Deniable Attribute-Based Encryption On Cloud Storage Without Inspection

Ms. Suchita Doke[1], Dr. Gayatri Bhandari[2]

Computer Engineering, JSPM'S Bhivrabai Sawant Institute of Technology & Research Wagholi, Pune-421207,Maharashtra,India

ABSTRACT

Cloud storage services became more and more standard. Outsourcing data to the cloud are beneficial for reasons of economy, scalability, and accessibility, but significant technical challenges remain. For the importance of privacy, several cloud storage encryption schemes are planned to protect information from people who do not have access. All such schemes assumed that cloud storage suppliers are safe and can't be hacked; but some authorities (i.e., coercers) might force cloud storage suppliers to reveal user secrets or confidential information on the cloud, therefore altogether circumventing storage encryption schemes. Most of the planned schemes also assume that cloud storage service suppliers or sure third parties handling key management are sure and can't be hacked; but, in observe, some entities might intercept communications between users and cloud storage suppliers and so compel storage suppliers to release user secrets by exploitation government power or different means that. During this case, encrypted information is assumed to be better-known and storage suppliers are requested to release user secrets. A brand new cloud storage encryption scheme is proposed that allows cloud storage suppliers to create convincing fake user secrets for the protection of user privacy. Since coercers can't tell if obtained secrets are true or not, the cloud storage suppliers make sure that user privacy continues to be firmly protected..

Keyword : *Deniable Encryption, Composite Order Bilinear Group, Attribute-Based Encryption, Cloud Storage*

1. INTRODUCTION

Cloud storage services are becoming more popular because users can store their data on cloud and cloud storage services can allow users to access this data anywhere at any time. Privacy is one elementary facet of this paradigm shifting is that information is being centralized or outsourced to the Cloud. From users perspective, as well as each people and IT enterprises, storing information remotely to the cloud in an exceedingly versatile on demand manner brings appealing benefits: relief of the burden for storage management, universal information access with free geographical locations, and rejection of cost on hardware, software, and personnel maintenance, etc. Whereas Cloud Computing makes these blessings a lot of appealing than ever, it conjointly brings new and difficult security threats towards users outsourced information. Since cloud service suppliers (CSP) area unit separate body entities, information outsourcing is really relinquishing users final management over the fate of their information. The overhead of victimization cloud storage ought to be decreased the maximum amount as potential, such user does not ought to perform too several operations to use the information. For instance, it is fascinating that users do not ought to worry concerning the requirement to verify the integrity of the information before or when the information retrieval. Besides, there is also quite one user accesses similar cloud storage, say in associate degree enterprise setting. For easier management, it is fascinating that the cloud server solely entertains verification request from one selected party. Cloud storage is currently gaining quality as a result of it offers a versatile on-demand information outsourcing service with nice advantages. By information outsourcing, users are often mitigated from the burden of native information storage and maintenance. However, the important fact is that users not have physical possession of the probably giant size of outsourced information that makes the information integrity protection in Cloud Computing.

The important issue in the cloud storage is the user privacy and for this reason the data stored on the cloud is typically encrypted and protected from access by other users. Considering the collaborative property of the cloud data, attribute-based encryption (ABE) is thought as one of the most suitable encryption schemes for cloud storage. There are various ABE schemes that have been proposed, including [1], [2], [3], [5]. Most of the proposed schemes assume cloud storage service providers or trusted third parties handling key management are trusted and cannot be hacked; however, in practice, some entities may intercept communications between users and cloud storage providers and then compel storage providers to release user secrets by using government power or other means. In this case, encrypted data are assumed to be known and storage providers are requested to release user secrets. As an example, in 2010, without notifying its users, Google released user documents to the FBI after receiving a search warrant. In 2013, Edward Snowden disclosed the existence of global surveillance programs that collect such cloud data as emails, texts, and voice messages from some technology companies. Once cloud storage providers are compromised, all encryption schemes lose their effectiveness. Thus it is difficult for cloud storage providers to fight against such entities to maintain user privacy through legal avenues. As one example, Lavabit was an email service company that protected all user emails from outside coercion; unfortunately, it failed and decided to shut down its email service.

