International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July 2016

An Analysis on Key-Aggregate Cryptosystem for Data Sharing in Cloud Storage

[1]KARNATI ANIL, [2]C. ISHAQ SHAREEF

[1]M.Tech Dept of CSE, PVKK Institute of Technology, Affiliated to JNTUA, AP, India .
[2]Assistant Professor, Dept of CSE, PVKK Institute of Technology, Affiliated to JNTUA, AP, India

Abstract

Cloud computing technology is widely used so that the data can be outsourced on cloud can accessed easily. Different members can share that data through different virtual machines but present on single physical machine. But the thing is user don't have physical control over the 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 or leak of users data. Privacy preserving in cloud is important make sure the users identity is not revealed to everyone. On cloud anyone can share data as much they want to i.e. only selected content can be shared. Cryptography helps the data owner to share the data to in safe way. So user encrypts data and uploads on server. Different encryption and decryption keys are generated for different data. The encryption and decryption keys may be different for different set of data. Only those set of decryption keys are shared that the selected data can be decrypted. Here a public-key cryptosystems which generate a ciphertext which is of constant size. So that to transfer the decryption rules for number of ciphertext. The difference is one can collect a set of secret keys and make them as small size as a single key with holding the same ability of all the keys that are formed in a group. This compact aggregate key can be efficiently sent to others or to be stored in a smart card with little secure storage.

Keywords: *Cloud storage, Attribute base encryption, Identity base encryption, Cloud storage, data sharing, key-aggregate encryption*

I. INTRODUCTION

Cloud computing is widely increasing technology; data can be saved on cloud remotely and can have access to huge applications with quality services which are shared among customers. As increase in outsourcing of data the cloud computing serves does the management of data.

Its flexible and cost optimizing characteristic motivates the end user as well as enterprises to store the data on cloud. The insider attack is one of security concern which's needs to be focused. Cloud Service provider need to make sure whether audits are held for users who have physical access to the server. As cloud service provider stores the data of different users on same server it is possible that user's private data is leaked to others. The public auditing system of data storage security in cloud computing provides a privacy-preserving auditing protocol.

It is necessary to make sure that the data integrity without compromising the anonymity of the data user. To ensure the integrity the user can verify metadata on their data, upload and verify metadata.

Suppose some day she wants to share few photos with her friend Bob, either she can encrypt all photos with one key and send to him or she can create encrypt with different keys and send it. The un-chosen data may be leaked to Bob if the single key generated for encryption so create distinct keys of data and send single key for sharing.

The main concern is how to share the data securely the answer is cryptography. The question is how can the encrypted data is to be shared. The user must provide the access rights to the other user as the data is encrypted and the decryption key should be send securely. For an example Alice keeps her private data i.e. photos on dropbox and she doesn't want to share it with everyone. As the attacker may access the data so it is not possible to rely on predefine privacy preserving mechanism so she all the photos were encrypted by her on encryption key while uploading it.

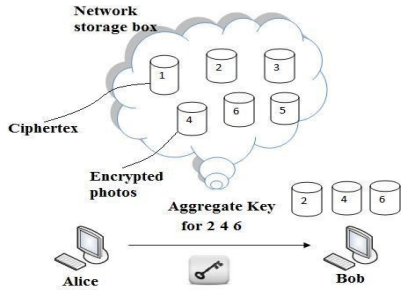


Fig 1 File sharing between Alice and Bob

A new way for public-key encryption is used called as key-aggregate cryptosystem (KAC). The encryption is done through an identifier of Ciphertext known as class, with public key. The classes are formed by classifying the ciphertext. The key owner has the master secret key which is helpful for extracting secret key. So in above senario now the Alice can send a aggregate key to Bob through a email and the encrypted data is downloaded from dropbox through the aggregate key. This is shown in figure1.

II. LITERATURE SURVEY

Cloud computing is visualized as architecture for succeeding generation. It has many facilities though have a risk of attacker who can access the data or leak the users identity. While setting a cloud users and service providers authentication is necessary. The issue arises whether loud service provider or user is not compromised. The data will leak if any one of them in compromised. The cloud should be simple, preserving the privacy and also maintaining users identity.

