ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

Sharing Secured Scalable Data in Cloud Environment Using Key Aggregate Cryptology

Poral Nagaraja[1], Ashwini Hongal[2]

Associate Professor, Dept. of CS&E., S.J.M. Institute Technology, Chitradurga, Karnataka, India[1]

M Tech Student, Department of CS&E, S.J.M. Institute of Technology, Chitradurga, Karnataka, India[2]

ABSTRACT: Cloud computing is a recently developing technology which can be used to access and store data easily. Cloud storage will provide good reliability and lowest cost. Its functionality is sharing data with other users securely, efficiently and flexibly in cloud environment. We introduce a special type of public key encryption called as Key-Aggregate cryptosystem (KAC). In KAC user encrypts message with public key and also with an identifier of cipher text. In KAC any set of secret keys can be aggregated and made them as single key.

KEYWORDS: Cloud Storage; Encryption; Decryption; Key Aggregate Cryptosystem (KAC)

I. INTRODUCTION

Cloud Computing is the emerging technology now a day's which is being followed by so many organizations throughout the world [2]. Therefore, we have to provide security for the user data, which is going to be stored in the cloud over different, sever throughout the world. Using cloud storage, users can remotely access and store their data and enjoy the on-demand applications and services from cloud computing resources. The users should be able to use the cloud storage as if it is local, without worrying about the protection of data integrity [3].

In Cloud computing technology, users can share their data through different virtual machines but data will be stored on single physical machine. But the thing is user don't have control over the physical machine and outsourced data. The need is to share data securely among users. The cloud service provider and users authentication is necessary to make sure no loss of user data. Providing Privacy in cloud storage is an important function to make sure that the users identity is not exposed to everyone.

Cryptography technique helps the data owner to share the data to store in a safe way. So user encrypts data with the help of encryption keys and uploads on server. Different encryption and decryption keys are generated for different data. At user side by using decryption keys the data will be decrypted. Only those set of decryption keys are shared so that the selected data can be decrypted. Here a public-key cryptosystem generates a constant size cipher text so as to transfer the decryption rules for number of cipher text. In KAC, user can collect a set of secret keys and make them as a single key of small size. This combined aggregate key can be securely sent to others or to be stored in a smart card.

Cryptography technique is divided in two ways: one is symmetric key encryption & second one is asymmetric key encryption. In symmetric key encryption, same keys are used for both encryption and decryption where as in asymmetric key encryption, different keys are used; public key for encryption and private key for decryption. In our approach, we use asymmetric key encryption, which is more flexible. This is shown in the Fig 1.

Suppose, X stores all her private data on Dropbox and she doesn't want to expose private data to everyone. Due to data leakage possibility, she does not trust on privacy mechanism provided by Dropbox. Before uploading data on to the server, she encrypts all the data. If Y asks her to share data, then X uses share function of Dropbox. But now the problem is sharing the encrypted data. There are two ways for her to share data: 1) With single secret key, X encrypts data and shares secret key directly with Y. 2) X encrypts data with distinct keys and share corresponding keys to Y.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

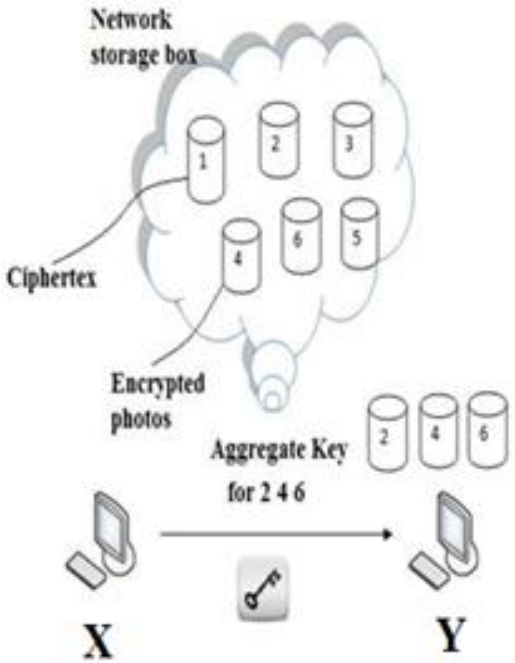

Fig 1: File Sharing Between X and Y

In the first method, the X's secret data will be leaked to the Y. In the second method, the number of generating secret keys will be increased as per the number of files she wants to share, which is expensive and requires more space to store these secret keys. Hence, the best solution for the above problem is, X encrypts data with distinct public keys, shares only single (constant size) decryption key. The decryption key is sent via secure channel and this key should be kept secret.

