ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Significant, Resourceful and Revocable Records Access Control For Multi Ability Cloud Storages

G.Usha Sree
M.Tech,
Department of Computer Science & Engineering,
TKR College of Engineering and Technology.

Dr.A.Suresh Rao
Professor & HOD,
Department of Computer Science & Engineering,
TKR College of Engineering and Technology.

Abstract:

Current Cloud computing is one of the emerge technologies. To protect the data and privacy of users the admittance control methods ensure that authorized user'sadmittance the data and the system. Cipher text-Policy Attribute-based Encryption (CP-ABE) is the appropriate method for data admittance control in cloud storage. However, CP-ABE schemes to data admittance control for cloud storage systems are difficult because of the attribute revocation problem. Specifically, this paper surveys a revocable multi-authority CP-ABE scheme. The attribute revocation method can efficiently achieve both forward security and backward security.

Keywords:

Cipher text-policy Attribute-based encryption (CP-ABE), cloud storage, data admittance control, multi-authority CP-ABE protocol.

I. INTRODUCTION:

All Data admittance control is an efficient way to ensure the data security in the cloud. Cloud storage services allows data owner to outsource their data to the cloud. Attribute-based encryption (ABE) [1] is a new concept of encryption algorithms that allow the encrypt or to set a policy describing who should be able to read the data. In an at-tribute-based encryption system, private keys distributed by an authority are associated with sets of attributes and cipher texts are associated with formulas over attributes. A user should be able to decrypt a cipher text if and only if their private key attributes satisfy the formula. In traditional public-key cryptography, a message is encrypted for a Specific receiver using the receiver's public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the conventional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g. roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (cipher text-policy ABE - CP-ABE).In cipher text-policy attribute-based encryption (CP-ABE) a user's private-key is associated with a set of attributes and a cipher text specifies an admittance policy over a defined universe of attributes within the system. A user will be able to decrypt a cipher text, if and only if his attributes satisfy the policy of the respective cipher text. Cipher text-Policy Attribute-based Encryption (CP-ABE) is considered as one of the most suitable scheme for data admittance control in cloud storage.

This scheme provides data owners more direct control on admittance policies [2]. However, CP-ABE schemes to data admittance control for cloud storage systems are difficult be-cause of the attribute revocation problem. So this paper produce survey on efficient and revocable data admittance control scheme for multi-authority cloud storage systems, where there are multiple authorities cooperate and each authority is able to issue attributes independently. CP-ABE thus allows to realize implicit authorization, i.e., authorization is included into the encrypted data and only people who satisfy the associated policy can decrypt data. Another nice feature is that users can obtain their private keys after data has been encrypted

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

with respect to policies. So data can be encrypted without knowledge of the actual set of users that will be able to decrypt, but only specifying the policy which allows decrypting. Any future users that will be given a key with respect to attributes such that the policy can be satisfied will then be able to decrypt the data. There are two types of CP-ABE systems: single-authority CP-ABE, and multi-authority CP-ABE. In single-authority CP-ABE scheme [3], where all attributes are managed by a single authority. In multi-authority CP-ABE [4], where attributes are from different domains and managed by different authorities. This method is more suitable for data admittance control of cloud storage systems. Users contain attributes those should be concerned by multiple authorities and data owners. Users may also share the data using admittance policy defined over attributes from different authorities.

CP-ABE TYPES:

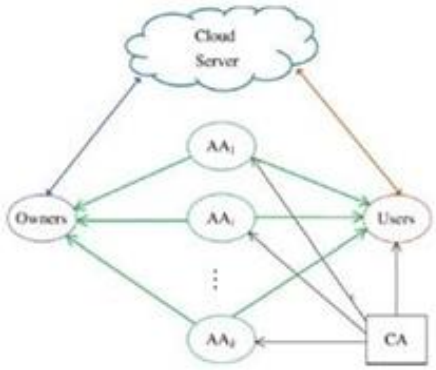
In CP-ABE scheme each user will be issued a secret key reflecting its attributes. A user can decrypt the data only when its attributes satisfy the admittance policies. There are two types of CP-ABE systems:

Single-authority CP-ABE
Multi-authority CP-ABE

In Single-authority CP-ABE scheme, where all attributes are managed by a single authority. In a Multi-authority CP-ABE scheme where attributes are from different do-mains and managed by different authorities. This method is more appropriate for data admittance control of cloud storage systems. Users contain attributes those should be is-sued by multiple authorities and data owners. Users may also share the data using admittance policy defined over attributes from different authorities.