As it is difficult for cloud service providers to fight against outside coercion, new encryption scheme is proposed that avoid this predicament. Allowing cloud storage providers to create fake user secrets in order to protect the user secrets. Given such fake user secrets, outside coercers can only obtained forged data from a users stored cipher text. Once coercers obtained the user secrets they think that these secrets are real, they will be satisfied and more importantly cloud storage providers will not have revealed any real secrets. Therefore, user privacy is still protected. This concept comes from a special kind of encryption scheme called deniable encryption

2. RELATED WORK

Cloud storage services are not safe because they can't protect users sensitive data. In order to achieve the security of user secrets stored on cloud storage by user, many of the encryption schemes are proposed. Still the security is not achieved at its best because some authorities may force cloud service provider to release the user secrets or confidential data on cloud. All such schemes assume that cloud service providers are trusted and can't be hacked, but in reality some entities intercept the communication between user and cloud storage providers and then force the cloud storage providers to release the users sensitive data.

So it is important that cloud storage must fight against such entities to maintain user privacy. Thus the deniable attribute based encryption scheme is implemented to allow cloud storage provider to protect the users confidential data from being released on cloud.

3. IMPLEMENTATION DETAILS

3.1 Existing System

Sahai and Waters first introduced the concept of ABE in which data owners can embed how they want to share data in terms of encryption. That is, only those who match the owner's conditions can successfully decrypt stored data. ABE is encryption for privileges, not for users. This makes ABE a very useful tool for cloud storage services since data sharing is an important feature for such services.

Cloud storage users are impractical for data owners to encrypt their data by pairwise keys. Moreover, it is also impractical to encrypt data many times for many people. With ABE, data owners decide only which kind of users can access their encrypted data. Users who satisfy the conditions are able to decrypt the encrypted data.

Disadvantages

1. Impossible to encrypt unbounded message, using one short key in non committing schemes.
2. The non interactive and fully receiver deniable scheme can not be achieved simultaneously.
3. Data redundancy is occur at each block of data.
4. Decrypted data with missing of contents at such blocks

3.2 Proposed System

The implementation of a deniable CP-ABE scheme that can make cloud storage services secure and audit free. In this scenario, cloud storage service providers are just regarded as receivers in other deniable schemes.

Block Wise Deniable ABE

A deniable CP-ABE scheme is built with two encryption environments at the same time, much like the idea proposed with multi dimensions. This approach removes obvious redundant parts in an existing ABE scheme by replacing prime order groups with composite order groups. Since the base ABE scheme can encrypt one block each time, deniable CPABE is certainly a block wise deniable encryption scheme.

The bilinear operation for the composite order group is slower than the prime order group, there are some techniques that can convert an encryption scheme from composite order groups to prime order groups for better computational performance.

Consistent Environment

Consistent environment means that one encryption environment can be used for multiple encryption times without system updates. The opened receiver proof should look convincing for all ciphertexts under this environment3, regardless of whether a ciphertext is normally encrypted or deniably encrypted. The deniability of the scheme comes from the secret of the subgroup assignment, which is determined only once in the system setup phase. By the canceling property and the proper subgroup assignment, the released fake key can be constructed to decrypt normal ciphertexts correctly.

Deterministic Decryption

Deniable CP-ABE extends a pairing ABE, which has a deterministic decryption algorithm, from the prime order group to the composite order group. The decryption algorithm is still deterministic; therefore, there is no decryption errors using deniable CP-ABE.

Advantages

1. No data redundancy
2. Builds consistent environment
3. No decryption errors
4. High computational performance
5. No security violence

4. SYSTEM ARCHITECTURE

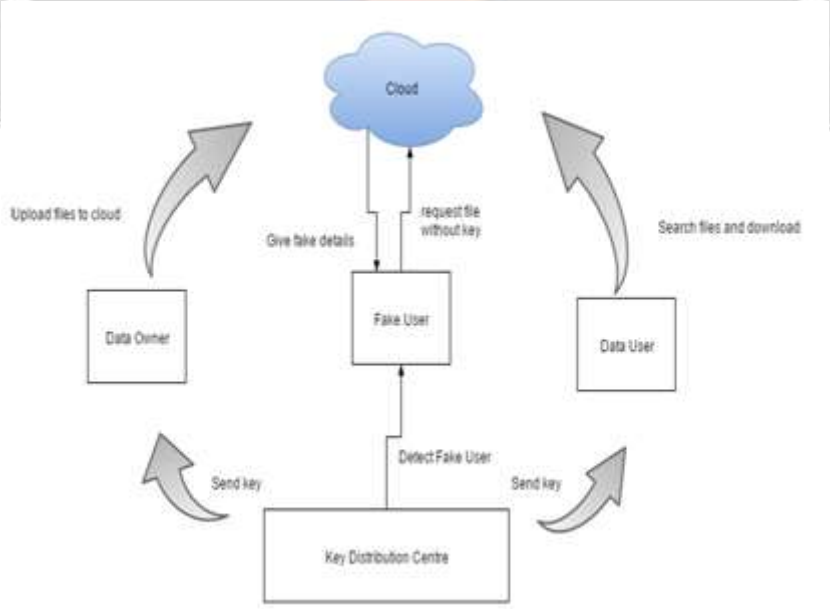

Fig. System Architecture

The system consists of three models: the data owner, the data user and the KDC(key distribution centre).

