Enhanced Retreat of Cloud Storage Data users by Using Improved Data Access Control Scheme for Multi-Authority Cloud Storage

Shafi Shaik[1], M. Geethalatha[2]

[1]M.Tech, CS, Rise Krishna Sai Prakasam Group of Institutions

[2]Associate Professor, CS, Rise Krishna Sai Prakasam Group of Institutions

Abstract: ***The number of user in cloud computing are increasing tremendously due to its advantage of providing flexible storage requirement. The users are started to share their sensitive information through the cloud due to its nature of providing convenience to users. The security of the data has to be assured to the users when storing their details into the cloud server. In the existing work an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems is proposed to support the authority access control get from the many attribute authorities. The users those who are having matching attributes as in the access policy defined in the cipher text can retrieve the entire data content. It aims to allow the users with eligible attributes to decrypt the entire data stored in the cloud server. However it cannot limit the users from accessing the data's which are not accessible to them. That is it cannot limit the data access control to the authorized users. In this work a novel algorithm namely Privacy enhanced Data Access Control Scheme is proposed to overcome the problem exist in the existing work. In the existing work data access control is limited to the user from the unauthorized users whereas in the proposed algorithm aim to limit the data access control to the authorized user.***

Keywords: access control; multi-authority; security; cloud storage

1. Introduction

One important service provided by cloud computing to the data owners to outsource their data in cloud is cloud storage. The method of data outsourcing and data access counters a major challenge in data access control. The reason is that the data owners cannot fully trust the cloud servers. Ciphertext-Policy Attribute-Based Encryption(CP-ABE) is considered as acceptable technology in cloud storage systems for data access control. In this scheme, there is an authority which is responsible for attribute management and key distribution. For multi-authority system, cipher text policy based encryption is deployed. It handles the attributes from different authorities. The encrypted plain text is integrated with attributes. By using the symmetric key encryption algorithm the data will be encrypted under the access control scheme came from the attribute authority. The CP-ABE system is classified into two types: single-authority CP-ABE, where single authority manages all the attributes, and multi-authority CP-ABE, where different authorities manages attributes from different domains. Multi-authority CP-ABE is most suitable for data access control in cloud storage systems, as multiple authorities issues attributes that user holds and the data owners can share their data‟s.

In this paper we propose Privacy enhanced Data Access Control Scheme. Before storing the data‟s in the cloud, the owner will encrypt the message with the different id‟s which are created randomly. After encryption, the aggregated key for the receiver in order to decrypt the message will be generated with the help of owner private key. The receiver can retrieve the content that he needed by decrypting the cipher text with the help of aggregated key and corresponding access permission id. In this work the data anonymity level is increased by wrapping the data values before data transmission. That is user request is achieved by wrapping around the user access permission details with the data before transmitting/ storing it in the server. Hence only the user who satisfies the corresponding access permission details like verification information only will gain access to it. Based on the access permission given to the users, the new encryption key will be generated for individual users. By using the encryption that is generated for the unique user, each user can download the data‟s which is only accessible to them.

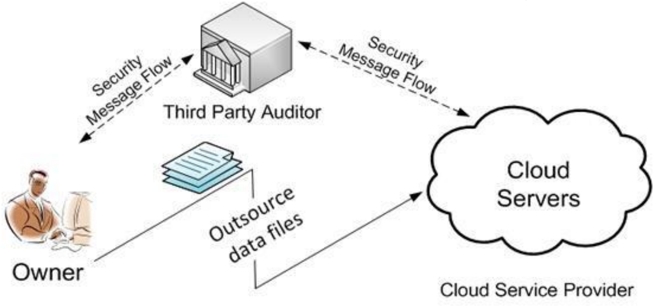
In our scheme, the key update is done by each attribute authority and not by the servers. The semi trusted natures of authorized user are eliminated where the data‟s are hidden from the authorized users also and it achieves more privacy and security over data‟s.

The remaining paper is structured as follows. Section II describes the background. Section III describes the structure and the system model. The construction of the data access control scheme is given in section IV. The security analysis is described in section V. The conclusion is given in section VI.

