INTERNATIONAL JOURNAL OF RESEARCH
In Advanced Engineering Technologies

Volume 4, Issue 1 JUNE 2015

# A NOVEL APPROACH FOR REVOCABLE MULTI-AUTHORITY CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION SCHEME IN CLOUD

**[1] CH.GAYATHRI, [2] CH.VENKATESWAR RAO**

[1] M.Tech Student, Department of CSE, Indur Institute Of Engineering and Technology, Medak, Telangana, India.

[2] Associate Professor, Department of CSE, Indur Institute Of Engineering and Technology, Medak, Telangana, India.

**ABSTRACT**— The number of user in cloud computing are increasing tremendously due to its advantage of providing flexible storage requirement. The users are started to share their sensitive information through the cloud due to its nature of providing convenience to users. The security of the data has to be assured to the users when storing their details into the cloud server. The main objective of this paper is to improve the security and the efficiency while sharing the data between data owner and the users. Based upon the attributes of the users we are going to share the data. One of the most challenging issues in confidential data sharing systems is the enforcement of data access policies and the support of policies updates. Cipher text policy attribute based encryption (CP-ABE) is becoming a promising cryptographic solution to this kind of problem. It enables data owners to define their own access policies over their user attributes and enforce the policies on the data to be distributed. In this paper we tend to propose a revocable multi-authority CP-ABE theme, and apply it because the underlying techniques to style the information access management theme. Our attribute revocation methodology will with efficiency deliver the goods each forward security and backward security. This survey shows that revocable multi-authority CP-ABE scheme is secure in the random oracle model and is more efficient than previous multi-authority CP-ABE.

Keywords— Revocation, Cloud Computing, Encryption, Certificate Authority (CA)

## I INTRODUCTION

Cloud computing, or one thing being within the cloud, is associate expression accustomed describe a spread of various kinds of computing ideas that involve an oversized variety of computers connected through a time period communication network like the net. In science, cloud computing could be a word for distributed computing over a network and means that the flexibility to run a program on several connected computers at an equivalent time. The phrase is additionally additional ordinarily accustomed ask network primarily based services that seem to be provided by real server hardware, that really are served up by virtual hardware, simulated by software system running on one or additional real machines. Such virtual servers don't physically exist and might thus be moved around and scaled up (or down) on the fly while not moving the top user—arguably, rather sort of a cloud. The recognition of the term may be attributed to its use in promoting to sell hosted services within the sense of application service provisioning

that run shopper server software system on an overseas location.

This paper is to propose one technique for secure file sharing victimization Attribute primarily based File Sharing. Enterprises sometimes store knowledge in internal storage and install firewalls to shield against intruders to access the info. They conjointly standardize knowledge access procedures to forestall insiders to disclose the data while not permission. In company, the info is going to be hold on in their server storage for sharing the secure files to their purchasers. The corporate administrator should have a viable thanks to shield their knowledge, particularly to forestall the info from revelation by unauthorized insiders. Storing the info in encrypted type could be a common technique of data privacy protection. Even have to visualize the right approved shopper is receiving the info or alternative hackers involving. For this checking, the attribute primarily based file sharing technique is planned.

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.

**II 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.

**III Data Access Control System in Multi Authority Cloud Storage**

There are five types of entities in the system AS IN Fig 1: 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.

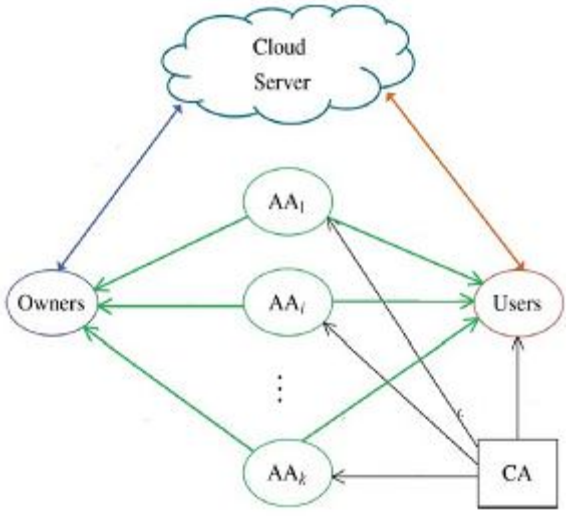

Fig. 1. System model of data access control in multi-authority cloud storage

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.

