International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 4, July- August 2017 ISSN 2278-6856

Multi Authority Access Control in Public Cloud Storage System

[1]K.Sai Mouni Sri, [2]B.Dilip Kumar Reddy

[1]PG scholar, Dept of CSE, G. Pulla Reddy Engineering College(Autonomous) Kurnool (District), Andhra Pradesh-518002, INDIA,

[2]Assistant Professor, Dept of CSE, G.Pulla Reddy Engineering College(Autonomous), Kurnool (District), Andhra Pradesh-518002, INDIA,

Abstract

Data access control is an efficient scheme to grant information security within the cloud but as a result of information outsourcing over the cloud servers which are untrusted, the data access management has become a troublesome issue in the public cloud. Attribute-based cryptographic (ABE) technique is taken into account as a most trustworthy cryptographical conducting tool to make sure data owner's direct control on their info in public cloud storage. The previous ABE schemes involve just one authority to require care of the whole attribute set, which could bring a single-point hindrance on every security and performance. Paper planned an efficient revocable decentralized manner CP-ABE information access management technique for multi-authority systems, wherever there exist multiple authorities and every authority is prepared to issue attributes independent to each other.

Keywords: Data Access control, Attributes-Based Encryption, Data storage, Multi-Authority

1. INTRODUCTION

Cloud storage is a vital service of cloud computing [1], that which offers service for data owners in hosting their information within the cloud. This new paradigm of information hosting and data access services introduces an excellent challenge to data access control. Because the cloud server can't be totally trustworthy by data owners, they'll not trust servers to do access control. Among the different ABE schemes, the [2], [3]Ciphertext-Policy Attribute-based encryption (CP-ABE) is one of the foremost technologies that are applicable for controlling the data access mechanism in cloud, also providing the data owner further direct control on access policies.

Cloud storage is versatile; however, security and privacy are accessible for the outsourced information becomes an important concern. To attain secure data transaction within the cloud, appropriate cryptography technique is employed. The data owner should encrypt the file and that file gets stored onto the cloud. If an anonymous person tries to download the file, then he/she can read the record only if they had the key that is employed to decrypt the file that has been encrypted by the owner. To beat that problem, the Cloud computing is one of the rising technologies, that contains an immense open distributed system. It's necessary to safeguard the info and privacy of the user. CPABE is the foremost techniques used for the data access control mechanism in the cloud storage. It provides data owner direct control on access policies. However, it's tough to use the existing schemes (CPABE) onto the data access control for the cloud storage systems because of the drawback of the revocation. For that, designed an efficient revocable data access control technique for the multiple-authority public cloud storage systems, whenever the different authorities exists side-by-side and if each authority able to issue the attributes independent to each other. Specifically, projected a multiple-authority CPABE technique with revocation and apply this to the techniques that are underlying, for designing the info access-control [4]. Sharing data multi-owner manner whereas keeping the data and privacy for the identity from a cloud which is not trust worthy, may be a difficult issue.

In the multiple-authority public cloud storage, the attributes belonging to the user could also be changed dynamically. A user might even be entitled some new attributes or revoked some current attributes. And his permission of information access ought to be modified consequently. However, existing attribute methods on revocation [9], [10] either rely on a server which is trustworthy or lack of potency, they're not appropriate for coping with the drawback of the revocation of attributes in the data access control in multiple-authority systems in public cloud storage. Therefore, the decentralized data access control strategy was introduced.

2. RELATED WORK

The most suitable schemes for the data access controlling mechanism in public clouds is an Attribute based Encryption. It ensures the data owners to have the direct control over the data by providing a fine-grained access control service on data. There are different ABE schemes were proposed, which can be further divided into two different categories; KP-ABE as well as CPABE.

In the KP-ABE schemes, the decrypt keys are combined with the access structures and the ciphertexts are labeled with a special attribute set, for attribute management and then for the distribution of keys, an authority is responsible. That authority may be HRD in a company, any office of registration in a university etc. The data owner defines the access policies and encrypts the info in

consistent with the outlined policies. Each user is going to be issued a secret key for its attributes. A user would decipher the info whenever its attributes match the access policies. Access control strategies make sure that authorized user access information of the system. Access control is a procedure that allows or restricts the access. Access Control identifies the unauthorized users who attempt to access a system. This mechanism plays a vital role for protection as well as it provides computer security.
In CP-ABE technique, there exists an authority which may be responsible for the attribute management and then provide key distribution. There are a 2 different CP-ABE systems: single authority[2], [3], [4], [5] CPABE, where all the attributes can be managed by only 1 authority, and multi authority [6], [7], [8] CPABE, where all the attributes are from completely different domains and can be managed by different authorities. Multiple-authority based CPABE is acceptable mostly for obtaining the data access control over cloud, because the users might hold the attributes issued by multiple authorities and the data owners may additionally share the information using access policy outlined over attributes from completely different authorities.