2. Background

In a multi-authority cloud storage system, attributes of user‟s can be changed dynamically. A user may be join some new attributes or revoked some current attributes In 2010, S. Yu, C. Wang, K. Ren, and W. Lou, worked on “Attribute Based Data Sharing with Attribute Revocation,‟‟. This paper use semi-trustable on-line proxy servers. This server enables the authority to revoke user attributes with minimal effort. This scheme was uniquely integrating the technique of proxy re-encryption with CP-ABE, and also enables the authority to delegate most of laborious tasks to proxy servers. The advantages of this scheme is More Secure against chosen cipher text attacks.Provide importance to attribute revocation which is difficult for CP-ABE schemes.

Various computing needs are to be provided for the users and companies, who use cloud services. Reliability and availability should be maintained with the Cloud Service Provider in the form of Data Centers, they are maintaining in any part of the world. Apart from these, customers who are worried about their data which contains sensitive information such as medical records or financial information and business related data has to be stored securely.



1. Security Risks in Single and Multi-authority cloud storage

While users outsource their confidential information to cloud, the cloud service provider verifies the user data with the Third Party Auditor without knowing the data; it verifies the integrity and correctness of data. In single cloud, due to any byzantine failure or service unavailability, network problems with disaster or some other leads the user data in risks. Even they had been protecting using Cryptosystems, Cloud Service Provider cannot assure the risk involved in Single cloud or Multi-authority cloud storage.

3. System Model and Security Model

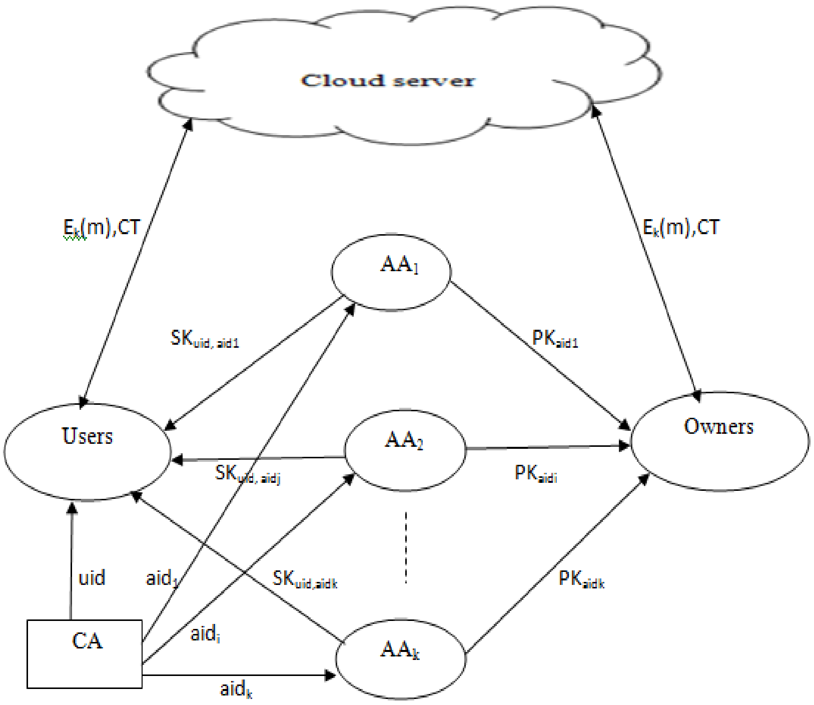
A. System Model

The data access control scheme which we consider in multi-authority cloud storage is described in Fig. 1. Five types of entities are there in the system: certificate authority(CA), attribute authority(AA), data owner, data consumer, the cloud server. The trusted certificate authority in the system is the CA. The system is set up and the registration of all user and AAs are accepted. The CA assigns the global unique id and also generates a global public key for each legal user.

AA is responsible for revoking user‟s attributes according to their role or identity. Every attribute is associated with single AA, but number of attributes are managed by AA. The attributes‟ structure and semantics are controlled by every AA. The public attribute key for each attribute it manages and a secret key or each user is generated by each AA.

