AN ANALYSIS OF KEY AGGREGATE CRYPTOSYSTEMS FOR SCALABLE CLOUD DATA SHARING

Mali Nilesh Dattatray
Research Scholar
Department of Engineering
Sunrise University, Alwar, Rajasthan.
nileshdmali@gmail.com

Dr. Rathod Sunil Damodar
Research Guide
Department of Engineering
Sunrise University, Alwar, Rajasthan.

Abstract

Technology for cloud computing is extensively employed so that data may be quickly accessible on the cloud and outsourced. Although the data is only present on one physical system, multiple members may share it via many virtual machines. However, the user has no direct physical access to the data that has been outsourced. Users must be able to safely exchange data.

To ensure that user data is neither lost or leaked, authentication between the cloud service provider and the user is required. It's crucial to protect user privacy in the cloud to prevent identity disclosure. Only chosen material may be shared, but everyone on the cloud can share data as much as they want to.

Data sharing may be done safely thanks to cryptography. User then uploads encrypted data to server. For various types of data, multiple encryption and decryption keys are created. For certain sets of data, multiple encryption and decryption keys may be required. Only the shared set of decryption keys allows for the decryption of the chosen data.

Here, a public-key cryptosystem produces ciphertext that has a fixed size. so that the decryption keys for various ciphertexts may be sent. The distinction is that one may assemble a collection of hidden keys and reduce them to the size of a single key while still possessing all of the properties of the keys that make up the group. This little aggregate key may be transmitted to people easily or kept on a smart card with a minimal amount of safe storage.

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

INTRODUCTION

The technology of cloud computing is rapidly advancing; data may be remotely kept in the cloud and users can access many apps with high-quality services that are offered to all clients. The cloud computing aids data management as data outsourcing increases.

The end user and businesses are motivated to store data in the cloud by its flexible and cost-saving features. One security issue that requires attention is the insider assault. Whether audits are conducted for users who have direct physical access to the server must be confirmed by the cloud service provider. Due to the fact that cloud service providers keep the data of several users on the same server, it is possible for users' sensitive information to be compromised. The public auditing system of cloud computing's data storage security offers an auditing methodology that protects privacy.

Without compromising the data user's anonymity, it is important to ensure data integrity. The user may submit and validate metadata on their own data to assure data integrity.

The primary issue is how to communicate the data safely, and encryption is the solution. How should encrypted data be communicated is the key question. Due to the fact that the data is encrypted and the decryption key must be sent securely, the user must grant the other user access permissions. As an example, Alice stores her private information, such as her

photographs, on Dropbox since she prefers not to share it with anybody. As the attacker could access the material, it is not viable to depend on predefined privacy-preserving mechanisms. As a result, she encrypted all of the images before uploading them using an encryption key.

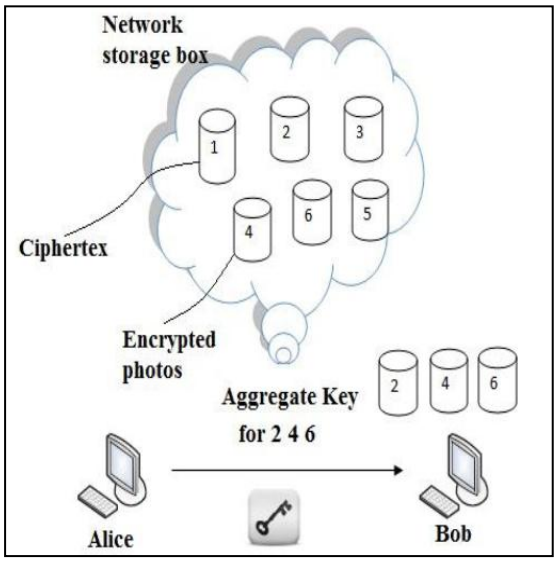

Fig 1 File sharing between Alice and Bob

If she ever wishes to give her buddy Bob a few images, she can either encrypt them all using the same key and send them to him, or she may generate individual encrypted files and transmit them. Create different keys for each piece of data and transmit a single key for sharing to prevent the unintentional data from being leaked to Bob if a single key is produced for encryption.

Key-aggregate cryptosystems (KAC) are a novel technique for public-key encryption. Through the use of a public key and the class Ciphertext identifier, encryption is performed. The ciphertext is categorized to create the classifications. The master secret key, which is used for extracting the secret key, belongs to the key owner. Now that the aggregate key can be sent to Bob over email in the scenario above, the encrypted data may be retrieved from Dropbox using the aggregate key.In figure1, this is shown.

LITERATURE SURVEY

A future generation's design is envisioned for cloud computing. Although it has numerous features, there is a chance that an attacker may get access to the data or reveal the identities of users. While configuring a cloud, authentication is required for users and service providers. If a loud service provider or user is not at risk, a problem develops. If any one of them is hacked, the data will leak. The cloud should be straightforward, protecting user identification and privacy.

The ability for users to utilize cloud storage in a flexible way is essential since it allows for local access to data that is really stored elsewhere. Examining the cloud-based data set is crucial. Thus, it is essential to permit a public audit for the integrity of data that has been outsourced via a third party auditor (TPA). TPA is advantageous for cloud service providers as well. It verifies that the data that was outsourced was accurate. With the least amount of communication and processing cost, TPA ought to be able to perform public auditability, storage accuracy, privacy preservation, and batch auditing.

