International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Upgraded Secrecy of Cloud Storage Data Users Using Improved Data Access Control Strategy for Multi-Authority Cloud Storage

Shaik Baazi[1], S. Sailaja[2]

[1]M.Tech, CSE, Rise Krishna Sai Gandhi Group of Institutions
[2]Associate Professor, CSE Dept, Rise Krishna Sai Gandhi Group of Institutions

Abstract: ***Cloud computing is one of the emerge technologies. To protect the data and Secrecy of users the access control strategy ensures that authorized users can access the data and the system. Cipher text-Policy Attribute-based Encryption (CP-ABE) is a method for data access control in cloud storage. However, CP-ABE schemes to data access control for cloud storage systems are difficult because of 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: CP-ABE, cloud storage, data access control, multi-authority CP-ABE protocol

1. Introduction

All Data access 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 encryptor to set a policy describing who should be able to read the data. In an attribute-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 access 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 access control in cloud storage.

This scheme provides data owners more direct control on access policies [2]. However, CP-ABE schemes to data access control for cloud storage systems are difficult because of the attribute revocation problem. So This paper produce survey on efficient and revocable data access 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 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 access 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 access 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 access policies. There are two types of CP-ABE systems:

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

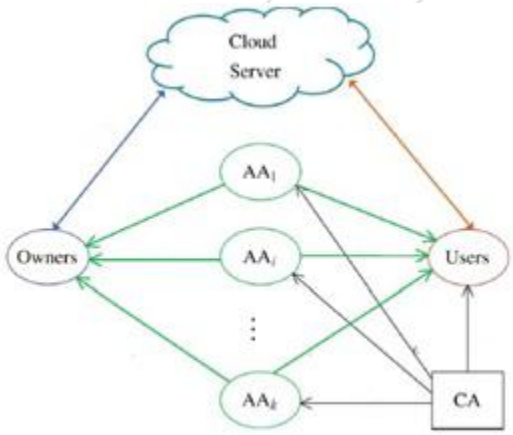
In Single-authority CP-ABE scheme, where all attributes are managed by a single authority. In a Multi-authority CP-ABE scheme where attributes are from different domains and managed by different authorities. This method is more appropriate for data access control of cloud storage systems. Users contain attributes those should be issued by multiple authorities and data owners. Users may also share

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

Data Access 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 attributes. 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 manages and a secret key. For each user reflecting his/her attributes.

2. Existing System

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.

Drawback

The storage overhead could be high if proxy servers keep all the proxy re-key. In 2011, S J. Hur and D.K. Noh, worked on Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems. This paper proposes an access control mechanism based on cipher text-policy attribute-based encryption to enforce access control policies with efficient attribute and user revocation method. The fine-grained access control can be achieved by dual encryption scheme. This dual encryption mechanism takes advantage of the attribute-based encryption and selective group key distribution in each attribute group. The advantage of this scheme is securely managing the outsourced data. This scheme achieve efficient and secure in the data outsourcing systems.

Drawback: • Huge issue in Enforcement of authorization policies and the support of policy updates.

Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation„„.The proposed Easier architecture that supports two approaches are fine-grained access control policies and dynamic group membership. Both scheme achieved by using attribute-based encryption, however, is that it is possible to remove access from a user without issuing new keys to other users or re-encrypting existing cipher texts. We achieve this by creating a proxy that participates in the decryption process and enforces revocation constraints. The advantage of this scheme is the Easier architecture and construction provides performance evaluation, and prototype application of our approach on Face book.

Drawback

• Does not Achieve Stronger Security Guarantees In 2013, S. Jahid, P. Mittal, and N. Borisov, worked on Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute Based Encryption,

This model proposes the use of dual system encryption methodology. The encryption techniques from Multi-authority ABE and Key-Policy ABE are combined into a single module. Use of MA-ABE technique proves beneficial for key management and flexible access and potential security threat of colluding users is handled by KP-ABE. The proposed framework has attempted to achieve data security by MA-ABE and data privacy by KP-ABE scheme. The overall security of the system has been improved.

Drawback:

• Existing attribute revocation methods rely on a trusted server or lack of efficiency also they are not suitable for dealing with the attribute revocation problem in data access control in multi-authority cloud storage systems. • Each Attribute authorities (AAs) is trusted but can be

corrupted by the adversary. Each user is dishonest and may try to obtain unauthorized access to data "Attribute Based Encryption with Verifiable Outsourced Decryption". This scheme changes the original model of ABE with outsourced decryption to allow for verifiability of the transformations in existing system. This new model constructs a concrete ABE scheme with verifiable outsourced decryption also does not rely on random oracles.

Drawback: Security Issue: Multi-authority CP-ABE protocol allows the central authority to decrypt all the cipher texts, be-cause it contains the master key of the system; Revocation Issue: Protocol does not support attribute revocation.

