IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 4, April 2016*

# Multi-authority ABE over Cloud System

**Asmita A. Jagtap[1], Prof. Sonali Mhatre[2]**

Lecturer, Information Technology, BVIT, Navi Mumbai, India [1]

Professor, Information Technology, BVCOE, Navi Mumbai, India [2]

**Abstract**: Cloud computing, is an emerging computing paradigm, enabling users to remotely store their data in a server and provide services on-demand. In cloud computing cloud users and cloud service providers are almost certain to be from different trust domains. Data security and privacy are the critical issues for remote data storage. A secure user enforced data access control mechanism must be provided before cloud users have the liberty to outsource sensitive data to the cloud for storage. With the emergence of sharing confidential corporate data on cloud servers, it is important to adopt an efficient encryption system with a fine-grained access control to encrypt outsourced data. Attribute-based encryption is a public key based encryption that enables access control over encrypted data using access policies and specified attributes. Cipher text-Policy Attribute-based Encryption (CP-ABE) is regarded as one of the most suitable scheme for data access control in cloud storage, because it gives data owners more direct control on access policies. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. The system proposed is, to design an efficient and revocable data access control scheme for multi-authority cloud storage systems, where there are multiple authorities co-exist and each authority is able to issue attributes independently. More specifically, it's a revocable multi-authority CP-ABE scheme, to ensure the data access control.

**Keywords**: Cloud Storage, Access Control, Attribute Revocation, Multi-authority.

## I. INTRODUCTION

A Cloud computing is a model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1].

However, moving the infrastructure and sensitive data from trusted domain of the data owner to public cloud will pose severe security and privacy risks. Data encryption, the most effective in regard to preventing sensitive data from unauthorized access. In traditional public key encryption or identity-based encryption systems, encrypted data is targeted for decryption by a single known user. Unfortunately, this functionality lacks the expressiveness needed for more advanced data sharing. To address these emerging needs, Sahai and Waters [3] introduced the concept of attribute-based encryption (ABE). Instead of encrypting to individual users, in ABE system, one can embed an access policy into the cipher text or decryption key. Thus, data access is self-enforcing from the cryptography, requiring no trusted mediator.

### A)Privacy in Cloud Environments

To preserve privacy of a client's data in the cloud, the data must be encrypted before it is sent to the cloud server (Hay, Nance and 2011; Hennessy et al. 2009; Tan, Liu and Wu 2011). The encrypted data is never decrypted at the cloud server to prevent any unauthorized entities from exposing the data contents and these unauthorized entities may include the cloud server (Agrawal, Abbadi and Wang 2012). For instance, Figure1 shows that a user's data is protected by the data owner and shared with other users. In such a scheme, the privacy of data does not depend on an implicit assumption of trust on the cloud provider or on the service level of agreement (SLA). Instead, it depends on the cryptography techniques used by the client to protect the data (Vimercati et al. 2010).

When an authorized user needs to access the data in the cloud, first he/she requests the data owner for an authorization to access the data. The data owner responds with the information that allows the user to request the data securely from the cloud provider. The access policies to the encrypted data are attached to the data and also protected. The cloud provider does not know the details of the policies and the role of the cloud provider is only to execute these policies.

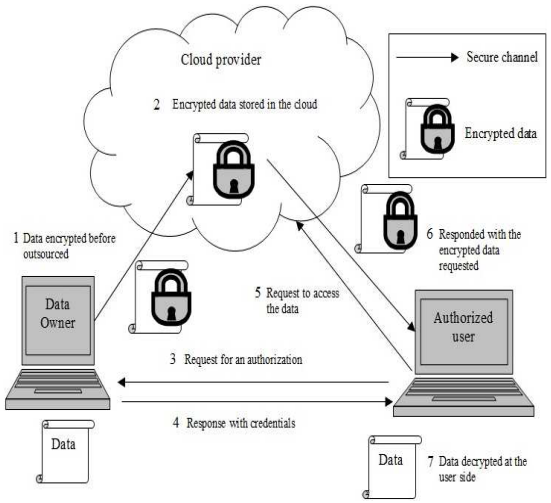


Fig 1:Basic Architecture of preserving data in the cloud


DOI 10.17148/IJARCCE.2016.5421

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 4, April 2016*

## II. LITERATURE SURVEY

The effective implementation for the security issues would be encrypting data by using certain encryption techniques such as:

**i. Symmetric Key Cryptography (SKC) based solutions**

Symmetric-key algorithms are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of cipher text. Vimercati et.al.[6] proposed a solution for securing outsourced data on semi-trusted servers based on symmetric key derivation methods , which can achieve fine-grained access control. Unfortunately, the complexities of file creation and user grant/revocation operations are linear to the number of authorized users, which is less scalable.

**ii. Public Key Cryptography(PKC) based solutions**

PKC based solutions were proposed due to its ability to separate write and read privileges. To realize fine-grained access control, the traditional public key encryption (PKE) based schemes proposed by J. Benaloh, M. Chase, E.Horvitz, and K. Lauter [1] in their work. They propose the solution scenario and shows how public and symmetric based encryption used , disadvantage of their solution is either incur high key management overhead, or require encrypting multiple copies of a file using different users' keys.

**iii. Attribute Based Encryption(ABE)**

Sahai and Waters proposed Identity-Based Encryption [9] in 2005, the first concept of the attribute-based encryption scheme through public key cryptography. Identity-Based Encryption in which identities as a set of descriptive attributes. In this scheme in which each user is identified by a set of attributes, and some function of this attributes is used to determine decryption ability for each cipher text. M.Pirretti, P. Traynor, P. McDaniel, and B. Waters proposed Secure attribute-based systems [6] in2006. This paper gave an implementation of the ABE encryption system with more complex access policy with (AND, OR gate) based on [9].