Data Owner:
The data owner is a user who outsources the data i.e confidential data to the cloud. He will first register himself and login to the system, along with it he will receive a key from the KDC which will be used for authentication purpose. In other words the secret key will help to detect if the user is authorized or not. After this process he may be able to upload files to the cloud.

Data User:
The data user is an end user who may need access to some data uploaded by the data owner. Even data user has to register and login to the system. KDC will provide a key to him based on which authentication will be done. The user may search for a file and download it based on the key.

KDC:
KDC will generate keys for owner and user. These keys will be used for authentication purposes. If the key given by KDC and the keys entered by the users matches then they are authorized. The keys are sent to registered email.

Fake users are also introduced in the system. They try to attack the data while downloading but as they may not receive secret key and if they just enter any random key then also they may download a file, but the file will be a fake file and not the original file. This is main concept of the project.

5. MODULE DISCRIPTION

Owner Module

Owner module is to transfer their files mistreatment some access policy. First they get the general public key for specific transfer file once obtaining this public key owner request the key for specific transfer file. Mistreatment that secret key owner transfer their file.

User Module

This module is employed to assist the consumer to go looking the file mistreatment the file id and file name .If the file id and name is inaccurate means that we tend to don't get the file, otherwise server raise the general public key and find the secret writing file. If u wish the secret writing file means that user have the key.

Distributed Key Policy Attribute Primarily Based Encryption

KP-ABE could be a public key cryptography primitive for one-to-many correspondences. In KP-ABE, data is related to attributes for every of that a public key half is characterized. The encryptor associates the set of attributes to the message by scrambling it with the scrutiny public key elements. Each consumer is assigned associate degree access structure that is generally characterized as associate degree access tree over data attributes, i.e., within hubs of the access tree square measure limit doors and leaf hubs square measure connected with attributes. Consumer secrets characterized to mirror the access structure that the consumer has the flexibility to decipher a cipher-text if and simply if the knowledge attributes fulfill his access structure.

6. EXPECTED RESULTS

Sr. No.	Packet Size(kb)	Encryption Time(sec)	Decryption Time(sec)
1.	153	1.6	1
2.	196	1.7	1.4
3.	312	1.8	1.6
4.	868	2.0	1.8

7. CONCLUSION

A deniable CP-ABE scheme is an audit free cloud storage service. The deniability feature makes coercion invalid, and the attribute based encryption property ensures secure cloud data sharing with a fine-grained access control mechanism. The proposed scheme provides a possible way to fight against immoral interference with the right of privacy and can be created to protect cloud user privacy with high computational performance.

REFERENCES

[1] A. Sahai and B. Waters, " Fuzzy identity-based encryption ", in Eurocrypt, 2005, pp. 457–473.

[2] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for finegrained access control of encrypted data ", in ACM Conference on Computer and Communications Security, 2006, pp. 89–98.

[3] S. Hohenberger and B. Waters, " Attribute-based encryption with fast decryption ", in Public Key Cryptography, 2013, pp. 162–179.

[4] K. Liang, L. Fang, D. S. Wong, and W. Susilo, " A ciphertextpolicy attribute-based proxy re-encryption with chosen-ciphertext security ", IACR Cryptology ePrint Archive, vol. 2013, p. 236, 2013.

[5] P. K. Tysowski and M. A. Hasan, " Hybrid attribute- and reencryption-based key management for secure and scalable mobile applications in clouds ", IEEE T. Cloud Computing, pp. 172–186, 2013.

[6] J. Bethencourt, A. Sahai, and B. Waters, " Ciphertext-policy attribute-based encryption ", in IEEE Symposium on Security and Privacy, 2007, pp. 321–334.

[7] M. H. Ibrahim, " A method for obtaining deniable public-key encryption ", I. J. Network Security, vol. 8, no. 1, pp. 1–9, 2009.

[8] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, " Deniable encryption ", in Crypto, 1997, pp. 90–104.