RAAC: Robust and Auditable Access Control with MultipleAttribute Authorities for Public Cloud Storage

ABSTRACT:

Data access control is a challenging issue in publiccloud storage systems. Ciphertext-Policy Attribute-Based Encryption(CP-ABE) has been adopted as a promising techniqueto provide flexible, fine-grained and secure data access controlfor cloud storage with honest-but-curious cloud servers. However,in the existing CP-ABE schemes, the single attribute authoritymust execute the time-consuming user legitimacy verification andsecret key distribution, and hence it results in a single-pointperformance bottleneck when a CP-ABE scheme is adopted ina large-scale cloud storage system. Users may be stuck in thewaiting queue for a long period to obtain their secret keys,thereby resulting in low-efficiency of the system. Although multiauthorityaccess control schemes have been proposed, theseschemes still cannot overcome the drawbacks of single-pointbottleneck and low efficiency, due to the fact that each of theauthorities still independently manages a disjoint attribute set.In this paper, we propose a novel heterogeneous framework toremove the problem of single-point performance bottleneck andprovide a more efficient access control scheme with an auditingmechanism. Our framework employs multiple attribute authoritiesto share the load of user legitimacy verification. Meanwhile,in our scheme, a *CA* (Central Authority) is introduced to generatesecret keys for legitimacy verified users. Unlike other multiauthorityaccess control schemes, each of the authorities in ourscheme manages the whole attribute set individually. To enhancesecurity, we also propose an auditing mechanism to detectwhich *AA* (Attribute Authority) has incorrectly or

maliciouslyperformed the legitimacy verification procedure. Analysis showsthat our system not only guarantees the security requirements butalso makes great performance improvement on key generation.

EXISTING SYSTEM:

- 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 salient feature of CP-ABE is that it grants data owners direct control power based on access policies, to provide flexible, fine grained and secure access control for cloud storage systems.
- In CP-ABE schemes, the access control is achieved by using cryptography, where an owner's data is encrypted with an access structure over attributes, and a user's secret key is labeled with his/her own attributes

DISADVANTAGES OF EXISTING SYSTEM:

- Since there is only one authority in charge of all attributes in single-authority schemes, offline/crash of this authority makes all secret key requests unavailable during that period. The similar problem exists in multi-authority schemes, since each of multiple authorities manages a disjoint attribute set.
- The inefficiency of the authority's service results in single-point performance bottleneck, which will cause system congestion such that users often cannot obtain their secret keys quickly, and have to wait in the system

queue. This will significantly reduce the satisfaction of users experience to enjoy real-time services.

- On the other hand, if there is only one authority that issues secret keys for some particular attributes, and if the verification enforces users' presence, it will bring about the other type of long service delay for users, since the authority maybe too far away from his/her home/workplace. As a result, single-point performance bottleneck problem affects the efficiency of secret key generation service and immensely degrades the utility of the existing schemes to conduct access control in large cloud storage systems.

PROPOSED SYSTEM:

- In this paper, inspired by the heterogeneous architecture with single *CA* and multiple *RAs*, we propose a robust and auditable access control scheme (named RAAC) for public cloud storage to promote the performance while keeping the flexibility and fine granularity features of the existing CP-ABE schemes.
- In our scheme, we seperate the procedure of user legitimacy verification from the secret key generation, and assign these two sub-procedures to two different kinds of authorities.
- There are multiple authorities (named attribute authorities, *AA*s), each of which is in charge of the whole attribute set and can conduct user legitimacy verification independently. Meanwhile, there is only one global trusted authority (referred as Central Authority, *CA*) in charge of secret key generation and distribution.