However, this work is dismissed after the proposal of KP-ABE and CP-ABE, which is more flexible and efficient. In 2006, Goyal et al. proposed an key-policy attribute-based encryption (KP-ABE) scheme [3]. In 2007 Bethencourt et al. proposed an ciphertextpolicy attribute based (CP-ABE) scheme [1].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. In key policy attribute-based encryption, the access policy is in user's private key, but the access policy is switched to the encrypted data in cipher text policy attribute-based encryption. And a set of descriptive attributes are associated with the user's private key, and the access policy is built in the encrypted data. The access structure of the encrypted data is corresponding to the user's private key with a set of descriptive attributes. If a set of attributes in user's private key satisfies the access structure of the encrypted data, the data user can decrypt the encrypted data; if it cannot, the data user cannot obtain the message. it means the user's key with attributes just satisfies the access structure of the encrypted data.

TABLE I

Comparison of Existing Schemes

| Techniques/ Parameter | PKI | ABE | KP-ABE | CP-ABE |
|---|---|---|---|---|
| Fine grained access control | Low | Low | Low, High if there is re-encryption. | Average |
| Computational Overhead | High | High | Most of computational overhead | Average |
| Collision Resistant | Low | Average | Good | Good |
| Remove Revocation Problem | No | No | No | Average |
| Remove Key Escrow Problem | No | No | No | Limited |

## III. PROBLEM STATEMENT

Attribute-based Encryption (ABE) is a promising technique that is very suitable for access control of encrypted data. Some access control schemes are proposed based on CP-ABE, since CP-ABE is more suitable for the access control in cloud storage systems than KP-ABE. It allows the data owners to define an access structure on attributes and encrypt the data under this access structure, such that the data owners can define the attributes that the user needs to possess in order to decrypt the cipher text.

There are two challenging issues in the design of multi authority access control schemes. The first issue is the problem of Collusion. Multiple users holding attributes from different authorities may collude together to obtain illegal access to the data. The CP-ABE scheme, usually rely on a global authority to collect and verify users' attributes and generate the secret keys for them. With the global authority, the collusion problem can be solved by using the key randomization mechanism as in the single authority schemes. However, the global authority is too powerful and it becomes a vulnerable point for security attacks and the performance bottleneck for large scale systems. Some multi-authority schemes are proposed to remove the global authority. The other issue is the difficulty of Attribute Revocation. Existing attribute revocation methods designed for single authority ABE [11]–[13] cannot be applied to multi-authority scenario. We design an efficient multi-authority ABE method without using a global authority and propose a multi-authority access control scheme for cloud storage systems.

## IV. PROPOSED SYSTEM

There are two challenging issues in the design of multi authority access control schemes for cloud storage systems. The first issue is the problem of Collusion. The other issue is the difficulty of Attribute Revocation.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 4, April 2016*

The system components will be a Central Authority(CA) and multiple attribute authorities(AAs) and users.

The system uses a hash function on the user's global identifier (GID) so that collusion resistance is ensured for multiple keys generated by different authorities.

Attribute revocation problem is solved by extending service time of secret key by providing GID for modifying Service Time Attributes.

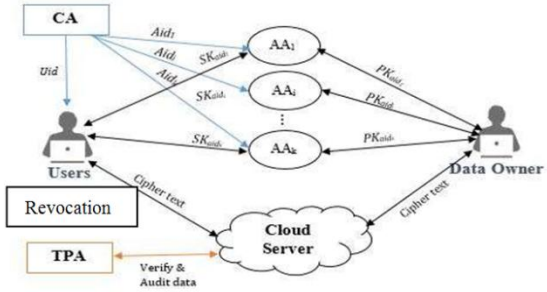


Fig 2: System architecture

## V. CONCLUSION

The MA-ABE scheme is an effective attribute revocation for the Multi-authority. Further the scheme removes key escrow problem of ABE because of its unique key issuing mechanism and enhances data privacy and confidentiality in the data sharing system. A revocable multi-authority CP-ABE scheme can support efficient attribute revocation. Also, we proposed third party auditor can audit the data for data loss and attack in the multi-authority CP-ABE scheme. So, the effective data access scheme for multi-authority Cloud storage is constructed.

## REFERENCES

[1]. J. Bettencourt, A. Sahai, and B.Waters"Ciphertext-policy attribute based encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007.
[2]. Stefan Brands. Rethinking Public Key Infrastructure and Digital Certificates – Building in Privacy. PhD thesis, Eindhoven Inst. of Tech. 1999.
[3]. W. Bagga, R. Molva, and S. Crosta. "Policy-based encryption schemes from bilinear pairings". In ASIACCS, page 368, 2006.
[4]. M. Abdalla, E. Kiltz, and G. Neven , "Generalized key delegation for hierarchical identity based encryption". In Computer Security ESORICS, pages 139-154, 2007.
[5]. S. Al-Riyami, J. Malone-Lee, and N. Smart. "Escrow-free encryption supporting cryptographic workflow". In Int. J. Inf. Sec., volume 5, pages217-229, 2006.
[6]. V. Goyal, O. Pandey, A. Sahai, B.Waters, "Attribute-based encryption for fine-grained access control of encrypted data". In: ACMCCS 2006, pp. 89-98 (2006)
[7]. Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, "AttributeSets: A Practically Motivated Enhancement to Attribute-Based Encryption", July 27, 2009
[8]. John Bethencourt, Amit Sahai, and Brent Waters. Cipher text-Policy Attribute-Based Encryption. In IEEE Symposium on Security and Privacy, pages 321–334. IEEE Computer Society, 2007.