EFFICIENT DATA SHARING WITH ATTRIBUTE REVOCATION FOR CLOUD STORAGE

Chakali Sasirekha[1], K. Govardhan Reddy[2]

[1]M.Tech student, CSE, Kottam college of Engineering, Chinnatekuru(V),Kurnool,Andhra Pradesh, India

[2]Assistant Professor, CSE , Kottam college of Engineering, Chinnatekuru(V),Kurnool,Andhra Pradesh, India

Abstract- **In a Cloud Computing the data security achieved by Data Access Control Scheme. 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. 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.**

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

I. INTRODUCTION

In recent years, the cloud computing technologies has developing technology in IT world. The cloud computing has many features like access anywhere from anywhere and at any time. The cloud computing has large data storage or data centers and also uses large servers for web application and services. Access control and authentication methods ensure the authorized users to access the data. But, its main concern is data security. Because, the cloud server cannot be fully trustworthy by data owners, they cannot believe on servers to do access control. Ciphertext-policy Attribute based encryption (CP-ABE) is one of the recent technologies for data access control in cloud storage, because it provides the data owner more direct control on access policies. In this scheme, the attribute authority is responsible for the maintaining the attribute and also responsible for key distribution for the attribute. The certificate authority is activates the user and attribute authority registration. The CA can be the Human resource department in an organization, registration office in a university, etc. The data owner encrypts depending on the access policies and attribute.

The access policies prevents the unauthorized person to access the data. Multi-Authority CP-ABE is suitable for data access control of cloud data storage. The user may be hold n number of attributes from any attribute authority. The data owners can share the data with attribute based encrypted method along with the access policy. For Example, A Human resource department, the data owners share the data by using the access policy “Project Manager AND Team Leader” or “Project Manager OR Team Leader”, where the attribute “Project Manager” have different access rules and the attribute “Team Leader” have different access rules.

It is very difficult to apply directly on multi-authority CP-ABE method to cloud storage because the attribute revocation issues for users. This issue happens when the revoked user cannot decrypt any ciphertext that requires the revoked attribute to decrypt (Backward security) and the newly entered users can also decrypt the previous published ciphertext if its public key and sufficient attributes (Forward security).

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). It provides the data owner to direct control on access policies. The Authority in this scheme is responsible for key distribution and attribute management. The authority may be the university Administration office, Staff maintenance (Human resource-HR) department in a company, etc. The data owner in CP-ABE scheme defines the access policies and encrypts data depending on the policies.

CP-ABE TYPES: In CP-ABE scheme for every user will be issued a secret key reflecting its attributes. A user can decrypt the data only when its attributes to 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 method, where all the attributes are managed by only one a single authority. In a Multiauthority CP-ABE scheme where attributes are from different attribute authorities. This method is more suitable for data access control of cloud storage systems. Data users contain attributes should be issued by multiple authorities and data owners. Data users may also share the data using access policy defined over attributes from different authorities.

II. RELATED WORKS

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.

[1] In 2010, S. Yu, C. Wang, K. Ren, and W. Lou, worked on "Attribute Based Data Sharing with Attribute Revocation,‟. This paper 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 proxyservers keep all the proxy re-key.

[2] In 2011, S J. Hur and D.K. Noh, worked on Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems. This paper proposes an 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 securelymanaging 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

[3] In 2011, S. Jahid, P. Mittal, and N. Borisov, worked on Easier : Encryption Based Access Control in Social Networks with Efficient Revocation‟.The proposed Easier architecture that supports two approaches are fine-grained access control policies and dynamic group membership.

Both scheme achieved by using attributebased encryption, however, is that it is possible to remove access from a user without issuing new keys to other users or re-encrypting existing cipher texts. We achieve this by creating a proxy that participates in the decryption process and enforces revocation constraints. 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.

[4], In 2013, S. Jahid, P. Mittal, and N. Borisov, worked on Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute Based Encryption, This model proposes the use of dual system encryption methodology. The encryption techniques from Multi-authority ABE and Key-Policy ABE are combined into a single module. Use of MA-ABE technique proves beneficial for key management and flexible access and potential security threat of colluding users is handled by KP-ABE. The proposed framework has attempted to achieve data security by MA-ABE and data privacy by KP-ABE scheme. The overall security of the system has been improved.

Drawback: Existing attribute revocation methodsrely on a trusted server or lack of efficiency also theyare not suitable for dealing with the attribute revocation problem in data access control in multi-authority cloud storage systems.

Each Attribute authorities (AAs) is trusted but can be corrupted by the adversary. Each user is dishonest and may try to obtain unauthorized access to data.

[5][6]"Attribute-Based Encryption with Verifiable Outsourced Decryption". This scheme changes the original model of ABE with outsourced decryption to allow for verifiability of the transformations in existing system. This new model constructs a concrete ABE scheme with verifiable outsourced decryption also does not rely on random oracles.

