Secure and DataAccess Control for Cloud Storage

ARUN PRASAD. V
IT
S.A. ENGINEERING COLLEGE
1923002@saec.ac.in

EZHILARASAN. E
IT
S.A. ENGINEERING COLLEGE
1923029@saec.ac.in

JASWANTH. B
IT
S.A. ENGINEERING COLLEGE
1923032@saec.ac.in

GUIDE:
A.M. SERMAKANI
IT
S.A. ENGINEERING COLLEGE
sermakani@saec.ac.in

Abstract— Secure cloud storage, an upcoming cloud service, is intended to ensure the secrecy of outsourced data while also providing flexible data access for cloud customers whose data is not physically under their control. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is recognized as one of the most promising strategies that may be used to ensure the service guarantee. Unfortunately, because to the inherent "all-or-nothing" decryption characteristic of CP-ABE, the deployment of CP-ABE may result in an unavoidable security violation known as the misuse of access credential (i.e., decryption privileges). In this work, we look at two major scenarios of access credential misuse: one on the semi-trusted authority side and one on the cloud user side. To mitigate the misuse, we propose the first accountable authority and revocable CP-ABE based cloud storage system with white-box traceability and auditing, referred to as Cloud. We also present the security analysis and further demonstrate the utility of our system via experiments.

Index Terms—Secure cloud storage, ciphertext-policy attribute-based encryption, access credentials misuse, traceability and revocation,auditing

1 INTRODUCTION

The widespread usage of cloud computing may pose an indirect risk to the security of outsourced data and the privacy of cloud users. A major problem here is ensuring that only authorized individuals have access to the data that has been outsourced to the cloud, at any time and from any location. One naïve method is to encrypt the data before uploading it to the cloud. Nevertheless, the method restricts additional data exchange and processing. This is because a data owner must download encrypted data from the cloud and re-encrypt it before sharing it suppose the data owner has no local copies of the data. In the context of cloud computing, fine-grained access control over encrypted data is desirable.

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) may be an effective method for ensuring data confidentiality and providing fine-grained access control in this situation. Organizations (for example, an institution like the University of Texas at San Antonio) and individuals can use a CP-ABE-based cloud storage system. (e.g. students, faculty members and visiting scholars of the university). Approved cloud users are then given access credentials (i.e., decryption keys) matching to their attribute sets (e.g., student role, faculty member role, or guest role), which they may use to access the outsourced data. Being a strong one-to-many encryption system, CP- ABE not only protects data saved in the cloud, but it also allows for fine-grained access control over the data. As we all know, the disclosure of any sensitive data stored in the cloud can have a wide variety of ramifications for the company and people (e.g.litigation, loss of competitive advantage, and criminal charges). The CP-ABE might assist us in preventing security breaches from outside adversaries. In particular, we provide a CP-ABE-based cloud storage platform in our study. We propose two accountable authority and revocable CP-ABE systems (with white-box traceability and auditing) that are completely secure in the standard model, referred to as ATER-CP-ABE and ATIR-CP-ABE, respectively, based on this (generic) architecture. Based on the two systems, we offer the Cloud design, which has the following capabilities.

1) The capacity to track malevolent cloud users. Users who reveal their login credentials can be tracked down and identified.

2) Responsible power. It is possible to identify a semi-trusted authority who produces and distributes access credentials to unauthorized people without sufficient authorization. This enables additional actions to be conducted (e.g., criminal investigation or civil litigation for damages and breach of contract).

3) Auditing. An auditor can detect whether a (suspected) cloud user has leaked his or her access credential.

4) Tracing requires "almost" no storage. We employ a Paillier-like encryption as an extractable commitment in

tracking malevolent cloud users, and we don't need to keep an identity table of users for tracing (unlike the previous technique).

5) Revocation of malicious cloud users. Access credentials for individuals who have been tracked and judged to be "compromised" can be withdrawn. We devise two procedures to effectively revoke the "traitor(s)." The ATER-CP-ABE provides an explicitly revocation mechanism in which a revocation list is explicitly specified in the algorithm Encrypt, whereas the ATIR-CP-ABE provides an implicitly revocation mechanism in which the encryption does not need to know the revocation list but a key update operation is required on a regular basis.