DATA ADMITTANCE CONTROL SYSTEM IN MULTI AUTHORITY CLOUD STORAGE:

There are five types of entities in the system AS IN Fig 1: a certificate authority (CA), attribute authorities (AAs), data owners (owners), the cloud server (server) and data consumers (users). The CA is a global trusted certificate authority in the system. It sets up the system and accepts the registration of all the users and AAs in the system. For each legal user in the system, the CA assigns a global unique user identity to it and also generates a global public key for this user. However, the CA is not involved in any attribute management and the creation of secret keys that are associated with attributes. For example, the CA can be the Social Security Administration, an independent agency of the United States government. Each user will be issued a Social Security Number (SSN) as its global identity. Every AA is an independent attribute authority that is responsible for entitling and revoking user's attributes according to their role or identity in its domain.



In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of at-tributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it man-ages and a secret key. For each user reflecting his/her attributes.

II.RELATED WORK:

Data access control scheme is more important hence more works have conducted in this field the important and related works have been discussed here. Cipher text-Policy Attribute Based encryption (CP-ABE) [1]: Cipher text-Policy Attribute Based encryption scheme represented a system for realizing complex access

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

control on encrypted data. Using this technique encrypted data is kept confidential even if the storage server is untrusted. The proposed system allows for a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over their attributes specifying which users can decrypt it. It was proved secure only under some general group heuristic, and not in other situations. Single Authority Cipher text-Policy Attribute Based encryption. Here there exist only one authority which provides attributes to multiple users. And all the attributes are Attribute Based Revocable Data Access Control for Multi Authority Cloud Storage managed by this authority only. This produced a security problem and overhead to the authority as all the users need to be maintained and managed by this authority only. It was not efficient too. Multi-Authority Cipher text-Policy Attribute Based encryption. Here multiple authorities exist in the system all the authorities are included in the distribution of the attributes to the users.

This scheme is more appropriate for data access control of cloud storage systems, as users may hold attributes issued by multiple authorities and data owner can share the data using access policies defined on the attributes by different authorities. This reduced the overhead of maintaining different users. Multi-authority CP-ABE scheme represented attribute revocation problem. Attribute Revocation. As multiple authorities exist there will be multiple attributes to the user and the attributes can be changed dynamically. That is a user can be given some new attributes by the authority or revoked some existing attributes. This kind of attribute revocation should be considered accordingly. The new scheme overcomes the problem of revocation but still there exist security problems in the existing system.

III.PROPOSED SYSTEM:

This paper, surveys a revocable multi-authority CP-ABE scheme, to solve the attribute revocation problem in the system.

This method is an efficient and secure revocation method. The attribute revocation method can efficiently achieve both forward security and backward security. In backward security scheme the revoked user cannot decrypt any new Cipher text that requires the revoked attribute to decrypt. In Forward security the newly joined user can also decrypt the previously published cipher texts, if it has sufficient attributes. Moreover, while updating the cipher texts, all the users need to hold only the latest secret key, rather than to keep records on all the previous secret keys.

OVERVIEW OF PROPOSED SYSTEM:

- Attribute revocation method can efficiently achieve both forward security and backward security.
- An attribute revocation method is efficient in the sense that it incurs less communication cost and computation cost, secure in the sense that it can achieve both backward security and forward security.

IV.PERFORMANCE ANALYSIS:

In this section, we analyze the performance of our scheme by comparing with the Ruj's DACC scheme and our previous scheme in the conference version, in terms of storage overhead, communication cost and computation efficiency. We conduct the comparison under the same se-curity level. Let jpj be the element size in the G;GT ;Zp. Suppose there are nA authorities in the system and each attribute authority AA_{aid} manages n_{aid}attributes. Let nU and nO be the total number of users and owners in the system respectively.

4.1 Storage Overhead:

The storage overhead is one of the most significant issues of the admittance control scheme in cloud storage

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Systems. Let $n_a = \sum_{k=1}^{n_A} n_{aid_k}$ denote the total number attributes in the system and $n_{a,uid} = \sum_{k=1}^{n_A} n_{uid,aid_k}$ denote the total number of attributes the user uid holds from all the AAs in the system. We compare the storage overhead on each entity in the system, as shown in Table 2.

TABLE 3
Communication Cost for Attribute Revocation

Operation	[13]	[14]	Our
Key Update	None	$n_{non\_x}\|p\|$	$n_{non\_x}\|p\|$
CT Update	$(n_{c\_x} \cdot n_{non\_x} + 1)\|p\|$	$n_{c\_aid}\|p\|$	$2\|p\|$

n_{non_x}: num of non-revoked users hold x;
n_{c_x}: num of ciphertexts contains x;
n_{c_aid}: num of attributes from the AA_{aid} in all ciphertexts.