Many cloud users want to transfer their data without divulging too much personal information to other users. In order to protect the identity of the data owner, user anonymity must be maintained. Similar demonstrative markings are used by Provable Data Possession (PDP) to cut down on server and network bandwidth. Without accessing it, PDA makes sure that untrusted cloud data is original. The user's anonymity is protected using the security mediator (SEM) method. Users are instructed to submit all of their data to SEM so that, even if it will provide data

verification, SEM won't be able to grasp the data. As long as the user is logged in at SEM, it shouldn't know who uploaded the file.

Attribute-Based Encryption (ABE) is an additional method for exchanging encrypted data. Instead of just encrypting individual pieces of data, it is more probable to encrypt the data with qualities that are analogous to user attributes. According to ABE, an attribute's description is taken into account to be set, meaning that only a certain key that matches the attribute may decode the ciphertext. If the user key and the attribute match, the ciphertext in question may be decrypted. The decryption is permitted when k characteristics are layered over the ciphertext and private key.

By using an integrated key graph and managing the group keys for various users with various access authority, multi group key management achieves hierarchical access control. Tree structure is used in the centralized key management scheme to reduce data processing, communication, and storage overhead. It refreshes it and maintains keying-related items. Every user receives an integrated key graph as a result.

A key component of identity-based cryptography is identity-based encryption (IBE). The user's public key includes specific information about the user's identity. The key might be a domain name or textual value, for example. Public key infrastructure deployment is carried by using IDE. For public key encryption, the user's identity is utilized as the identification string. Private key generator (PKG) is a reputable entity in IBE that distributes secret keys to users in accordance with user identities and holds the master secret key. To encrypt the data, the data owner works with the public good and the user's identification. Using the secret key, the ciphertext is decoded.

In a system with many attribute authorities, several characteristics are examined in relation to the decryption key, and the user is required to get a specific key connected to each attribute in order to decode a message. Users who possess attribute identification are given the decryption keys separately, without communication between one another. As different attributes are provided by various authorities, multi-authority attribute-based encryption enables real-time deployment of attribute-based privileges. The attribute authorities guarantee the user privilege's honesty, allowing the central authority to preserve secrecy.

KEY-AGGREGATE ENCRYPTION

There are five polynomial-time techniques for key aggregate encryption.

Setup Phase

The setup process for an account on a server that is not trusted is carried out by the data owner. The sole security parameter used by the setup procedure is implicit.

KeyGen Phase

In order to produce the public or master key pair (pk, msk), the data owner must complete this step.

Encrypt Phase

Anyone who wishes to transmit the encrypted data must complete this step. The encryption algorithm Encrypt (pk, m, i) accepts as input the public parameters pk, a message, and i designating the ciphertext class. The method encrypts message m and generates a ciphertext C that can only be decrypted by a user who has a set of characteristics that satisfy the access structure.

• Input: a message m, an index i, and a

public key pk
• Ciphertext C is the output.

Extract Phase

The data owner uses this to provide a delegate authority to decode a certain collection of ciphertext classes.
• Input consists of a master-secret key, mk, and a set S of indices that represent several classes.
• The aggregate key for set S, indicated by kS, is outputs.

Decrypt Phase

The candidate with the decryption authority carries out this. The decryption method, Decrypt (kS, S, i, C), accepts as inputs public parameters pk, a ciphertext C, and i designating ciphertext classes for a collection S of characteristics.
• Where index i = ciphertext class, input equals kS and the set S.
• If element i of S, outputs = m

DATA SHARING

KAC is intended for data exchange. The owner of the data may securely and in any quantity distribute the data. The delegation of power may be transferred quickly and securely using KCA. Figure 2 illustrates the goal of KCA.

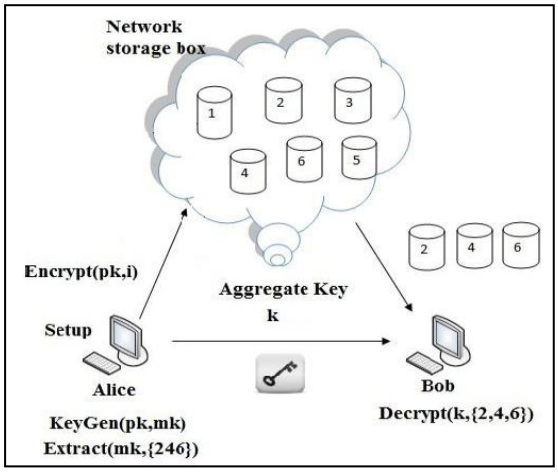

Fig 2 Use of KAC for data sharing

Alice initially completes the Setup before sharing specific info on the server. Later, by running KeyGen, the public/master key pair (pk, mk) is produced. The public key pk and parameter are made public, while the msk master key is kept a secret. Anybody may encrypt data, which is then uploaded to a server. The other users may access such data with the decrypting authority. Alice may do the aggregate key KS for her buddy Bob by running Extract (mk, S) if she wishes to share a set S of her data with him. kS is a constant size key, and sharing the key over secure email is possible. When Bob has the aggregate key, he can access and download the data.

CONCLUSION

Flexible data sharing is essential to cloud computing. Users like to share their info on the cloud with other users. Data outsourcing to a server might result in user privacy information being exposed to the public. One method that enables sharing of chosen material with targeted candidates is encryption. Sharing decryption keys in a safe manner is crucial. Delegation of secret keys for various ciphertext classes in cloud storage is made possible by public-key cryptosystems. The delegatee receives a secure, constant-size aggregate key. Since they grow quickly and have a finite number of classes, it is necessary to maintain an adequate number of ciphertext classes.

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.