3. Proposed System

This paper, surveys a revocable multi-authority CP-ABE scheme [5], 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.

4. Performance Analysis

In this section, we analyze the performance of our scheme by comparing with the Ruj"s DACC scheme [13] and our previous scheme in the conference version [14], in terms of storage overhead, communication cost and computation efficiency. We conduct the comparison under the same security level. Let jpj be the element size in the G;GT ;Zp. Suppose there are nA authorities in the system and each attribute authority AAaid manages naid 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 access control scheme in cloud storage 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 [14], each AAaid 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 nO in the system. In our scheme, besides the storage of attributes, each AAaid 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 user"s nU in the system.

2) Storage Overhead on Each Owner:

The public parameters contribute the main storage overhead on the owner. Besides the public parameters, in [13], owners are required to re-encrypt the cipher texts and in [14] 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 system.

5. Related Work

Cipher text-Policy Attribute-Based Encryption (CP-ABE) [2]-[3] is a promising technique that is designed for access control of encrypted data.

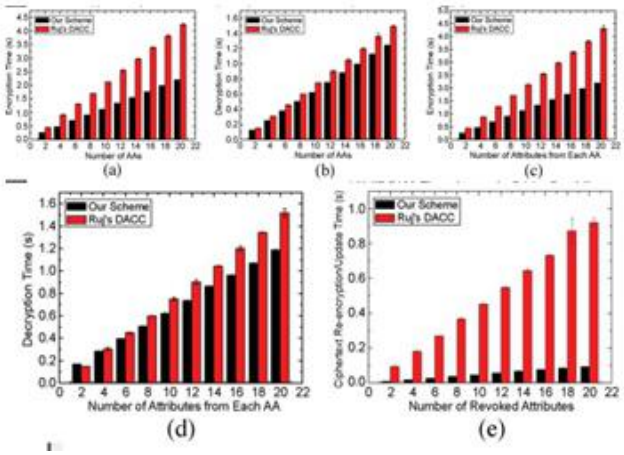


Figure 3: Comparison of Computation Time. (a) Encryption. (b) Decryption. (c) Encryption. (d) Decryption. (e) Re-encryption

There are two types of CP-ABE systems: single authority CP-ABE [2], [3], [4], [5] where all attributes are managed by a single authority, and multi-authority CP-ABE [6],[7], [8] 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 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 [9], [11] 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 [13], where an attribute revocation method is presented for the Lewko and Waters‟ decentralized ABE scheme [8]. 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.

6. Conclusion

In this paper, we proposed a revocable multi-authority CPABE scheme that can support efficient attribute revocation. Then, we constructed an effective data access 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.

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 Policy Attribute-Based Encryption,‟‟ in Proc. IEEE Symp. Security and privacy (S&P‟07), 2007, pp. 321-334.
[3] B. Waters, „„Ciphertext-Policy Attribute-Based Encryption: An Expressive, 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, and A. Sahai, „ „Bounded Ciphertext Policy Attribute Based Encryption,‟‟ in Proc. 35th Int‟l Colloquiumon 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 Encryption and (Hierarchical) Inner Product Encryption,‟‟ in Proc. Advances in Cryptology-EUROCRYPT‟ 10, 2010, pp. 62-91.
[6] M. Chase, „„Multi-Authority Attribute Based Encryption,‟‟ in Proc. 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 Security in 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 Based Encryption,‟‟ in Proc. Advances in Cryptology EUROCRYPT‟11,2011, pp. 568-588.
[9] S. Yu, C. Wang, K. Ren, and W. Lou, „„Attribute Based Data Sharing with Attribute Revocation,‟‟ in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS‟10), 2010,pp. 261-270.
[10] 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.
[11] J. Hur and D.K. Noh, „„Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,‟‟ IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.
[12] S. Jahid, P. Mittal, and N. Borisov, „„Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,‟‟ in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS‟11), 2011, pp. 411-415.
[13] 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.
[14] K. Yang and X. Jia, „„Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage,‟‟ in Proc. 32th IEEE Int‟l Conf. Distributed Computing Systems (ICDCS‟12), 2012, pp. 1-10.
[15] D. Boneh and M.K. Franklin, „„Identity-Based Encryption from the Weil Pairing,‟‟ in Proc. 21st Ann. Int‟ Cryptology Conf.: Advances in Cryptology - CRYPTO‟ 01, 2001, pp. 213-229.
[16] A.B. Lewko and B. Waters, „„New Proof Methods for Attribute- Based Encryption: Achieving Full Security through Selective Techniques,‟‟ in Proc. 32st Ann. Int‟l Cryptology Conf.: Advances in Cryptology - CRYPTO‟12, 2012, pp. 180-198