Volume 5, Issue 10, October-2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Efficient User Revocable Data Access Control for Centralized Authority Cloud Storage

Uppala Teja Priya[1], Kotha Mohan krishna[2]
[1] (M.Tech) –CSE, Vasireddy Venkatadri Institute of Technology (VVIT), Nambur (v), Guntur, Andhra Pradesh, India
[2] Assistant Professor, Dept of CSE, Vasireddy Venkatadri Institute of Technology (VVIT), Nambur (v), Guntur, Andhra Pradesh, India

Abstract: Cloud computing is one of the emerging technologies in order to outsource huge volume of data inters of storage and sharing. To protect the data and privacy of users the access control methods ensure that authorized users access the data and the system. Fine grained-approach is the appropriate method for data access control in cloud storage. However, Data access control is an effective method to assure the data security in the cloud. Due to data outsourcing and untrusted cloud servers, the data access control becomes a difficult problem in cloud storage systems. Ciphertext-Policy Attribute based Encryption (CP-ABE) is expressed as one of the most appropriate technologies for data access control in cloud storage, because it gives data owners direct control on access policies. However, it is difficult to apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. To overcome existing problems we introducing centralized attribute authority, and CAA will take the attribute from the users and they will generate the secrete Hash key .data owner will encrypt the file based on CAA public key and secrete key. Here CA will not decrypt the cipher text because it is associated with CAA public key and secrete key.

Key Terms: Fine-grained access policy, policy based access controlling, multi-authority, CP-ABE.

I. INTRODUCTION

Data access control is a productive approach to assurance the information security in the cloud. Cloud storage services permits data owner to outsource their information to the cloud. Attribute based encryption (ABE) [1] is another idea of encryption algorithms that permit the encryptor to set an approach portraying who ought to have the capacity to peruse the information. Quality based encryption framework, all the characteristic sets are Cloud by an authority. A client should to have the capacity to decode a ciphertext if and if their quality set fulfill. In expected public key cryptography, a message is scrambled for a particular aerial utilizing the recipient's public key. Identity based encryption (IBE) changed the normal comprehension of Public key cryptography by permitting the general population key to be a subjective string, 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 (ciphertext-policy ABE - CP-ABE). In Ciphertext-policy attribute-based encryption (CP-ABE) a user's private-key is related with a set of attributes and a ciphertext indicate an access policy above a defined universe of attributes within the system. A user will be able to decrypt a ciphertext, if and only if his attributes satisfy the policy of the relevant ciphertext. Fine–grained schema is considered as solitary of the mainly appropriate system for data access control in cloud storage. This system provides data owners more straight control on access policies at cloud level [2].

II. RELATED WORK

A. Attribute Based Encryption (ABE)

Sahai& Waters in 2005 proposed a system in which data is encrypted at the fine grained level & named as ABE([5],[8]). In ABE a owner can encrypt data specifying attribute set &numbered as a access control over attribute set, such that only a user with at least d of given attribute can decrypt message.

B. Key Policy Attribute Based Encryption (KPABE)

V.Goyal ,O. pandey , Sahai& Waters proposed a KPABE scheme [8].In this method type of public key encryption, the secrete key of a user & the Cipher Text (CT) are dependent upon attributes. In such a system, the decryption of CT is possible only if the set of attributes of the user key matches the attributes of CT. **C. Cipher Text Attribute Based Encryption (CPABE)** Sahai et al suggest new modification in this in existing ABE called CPABE ([3],[8]) .In this method user secret key related with a set of attribute & ach CT embedded with an access structure. It removes the need for knowing the identity of the user's-ABE improves the disadvantages of KP-ABE that the encrypted data cannot choose who can decrypt it. But it is difficult in user revocation.

D. Identity Based Encryption (IBE)

M.F ranklin, D. Bonch in 2001 introduced an identity based encryption scheme ([8],[9]). In this data is encrypted using ID of user by owner. Decryption takes place by using secrete key for relevant ID which have been used during encryption. This secrete key is received by user from key generation center (KGC). Main drawback of such a system is that, KGC have power to decrypt all CT over cloud. Another version of IBE is Hierarchical identity based encryption (HIBE).It is hierarchical form of IBE.

