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

Secured Data Sharing In Cloud through Key Aggregation

[1]Aruna Kumara B, [2]Aravinda Thejas Chandra

[1]PG Scholar, Dept. of CSE, SJC Institute of Technology, Chickballapur, Karnataka, India

[2]Associate Professor, Dept. of CSE, SJC Institute of Technology, Chickballapur, Karnataka, India

ABSTRACT: This paper demonstrates the sharing of data in cloud in a safety and unique way. The data sharing in cloud is a requisite functionality and providing security to this data during data sharing. It is an important and essential functionality, because the data might be susceptible to privacy and security issues which will minimizes the efficiency. The present work guarantees solutions to above concerns such that efficiency, privacy and security during sharing of data. A new public key encryption called key aggregation technique is discussed in this work. Key aggregation technique produces constant size ciphertexts, so that decryption of any set of ciphertexts is possible. Here, the individuals can aggregate any number of secret keys into a single one by holding the power of all keys. One who holds the aggregated key can share the key for accessing of files by maintaining the confidentiality of other files which he wouldn't like to share. This aggregated key can be sent to others for decryption of ciphertext sets.

KEYWORDS: cloud storage, key aggregation, data sharing, master secret key.

I. INTRODUCTION

In recent years cloud storage is a very popular storage system. Cloud storage is nothing but storing of data on cloud which is usually maintained by third party. It is highly fault tolerant through redundancy and distribution of data. Here third party is the one who is responsible for keeping of data available, accessible and physical environment should be protected and running at all time. It is used as core technology for many services.

While considering about privacy of data, we cannot completely depend on the authentication technique, because unexpected privilege will expose all data. So, encrypt the data before uploading it onto the cloud with the data owner's key. We know that data sharing is an important functionality in cloud storage. For instance an organization may let their employees to access some portion of sensitive data. Here, the challenging task is how to share encrypted data. In traditional way users can download the encrypted data from storage, decrypt it and send it to others for sharing, but this loses the importance of cloud storage.

There are two major ways in cryptographic technique – 1. In Symmetric key encryption, same key is used in both encryption and decryption. 2. In Asymmetric key encryption different keys are used, shared key for encryption and secret key for decryption. Asymmetric key encryption is more flexible and suitable to our approach.

Assume that Sita puts all her private data on Amazon and she does not want to expose all her private data to everyone. Due to the possibility of leakage of data, she is not feeling safety of data by the privacy mechanism provided by Amazon. So she encrypts all data before uploading onto the cloud server. If Ram asks her to share some data which is related to him, then Sita use the share function of Amazon. But, here the problem is how to share encrypted data. There are 2 traditional ways, - 1. Sita encrypts all data with single secret key and shares it directly with the Ram. 2. Sita encrypts data with different keys and sends Ram the corresponding keys. In first approach, all the private information will expose to Ram, which is inadequate. In second approach, number of keys will be increased as many as the number of files increased, which may be thousand or lacks sometimes. Transferring of these keys requires a secure channel which can be expensive.

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

So, the solution for the above problem is Sita encrypts her data with distinct public keys, but sends single decryption key of constant size to Ram. This single key is generated by aggregating all the keys by encompassing the power of all keys which supports flexible delegation in the sense that any subset of the ciphertexts is decryptable [1].

RELATED WORK

In the "Attribute Based Encryption" approach, a new scheme is developed for encrypted data sharing using cryptosystem. In this approach an attribute will be allocated to each ciphertext, and the ciphertext will be decrypted by master – secret key holder by extracting secret key for policy of these attributes. For instance, consider the private key for the policy (2v4v7v9), here an individual can decrypt ciphertexts which are tagged with class 2, 4, 7 or 9. This paper deals with collusion resistance but size of the key increases with respect to the number of attributes in the sense size of the ciphertext is not constant [2].

Benaloh et al developed a scheme which worked on patient controlled encryption. It assures privacy of e – records. In this paper an efficient system is built which allows patients both to expose and access rights with others and to search for the records [3].

