and decryption.

2. Asymmetric key encryption is nothing but different keys are used for encryption and decryption.

Public key - Encryption
Private key - Decryption

Consider Alice put her data that may be photo or any other information and she does not want to expose her data to everyone. Due to data leakage possibilities that means chances available to accessing her data by unauthorized. So she encrypt all data with her own key before uploading to the server. If Bob ask her to share some particular data then Alice use share function. There are two ways:

1. Alice encrypt all her data with single secret key and share that secret key directly with the Bob.
2. Alice can encrypt data with distinct keys and send Bob corresponding keys via secure channel like mail, message.

Best solution from these two Alice encrypt data with distinct keys and send Bob corresponding key and the key send via secure channel as mail or message.

II. RELATED WORK

SYMMETRIC KEY ENCRYPTION

Benaloah et al. [2] explained an encryption method which is proposed for transmitting lot of keys in multiple network[3]. In this method select two prime number p and q. A master key is chosen at random and every distinct prime number has been achieved with associated class. These prime number store in the public system parameter. Afterthat a constant size key is generated as well as generated access rights for S. This method is used to generate a secret value rather than a pair of public/secret keys, by using this method to reduce the key size of symmetric key encryption.

III. KEY AGGREGATE CRYPTOSYSTEM

Key aggregate cryptosystem is nothing but encrypt using public key, identifier of ciphertext is also known as class. Ciphertext contain different classes. A master secret key is used to maintain the master secret holds by key owner. Master secret key is used to extract secret keys from different classes ,the extracted key have an aggregate key which is as compact as secret key for each and every single class.

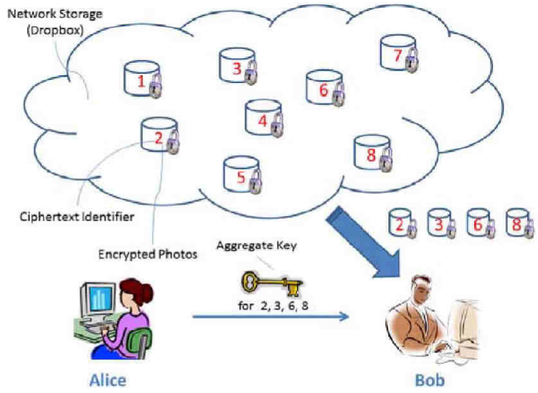

Fig. 1. Exampl of using KAC data sharing

From this diagram Alice put her photo or data to the network storage. Bob ask her to share some photo,Alice encrypt all data using her secret key that may be public key and send aggregate key of set of secret key to Bob.Bod extract data using aggregate key.

IV. FRAMEWORK

Key aggregate encryption contain Setup, KeyGen, Encrypt, Extract, Decrypt.

1. Setup : The data owner establish public system parameter through setup.
2. KeyGen : It is used to generate public and master secret key pair and it is executed by data owner.
3. Encrypt : It is executed by data owner for message and index which is compute ciphertext.
4. Extract : It is used to extract the particular set of ciphertext classes and its also exacuted by data owner.
5. Decrypt : It is executed by a delegate who got , an aggregated key generated by Extract. On input, set ,an index denoting the ciphertext class belongs to and output is decrypt result.

V. SHARING DATA USING KAC

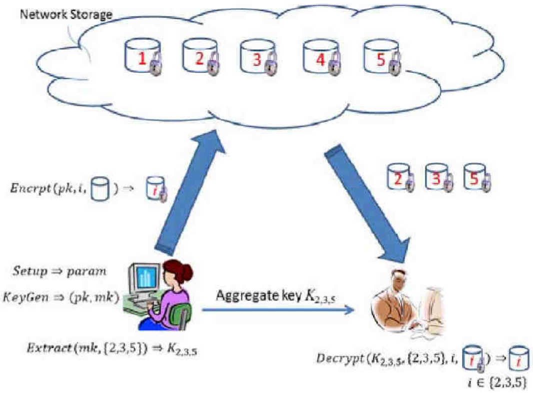
Network Storage
1
2
3
4
5
Encrpt(pk, i,) → i
2
3
5
Setup ⇒ param
KeyGen ⇒ (pk, mk)
Aggregate key $K_{2,3,5}$
Extract(mk, {2,3,5}) ⇒ $K_{2,3,5}$
Decrypt($K_{2,3,5}$, {2,3,5}, i, i) ⇒ i
i ∈ {2,3,5}

Fig. 2. Data sharing using KAC

This diagram shows how to share data using key aggregate concept.A canonical application of KAC is data sharing. The key aggregate property is useful when we expect delegation to be efficient and flexible. In this method used to avoid unauthorized access due to providing aggregate key. Data sharing using KAC, Figure 2. Suppose Alice wants to share her data m1,m2………..,mn on the server. Alice first perform setup to get param and used KeyGen to get the public/master key pair. Encrypted data are uploaded to the server and decrypt the extract data. Finally Bob receive their original data using KAC.

VI. CONCLUSION

KAC concept is used for sharing the information in secure manner. Public key cryptosystem support extract the original data from the cloud storage. And also used to transfer the data very securely.It also used to avoid unauthorized access.

REFERNCES

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

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

[3] 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.

[4] 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.

[5] S.S.M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R.H. Deng, “Dynamic Secure Cloud Storage with Provenance,” Cryptography and Security, pp. 442-464, Springer, 2012.

[6] 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.

[7] M.J. Atallah, M. Blanton, N. Fazio, and K.B. Frikken, “Dynamic and Efficient Key Management for Access Hierarchies,” ACM Trans. Information and System Security, vol. 12, no. 3, pp. 18:1-18:43, 2009.

[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,” Proc. ACM Workshop

Cloud Computing Security (CCSW ’09), pp. 103-114, 2009.

[9] 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.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,” Proc. 13th ACM Conf. Computer and Comm. Security (CCS ’06), pp. 89-98, 2006.