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

A New Approach for Data Access Control for Multi-Authority Cloud Storage


S.Rainy Sushma
M.Tech Student,
Department of CSE,
Sree Rama institute of Technology and Science,
Kuppenakuntla, Penuballi, Khammam,TS India.


S.Suresh
Assistant Professor,
Department of CSE,
Sree Rama institute of Technology and Science,
Kuppenakuntla, Penuballi, Khammam,TS India.

ABSTRACT:

Data access control is an effective way to ensure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a challenging issue in cloud storage systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. In this paper, we design an expressive, efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. Specifically, we propose a revocable multi-authority CP-ABEscheme, and apply it as the underlying techniques to design the data access control scheme. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

Index Terms:
Access control, multi-authority, CP-ABE, attribute revocation, cloud storage

INTRODUCTION:

CLOUDstorage is an important service of cloud computing , which offers services for data owners to host their data in the cloud. This new paradigm of data hosting and data access services introduces a great challenge to data access control. Because the cloud server cannot be fully trusted by data owners, they can no longer rely on servers to do access control. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable technologies for data access control in cloud storage systems, because it gives the data owner more direct control on access policies. In CP-ABE scheme, there is an authority that is responsible for attribute management and key distribution. The authority can be the registration office in a university, the human resource department in a company, etc. The data owner defines the access policies and encrypts data according to the policies. 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, 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 data access control of cloud storage systems, as users may hold attributes issued by multiple authorities and data owners may also share the data usingaccess policy defined over attributes from different authorities. For example, in an E-health system, data owners may share the data using the access policy "Doctor AND Researcher", where the attribute "Doctor" is issued by a medical organization and the attribute "Researcher" is issued by the administrators of a clinical trial. However, it is difficult to directly apply these multi-authority CP-ABE schemes to multi-authority cloud storage systems because of the attribute revocation problem.

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

Existing System:
System Model:

We consider a data access control system in multi-authority cloud storage, as described in Fig. 1. There are five types of entities in the system: 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.

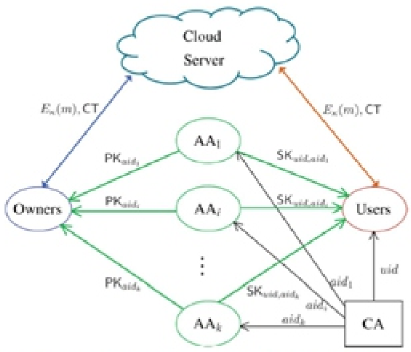

Fig. 1. System model of data access control in multi-authority cloud storage.

Proposed System:

In this section, we first give an overview of the challenges and techniques. Then, we propose the detailed construction of our access control scheme which consists of five phases: System Initialization, Key Generation, Data Encryption, Data Decryption and Attribute Revocation. To design the data access control scheme for multi authority cloud storage systems, the main challenging issue is to construct the underlying Revocable MultiauthorityCP-ABE protocol. In [6], Chase proposed a multi-authority CP-ABE protocol, however, it cannot be directly applied as the underlying techniques because of two main reasons: 1) Security Issue: Chase's multi-authority CP-ABE protocol allows the central authority to decrypt all the ciphertexts, since it holds the master key of the system;

2) Revocation Issue: Chase's protocol does not support attribute revocationWe propose a new revocable multi-authority CP-ABE protocol based on the single-authority CP-ABE proposed by Lewko and Waters in [16]. That is we extend it to multiauthority scenario and make it revocable. We apply the techniques in Chase's multi-authority CP-ABE protocol [6] to tie together the secret keys generated by different authorities for the same user and prevent the collusion attack. Specifically, we separate the functionality of the authority into a global certificate authority (CA) and multiple attribute authorities (AAs). The CA sets up thesystem and accepts the registration of users and AAs in the system.7 It assigns a global user identity uid to each user and a global authority identity aid to each attribute authorityin the system. Because the uid is globally unique in the system, secret keys issued by different AAs for the same uid can be tied together for decryption. Also, because each AA is associated with an aid, every attribute is distinguishable even though some AAs may issue the same attribute.

