National Conference on Engineering Innovations and Solutions (NCEIS – 2018)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 6 | ISSN : 2456-3307

# Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage

**Miss. Pushpalatha R[1] , Rakshinda Tabassum[2]**
[1]Assistant Professor, Department of CS&E VTU PG Centre, Mysurum, Karnataka , India
[2]M.Tech in CS&E VTU PG Centre, Mysuru, Karnataka, India

## ABSTRACT

Data access control is a challenging issue in public cloud storage systems. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has been adopted as a promising technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-curious cloud servers. However, in the existing CP-ABE schemes, the single attribute authority must execute the time-consuming user legitimacy verification and secret key distribution, and hence it results in a single-point performance bottleneck when a CP-ABE scheme is adopted in a large-scale cloud storage system. Users may be stuck in the waiting queue for a long period to obtain their secret keys, thereby resulting in low-efficiency of the system. In this paper, we propose a novel heterogeneous framework to remove the problem of single-point performance bottleneck and provide a more efficient access control scheme with an auditing mechanism. Our framework employs multiple attribute authorities to share the load of user legitimacy verification. Meanwhile, in our scheme, a *CA* (Central Authority) is introduced to generate secret keys for legitimacy verified users. To enhance security, we also propose an auditing mechanism to detect which *AA* (Attribute Authority) has incorrectly or maliciously performed the legitimacy verification procedure. Analysis shows that our system not only guarantees the security requirements but also makes great performance improvement on key generation.

**Keywords:** Cloud storage, access control, CP-ABE.

## I. INTRODUCTION

Cloud storage is the important service provided by the cloud computing. There are various benefits of the cloud storage system some of them include, better accessibility, greater reliability, continuous deployment and stronger protection and many more to name. Though the cloud storage contains many benefits it faces some issues in the access control which is a critical issue. The traditional access control methods are not suitable in cloud storage hence it has become a challenging issue.

Few schemes have been proposed to solve the issue of the data access in the cloud storage like, Ciphertext- policy Attribute- based Encryption (CP-ABE) which is more promising. This technique grants the direct control for data owners for flexible, fine grained and secure access control in cloud storage. CP-ABE have been divided into two categories single authority scenario and multi authority scenario. The existing single authority is neither efficient nor robust in key generation. Since it is a single authority system it is time consuming for the verification these results in the performance bottleneck. Single point performance bottleneck affects the efficiency of secret key generation and degrades the utility of the existing schemes to to conduct access control in large cloud storage system.

The main process to avoid the single point bottleneck is to introduce multiple authorities to

jointly manage the whole attribute set. By including multiple authorities the single point bottleneck can be reduced to some extent. Since there are various authorities performing the same operation it is difficult to identify the particular attribute which commits any malicious mistake. This work is inspired by the heterogenous architecture with single certificate authority (CA) and multiple registration authorities (RAs). There are multiple authorities (AAs) which are in charge of the whole attribute set which conducts user legitimacy verification. There is only one single global authority to generate secret key for the user on the basis of received intermediate key.

## II. RELATED WORK

**Towards efficient content-aware search over encrypted outsourced data in cloud**

**AUTHORS:** Z. Fu, X. Sun

With the increasing adoption of cloud computing, a growing number of users outsource their datasets into cloud. The datasets usually are encrypted before outsourcing to preserve the privacy. However, the common practice of encryption makes the effective utilization difficult; for example, search the given keywords in the encrypted datasets. Many schemes are proposed to make encrypted data searchable based on keywords. However, keyword-based search schemes ignore the semantic representation information of user's retrieval, and cannot completely meet with users search intention. Therefore, how to design a content-based search scheme and make semantic search more effective and context-aware is a difficult challenge. In this paper, we proposed an innovative semantic search scheme based on the concept hierarchy and the semantic relationship between concepts in the encrypted datasets. More specifically, our scheme first indexes the documents and builds trapdoor based on the concept hierarchy. To further improve the search efficiency, we utilize a tree-based index structure to organize all the document index vectors. Our experiment results based on the real world datasets show the scheme is more efficient than previous scheme. We also study the threat model of our approach and prove it does not introduce any security risk.

**A dynamic secure group sharing framework in public cloud computing**

**AUTHORS:** K. Xue and P. Hong

With the popularity of group data sharing in public cloud computing, the privacy and security of group sharing data have become two major issues. The cloud provider cannot be treated as a trusted third party because of its semi-trust nature, and thus the traditional security models cannot be straightforwardly generalized into cloud based group sharing frameworks. In this paper, we propose a novel secure group sharing framework for public cloud, which can effectively take advantage of the cloud servers' help but have no sensitive data being exposed to attackers and the cloud provider. The framework combines proxy signature, enhanced TGDH and proxy re-encryption together into a protocol. By applying the proxy signature technique, the group leader can effectively grant the privilege of group management to one or more chosen group members. The enhanced TGDH scheme enables the group to negotiate and update the group key pairs with the help of cloud servers, which does not require all of the group members been online all the time. By adopting proxy re-encryption, most computationally intensive operations can be delegated to cloud servers without disclosing any private information. Extensive security and performance analysis shows that our proposed scheme is highly efficient and satisfies the security requirements for public cloud based secure group sharing.