**IV EXISTING SYSTEM**

In a multi-authority cloud storage system, attributes of user's will be modified dynamically. A user could also be part of some new attributes or revoked some current attributes.

In 2010, S. Yu, C. Wang, K. Ren, and W. Lou, worked on, "Attribute based mostly knowledge Sharing with Attribute Revocation". This paper use semi-trustable on-line proxy servers. This server permits the authority to revoke user attributes with marginal effort.

This theme was unambiguously desegregation the technique of proxy re-encryption with CPABE, and conjointly permits the authority to delegate most of gruelling tasks to proxy servers. The blessings of this theme is a lot of Secure against chosen cipher text attacks. Give importance to attribute revocation that is tough for CP-ABE schemes.

**Drawback:**

- The storage overhead might be high if proxy servers keep all the proxy re-key.

In 2011, S J. Hur and D.K. Noh, worked on "Attribute-Based Access management with economical Revocation in knowledge Outsourcing Systems". This paper proposes associate access management mechanism supported cipher text-policy attribute-based encoding to enforce access management policies with economical attribute and user revocation technique. The fine-grained access management may be achieved by twin encoding theme. This twin encoding mechanism takes advantage of the attribute-based encoding and selective cluster key distribution in every attribute cluster. The advantage of this theme is firmly managing the outsourced knowledge. This theme delivers the goods economical and secure within the knowledge outsourcing systems.

**Drawback:**

- Huge issue in social control of authorization policies and also the support of policy updates

**V PROPOSED SYSTEM**

This paper, surveys a revocable multiauthority CP-ABE scheme [5], to solve the ttribute 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 cipher texts, 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.

**VI 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.

**Comparative Study of Existing (Multiauthority Cp-Abe Scheme) Vs Proposed (Revocable Multi Authority Cp - Abe Scheme)**

| SNO | methods | EXISTING(Multiauthority CP-ABE Scheme) | PROPOSED(revocable Multiauthority CP-ABE scheme) |
|---|---|---|---|
| 1 | **Entities** | Certificate authority (CA), Attribute authorities (AAs), Data owners (owners), Cloud server(server) Data consumers (users). | Global Certificate authority (CA), Multiple Attribute authorities (AAs), Data owners (owners), Cloud server(server) Data consumers (users). |
| 2 | **Attributes** | Every secret key is associated with a single AA. | Every secret key is associated with a Multiple AA. |
| 3 | **Certificate authority (CA),** | The CA sets up the system and accepts the registration of all the users and AAs in the system | 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. |
| 4 | **Data consumers (Users).** | 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. | For each legal user in the system, AA assigns a global user identity uid to each user |
| 5 | **Attribute authorities (AAs),** | Every AA is an independent attribute authority that is Responsible for entitling and revoking users attributes. | The uid is globally unique in the System. Secret keys are issued by different AAs for the same uid |
| 6 | **Data owners (owners),** | Each owner first divides the data into several components and encrypts | Data owners may share the data using access policy |

| | | | |
|---|---|---|---|
| | | each data component with different content keys by using symmetric encryption techniques. | defined over Attributes from different authorities. |
| **7** | **Cloud server** | Cipher Text stored and updated into the Cloud Server. | Cipher Text updated into the Cloud Server. |

## CONCLUSION

This survey 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, Available at: www. researchpublish.com

[8] 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.

[9] S. Ruj, A. Nayak, and I. Stojmenovic, ''DACC: Distributed Access Control in Clouds,'' inProc. 10th IEEE Int'l Conf. TrustCom, 2011, pp. 91-98.

[10] K. Yang and X. Jia, ''Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage,'' inProc. 32th IEEE Int'l Conf. Distributed Computing Systems (ICDCS'12), 2012, pp. 1-10.