E. Multi Authority Attribute Ciphertext Based Encryption (MA-CPABE)

MA-ABE is introduced by Chase[1] .It consist of single centralized authority ,which is responsible for issuing secrete key to user and there are multi attribute authorities, from which, each AA is responsible for monitoring attribute and issuing it to user for decryption CT. But main drawback of such a system that single CA has power to decrypt any CT on cloud. Hence user cannot fully trust on cloud server because this single CA issue UID & AID to user & attribute authority respectively. By using this UID &AID CA can decrypt any CT on cloud.

III. EXISTING 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.

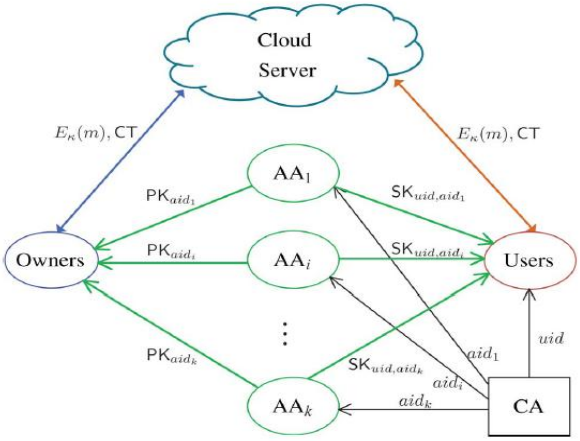

Fig. 1. System Architecture

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 ciphertext 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 (1^λ): (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 at least t+1 honest attribute authorities.
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.
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.

III. PROPOSED SYSTEM

In our proposed system we achieve the various challenges which are presented in the presented system; it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. To overcome existing problems we introducing centralized attribute authority, and CAA will take the attribute from the users and they will generate the secrete Hash key .data owner will encrypt the file based on CAA public key and secrete key. Here CA will not decrypt the cipher text because it associated with CAA public key and secrete key.
This paper, surveys a revocable centralized authority Fine -grained access control scheme [5], to solve the attribute revocation problem in the system. This scheme is an efficient and secure revocation. 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 ciphertext, 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.

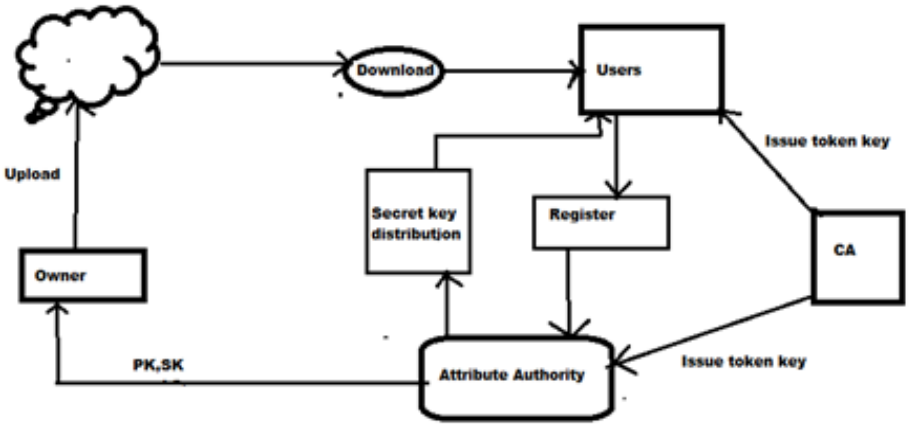

Fig 2. Proposed System Architecture

SYSTEM FUNCTIONING

1. Certificate Authority
2. Attribute Authorities
3. Owners
4. Cloud Server
5. Users

Certificate Authority:
The CA is a master trusted certificate authority in the structure. 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 master unique user identity and

attributes authority and also generates a master 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.

Attribute Authorities:
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.

Users:
Each user has a master identity in the system. A user may be entitled a set of attributes which may come from centralized attribute authorities. The user will receive a secret hash key associated with its attributes entitled by the corresponding attribute authorities which is issued by the CAA.

Data Owners:
Each Data owner first split the data into numerous components according to the logic granularities and encrypts each data component with different content keys by using symmetric encryption techniques. Then, the owner defines the access policies over attributes from centralized attribute authorities and encrypts the content keys under the policies.