**Attribute-based access to scalable media in cloud-assisted content sharing**

**AUTHORS:** Y. Wu, Z. Wei

This paper presents a novel Multi-message Ciphertext Policy Attribute-Based Encryption (MCP-ABE) technique, and employs the MCP-ABE to design an access control scheme for sharing scalable media based on data consumers' attributes (e.g., age, nationality, or gender) rather than an explicit list of the consumers' names. The scheme is efficient and flexible because MCP-ABE allows a content provider to specify an access policy and encrypt multiple messages within one ciphertext such that only the users whose attributes satisfy the access policy can decrypt the ciphertext. Moreover, the paper shows how to support resource-limited mobile devices by offloading computational intensive operations to cloud servers while without compromising data privacy.

## III. METHODOLOGY

3.1 **System model:** the model for this proposal mainly includes five entities Central Authority (CA), multiple attribute authorities (AAs), many data owners (Owners), many Data consumers (Users) and a cloud service provider with multiple cloud servers.

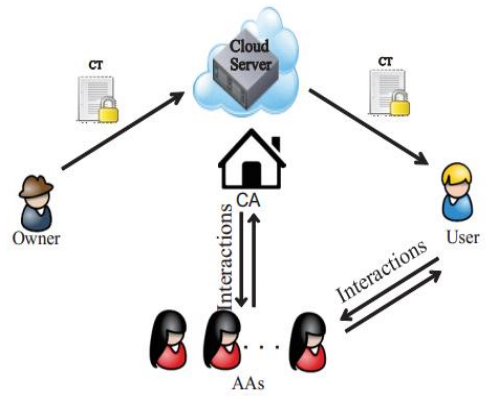


**Figure 1**

- The Central authority: It is the administrator of the entire system. It is responsible for setting up the system parameters and generating public key for each attribute of the universal attribute set. It is also responsible for generating secret keys for the user on the basis of the received intermediate key associated with the user's legitimate attribute verified by an AA.
- The attribute authorities (AAs): It performs the user legitimacy verification and generates intermediate key for verified users. This involves multiple authorities to share the responsibility of user legitimacy verification and each AA can perform this process independently for any user. Intermediate key is a new concept to assist CA to generate keys.
- The data owner (owner): Owner defines the access policy about who can access the each file and encrypts the file under defined policy. Each owner encrypts data with symmetric encryption algorithm. The owner formulates access policy over an attribute set and encrypts the symmetric key under the policy obtained from CA.
- The data consumer (User): A global user Id is assigned by CA. the user possesses a set of attributes and equipped with a secret key associated with attribute set. The user can get any encrypted data from the cloud server only if the user satisfies the access policy.
- The Cloud server: It is a public platform for owners to share their encrypted data. The cloud server does not allow controlling the data access. The encrypted data from the cloud server can be accessed by any user.

**3.2 Security Requirements:** the following security requirements need to be fulfilled for the guaranteed secure access control in public cloud storage.

- Data Privacy: the contents of the data must be kept private to unauthorized users as well as the cloud server.
- Resistance to Collusion: Unverified users colluding with each other would not be able to

combine their attributes to decrypt a ciphertext which each of them cannot decrypt alone.

- Accountability of AA: An auditing mechanism is devised to ensure that the misbehavior of the AA can be detected to prevent AAs' abusing their power without being detected.
- No ultra vires for any AA: An AA should not be assigned an unauthorized power to generate secret keys for users. These security requirements are proposed based on the hierarchical framework.

## IV. IMPLEMENTATION

The proposed scheme consists of five phases, namely System Initialization, Encryption, Key Generation, Decryption, and auditing and tracing.

A hierarchical framework with single central authority (CA) and multiple attribute authorities (AAs) to achieve robust and efficient access control for public cloud storage and remove the single point bottle neck and enhance the system efficiency. In the proposed RAAC system key generation is divided into two subgroups 1) verifying legitimacy of users 2) the process of secret key generation and distribution. The user legitimacy verification is performed by multiple Attribute authorities and they are able to verify attributes independently. Intermediate key is generated by the attribute authority after the successful verification and sent to the Central authority. The process of secret key generation and distribution is performed by the central authority that generates secret key associated with user's attribute set without any further verification.

