www.ijecs.in

*International Journal Of Engineering And Computer Science ISSN:2319-7242*
*Volume 7 Issue 6 June 2018, Page No. 24066-24070*
*Index Copernicus Value (2015): 58.10, 76.25 (2016) DOI: 10.18535/ijecs/v7i6.08*

# Multiple Attribute Authorities for Public Cloud Storge using a Robust Audit able Access Control

**Nikhil Kumar Singh[1], Prateek Kumar[2], Vishvendra Singh[3], Chandrakala B.M [4],**

[1,2,3]B.E., Dept of ISE Dayananda Sagar College of Engineering Kumaraswamy Layout, Bangalore
[4]Associate Professor, Dept of ISE Dayananda Sagar College of Engineering Kumaraswamy Layout, Bangalore

## 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. Although multiauthority access control schemes have been proposed, these schemes still cannot overcome the drawbacks of single-point bottleneck and low efficiency, due to the fact that each of the authorities still independently manages a disjoint attribute set. 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. Unlike other multiauthority access control schemes, each of the authorities in our scheme manages the whole attribute set individually. 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.

## Introduction

Cloud storage is a promising and important service paradigm in cloud computing. Benefits of using cloud storage include greater accessibility, higher reliability, rapid deployment and stronger protection, to name just a few. Since cloud storage is operated by cloud service providers, who are usually outside the trusted domain of data owners, the traditional access control methods in the Client/Server model are not suitable in cloud storage environment. The data access control in cloud storage environment has thus become a challenging issue. To address the issue of data access control in cloud storage, there have been quite a few schemes proposed, among which Ciphertext-Policy Attribute-Based Encryption (CP-ABE) is regarded as one of the most promising techniques. A straight forward idea to remove the single-point bottleneck is to allow multiple authorities to jointly manage the universal attribute set, in such a way that each of them is able to distribute secret keys to users independently. By adopting multiple authorities to share the load, the influence of the single-point bottleneck can be reduced to a certain extent. However, this solution will bring forth threats on security issues. Since there are multiple functionally identical authorities performing the same procedure, it is hard to find the responsible authority if mistakes have been made or malicious behaviors have been implemented in the process of secret key the generation and distribution. A straight forward idea to remove the single-point bottleneck is to allow multiple authorities to jointly manage the universal attribute set, in such a way that each of them is able to distribute secret keys to users independently. By adopting multiple authorities to share the load, the influence of the single-point bottleneck can be reduced to a certain extent. However, this solution will bring forth threats on security issues. Since there are multiple functionally identical authorities performing the same procedure, it is hard to find the responsible authority if mistakes have been made or malicious behaviors have been implemented in the process of secret key generation and distribution. For example, an authority may falsely distribute secret keys beyond user's legitimate attribute set. Such weak point on security makes this straight forward idea hard to meet the security requirement of access control for public cloud storage. Our recent work, TMACS, is a threshold multi-authority CP-AB

access control scheme for public cloud storage where multiple authorities jointly manage a unifor m attribute set. Actually, it addresses the single-point bottleneck of performance and security, but introduces some additional overhead. Therefore, in this paper, we present a feasible solution which not only promotes efficiency and robustness, but also guarantees that the new solution is as secure as the original single-authority schemes.

**Related Work**

Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has so far been regarded as one of the most promising techniques for data access control in cloud storage systems. This technology offers users flexible, fine-grained and secure access control of outsourced data. It was first formulated by Goyal et al. in. Then the first CP-ABE scheme was proposed by Benthencourt et al. in, but this scheme was proved secure only in the generic group model. Subsequently, some cryptographically stronger CP-ABE constructions were proposed, but these schemes imposed some restrictions that the original CP-ABE does not have. In, Waters proposed three efficient and practical CP-ABE schemes under stronger cryptographic assumptions as expressive as. To improve efficiency of this encryption technique, Emura et al. proposed a CP-ABE scheme with a constant ciphertext length. Unlike the above schemes which are only limited to express monotonic access structures, Obtrovsky et al. proposed a more expressive CP-ABE scheme which can support non-monotonic access structures.

In, the authors respectively proposed CP-ABE schemes with efficient attribute revocation capability for data outsourcing systems. Wu et al. proposed a Multi-message Ciphertext-Policy AttributeBased Encryption(MCP-ABE) which encrypts multiple messages within one ciphertext so as to enforce flexible attribute-based access control on scalable media.