2. RELATED WORK AND OUR APPROACH

2.1 Related Work

Cloud storage investigates novel data storage applications, so that data owners no longer bear entire responsibility for data management. Nevertheless, because data ownership and data access are separated in the cloud, the administration of data, software, physical computers, and platforms must be transferred to cloud service providers, leaving the data owner with limited control over virtual machines. In addition, several attribute revocation techniques for CP-ABE systems have been presented in the literature. It defines the revocable storage problem and provides a completely secure ABE structure based on ciphertext delegation. Another idea is to create a revocable multi-authority CP-ABE system that provides both forward and backward security. Recently, somebody proposed an attribute updating mechanism to accomplish dynamic attribute changes (such as revoking previous attribute and re-granting previously revoked attribute).

Unfortunately, the aforementioned research studies do not take into account key generation authority mis-behaver, auditing feasibility, or revocation (of misbehaver). These are the issues we hope to address in this study.

2.1 Our Approach

An overview of the technique we employ to achieve harmful cloud user traceability, responsible authority, auditing, and malicious cloud users. As previously noted, we leverage a Paillier-like encryption as an extractable promise to provide white-box tracking when hostile cloud users leak access credentials. In particular, the extractable commitment enables us to commit a user's identity when he or she seeks an access credential. The commitment is considered a component of the certification. A user cannot divulge and further "alter" the identity that is "encoded" in the credential due to the concealing and binding mechanism of the Paillier-like extractable commitment.

We may utilize the Trace technique to retrieve the user's identity from the related credential by using a trapdoor. Prior to the tracing phase, the access credential must perform an access credential sanity check (i.e., using the key sanity check technique). To achieve responsible authority, an access credential is jointly decided by both the authority and the associated user. This precludes the authority from having "absolute" control over the credential. The user is permitted to get the credential uac (based on his/her qualities and identity) from the authority via a secure access credential generation protocol. We give two effective revocation procedures to expressly or indirectly revoke harmful users. For explicit revocation, we explicitly mention a revocation list RL in the algorithm Encrypt. The master secret key an is divided into two halves during the execution of the algorithm Key Gen: one for access control and the other for revocation. Malicious users in RL will be unable to decipher any new ciphertext since the sub-master secret key corresponding to the revocation section cannot be wiped out during decryption. The Encrypt operation does not need to know the revocation list for implicit revocation.

To share the master secret key a between the secret key and the update key, we utilise a (random secret) first degree polynomial (*f*ðwÞ ¼ uw þ a) and *f*ð1Þ; *f*ðtÞ, where *f*ðtÞ is used for access control and ft is for revocation. Because hostile users in RL cannot access the update keys, they are unable to decipher any new ciphertext. The revocability attribute is obtained by combining the above-mentioned traceability and revocation techniques. In particular, the traceability method ensures that once a user is detected as malevolent (leaking credentials), his or her identity is placed on a revocation list.

3. FRAMEWORK MODEL AND DESIGN GOAL

Fig. 1 describes our CP-ABE based cloud storage system,with the following key entities:

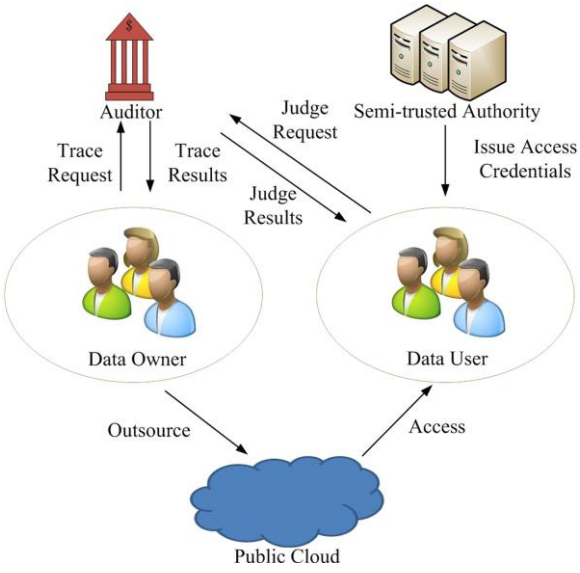

Fig. 1. CP-ABE based cloud storage system.