1) Storage Overhead on Each:

AA Each AA needs store the information of all the attributes in its domain. Besides, in , each AA_{aid}also needs to store the secret keys from all the owners, where the storage overhead on each AA is also linear to the total number of owners n_O in the system. In our scheme, besides the storage of attributes, each AA_{aid}also needs to store a public key and a secret key for each user in the system. Thus, the storage overhead on each AA in our scheme is also linear to the number of usersn_U in the system.

2) Storage Overhead on Each Owner:

The public parameters contribute the main storage over-head on the owner. Besides the public parameters, owners are required to re-encrypt the cipher texts and owners are required to generate the update information during the revocation, where the owner should also hold the encryption secret for every cipher text in the sys-tem.

V.RELATED WORK:

Cipher text-Policy Attribute-Based Encryption (CP-ABE) is a promising technique that is designed for access control of encrypted data.

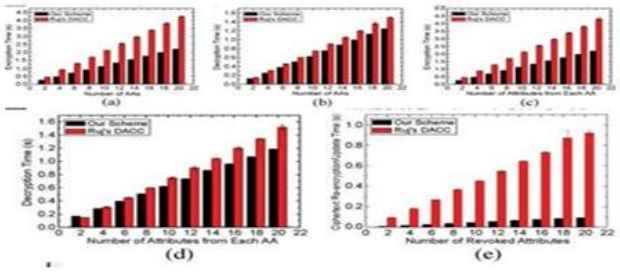


Fig. 3. Comparison of Computation Time. (a) Encryption. (b) Decryption. (c) Encryption. (d) Decryption.(e) Re-encryption.

There are two types of CP-ABE systems: single authority-ABE where all attributes are managed by a single authority, and multi-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 and the data owners may share the data using admittance 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 admittance control for such multi-authority cloud storage systems. To achieve revocation on attribute level, some re encryption- based attribute revocation schemes are proposed by relying on a trusted server. We know that the cloud server cannot be fully trusted by data owners, thus traditional attribute revocation methods are no longer suitable for cloud storage systems. Ruj,Nayak and Ivan proposed a DACC scheme, where an attribute revocation method is presented for the Lewko and Waters' decentralized ABE scheme. Their attribute revocation method does not require a fully trusted server. But, it incurs a heavy communication cost since it requires the data owner to transmit a new cipher text component to every non-revoked user.

VI.CONCLUSION:

In this paper, we proposed a revocable multi-authority CPABE scheme that can support efficient attribute re-vocation.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Then, we constructed an effective data admittance control scheme for multi-authority cloud storage systems. We also proved that our scheme was provable secure in the random oracle model. The revocable multi-authority CPABE is a promising technique, which can be applied in any remote storage systems and online social networks etc.

VII.REFERENCES:

[1] P. Mell and T. Grance, ‘‘The NIST Definition of Cloud Computing,’’ National Institute of Standards and Technology,Gaithersburg, MD, USA, Tech. Rep., 2009.

[2] J. Bethencourt, A. Sahai, and B. Waters, ‘‘Ciphertext- PolicyAttribute-Based Encryption,’’ in Proc. IEEE Symp. Security andprivacy (S&P’07), 2007, pp. 321-334.

[3] B. Waters, ‘‘Ciphertext-Policy Attribute-Based Encryption: AnExpressive, Efficient, and Provably Secure Realization,’’ in Proc.4th Int’l Conf. Practice and Theory in Public Key Cryptography (PKC’11), 2011, pp. 53-70.

[4]V. Goyal, A. Jain,O. Pandey, andA. Sahai, ‘‘Bounded Cipher text Policy Attribute Based Encryption,’’ in Proc. 35th Int’l Colloquium on Automata, Languages, and Programming (ICALP’08), 2008,pp. 579-591.

[5] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters,‘‘Fully Secure Functional Encryption: At-tribute-Based Encryptionand (Hierarchical) Inner Product Encryption,’’ in Proc.Advances in Cryptology-EURO-CRYPT’10, 2010, pp. 62-91.

[6]M. Chase, ‘‘Multi-Authority Attribute Based Encryption,’’ inProc. 4th Theory of Cryptography Conf. Theory of Cryptography(TCC’07), 2007, pp. 515-534.

[7]M. Chase and S.S.M. Chow, ‘‘Improving Privacy and Securityin Multi-Authority Attribute-Based Encryption,’’ in Proc. 16thACM Conf. Computer and Comm. Security (CCS’09), 2009,pp. 121-130.

[8] A.B. Lewko and B. Waters, ‘‘Decentralizing Attribute- BasedEncryption,’’ in Proc. Advances in Cryptology- EUROCRYPT’11,2011, pp. 568-588.