The flexible use of cloud storage for user is a need as it is seams accessing data locally though that is present at remote side. It is important to inspect the data set on the cloud. So it is necessary to allow a public audit for integrity of outsourced data through third party auditor (TPA). TPA is also beneficial for cloud service provider. It checks the correctness of the outsourced data. TPA should be able to do public auditability, storage correctness, privacy preserving, Batch auditing with minimum communication and computation overhead.

There are many cloud users who wants to upload there data without providing much personal details to other users. The anonymity of the user is to be preserved so that not to reveal the identity of data owner. Provable data possession (PDP) uses similar demonstrating marks to reduce computation on server, and network traffic. PDA ensures the data present on cloud which is un-trusted is original without accessing it. Security mediator (SEM) is approach allows the user to preserve the anonymity. Users are meant to upload all their data to SEM so that the SEM is not able to understand the data although it's going to generate the verification on data. As the users are signed at SEM it should not know the identity of uploader.

Another way for sharing encrypted data is Attribute-Based Encryption (ABE). It is likely to encrypt the data with attributes which are equivalent to users attribute rather than only encrypting each part of data. In ABE attributes description is considered as set so that only a particular key which is matched with attribute can decrypt the ciphertext. The user key and the attribute are matched if it matches it

can decrypt a particular ciphertext. When there are k attributes are overlay among the ciphertext and a private key the decryption is granted.

A multi group key management accomplishes a hierarchical access control by applying an integrated key graph also handling the group keys for different users with multiple access authorities. Centralized key management plan uses tree structure to minimize the data processing, communication and storage overhead. It maintains things related to keying and also updates it. It accomplishes an integrated key graph for every user.

Identity-based encryption (IBE) is a vital primary thing of identity bases cryptography. The public key of user contains distinct information of user's identity. The key can be textual value or domain name, etc. IDE is used to deploy the public key infrastructure. The identity of the user is used as identity string for public key encryption. A trusted party called private key generator (PKG) in IBE which has the master secret key and gives secret key to users according to the user identity. The data owner collaborate the public value and the identity of user to encrypt the data. The ciphertext is decrypted using secret key.

In a multi attribute-authorities numbers of attributes are analyzed regarding the decryption key and the user must get a particular key related to the attribute while decrypting a message. The decryption keys are allocated independently to users those who have attribute identity without interaction between each other. Multi-authority attribute-based encryption allows real time deployment of attribute based privileges as different attributes are issued by different authorities. The attribute authorities ensure the honesty of the user privilege so the confidentiality is maintained by central authority.

III. EXISTING SYSTEM

In this existing system, a user provides an untrusted server, say a proxy operated by a cloud service provider with a transformation key TK that allows the latter to transfer any ABE cipher text CT satisfied by that users attributes or access policies into a simple cipher text CT and it only incurs a small overhead for the user to recover the plain text from transformed cipher text CT. The security property of the ABE scheme with outsourced decryption guarantees that an adversary (including the malicious server) be not able to learn anything about the encrypted message; however, the scheme provides no guarantee on the correctness of the transformation done by the cloud server. In the cloud computing setting, cloud service providers may have strong financial incentives to return incorrect answers, if such answers require less work and are unlikely detected by users.

IV. PROPOSED KEY-AGGREGATE ENCRYPTION

A key aggregate encryption has five polynomial-time algorithms as

A. Setup Phase

The data owner executes the setup phase for an account on server which is not trusted. The setup algorithm only takes implicit security parameter.

B. Key Gen Phase

This phase is executed by data owner to generate the public or the master key pair (pk, msk).

C. Encrypt Phase

This phase is executed by anyone who wants to send the encrypted data. Encrypt (pk, m, i), the encryption algorithm takes input as public parameters pk, a message m, and i denoting ciphertext class. The algorithm encrypts message m and produces a ciphertext C such that only a user that has a set of attributes that satisfies the access structure is able to decrypt the message.