This paper proposes the multi-authority data access control for cloud storage with ABE scheme and is organized as follows. **Section I** provide an Introduction. **Section II** discusses Background and Related work. **Section III** discusses existing methodologies. **Section IV** discusses System and security model. Finally, **section V** Conclude this paper.

3. EXISTING METHODOLOGIES

The brief structure of TMACS in the Fig. 1. In this approach TMACS, *AA*s ought to register to *CA* for obtaining the corresponding identity and certificate for attribute-authorities (aid, aid.cert). After that, *AA*s involving in the system construction, assists *CA* in completing the setting-up of the system parameters. *CA* accepts the users' registration and issues the identity as well as the certificate for each legal user (uid, uid.cert). With this certificate and identity, the user can contact with any *AA*s one by one to gain his/her secret key (*SK*). Owners who want to share and store their data in the public cloud, obtain the public key (*PK*) from *CA*. Then, the owner encrypts his/her data under the predefined access-policy and uploads the ciphertext, *CT* to the cloud. Users can freely download the ciphertext (*CT*) that he/she is interested in from the cloud server. However, he/she can't decrypt the ciphertext that was encrypted by the owner, unless his/her set of attributes gets matched with the access policy that was hidden in the data that was encrypted.

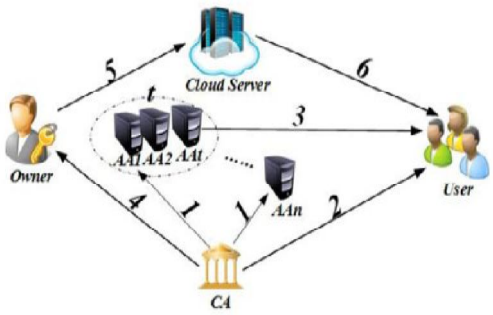

Fig 1: Basic protocol flow
(1) *AA* registers to obtain (*aid; aid:cert*) from CA;
(2) User registers to obtain (*uid; uid:cert*)from CA;
(3) User gains his/her *Secret Key* from any *k* out of *m AA*s;
(4) Owner obtains *Public Key* from the *CA*;
(5) Owner uploads ciphertext to the cloud server;
(6) User downloads ciphertext from the cloud server

To obtain secure information sharing for dynamic groups within the cloud, Authors expect to mix the group signature and dynamic broadcast cryptography techniques with each other. This group signature theme allows the users to use the cloud resources anonymously, and also this dynamic broadcast cryptography technique permits the data owners to firmly share their files with others as well as newly joined users.

Fig. 2: System model for MONA

DAC-MACS contain five steps namely, System Initialization, Generation of secret key, Encryption of data, Decryption and then Attribute Revocation. The authors outsourced the decryption mainly by utilizing a token-based-decryption method.

4. SYSTEM MODEL AND SECURITY MODEL

We consider a data access control system in multi-authority cloud storage, as described in Fig. 3. There are 5 kinds of entities within the system: a certificate authority, attribute authorities, data owners, the cloud server and the data consumers.
The Certificate Authority could accepts the registration of all the users and Attribute Authorities within the system. The Certificate Authority assigns globally unique identity for users and Attribute authorities and generates a global public key for the user.

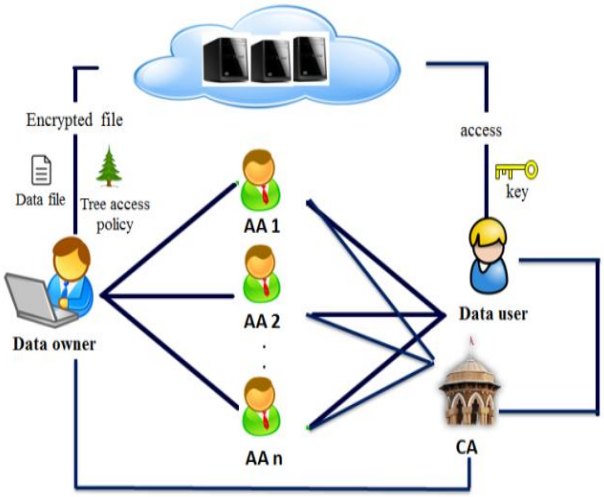

Fig 3: System model of data access control in multi-authority cloud storage.