This architecture states that the owner outsources the data with the semi-trusted cloud servers with encrypted cryptosystems. When users want to access the data from cloud servers, users has to be maintained by the Certificate Authority who issues the authentication certificate to user to access data. After obtaining the certificate user and owners share the data with the attributes verification for data access.

In this system each user has a global identity. The user can have set of attributes which come from multiple attribute authorities. The corresponding attribute authorities entitle its user associated with a secret key. The data is divided into several components by the owner and each data component is encrypted with different content keys using symmetric encryption.



The access policies over the attributes are defined are defined by the owner and encrypts the content keys under the policies. The owner then sends the encrypted data together with the ciphertexts to the cloud server. The user is able to decrypt the ciphertext only when the user‟s attributes satisfy the access policy defined in the ciphertext. The different number of content keys is decrypted by users with different attributes and from same data different information‟s are obtained.

B. Structure

The structure of the data access control scheme for multi-authority cloud storage system consists of following phases.

Phase 1: System initialization.

- **CASetup** (1λ): (GMK, GPP, (GPK‟uid, GPK‟uid), (GSKuid;GSK‟uid), Certificate(uid)). The CA setup algorithm is run by the CA. It takes no input other than the implicit security parameter λ. It generates the global master key GMK of the system and the global public parameters GPP. For each user uid, it generates the user‟s global public keys (GPKuid, GPK‟uid), the user‟s global secret keys (GSKuid , GSK‟uid) and a certificate Certificate (uid) of the user.
- **AASetup** (Uaid):(SKaid, PKaid, {VKxaid, PKxaid }xaid ϵ Uaid). The attribute authority setup algorithm is run by each attribute authority. It takes the attribute universe Uaid managed by the AAaid as input. It outputs a secret and public key pair (SKaid, PKaid) of the AAaid and a set of version keys and public attribute keys {VKxaid, PKxaid }xaid ϵ Uaid for all the attributes managed by the AAaid.

Phase 2: Attribute Authority's key management.

- **Secret Key Distribution:** A randomized algorithm takes as input the authority‟s secret key SK, a user u's UID, and a set of attributes Aku in the authority AAk's domain (We will assume that the user's claim of these attributes has been verified before this algorithm is run, Au = {Aku , k = 1, . . . , n}). Output a secret key Du for the user u.
- **Access Permission id Distribution:** The collected attributes from all attribute authorities (AC) will be sent to the users for the encryption purpose.

Phase 3: Data Encryption.
The data owner runs the encryption algorithm to encrypt the content keys. By using symmetric encryption method the data is encrypted with content keys. A randomized algorithm takes as input an attribute set of a message M, the system public parameters PK and outputs the ciphertext C.

Phase 4: Data Decryption.
To obtain the content keys, the users first run the decryption algorithm and use them to decrypt data‟s further.

Interpolation will be done: A deterministic algorithm takes as input a ciphertext C, which was encrypted under an attribute set and decryption key. Output a message m for atleast t+1 honest attribute authorities.

C. Security Model

The following assumption is made in multi-authority cloud storage systems:

- In the system the CA is fully trusted. It will not co-operate secretly with any user and should be prevented from decrypting the ciphertext by itself.
- The trusted AA can be corrupted by the adversary.
- The server is curious about the content of data to be encrypted or to the message received. But the server is honest and will execute the task assigned by each attribute authority correctly.
- The dishonest user may co-operate secretly to obtain the unauthorized access of data.

4. Data Access Control Scheme

The overview of constraints and techniques is given in the system. The construction of access control scheme consists of five phases: System initialization, Key Generation, Data Encryption, Data Decryption and Attribute Revocation.

A. Overview

The major constraint to design the data access control scheme is to develop the Revocable multi-authority CP-ABE protocol. This protocol is not directly deployed because of the two major reasons:
1) *Security Constraint*: The central authority holds the master key of the system and is allowed to decrypt the ciphertexts.
2) *Revocation Constraint:* Attribute revocation is not supported by this protocol.

