Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Study on Revocable Data Access Control Scheme for Multi-Authority Cloud Storage Systems

[1]Kirthi Gopi Raju, [2]Dr K. Suresh Babu
[1] (M.Tech), [2] Professor
[1, 2] Dept of Computer Science & Engineering Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

Abstract: ***Cloud computing multi-tenancy feature, which provides privacy, security and access control challenges, because of sharing of physical resources among untrusted tenants. In order to achieve safe storage, policy based file access control, policy based file assured deletion and policy based renewal of a file stored in a cloud environment, a suitable encryption technique with key management should be applied before outsourcing the data. 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. However, CP-ABE schemes to data access control for cloud storage systems are difficult because of the attribute revocation problem. So this paper produce investigation on competent 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. Specifically, this paper surveys a revocable multi-authority CP-ABE scheme. The attribute revocation method can efficiently achieve both forward security and backward security.***

Key Terms: Renewal policy, policy based access. Access control, multi-authority, CP-ABE, attribute revocation, cloud storage

I. INTRODUCTION

Now a day's cloud computing is a rationally developed technology to store data from more than one client. Cloud computing is an environment that enables users to remotely store their data. Remote backup system is the advanced concept which reduces the cost for implementing more memory in an organization. It helps enterprises and government agencies reduce their financial overhead of data management. They can archive their data backups remotely to third party cloud storage providers rather than maintain data centers on their own. An individual or an organization may not require purchasing the needed storage devices. Instead they can store their data backups to the cloud and archive their data to avoid any information loss in case of hardware / software failures. Even cloud storage is more flexible, how the security and privacy are available for the outsourced data becomes a serious concern. There are three objectives to be main issue Confidentiality – preserving authorized restrictions on information access and disclosure. The main threat accomplished when storing the data with the cloud. Integrity – guarding against improper information modification or destruction. Availability – ensuring timely and reliable access to and use of information.

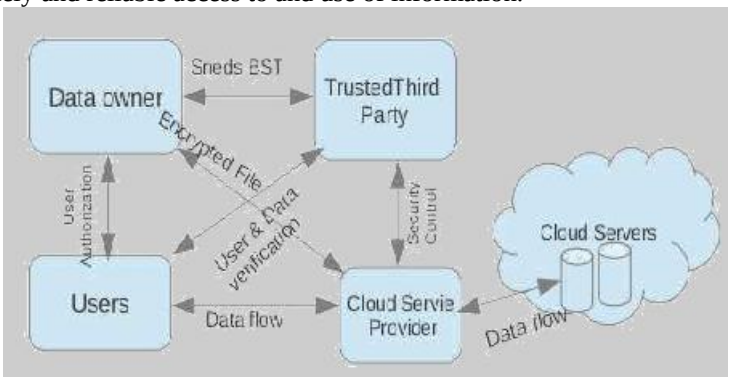

Fig1: Example diagram for data sharing with cloud storage.

To achieve secure data transaction in cloud, suitable cryptography method is used. The data owner must encrypt the file and then store the file to the cloud. If a third person downloads the file, he/she may view the record if he/she had the key which is used to decrypt the encrypted file. Sometimes this may be failure due to the technology development and the hackers. To overcome the problem Cloud computing is one of the emerging technologies. The cloud computing contains huge open distributed system. It is important to protect the data and privacy of users. Access Control methods ensure that authorized users access the data and the system. Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may

also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security. Cloud Storage: The Cloud storage is an important service of cloud computing. The Cloud Storage offers services for data owners to host their data into the cloud. A great challenge to data access control scheme was data hosting and data access services. Because data owners does not fully trust the cloud servers also they can no longer rely on servers to do access control The data access control becomes a challenging issue in cloud storage systems because of data outsourcing and untrusted cloud servers. Therefore Cloud storage is a model of data storage where the digital data is stored in logical pool.

CP-ABE: One of the most suitable technologies for data access control in cloud storage systems is Cipher text-Policy Attribute-based Encryption (CP-ABE). This scheme provides the data owner more direct control on access policies. The Authority in CP-ABE scheme is responsible for attribute management and key distribution. The authority may be the university registration office, the human resource department in a company, etc. The data owner in CP-ABE scheme defines the access policies and encrypts data according to the policies. 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 2: 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.

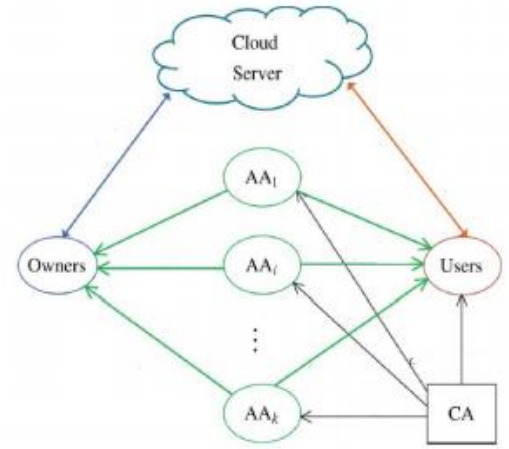

Fig2. Decentralized manner data access Controlling

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.

II. 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.

SOME OF THE SCHEMES:

ATTRIBUTE BASED DATA SHARING WITH ATTRIBUTE REVOCATION SCHEME

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 CPABE, 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. Storage system, attributes of user's can be changed dynamically. A user may be join some new attributes or revoked some current attributes.