The details of the proposed RAAC scheme are as explained as follows.

1) System Initialization: The central authority generates public key for each attribute and master secret key which implicitly exists in the system and doesn't need to be obtained by any other entity. The other task of the CA in this operation is handling attribute authorities' and users' registrations. The central authority generates a pair of keys to sign and verify which attribute is publicly known by each entity in the system.

   Each attribute authority sends a registration request to CA during system initialization. For each legal attribute authority CA assigns a unique identity and randomly chooses private key. The Central authority generates certificate which include the public key and sends it with the corresponding private key to the attribute authority with its ID. Each user also receives its private key and the certificate Id from the central authority.
2) Encryption: The process of encryption is carried out by data owner. The owner chooses a random number as a symmetric key and encrypts the plain text with symmetric encryption algorithm. The owner encrypts the symmetric key using Ciphertext policy Attribute Based Encryption (CP-ABE) under the access policy defined by the user.
3) Key Generation: The process is different from existing CP-ABE schemes. It involves selected AA and CA. The key generation procedure is divided into 4 steps

   **Step 1: U -→ AA** A user with the authenticated Id requests the secret key to the selected AA and shows the certificate Id for the validation.

   **Step 2: AA → CA** The AA verifies the user legitimacy by CA. After the successful verification the AA receives the timestamp value from CA and generates intermediate key. The AA finally receives the attribute set which include the User IDs and sends the secure message to the CA.

   **Step 3&4: CA →AA → U** after receiving message from AA the CA checks whether the transmission delay is within the allowed time. The CA makes sure that the request from AA is

not used by the same user. This prevents AAs collusion attack. CA Continues to generate secret keys for users using Master secret key. With the relay of AA, CA securely sends secret keys to the user.

4) Decryption: This procedure is performed by the user. User can freely query and download any encrypted data from the public cloud storage. User cannot decrypt unless attribute set satisfies the access structure embedded in the ciphertext. If the access structure is satisfied it computes to obtain symmetric key which helps in decryption.
5) Auditing and Tracing: Auditing and tracing is periodically performed or event triggered by CA to ask the suspected users to submit certificate Id. In order to obtain the data the users have to cooperate to perform the process correctly. To implement the effective tracing CA must confirm the received key components belong to the given user.

The tracing process is executed in following two sub groups.

### Secret key ownership confirming

CA randomly selects suspected attribute and asks to securely submit secret key components.

### AA Tracing

Executed to trace and confirm which AA has generated the suspected user's secret key. CA uses Master secret key to recover public key associated with AA.

## IV.CONCLUSIONS

In this paper, we proposed a new framework, named RAAC, to eliminate the single-point performance bottleneck of the existing CP-ABE schemes. By effectively reformulating CPABE cryptographic technique into our novel framework, our proposed scheme provides a fine-grained, robust and efficient access control with one-*CA*/multi-*AA*s for public cloud storage. Our scheme employs multiple *AA*s to share the load of the time-consuming legitimacy verification and standby for serving new arrivals of users' requests. We also proposed an auditing method to trace an attribute authority's potential misbehavior. We conducted detailed security and performance analysis to verify that our scheme is secure and efficient. The security analysis shows that our scheme could effectively resist to individual and colluded malicious users, as well as the honest-but-curious cloud servers. Besides, with the proposed auditing & tracing scheme, no *AA* could deny its misbehaved key distribution. Further performance analysis based on queuing theory showed the superiority of our scheme over the traditional CP-ABE based access control schemes for public cloud storage.

## V. REFERENCES


[1] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing," IEEE Transactions on Cloud Computing, vol. 2, no. 4, pp. 459–470, 2014.

[2] Y. Wu, Z. Wei, and H. Deng, "Attribute-based access to scalable media in cloud-assisted content sharing," IEEE Transactions on Multimedia, vol. 15, no. 4, pp. 778–788, 2013.

[3] J. Hur, "Improving security and efficiency in attribute based data sharing," IEEE Transactions on Knowledge and Data Engineering, vol. 25, no. 10, pp. 2271–2282, 2013.

[4] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214–1221, 2011.

[5] J. Hong, K. Xue, W. Li, and Y. Xue, "TAFC: Time and attribute factors combined access control on time sensitive data in public cloud," in Proceedings of 2015 IEEE Global Communications Conference (GLOBECOM 2015). IEEE, 2015, pp. 1–6.

[6] Y. Xue, J. Hong, W. Li, K. Xue, and P. Hong, "LABAC: A location-aware attribute-based access control scheme for cloud storage," in Proceedings of 2016 IEEE Global Communications Conference (GLOBECOM 2016). IEEE, 2016, pp. 1–6.