Based on the basic ABE scheme, Chase et al. proposed the first multi-authority scheme which allows multiple independent authorities to monitor attributes and distribute corresponding secret keys,but involves a central authority (CA). Subsequently, some multi-authority ABE schemes without CA have been proposed, such as. Since the first construction of CP-ABE, a great many multiauthority schemes have been conducted over CP-ABE. Muller et al. proposed the first multi-authority CP-ABE scheme in which a user's secret key was issued by an arbitrary number of attribute authorities and a master authority. Then Lewko et al. proposed a decentralized CP-ABE scheme where the secret keys can be generated fully by multiple authorities without a central authority. Ruj et al. applied Lewko's work for access control in cloud storage systems, and also proposed a revocation method. Lin et al. proposed a decentralized access control scheme based on threshold mechanism.

Recently, we considered the single-point performance bottleneck of CP-ABE based schemes and devised a threshold multi-authority CP-ABE access control scheme in our another work. Different from other multi-authority schemes, in, multiple authorities jointly manage a uniform attribute set. Taking advantage of (t,n) threshold secret sharing, the master secret key can be shared among multiple authorities, and a legal user can generate his/her secret key by interacting with any t authorities. This scheme actually addressed the single-point bottleneck on both security and performance in CP-ABE based access control in public cloud storage. However, it is not efficient, because a user has to interact with at least t authorities, and thus introduces higher interaction overhead.

**Approach**

Our scheme consists of five phases, namely System Initialization, Encryption, Key Generation, Decryption, and Auditing & Tracing.

To achieve a robust and efficient access control for public cloud storage, we propose a hierarchical framework with single CA and multiple AA store move the problem of single-point performance bottleneck and enhance the system efficiency. In our proposed RAAC scheme, the procedure of key generation is divided into two sub-procedures:

1) the procedure of user legitimacy verification;

2) the procedure of secret key generation and distribution.

The user legitimacy verification is assigned to multiple AAs, each of which takes responsibility for the universal attribute set and is able to verify all of the user's attributes independently. After the successful verification, this AA will generate an intermediate key and send it to CA. The procedure of secret key generation and distribution is executed by the CA that generates the secret key associated with user's attribute set without any more verification. The secret key is generated using the intermediate key securely transmitted from an AA and the master secret key. In our one-CA/multiple-AAs construction, CA participates in the key generation and distribution for security reasons: To enhance auditability of corrupted AAs, one AA cannot obtain the system's master secret key in case it can optionally generate secret keys without any supervision. Meanwhile, the introduction of CA for key generation and distribution is acceptable, since for a large-scale system, the most time consuming workload of legitimacy verification is offloaded and shared among the multiple AAs, and the computation workload for key generation is very light. The procedure of key generation and distribution would be more efficient than other existing schemes. To trace an AA's misbehavior in the procedure of user legitimacy verification, we first find the suspected data consumer based on abnormal behavior detection, which is similar to the mechanisms used in. For a suspected user, our scheme can trace the responsible AA who has falsely verified this user's attributes and illegitimately assigned secret keys to him/her.

**Architecture**

The system model of our design is shown in Fig. 1, which involves five entities: a central authority (CA), multiple attribute authorities (AAs), many data owners (Owners), many data consumers (Users), and a cloud service provider with multiple cloud servers(here, we mention it as cloud server.).

• The central authority (CA) is the administrator of the entire system. It is responsible for the system construction by setting up the system parameters and generating public key for each attribute of the universal attribute set. In the system initialization phase, it assigns each user a unique Uid and each attribute authority a unique Aid. For a key request from a user, CA is responsible for generating secret keys for the user on the basis of the received intermediate key associated with the user's legitimate attributes verified by an AA. As an administrator of the entire system, CA has the capacity to trace which AA has incorrectly or maliciously verified a user and has granted illegitimate attribute sets.

• The attribute authorities (AAs) are responsible for performing user legitimacy verification and generating intermediate keys for legitimacy verified users. Unlike most of the existing multi-authority schemes where each AA manages a disjoint attribute set respectively, our proposed scheme involves multiple authorities to share the responsibility of user legitimacy verification and each AA can perform this process for any user independently. When an AA is selected, it will verify the users' legitimate attributes by manual labor or authentication protocols, and generate an intermediate key associated with the attributes that it has legitimacy-verified. Intermediate key is a new concept to assist CA to generate keys.