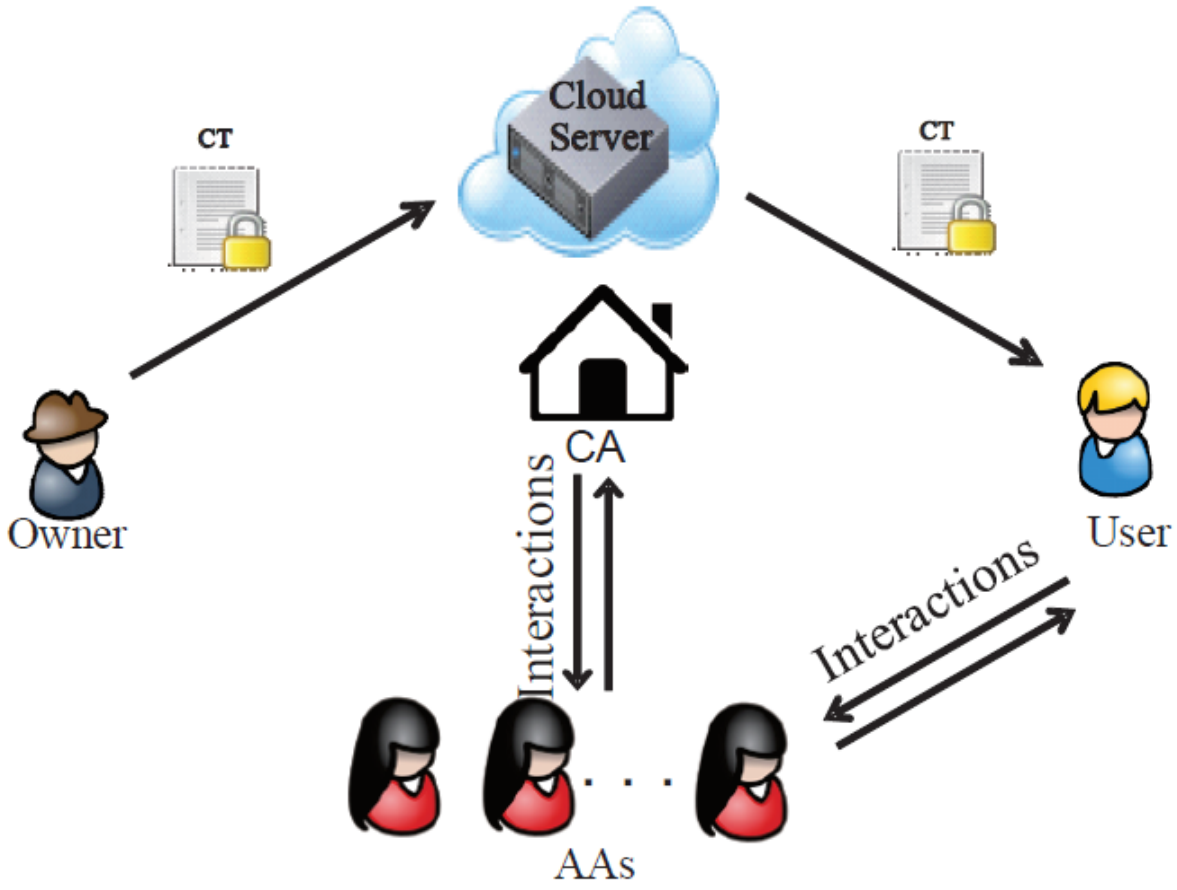
- Before performing a secret key generation and distribution process, one of the *AA*s is selected to verify the legitimacy of the user's attributes and then it generates an intermediate key to send to *CA*. *CA* generates the secret key for the user on the basis of the received intermediate key, with no need of any more verification. In this way, multiple *AA*s can work in parallel to share the load of the time consuming legitimacy verification and standby for each other so as to remove the single-point bottleneck on performance.
- Meanwhile, the selected *AA* doesn't take the responsibility of generating final secret keys to users. Instead, it generates intermediate keys that associate with users' attributes and implicitly associate with its own identity, and sends them to *CA*. With the help of intermediate keys, *CA* is able to not only generate secret keys for legitimacy verified users more efficiently but also trace an *AA*'s mistake or malicious behavior to enhance the security.

ADVANTAGES OF PROPOSED SYSTEM:

- To address the single-point performance bottleneck of keydistribution existed in the existing schemes, we propose arobust and efficient heterogeneous framework with single*CA*(Central Authority) and multiple *AA*s (Attribute Authorities)for public cloud storage.
- The heavy load of userlegitimacy verification is shared by multiple *AA*s, each ofwhich manages the universal attribute set and is able toindependently complete the user legitimacy verification,while *CA* is only responsible for computational tasks.

- To the best of our knowledge, this is the first work thatproposes the heterogeneous access control framework toaddress the low efficiency and single-point performancebottleneck for cloud storage.
- We reconstruct the CP-ABE scheme to fit our proposedframework and propose a robust and high-efficient accesscontrol scheme, meanwhile the scheme still preserves thefine granularity, flexibility and security features of CPABE.
- Our scheme includes an auditing mechanism that helpsthe system trace an *AA*'s misbehavior on user's legitimacyverification.

SYSTEM ARCHITECTURE:



SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium Dual Core.
- Hard Disk : 120 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse
- Ram : 1 GB

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE
- Tool : Netbeans 7.2.1
- Database : MYSQL

REFERENCE:

KaipingXue, *Senior Member, IEEE,* YingjieXue, Jianan Hong, Wei Li, HaoYue, *Member, IEEE,*David S.L. Wei, *Senior Member, IEEE,* and Peilin Hong, "RAAC: Robust and Auditable Access Control with MultipleAttribute Authorities for Public Cloud Storage", **IEEE Transactions on Information Forensics and Security, 2017.**