Drawback: Security Issue: Multi-authority CP-ABE protocol allows the central authority to decrypt all the cipher texts, because it contains the master key of the system;

Revocation Issue: Protocol does not support attribute revocation.

III. PROPOSED SYSTEM

We designed a data access control for Multi-Authority cloud storage as fig .1 shows, there are six types of entities in system: The cloud server(server), the data owner, the attribute authority (AA), the Certificate authority (CA), the data users (User) and the third party auditor (TPA).

The CA is a global trusted certificate authority, which accepts the user and AA registration. The CA is distributes the global public key and global secret key for each legal user. But it is not involved in any attribute management and also creation of secret keys that are associated with attributes. For example, CA is like a Unique Identification Authority of India (UIDAI), for Indian government. Each user will be issued a Unique Identification Number (AADHAAR Number) as its Identity. Every AA is a separate attribute authority. AA is responsible for create an attribute and revoke the attributes for user.

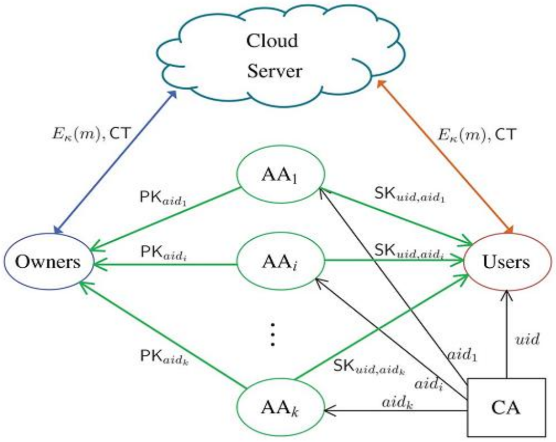

Fig.1. System model of data access control in multi-authority cloud storage.

The attribute is created by the role or identity of user. Each AA has maintaining the n number of attributes. AA generates the public key and private key for the each attribute it manages.

The user has a global identity in the system. They may be create a set of attributes which comes for multiple attribute authority and also receives a secret key for their attributes. The data owners encrypts the data along with the access policies with the set of public key of the attributes. The data owner updates the ciphertext into the cloud server. The user can decrypt when the attributes satisfy the access policy along with the ciphertext, the user can decrypt the ciphertext.

Security Framework

Fig.2 shows a schematic representation of the proposed security framework. The framework has been built using the below defined components of layers. The proposed scheme is used to control the out sourced data and provide the standard quality of the cloud storage service for the cloud users with an efficient encryption and decryption computations and multiple key server with key splitter techniques. This multi-authority CP-ABE provides authority that is answerable for attribute management, efficient computation, key distribution and the revocation methods. There are seven layers defined in the proposed scheme. The functionality of those layers can be summarized as follows:

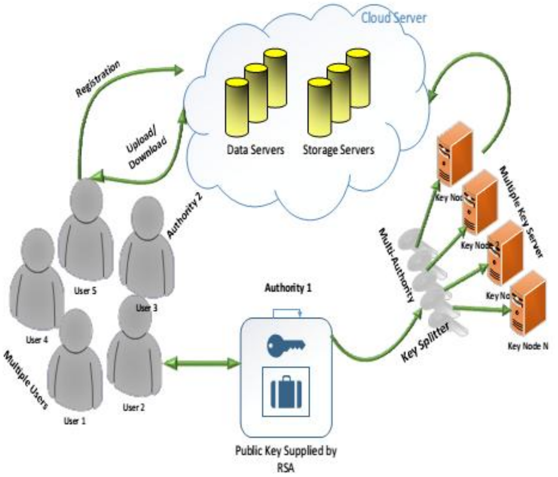

Fig.2 Proposed Security Framwork (FAC-MACS)

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.

IV. CONCLUSION

This paper mainly describes about the methods and algorithms, which are used for providing the high end of security in cloud storage system and accessing data effectively and securely. In this paper, we proposed an effective attribute revocation method for the Multi-authority CP-ABE method. Also, we proposed third party auditor can audit the data for data loss and attack in the multi-authority CP-ABE method. We construct the effective data access method for multi-authority cloud storage. This technique, which can be applied in any social networks and cloud data center's 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] 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. Keromyt is, 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] S. Vishnupriya, C. swathi and Lina Dinesh, "Improved Privacy of Cloud Storage Data users by Using Enhanced Data Access Control Scheme for Multi-Authority Cloud Storage," in International Journal of Computer Science & Communication Networks, vol 4,2014, pp 165-168.

BIODATA

Author

Chakali Sasirekha presently pursuing her M.Tech in CSE, Kottam College of Engineering, Chinnatekuru (V),Kurnool,Andhra Pradesh, India.

Co-Author

Mr.K. Govardhan Reddy received M.Tech. Presently working as Assistant Professor in Kottam College of Engineering,Chinnatekuru (V), Kurnool, Andhra Pradesh, India.