1. Before outsourcing (encrypted) data to a public cloud, data owners (DOs) encrypt their data in accordance with the necessary access regulations (PC).
2. PC manages data access requests from data users and saves outsourced (encrypted) data from DOs (DUs)
3. Approved DUs have access to the outsourced data (e.g., can download and decrypt it).
4. A semi-trusted authority (AT) produces system parameters and gives DUs with access credentials (i.e., decryption keys).
5. Auditor (AU) is trusted by other organizations and is in charge of audit and revocation procedures, as well as returning trace and audit findings to DOs and DUs.

The PC is truthful-but-curious in that it may obtain additional knowledge about the outsourced (encrypted) data but will not stray from the requirements (i.e., correctly executing tasks assigned by DOs). AT is semi-trusted in the sense that it may (re-)distribute access credentials to unauthorized individuals while generating system parameters (to be shared with AU) honestly. A completely trustworthy AU maintains a duplicate of the system parameters shared by AT. Our objective is to present a revocable and responsible Cloud with white-box traceability and auditing to meet the following requirements:
(1) Security assurances should be provided to ensure data confidentiality and access control flexibility over encrypted data.
(2) Computation should be cost-effective, with a focus on traceability and revocability.
(3) Audit, track, and revocation operations should be efficient in order to reduce the time it takes to catch a system betrayer.

4. SYSTEM SPECIFICATION

1) The capacity to track malevolent cloud users. Users who reveal their login credentials can be tracked down and identified.
2) Responsible power. It is possible to identify a semi-trusted authority who produces and distributes access credentials to unauthorized user(s) without sufficient authorization. This enables additional actions to be conducted (e.g. criminal investigation or civil litigation for damages and breach of contract).
3) Examining. An auditor can detect whether a (suspected) cloud user has leaked his or her access credential.
4) Tracing requires "almost" no storage. We employ a Paillier-like encryption as an extractable commitment in tracking malevolent cloud users, and we don't need to keep a user identification table for tracing.
5) Revocation of malicious cloud users. Access credentials for individuals who have been tracked and judged to be "compromised" can be withdrawn. We devise two procedures to effectively revoke the "traitor(s)." The ATER-CP-ABE provides an explicitly revocation mechanism in which a revocation list is explicitly specified in the algorithm Encrypt, whereas the ATIRCP-ABE provides implicit revocation in which the encryption does not need to know the revocation list but a key update operation is required on a regular basis.

5. BACKGROUND

5.1 Preliminaries

We define ½*l*] ¼ **f**1*; 2; . . . ; l*g to be *l* 2 N and ½0*; l*] ¼ ½*l*] [**f**0g, for *s* ← *S*, *s* is picked randomly from *S*.

Definition 1 (Access Structure). We define an access structure (respectively, monotone access structure) on S as a collection (respectively, monotone collection) A 2S of non-empty sets of attributes. A collection A 2S is monotone if 8B; C 2 A: if B 2 A and B C, then C 2 A. The permitted sets are those in A, while the illegal sets are those not in A.

Definition 2 (Linear Secret-Sharing Scheme (LSSS). Let S and p stand for universe and prime, respectively. A secret-sharing scheme with domain of secrets Zp realizing access structure on S is linear (over Zp) if (1) the shares of a secret s 2 Zp for each attribute form a vector over Zp; (2) for each access structure A on S, there exists a matrix M with l rows and n columns known as the share-generating matrix for i ¼ 1.

We define the following games to demonstrate if a system meets the aforementioned security standards. The IND-CPA Match.

5.2 Complexity Assumptions

Assumption 1 (Subgroup Decision Problem for Primes). *Given a group generator , define the following distribution:* G ¼ ðN ¼ $p_1p_2p_3$*; G; G*$_T$ *; e*Þ ← G, *g* ← G_{p_1}*;* X_3

The benefit of A in violating this assumption is defined as: Adv1G;AðλÞ ¼ jPr½AðD; T1Þ ¼ 1] — Pr½AðD; T2Þ ¼ 1]j. We say that G satisfies Assumption 1 if Adv1G;AðλÞ is a negligible function of λ for any probabilistic polynomial-time (PPT) algorithm A.