- Input= public key pk, an index i, and message m
- Output = ciphertext C.

D. Extract Phase

This is executed by the data owner for delegating the decrypting power for a certain set of ciphertext classes to a delegate.

- Input = master-secret key mk and a set S of indices corresponding to different classes
- Outputs = aggregate key for set S denoted by k_S.

E. Decrypt Phase

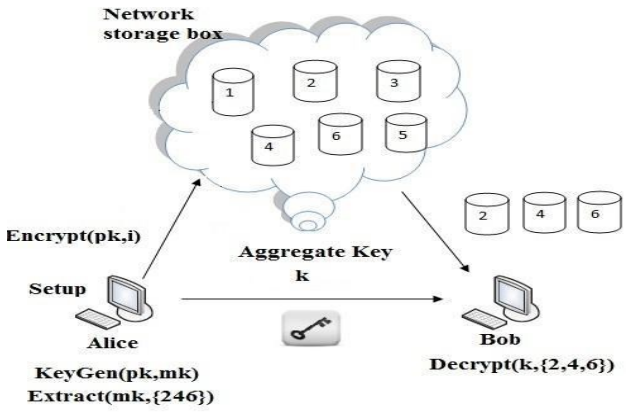
This is executed by the candidate who has the decryption authorities. Decrypt (k_S, S, i, C), the decryption algorithm takes input as public parameters pk, a ciphertext C, i denoting ciphertext classes for a set S of attributes.

- Input = k_S and the set S, where index i = ciphertext class
- Outputs = m if i element of S

F. DATA SHARING

KAC in meant for the data sharing. The data owner can share the data in desired amount with confidentiality. KCA is easy and secure way to transfer the delegation authority. The aim of KCA is illustrated in Figure 2.

For sharing selected data on the server Alice first performs the Setup. Later the public/master key pair (pk, mk) is generated by executing the KeyGen. The msk master key is kept secret and the public key pk and param are made public. Anyone can encrypt the data m and this data is uploaded on server. With the decrypting authority the other users can access those data. If Alice is wants to share a set S



.

Fig 2 Use of KAC for data sharing

of her data with a friend Bob then she can perform the aggregate key KS for Bob by executing Extract (mk, S). As kS is a constant size key and the key can be shared through secure e-mail. When the aggregate key has got Bob can download the data and access it.

V. CONCLUSION

To Share data flexibly is vital thing in cloud computing users prefer to upload there data on cloud and among different users. Outsourcing of data to server may lead to leak the private data of user to everyone. Thus data privacy and security is maintained by designing a public key cryptosystem called as Key Aggregate Cryptosystem (KAC). This KAC helps user to share their data partially over cloud with constant size key pair of public-master keys and also receiver can decrypt this data with single constant size aggregate key. This helps us to create Patient-Controlled Encryption (PCE) system. There are some limitation to the existing system like predefined bound of the number of maximum ciphertext classes and system is prompt to leakage of key.

REFERENCES

[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," in Applied Cryptography and Network Security – ACNS 2012, ser. LNCS, vol. 7341. Springer, 2012, pp. 526–543.
[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, 2013.
[3]. B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Dataon the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.
[4]. 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" IEEE Transactions On Parallel And Distributed System, Vol 25, No. 2 February 2014.

[5]. 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.
[6]. Y. Sun and K. J. R. Liu, "Scalable Hierarchical Access Control in Secure Group Communications," in Proceedings of the 23th IEEE International Conference on Computer Communications (INFOCOM '04). IEEE, 2004.
[7]. D. Boneh and M. K. Franklin, "Identity-Based Encryption from the Weil Pairing," in Proceedings of Advances in Cryptology – CRYPTO '01, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–229.
[8]. M. Chase and S. S. M. Chow, "Improving Privacy and Security in Multi-Authority Attribute-Based Encryption," in CM Conference on Computer and Communications Security, 2009, pp. 121–130.