The attribute authorities are responsible for attribute management and key generation. In contrast from the other existing multi-authority CP-ABE systems, all AAs jointly manage the whole attribute set, i.e., any single AA cannot assign users' secret keys alone for the master key is shared by all AAs. All AAs cooperate with each other to share the master key. Each AA gain a piece of master key share as its private key, then each AA sends its corresponding public key to CA to generate one of the system public keys. Each AA only should generate its corresponding secret key independently for the users.

The data owner (Owner) encrypts his/her file and defines access policy that can get access to his/her data. Each owner encrypts his/her data with a symmetric encryption algorithm like AES and DES. Then the owner formulates an access policy over an attribute set and encrypts the symmetric key under the policy according to attribute public keys that were gained from CA. Here, the symmetric key is the key used in the former process of symmetric encryption. After that, the owner sends the whole encrypted data and the encrypted symmetric key to store in the cloud server.

The data consumer (User) is assigned with a global user identity uid from CA, and applies for his/her secret keys from AAs with his/her identification. The user can decrypt the encrypted data if and only if his/her attribute set satisfies the access policy hidden inside the encrypted data. The cloud server provides a platform for the owners for storing and sharing their data that is in encrypted form. The encrypted data which is stored in the cloud server can be downloaded/ accessed freely by any data consumer who accepts the policy.

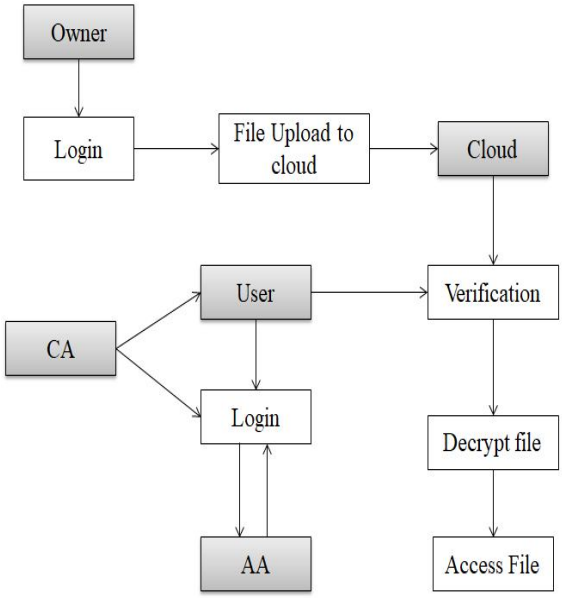

Fig 4: Data Flow Diagram

5. CONCLUISON

We propose a decentralized data access control technique with the concept of revocation for multiple-authority in the cloud storage systems. It minimizes decryption overhead on users based on the attributes. This ABE technique provides security for the data that is being shared in the cloud. This scheme 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, andA. Sahai, ''Bounded Ciphertext 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: Attribute-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. 16th ACM 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] B. Dilip Kumar Reddy, K. SaiMouni Sri, "A Survey on Multi Authority Access Control System in Cloud Storage", in proc. International Journal of Scientific Engineering and Technology Research, April-2017, Pages: 2635-2637

[11] Dilip Reddy. B, DrN.Kasiviswanath, DrS.ZahoorUlqHuq, "Peer to Peer Distributed Data Storage with Security in Cloud Computing", in proc. to IJESRT International Journal of Engineering Sciences & Research Technology, vol.6 June. 2014,pp. 402-406

Author

K.SaiMouni Sri, student pursuing M.Tech in Computer Science and Engineering from G Pulla Reddy Engineering College, Kurnool affiliated to Jawaharlal Nehru Technological University, Anantapur, AP 515002 India

B. DilipKumar Reddy, Assistant Professor in Computer Science and Engineering Dept. GPREC Kurnool, AP 518007 India. Research interest in the areas of computer networks.