Based on single-attribute CP-ABE a fresh revocable multi-authority CP-ABE protocol. In this method, to prevent illegal co-operation, we combine the secret keys produced by various authorities for same user. The functionality of authority is separated as global certificate authority (CA) and multiple attribute authority (AAs). The system is setup up by CA and registration of the user‟s and AAs are accepted. For each user, a global user identity *uid* and for each attribute authority, a global authority identity *aid* are assigned. Because of the globally unique uid, the secret key issued by various AAs for same user are combined together for decryption.

To overcome the security constraints, despite of using the system unique public key to encrypt data, our method needs all attribute authorities to provide their own public key to encrypt data combined with global public parameter. In this scheme the certificate authority is prevented from decrypting the ciphertexts.

The attribute revocation problem is solved by assigning the version number for each attribute. An attribute revocation happens only when the components associated with the revoked attribute in secret keys and ciphertexts needs to be updated. When the user‟s attribute is revoked from its corresponding AA, it generates a fresh version key for this revoked attributes and update key is generated. With the generated update key all user who are holding the revoked attribute can update its secret key. The revoked attribute can be updated to new version using the update key. The efficiency can be improved by using the proxy re-encryption method for selecting the workload of ciphertext update, so that freshly joined user can able to decrypt the data that was published earlier.

B. System Initialization

The system initialization consists of two steps: CA setup and AA setup.

1. CA Setup

Taking input as security parameter, the CA sets up the system using the CAsetup Algorithm. The CA registers both user and AA.

- **User Registration:** During system initialization each and every user should register to CA. The global unique user id *uid* is assigned to user by the CA, if the user is a legal user.
- **AA Registration:** During system initialization the AA should register to CA. The CA assigns a global attribute authority identity *aid* if the AA is the legal authority.

2. AA Setup

In this algorithm, the set of user attributes and data owner attributes are stored in data set, which provides the secret key obtained by matching the public key pair AAaid as input.
SkeyGen(GPP,GPKuid,GPkuid,GSKuid,SKaid,Suid,aid…) ={GPK,(PKaid1..n)with uidK} =SKuidnaidn

C. Secret Key Generation

When data owners outsource their data with some attributes and is encrypted by attributes identity (aid) then it authenticates with user identity (uid), which is issued by CA. {GPK□ (PKuid1,aid1 = g1r1uid,aid,…gnrnuidnaidn) =GPKuid1…n,aid1..n. The secret key SKuid,aid only contains the first component Kuid,aid, if the user uid does not hold any attribute from AAaid.

D. Data Encryption by Owners

Before outsourcing the data‟s to cloud, the data owner first partitions the data into several components according to logical granularities as m={m1,….mn}. For example, data can be partitioned into {name, address, employee, salary, contact number}, next the data components is encrypted with different content keys{k1,…..,kn} using symmetric encryption method, last the access structure mechanism Mi is defined for each content key ki(i=1,…,n). The encryption algorithm takes GPP as input, a collection of publis keys fpr all AAs and outputs the ciphertext CT= GPP,{PKaidk} aidk =k(ΠaidЄAAsPK aidk =PKaid1..n

E. Data Decryption by Users

In existing scenario, user login in to the CSPs and the data's can be downloaded with the normal registration, but in existing system the CA will check the user authentication entity. The user can obtain the content key only when it satisfies the access structure defined in the ciphertext CT. The decryption is as follows Decrypt(CT,GPKuid,GSKuid{SKuid,aid}□ K = (ΠaidЄAAsK'aidkuidk} =(ΠaidЄAAsguid,ruid..n) =CT,GPKuid,GSKuid =Kuid.

5. Security Analysis

Our data access control is secure when we achieve both forward security and backward security such as the AAid and GPPuidaid at the time of data encryption and along with ciphertext CT, GPKuid,GSKuid we obtain the K to decrypt the content.