ATTRIBUTE-BASED ACCESS CONTROL WITH EFFICIENT REVOCATION IN DATA OUTSOURCING SYSTEMS SCHEME

Some of the 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 SCHEME

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

III. PROPOSED SYSTEM

This paper, surveys a revocable multiauthority 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 ciphertexts, 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.

1. ENTITIES

EXISTING(MULTIAUTHORITY CP-ABE SCHEME)

- Certificate authority (CA), Attribute authorities (AAs), Data owners (owners), Cloud server(server) Data consumers (users) [5][6].

PROPOSED(REVOCABLE MULTIAUTHORITYCP-ABE SCHEME)

- Global Certificate authority (CA), Multiple Attribute authorities (AAs), Data owners (owners), Cloud server(server) Data consumers (users).

1. ATTRIBUTE

EXISTING(MULTIAUTHORITY CP-ABE SCHEME) : Every secret key is associated with a single AA.[2]

PROPOSED(REVOCABLE MULTIAUTHORITYCP-ABE SCHEME): Every secret key is associated with a Multiple AA.

2. CERTIFICATE AUTHORITY (CA)

MULTIAUTHORITY CP-ABE SCHEME :The CA sets up the system and accepts the registration of all the users and AAs in the system [3].

REVOCABLE MULTIAUTHORITYCP-ABE SCHEME: The CA sets up the system and accepts the registration of users and AAs in the system. CA assigns global authority identity aid to each attribute in the system

3. DATA CONSUMERS (USERS).

MULTIAUTHORITY CP-ABE SCHEME :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[4].

REVOCABLE MULTIAUTHORITYCP-ABE SCHEME:: For each legal user in the system, AA assigns a global user identity uid to each user

4. ATTRIBUTE AUTHORITIES (AAS)

MULTIAUTHORITY CP-ABE SCHEME :Every AA is an independent attribute authority that is Responsible for entitling and revoking usersattributes [1].

REVOCABLE MULTIAUTHORITYCP-ABE SCHEME:: The uid is globally unique in the system .Secret keys are issued by different AAs for the same uid

5. DATA OWNERS (OWNERS)

MULTIAUTHORITY CP-ABE SCHEME :Each owner first divides the data into several components and encrypts each data component with different content keys by using symmetric encryption techniques [2].

REVOCABLE MULTIAUTHORITYCP-ABE: Data owners may share the data using access policy definedover attributes from different authorities. \

6. CLOUD SERVER

MULTIAUTHORITY CP-ABE SCHEME :Cipher Text stored and updated into the Cloud Server[4]

REVOCABLE MULTIAUTHORITY CP-ABE:: Cipher text updated into the cloud server

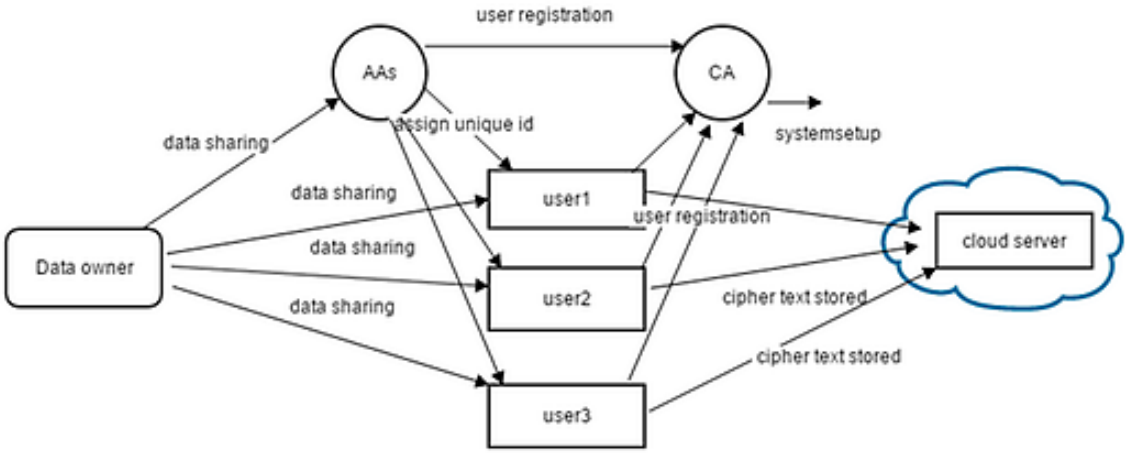

Fig3. System Architecture:

IV. CONCLUSION

This investigation explains a revocable multi-authority CP-ABE scheme that can support efficient attribute revocation. Then the effective data access control scheme for multi-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 multi-authority CPABE scheme with Verifiable outsourced decryption and proved that it is secure and verifiable .The revocable multi-authority CPABE is a efficient technique, which can be applied in any remote storage systems and online social networks etc.

REFERENCES

[1] 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.

[2] 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.

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

[5] Kan Yang, and Xiaohua Jia, Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage," IEEE transactions on parallel and distributed systems, vol. 25, no. 7, July 2014.

[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 withMulti-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] A.Shekinah prema sunaina,"Study on Competent and Revocable Data Access Control Scheme for Multi-Authority Cloud Storage Systems" International Journal Of Computer Engineering In Research Trends Volume 2, Issue 5, May 2015, pp 365-368 , Issn (Online): 2349-7084. www.ijcert.org