Identity Based Encryption (IBE) is a scheme of shared – key encryption. Here, the shared key of a user will be set as an identity sting of the user. Here, secret key generator is a trusted third party who holds master – secret key. In this approach a secret key will be issued to each user by the trusted party. Encryption of original data takes place by considering the identity of the user and public parameter. The receiver will decrypt the ciphertext by his own secret key. In this scheme a single shared key is used to decrypt many number of ciphertexts encrypted with distinct public keys which are close in certain metric space, but it won't suitable when the identities are selected arbitrarily [4] [5].

II. ARCHITECTURE

The proposed system architecture is an efficient and flexible shared – key encryption approach. In this approach a powerful decryption key is developed, which allows any number of ciphertexts can be decryptable without increasing the size of the decryption key with respect to the number of files increased.

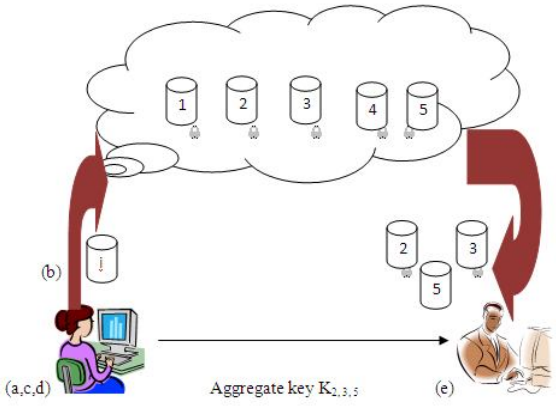

Figure 1: System Architecture

In this approach, users encrypt original data by using shared key and an identifier of ciphertext called class. In this way ciphertext are again classified into different classes. The owner of the data holds a key called master – secret key. This master secret key is used to extract secret keys of all distinct classes into a single key called aggregated key which has the power of all keys. By this solution, Sita can directly send the aggregated key to Ram via a secured channel. Now Ram can download the encrypted data from Sita's Amazon space and then decrypt the encrypted data by the aggregated key. This scenario is depicted in Figure 1.

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

First (a) a data owner will register at an untrusted cloud server. Next (b) data owner uploads original data m onto cloud server and a master – secret key is generated. In the step (c) data will be encrypted into constant size ciphertext C. In the step (d), an aggregated key will be generated. In the final step (e) on receiver side, a delegatee will decrypt the ciphertext C into original message m.

III. IMPLEMENTATION

The key aggregation approach contains 4 main modules:

i) Authentication and Authorization
ii) Encryption
iii) Aggregate key
iv) Decryption

Authentication and Authorization

These are requisite during data sharing. So the data owner should be registered before uploading data onto the cloud and only the registered users will perform session activities.

Encryption

Original data should be encrypted before uploading onto the cloud and sharing with others. Encryption will be done by public key, an index I which denotes the ciphertext class and original data m and it outputs the ciphertext C.

Aggregate Key

Whenever the data has to be accessed by the user, permission has to be granted with decryption keys. Here, the data owner will extracts the power of all keys of files which are requested by the user into a single key called aggregate key. This key will be generated using master – secret key and a set S which indicates indices of corresponding to different classes.

Decryption

On receiver side, the user will receive the aggregate key and will decrypt the ciphertext C into original message m by selecting the set S and aggregate key.

IV. CONCLUSION

Providing privacy mechanism to the user's data is the essential feature in the cloud storage. In cloud storage, number of ciphertexts increases rapidly without any restrictions. In this project we consider how to develop an efficient and flexible encryption scheme which decrypts any number of subset of ciphertext by a single secret key. Here a delegate will always get a constant size aggregate key. So decryption of any number of ciphertexts is possible by an aggregate key.

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 Storage‖, IEEE Transactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year: 2014.
[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ―Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data, in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06). ACM, 2006, pp. 89–98.
[3] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, ―Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records, ‖ in Proceedings of ACM Workshop on Cloud Computing Security (CCSW '09). ACM, 2009, pp. 103–114.
[4] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc.22nd Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT '05), vol. 3494, pp. 457-473, 2005.
[5] F. Guo, Y. Mu, and Z. Chen, "Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key", Proc. Pairing-Based Cryptography Conf. (Pairing '07), vol. 4575, pp. 392-406, 2007.