SECURITY ANALYSIS:

We prove that our data access control is secure under the security model we defined, which can be summarized as in the following theorems.

Backward Security:

During the secret key update phase, the corresponding AA generates an update key for each non-revoked user. Because the update key is associatedwith the user's global identity uid, the revoked user cannot use update keys of other non-revoked users to update its own secret key, even if it can compromise some non-revoked users. Moreover, suppose the revoked user can corrupt some other AAs (not the AA corresponding to the revoked attributes),

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

the item HðxaidÞvxaid _aid_aid in the secret key can prevent users from updating their secret keys with update keys of other users, since _aid is only known by the AAaid and kept secret to all the users. This guarantees the backward security.

Forward Security:

After each attribute revocation operation, the version of the revoked attribute will be updated. When new users join the system, their secret keys are associated with attributes with the latest version. However, previously published ciphertexts are encrypted under attributes with old version. The ciphertext update algorithm in our protocol can update previously published ciphertexts into the latest attribute version, such that newly joined users can still decrypt previously published ciphertexts, if their attributes can satisfy access policies associated with ciphertexts. This guarantees the forward security.

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: single authority CP-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 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.

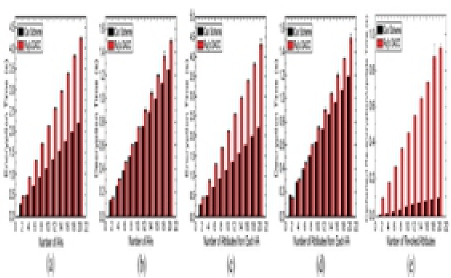

Fig.3 Comparison of Computation Time. (a) Encryption. (b) Decryption. (c) Encryption. (d) Decryption. (e) Re-encryption.

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.

ACKNOWLEDGMENT:

This work was supported by the Research Grants Council of Hong Kong under Project CityU 114112.

REFERENCES:

[1] P. Mell and T. Grance, "The NIST Definition of CloudComputing," 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 CiphertextPolicy 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: Attribute-Based Encryptionand (Hierarchical) Inner Product Encryption," in Proc.Advances in Cryptology-EUROCRYPT'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.

[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based DataSharing 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 SecureSharing of Personal Health Records in Cloud Computing UsingAttribute-Based Encryption," IEEE Trans. Parallel DistributedSystems, vol. 24, no. 1, pp. 131-143, Jan. 2013.

[11] J. Hur and D.K. Noh, "Attribute-Based Access Control withEfficient Revocation in Data Outsourcing Systems," IEEETrans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221,July 2011.

[12] S. Jahid, P. Mittal, and N. Borisov, "Easier: Encryption-BasedAccess Control in Social Networks with Efficient Revocation," inProc. 6th ACM Symp. Information, Computer and Comm. Security(ASIACCS'11), 2011, pp. 411-415.

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

[14] K. Yang and X. Jia, "Attribute-Based Access Control forMulti-Authority Systems in Cloud Storage," in Proc. 32th IEEEInt'l Conf. Distributed Computing Systems (ICDCS'12), 2012,pp. 1-10.

[15] D. Boneh and M.K. Franklin, "Identity-Based Encryption fromthe Weil Pairing," in Proc. 21st Ann. Int'l 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 SelectiveTechniques," in Proc. 32st Ann. Int'l Cryptology Conf.: Advances inCryptology - CRYPTO'12, 2012, pp. 180-198.

Author's:

S.Rainy Sushma is a student of Sree Rama Institute of Technology & Science, Kuppenakuntla,Penuballi, Khammam, TS,India.Presently she is Pursuing her M.Tech (CSE) from this collegeHis area of interests includes Information Security, Cloud Computing, Data Communication & Networks.

S. Suresh well known author and excellent teacher. He is working as a H.O.D for the Department of M.Tech., Computer Science & Engineering, Sree Rama Institute of Technology & Science, Kuppenakuntla, Penuballi, Khammam. He has vast teaching experience in various engineering colleges. To his credit couple of publications both National& International conferences / journals. His area ofInterest includes Data Warehouse and Data Mining,information security, Data Communications &Networks, Software Engineering and otheradvances in Computer Applications. He has guided many projects for Engineering Students