• The data owner (Owner) defines the access policy about who can get access to each file, and encrypts the file under the defined policy. First of all, each owner encrypts his/her data with asymmetric encryption algorithm. Then, the owner formulates access policy over an attribute set and encrypts the symmetric key under the policy according to public keys obtained from CA. Afterthat, the owner sends the whole encrypted data and the encrypted symmetric key (denoted as ciphertext CT) to the cloud server to be sto red in the cloud.

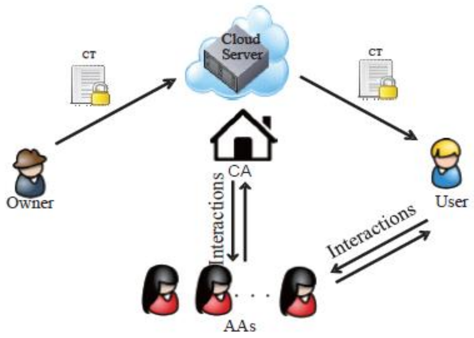

Fig. 1. System model

• The data consumer (User) is assigned a global user identity Uid by CA. The user possesses a set of attributes and is equipped with a secret key associated with his/her attribute set. The user can freely get any interested encrypted data from the cloud server. However, the user can decrypt the encrypted data if and only if his/her attribute set satisfies the access policy embedded in the encrypted data.

• The cloud server provides a public platform for owners to store and share their encrypted data. The cloud server doesn't conduct data access control for owners. The encrypted data stored in the cloud server can be downloaded freely by any user.

## Conclusion

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-AAs for public cloud storage. Our scheme employs multiple AAs 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.

## References

[1] Kaiping Xue, Senior Member, IEEE, Ying jie Xue, Jianan Hong, Wei Li, Hao Yue, M ember, IEEE,
David S.L. Wei, Senior Member, IEEE, an d Peilin Hong (Base paper)

[2] P. Mell and T. Grance, "The NIST definiti on of cloud computing," National Institute of Standards
and Technology Gaithersburg, 2011.

[3] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huan g, "Enabling personalized search over encr ypted
outsourced data with efficiency improvem ent," IEEE Transactions on Parallel & Dist ributed Systems, vol. 27, no. 9, pp. 2546–2559, 2016.

[4] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficient content-aware search over encryp ted
outsourced data in cloud," in in Proceeding s of 2016 IEEE Conference on Computer Communications
(INFOCOM 2016). IEEE, 2016, pp. 1–9.

[5] 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.

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

[7] 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.

[8] J. Hong, K. Xue, W. Li, and Y. Xue, "TAFC: Time and attribute factors combined access control on timesensitive data in public cloud," in Proceedings of 2015 IEEE Global Communications

Conference (GLOBECOM 2015). IEEE, 2015, pp. 1–6.

[9] 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.

[10] A. Lewko and B. Waters, "Decentralizing attribute-based encryption," in Advances in Cryptology–EUROCRYPT 2011. Springer, 2011.

[11] K. Yang, X. Jia, K. Ren, and B. Zhang, "DAC-MACS: Effective data access control for multi-authority cloud storage systems," in Proceedings of 2013 IEEE Conference on Computer Communications (INFOCOM 2013). IEEE, 2013.

[12] J. Chen and H. Ma, "Efficient decentralized attributebased access control for cloud storage with user revocation," in Proceedings of 2014 IEEE International Conference on Communications (ICC 2014). IEEE, 2014, pp. 3782–3787.

[13] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in Proceedings of the 16th ACM conference on Computer and Communications Security (CCS 2009). ACM, 2009, pp. 121–130.

[14] M. Lippert, E. G. Karatsiolis, A. Wiesmaier, and J. A. Buchmann, "Directory based registration in public key infrastructures." in Proceedings of the 4th International Workshop for Applied PKI (IWAP 2005), 2005, pp. 17– 32.

**[15]** W. Li, K. Xue, Y. Xue, and J. Hong, "TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage," IEEE Transactions on Parallel & Distributed Systems, vol. 27, no. 5, pp. 1484– 1496, 2016.