5.3 Zero-Knowledge Proof of Knowledge of Discrete Log

Informally, the zero-knowledge proof of knowledge (ZK-POK) of the discrete log protocol allows a prover to establish (to a verifier) that it possesses the discrete log t of a given group element T. Such a protocol has the following properties: zero-knowledge (proving that a simulator S can construct the view of a verifier in the protocol without being given the witness as input) and proof of knowledge (proving that a knowledge-extractor Ext can interact with the prover to extract the witness using the rewinding technique).

6. THE MODEL OF ATER-CP-ABE

6.1 Definition

An Responsible and Explicitly Revocable Authority CP-ABE with White-Box Traceability and Auditing (ATER-CP-ABE) is a CP-ABE technique capable of holding the misbehaving authority accountable, tracing malicious users using a given decryption key, determining if the suspect is guilty, and expressly rescinding harmful users. We rewrite the Setup, Encrypt, and We will now present our ATER-CP-ABE scheme.

6.2 Security

The ATER-CP-ABE system is secure if the three conditions listed below are met.

(1) It must meet the standard CP-ABE semantic security idea of ciphertext indistinguishability under selected plaintext assaults (IND-CPA).

(2) It is impossible for the authority to generate a decryption key sk such that the algorithm Trace (which takes sk as input) generates an identity id and the algorithm Audit (which takes id as input) finds that the corresponding user is guilty.

7. THE MODEL OF ATIR-CP-ABE

7.1 Definition

The Accountable Authority and Implicitly Revocable CP- ABE with White-Box Traceability and Auditing (ATIR-CP- ABE) system is similar to the ATER-CP-ABE scheme, We alter Setup by adding a revocation list, Encrypt by adding a current time attribute, and Key Update to accomplish implicit revocation of

rogue users. The ATIR-CP-ABE algorithms are nearly identical to those of the ATER-CP-ABE.

- Key Update: Given an input pp; msk, a current time attribute x, and a revocation list RL, the method generates and delivers the update key skx;RL for time period x to all non-revoked users.
- Encrypt outputs a ciphertext ct on input pp, a plaintext message m, an access structure A over the universe of attributes, and a present time attribute x.

7.2 Security

ATIR-CP-security ABE's requirements are identical to those of ATER-CP-ABE. Similarly, four security games must be defined: IND-CPA, Dishonest-Authority, Dishonest-User, and Key Sanity Check.

8. ATER-CP-ABE

8.1 Construction

- Setup: The procedure invokes the group generator G using as input and produces a bilinear group G of order N ¼ p1p2p3 (i.e., three unique primes), Gpi the subgroup of order pi in G, and g; g3 the generator of the subgroups Gp1; Gp3.It selects a; a; k; m 2 ZN and v 2 Gp1 at random.
- KeyGen: In the key generation protocol, both AT and interact as follows.
  ATER-CP-ABE have option Encrypt, Decrypt, Key Sanity Check, Trace, Audit.

9. THE PROPOSED CLOUD

We propose the Cloud based on ATER-CP-ABE and ATIR-CP-ABE. The system functions as follows. AT produces the system parameters initially in order to configure the system and then communicates the full system parameters (including public and private parameters) with AU. The public parameters are then published. AT also produces access credentials (decryption keys) for DUs based on their IDs and qualities.

DOs encrypt their data using access controls they choose, and then outsource the encrypted data to PC. To gain access to the underlying data, any authorized DU can decode the outsourced ciphertexts. A DU is approved if his or her collection of attributes fulfils the access policy imposed over the outsourced data. Cloud works as follows.

- System setup
- Cloud User Enrollment
- File Out Source
- File Access
- Access Credential Update
- Trace and Audit

Our Cloud was created with safe cloud storage in mind. A storage subscriber can be detected while engaging in some illegal activities, such as "sharing" storage and decryption rights with other non-subscribers. A cloud server may become aware of certain odd data access. Unusual events might include the circumstance where the access number of some specific encrypted files is dramatically raised, or the data access time is abruptly modified. These occurrences might be saved in a log, which would include the login time, IP address, and encrypted files. When a "decryption" device is discovered, the server may utilize the Trace technique to hunt out the malicious insider (using the log history as input) and revoke their access.