Cloud Server:
Then, the owner sends the encrypted data to the cloud server together with the ciphertext i.e. (attribute set). They do not rely on the server to do data access control. But, the access control happens inside the cryptography. That is only when the user's attributes satisfy the access policy defined in the cipher text i.e. fine-grained access control; the user is able to decrypt the ciphertext. Thus, users with different attributes can decrypt different number of content keys and thus obtain different granularities of information from the same data
Fine-grained Access Control. Fine-grained access control systems facilitate granting differential access rights to a set of users and allow edibility in specifying the access rights of individual users. Several techniques are known for implementing fine grained access control.
Our proposed system performs a secure data transaction in the cloud; the suitable cryptographic method is used .i.e. RSA algorithm. The owner must encrypt the file with some specified attributes, with owner's private key which was generated by the AA.
Setup Phase: in this phase data owner can obtain Private Key from AA ,get his public key and get Time interval tag from Time server for data availability and collect all this things as attribute set and apply RSA algorithm to encrypt the data be out sourcing to Cloud server.
Encrypt: in this phase data will encrypted along with attribute set, which consist of E(M,Pk,T,Puk)-→RSA→CT, where M: Message,Pk: Private Key which is generated by KDC,T: Time Interval ,Puk: Public Key
Decrypt: in this phase data will be decrypted along with Attribute set, which consist of D(CT)→RSA→M,Pk,T,Puk..
Before to outsource the data into cloud server data Owner can upload encrypted data into cloud server. If a third person want to access that file remotely from cloud server, user need be authorized by the cloud server i.e. here fine grained approach will be performed at cloud level soon after authorized by cloud server, cloud server send encrypted content to user, now user need to get Decrypted keys that is Private key and Public Key by the Trustee it will done based on user Identity. Users may view the record if the user had the key which is used to decrypt the encrypted file [6] . Sometimes this may be a failure due to the technology development and the hackers. The key distribution center is a server that is responsible for cryptographic key management. The public key is time-based, it means if key will be deleted or removed by the key manager when an expiration time is reached, where the expiration time is specified when the file is first declared or uploaded . Without the public key, the private key and hence the data file remain encrypted and are deemed to be inaccessible. Thus, the main security property of file assured deletion is that even if a cloud provider does not remove expired file copies from its storage, those files remain encrypted and unrecoverable[6]. We propose a policy based file access [6] and policy based file assured deletion [6], [7], [8] for better access to the files and delete the files which are decided no more.
Our system also has the added feature of fine grained access control in which only valid users are able to decrypt the loading information. The system prevents replay attacks and supports creation, modification, and reading data collected in the cloud.

ADVANTAGES:
Cloud access control of data collected in cloud so that only certified users with fully valid attributes can read them. The confirmation of users who collection and modify their data on the cloud. The identity of the user is secure from the cloud during confirmation.

IV. CONCLUSION

This investigation explains a revocable centralized -authority Fine-grained scheme that can support efficient attribute revocation. Then the effective data access control scheme for centralized -authority cloud storage systems is proposed. It

eliminates Decryption overhead for users according to attributes .This secure attribute based cryptographic technique for robust data security that's being shared in the cloud .This revocable centralized-authority Fine-grained scheme with Verifiable outsourced decryption and proved that it is secure and verifiable

REFERENCES

[1] Kan Yang, and XiaohuaJia, "Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage," IEEE transactions on parallel and Cloud systems, vol. 25, no. 7, july 2014.

[2] J. Hur and D.K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel Cloud Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

[3] 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.

[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 Cloud Systems, vol. no. 1, pp. 131-143, Jan. 2013. 24,

[5] 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.

[6] MrSanthoshkumarB.J,M.Tech, Amrita VishwaVidyapeetham, Mysore Campus, India "Attribute Based Encryption with Verifiable Outsourced Decryption." In International Journal of Advanced Research in Computer Science and Software Engineering"Volume 4, Issue 6, June 2014,ISSN: 2277 128X.

[7] Tejaswini R M1, Roopa C K2 , Ayesha Taranum "Securing Cloud Server & Data Access withCentralizedized-Authorities" International Journal of Computer Science and Information Technology Research ISSN 2348-120X Vol. 2, Issue 2, pp: (297-302), Month: April-June 2014,

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

[9] 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.

[10] B.Natraj Kumar, M.Sri Lakshmi and Dr S.Prem Kumar,"Investigation on Revocable Fine-grained Access Control Scheme for Multi-Authority Cloud Storage Systems." International Journal of Computer Engineering In Research Trends. Volume 2, Issue 8, August 2015, PP 486-491, ISSN (Online): 2349-7084. www.ijcert.org.

[11] 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.

