Volume 2, Issue 12, December-2015, pp. 1182-1187 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Efficient Data Access Control for Multi-Authority Cloud Storage using CP-ABE.

[1]PRAVEEN KUMAR , [2]S.NAGA LAKSHMI

[1](M.Tech) CSE, Dept. of Computer Science and Engineering

[2]Assistant Professor, Dept. of Computer Science and Engineering

Priyadarshini Institute of Technology & Science

Abstract: Security and data privacy is paramount to cloud users seeking to protect their gigabytes of vibrant business data from the inquisitive eyes of unauthorized users who are attempting to exceed their authority and also it becomes a challenging issue in cloud storage systems. Ciphertext-Policy Attribute-based Encryption (CP-ABE) is observed as one of the most seemly technologies for data access control in cloud storage, because it gives more direct control access strategies to the cloud data owners. This CP-ABE scheme provides intrinsic security mechanisms designed to minimize the security attacks and threats in cloud system. In this paper, we design a Fortified Access control for Multi-Authority Cloud Storage Systems, where the process of data access control is strengthened to ensure the safety of the cloud data. Fortified access control to discourse not only the data privacy difficulties in existing control scheme, by using multiple authorities in the cloud storage system, the proposed scheme can efficiently reaches the tenable access control and revokes the anonymous access to the cloud data. The study and simulation analysis illustrates that proposed well organized Fortified Access Control is both secure and efficient for Cloud Storage Systems.

Key Terms: access control; multi-authority; security; cloud storage

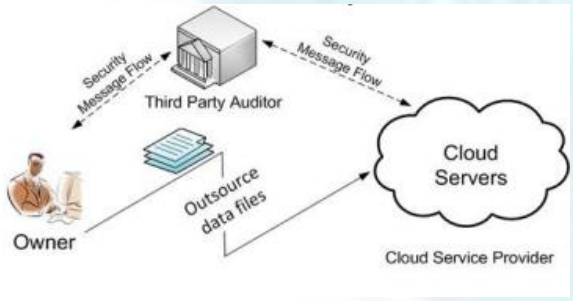
I.INTRODUCTION

Similar to Cloud Computing, Cloud Storage has also been growing in popularity recently due to many of the same reasons as Cloud Computing. Cloud Storage delivers virtualized storage on demand, over a network based on a request for a given quality of service (QoS). There is no necessity to purchase storage or in some cases even provision it before storing data. Cloud Storage is an important package of cloud computing, which offers pacts for cloud data vendors to host their data in the cloud. This new prototype of data hosting and access services introduces a great challenge to data access control. Because the cloud data vendors cannot be fully trust on cloud server and they are not equipped to trust on servers to control the data access. Ciphertext-Policy AttributeBased Encryption is viewed as one of the most appropriate technologies for data access control in cloud storage systems, because if offers more direct access control policies and strategies to the cloud data vendors. In CP-ABE scheme, there is a distinct authority that is responsible for attribute management, key generation, key transfer and key distributions. The authority can be the registered office located in different locations. The cloud data vendors can state the access strategies and encrypt the data according to the strategies. Each user will be supplied a secret key reproducing its attributes. The data can be decrypted the cloud users by verifying its attributes based on the access strategies.

CP-ABE

CP-ABE offers two types of systems: 1.Single Authority CP-ABE 2.Multi-Authority CP-ABE Single Authority CP-ABE: Attributes of the cloud data vendors are managed by sole authority. Extensive research has done for single authority in cloud storage system, a user may clench attributes issued by multiple authorities and the data

owners may share the data with the user managed to different authorities which is a great challenge in single authority. Multi-Authority CP-ABE: Attributes of the different domains and cloud data vendors are managed by different authorities. Multi-Authority CP-ABE is more apt scheme for data access control of cloud storage systems, as users may clench attributes issued by multiple authorities and data owners may also share the data using access policy defined over attributes from different authorities. In this paper, we first propose a Fortified multi-authority CPABE scheme, where an expressive, efficient and more secured revocation method is proposed to solve the attribute revocation and anonymous data access problems in the cloud storage system. Efficiency in computation and attribute revocation are the critical requirements while designing the access control schemes. In Efficient Computation, there are three operations required namely 1.Encryption 2.Decryption 3.Revocation In Efficient Attribute Revocation, there are two requirements 1.Backward Security 2.Forward Security In this paper, we design a new fortified multi-authority CP-ABE scheme with efficient decryption and offer an efficient attribute revocation method, and then an



II. BACKGROUND

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

Fig 1. Cloud Storage Scenario

. 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.

III. SYSTEM MODEL AND SECURITY MODEL

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 is 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.

Proxy layer: This proxy layer acts as interface between the users and the rest of the servers available in the cloud.

Cloud data server layer: Data server has two different entities can be recognized as the cloud users and the

cloud service provider. Multiple data servers are proposed in this scheme to avoid the traffic. Cloud

data storage server layer: All the data and the files are stored in these storage servers which are stored by the both individual customers and organizations. Similar to data server there are multiple storage servers are introduced to handle big volume of data

Cloud Key server layer: Multiple key servers are proposed in this scheme for efficient computation and attribute revocation method. Key server is used to store the secret key that are encrypted or fragmented by the key splitter.

Key splitter: Key splitter is used to divide cryptographic key K in n safe pieces K1, K2, Kn Such that knowledge of any J pieces can be used to compute K easily. These pieces are assigned to N nodes. Shamir's algorithm is to divide Key in n parts, Kz, Kn such that there is a special part Kt which contains the information of all other parts, and K cannot be computed without Kt. However, K cannot be computed without especial part Kt.

Cloud consumers layer: Cloud users are the one who have the data to be stored in the cloud and depend on cloud for data computation and transformation. Cloud consumers can be both customers and individual organizations.

Cloud service provider (CSP): This layer owns, built and manages the storage servers in distributed manner and functions as live cloud computing systems.

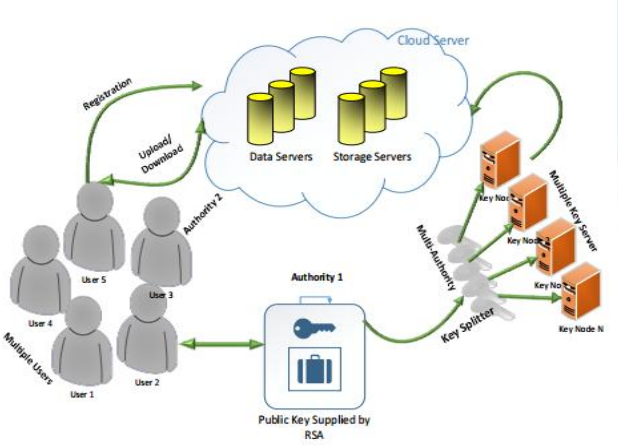


Fig 2. System Architecture

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.

STRUCTURE The structure of the data access control scheme for multiauthority 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.

SECURITY MODEL

The following assumption is made in multi-authority cloud storage systems: In the system the CA is fully trusted. It will not cooperate 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.

IV. 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 multiauthority 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 is assigned. Because of the globally unique uid, the secret key issued by various AAs for same user is 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 ciphertext. 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 ciphertext 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.

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 public keys fpr all AAs and outputs the ciphertext

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.

V. 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 ciphertext are encrypted under 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.

VI. 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 AttributeBased 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.