1. Forward Security

The version of the revoked attribute is updated after attribute revocation problem. The secret keys are associated with attributes with the latest version, when a fresh user joins the system. The early published ciphertexts are encryptedunder attributes with previous version. The early published ciphertext can be updated to new version by using ciphertext update algorithm, so that the new user's can decrypt the previously published ciphertexts,if their attribute satisfy the access policy defined in the ciphertext. The forward security is guaranteed.

2. Backward Security

The *AA* generates an update key for each non revoked user, during the secret key update phase. The revoked user cannot use update keys of other non-revoked users to update its own secret key, because the update key is associated with the user's global identity *uid*, even if it may compromise to some non-revoked users. Moreover, suppose the revoked user can corrupt some other AAs, the item in the secret key can prevent users from updating their secret keys with update keys of other users. This guarantees backward security.

6. Related Work

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) [2]-[3] is a promising technique that is designed for access control of encrypted data. There are two types of CP-ABE systems: singleauthorityCP-ABE [where all attributes aremanaged by a single authority, andmulti-authority CP-ABE where attributes are from different domains and managed by different authorities. Multi-authority CP-ABE is more appropriate for the access control of cloud storage systems, as users may hold attributes issued by multiple authorities

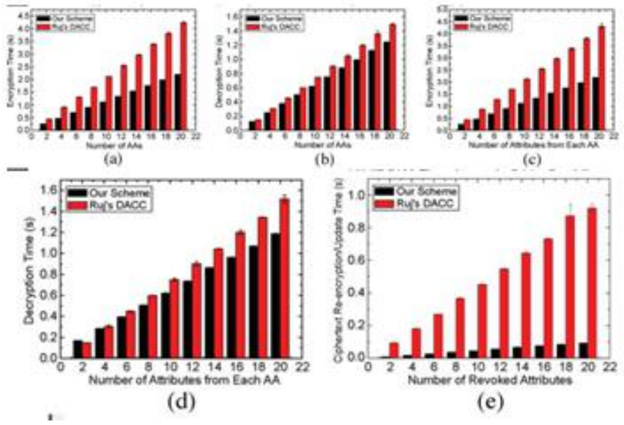


Figure 3: Comparison of Computation Time. (a) Encryption. (b) Decryption. (c) Encryption. (d) Decryption. (e) Re-encryption.

and the data ownersmay share the data using access policy defined over attributes from different authorities.

However, due to the attribute revocation problem, these multi-authority CP-ABE schemes cannot be directly applied to data access control for such multi-authority cloud storage systems. To achieve revocation on attribute level, some reencryption- based attribute revocation schemes are proposed by relying on a trusted server.

7. Conclusion

Although the use of cloud computing has rapidly increased, the security in cloud is major issue, and at the same time users don't want to lose their data. In this paper, we introduced a novel approach called Distributed key distribution mechanism. Then the effective data access control scheme is constructed for multi-authority cloud storage systems. This technique can be deployed in any social networks and remote storage systems.

References

[1] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy (SP '07), pp. 321-334, 2007.

[2] P. Mell and T. Grance, „„,The NIST Definition of Cloud Computing,"" National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep., 2009.

[3] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, „Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption,"" in Proc. Advances in cryptology-EUROCRYPT'10, 2010, pp. 62-91.

[4] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, „„,Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,"" IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan. 2013.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS '10), 2010.

[6] J. Hur and D. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Transactions on Parallel and Distributed Systems*, 2010.

[7] S. Ruj, A. Nayak, and I. Stojmenovic, DACC: Distributed Access Control in Clouds,"" in Proc. 10th IEEE Int'l Conf. TrustCom, 2011, pp. 91-98

[8] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in *ACM Conference on Computer and Communications Security*, E. Al-Shaer, A. D. Keromytis, and V. Shmatikov, Eds. ACM, 2010, pp. 735–737.

[9] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security, vol. 19, pp. 367-397, 2010.

[10] D. Boneh and M.K. Franklin, „„,Identity-Based Encryption from the Weil Pairing,"" in Proc. 21st Ann. Int'l Cryptology Conf.: Advances in Cryptology - CRYPTO'01, 2001, pp. 213-229.