II. RELATED WORK

In [2] one of the top seven cloud security threats is Identity security and privacy. There are a few identity management solutions proposed as the solutions for these problems. However, none of these can satisfy all desirable properties. In [3] Cloud Computing is the very popular technology. Now a day's cloud is being followed by so many organizations in the world. Therefore, we have to provide sufficient security for the stored data; Encryption will be a good technique in protecting data on the cloud. In [5] one concern in using cloud storage is that the sensitive data should be confidential to the servers which are outside the trust domain of data owners.

III. PROPOSED FRAMEWORK

In this paper, we proposed that how to protect users' data privacy with cryptographic schemes, which are getting more versatile and often involve multiple keys for a single application. Here we consider how to combine secret keys in public-key cryptosystems which support delegation of secret keys for different cipher text classes in cloud storage. The user can always get an aggregate key of constant size. KAC approach is more flexible than hierarchical key assignment approach which saves spaces if all key-holder users share a similar set of privileges.

IV. RESULTS AND DISCUSSIONS

The simulation study includes the following modules. This is shown in Fig 2:

1. Setup Phase
2. KeyGen Phase

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

3. Extract Phase
4. Encrypt Phase
5. Decrypt Phase

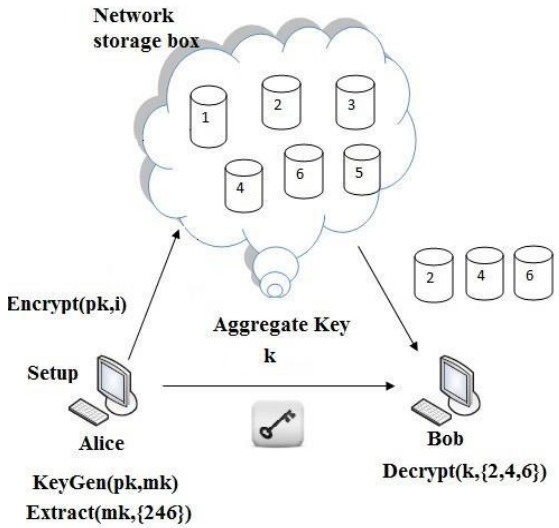

Fig 2: Data Sharing in Cloud storage Using KAC

1. Setup Phase: This phase is executed by data owner. This takes input as security level parameter and number of cipher text classes 'n', it outputs the public system parameter 'param'.
2. KeyGen Phase: This phase is executed by data owner to generate the public or the master key pair (pk, mk).
3. Encrypt Phase: This phase is executed by any user who wants to encrypt his data. The function Encrypt (pk, m, i) takes input as public parameters pk, a message m, and i denoting cipher text class. The algorithm encrypts message m and produces a cipher text C.
4. Extract Phase: This phase is executed by data owner for delegating the decrypting power for certain set of cipher text classes and it outputs the aggregate key denoted by K.
5. Decrypt Phase: This phase is executed by user who has authorities to decrypt message.

Table 1: Comparison between Existing System vs. Proposed System

Method	Existing System	Proposed System
Technique	Key-Policy Attribute-Based Encryption (KP-ABE)	Key Aggregate Cryptosystem (KAC)
Key Used	Symmetric Key	Asymmetric Key
Size Of The Key	constant-size decryption key	constant-size decryption key
Relationship between Classes	Required	Required

V. CONCLUSION AND FUTURE WORK

Sharing data flexibly and securely is the main issue in cloud computing. Users prefer cloud to upload their data with different users. Uploading of data to server may lead to leakage of private data of user to everyone. Encryption is the best solution, which is provided to share selected data with desired users. Sharing of decryption keys in secure way plays important role. Public-key cryptosystems provide delegation of secret keys for different cipher text classes in

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 5, May 2015

cloud storage. The delegate gets securely a constant size of an aggregate key in order to maintain limited number of cipher text classes.

REFERENCES

1. Cheng-Kang Chu ,Chow, S.S.M, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng , ―Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storagel, IEEE Transactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year: 2014.
2. S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment," in Applied Cryptography and Network Security – ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.
3. L. Hardesty, "Secure computers aren't so secure," MIT press, 2009, http://www.physorg.com/news176107396.html.
4. 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, 2013.
5. B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.
6. S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng, "Dynamic Secure Cloud Storage with Provenance," in Cryptography and Security: From Theory to Applications - Essays Dedicated to Jean-Jacques Quisquater on the Occasion of His 65th Birthday, ser. LNCS, vol. 6805. Springer, 2012, pp. 442–464.
7. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proceedings of Advances in Cryptology - EUROCRYPT '03, ser. LNCS, vol. 2656. Springer, 2003, pp. 416–432.