10. ADVANTAGES AND DISADVANTAGES

10.1 Advantages

1) Key Generation – In Proposed System the key generation is automatic. You don't need to type the attribute keys. Just click on it.

2) Data Integrity - Reducing cloud users' burden of storage management and equipment maintenance. Avoiding investing a large amount of hardware and software. Enabling the data access independent.

3) Security and Privacy - High accessibility, availability and reliability make cloud computing a better solution for interoperability problems.

4) SeDaSC - Data confidentiality and integrity; Access control; Insider threat security

10.2 Disadvantages

1) The existing CP-ABE based cloud storage systems fail to consider the case where access credential is misused.

2) Key Generation – In Existing System the key generation is Manual technique. We want to enter manually. So it is time consuming and also hard to remember the key to use it.

3) Data Storage May Not Be Safe - All of your data is saved on the cloud when you use cloud computing. That is all very well, but how secure is the cloud? Unauthorized users cannot access your personal data, can they?

11. EVALUATION

The complexity of ciphertext policy affects both the encryption and decryption times in CP-ABE systems. To account for this, we create ciphertext rules with the form (S1 and S2... and Sl) to mimic the worst-case scenario, where Si is an attribute. In other words, we may include our approach into a more effective CP-ABE to improve efficiency.

12. CONCLUSION AND FUTURE WORK

We tackled the problem of credential leakage in CP-ABE- based cloud storage systems in this study by establishing aresponsible authority and revocable Cloud that provides white-box traceability and auditing (referred to as Cloud). This is the first CP-ABE-based cloud storage solution thatoffers white-box traceability, responsible authority, auditing, and effective revocation all at the same time. Cloud, in particular, enables us to track down and deactivate rogue cloud users (leaking credentials). Our solution may also be employed when the semi-trusted authority redistributes the users'

credentials. The planned Cloud appears to be private and traceable. Private traceability only allows the tracing algorithm to be run by the system administrator, whereas partial/full public traceability allows the administrator, authorized users, and even anyone without access to the system's secret information to complete the trace. Our future work will involve expandingCloud to give "partial" and "complete" public traceability without sacrificing speed.

REFERENCES

[1] M. Ali et al., "SeDaSC: Secure data sharing in clouds," IEEE Syst. J., vol. 11, no. 2, June 2017, pp. 395-404.

[2] M. Ali, S. U. Khan, and A. V. Vasilakos, "Cloud Computing Security: Opportunities and Challenges," Inf. Sci., vol. 305, pp. 357-383, 2015.

[3] M. Armbrust et al., "A View of Cloud Computing," ACM Communications, vol. 53, no. 4, 2010, pp. 50-58.

[4] N. Attrapadung and H. Imai, "Attribute-based encryption supporting direct/indirect revocation modes," in proceedings of the IMA International Conference on Cryptography Coding, 2009, pp.278-300.

[5] A. Beimel, PhD thesis, Israel Institute of Technology, Faculty of Computer Science, Technion, Haifa, Israel, 1996.

[6] M.Bellare and O. Goldreich, “On Defining Proofs of Knowledge”, Proc,Annual International Cryptology Conference, 1992, pp. 390-420.

[7] D. Boneh and X. Boyen, "Short signatures without random oracles," in Proceedings of the International Conference on Theory and Applications of Cryptographic Technology, 2004, pp. 56-73.

[8] H. Cai, B. Xu, L. Jiang, and A. V. Vasilakos, "IoT-based large data storage systems in cloud computing: Perspectives and difficulties," IEEE Internet Things J., vol.4, no. 1, Feb. 2017, pp. 75-87.

[9] J. Chen, R. Gay, and H. Wee, "Improved dual system ABE in prime-order groups via predicate encodings," in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 595-624, 2015.

[10] A. De Caro and V. lovino, “JPBC, Java paring- based cryptography”, IEEE Symposium on computer Communications, 2011, pp. 850-855.