Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

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

Sadiya Kouser C A[1], Priyanka D P[2], Preethi S[3], Umme Saliyath[4], Zabiha Khan[5], Mohammed Elahi[6]

[123&4] Students, Dept. of CSE, Ghousia College of Engineering, Ramanagaram, Karnataka.

[5&6] Asst. Professor, Dept. of CSE & ECE, Ghousia College of Engineering Ramanagaram, Karnataka..

----------**********----------

Abstract:

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. 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. 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. Unlike other multi authority access control schemes, each of the authorities in our scheme manages the whole attribute set individually.

Keywords: **Frame work, CP-ABE, Central Authority, Security Key, Cloud Sever, Data Owner, Data User**

----------**********----------

INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers. The goal of cloud computing is to apply traditional supercomputing, or high-performance computing power, normally used by military and research facilities, to perform tens of trillions of computations per second, in consumer-oriented applications such as financial portfolios, deliver personalized information.

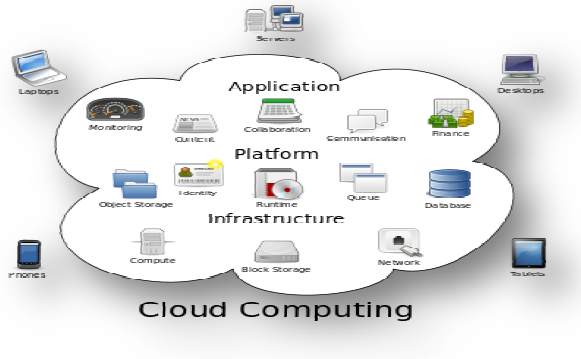


Fig: Cloud Computing

PROBLEM STATEMENT

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.
- 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

DRAWBACKS 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.
- 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.

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.
- In our scheme, we separate 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.
- 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.
- 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*. , *CA* is able to not only generate secret keys for legitimacy verified users more efficiently but also trace an *AA*'s mistake.

METHODOLOGY

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.

Proposed RAAC schemes are: System Initialization, Encryption, Key Generation, Decryption, Auditing and Tracing

MODULES:

- System Framework
- The Central Authority (CA)
- Attribute Authorities (AAs)
- Data owner (Owner)
- Data Consumer (User)
- Cloud Server

MODULES DESCRIPTION:

System Framework:

We propose a hierarchical framework with single *CA* and multiple *AA*s to remove 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. Our scheme consists of five phases, namely System Initialization, Encryption, Key Generation, Decryption, and Auditing & Tracing.

The Central Authority (CA):

Central Authority 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*.

Attribute Authorities (AAs):

Multiple *AA*s to remove the problem of single-point performance bottleneck and enhance the system efficiency. 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. 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.

Data Owner (Owner):

Data 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 a symmetric 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*. After that, the owner sends the whole encrypted data and the encrypted symmetric key (denoted as ciphertext *CT*) to the cloud server to be stored in the cloud.

Data Consumer (User):

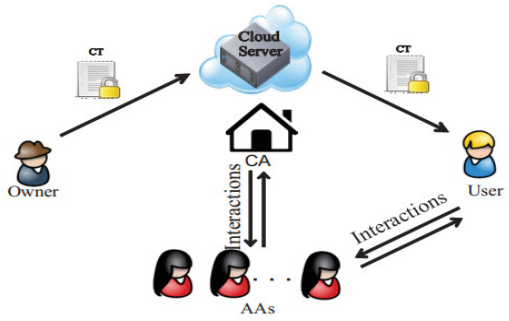
Data Consumer is assigned a global user identity *Uid* by *CA*. The user possesses a set of attributes and is equipped with a secret key associated with his/her attribute set. The user can freely get any interested encrypted data from the cloud server. However, the user can decrypt the encrypted data if and only

if his/her attribute set satisfies the access policy embedded in the encrypted data.

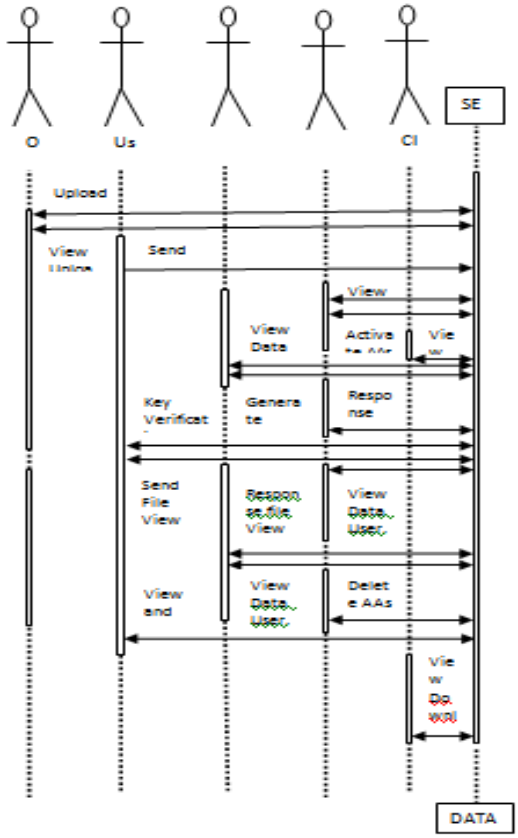
Cloud Server:

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.

SYSTEM ARCHITECTURE:

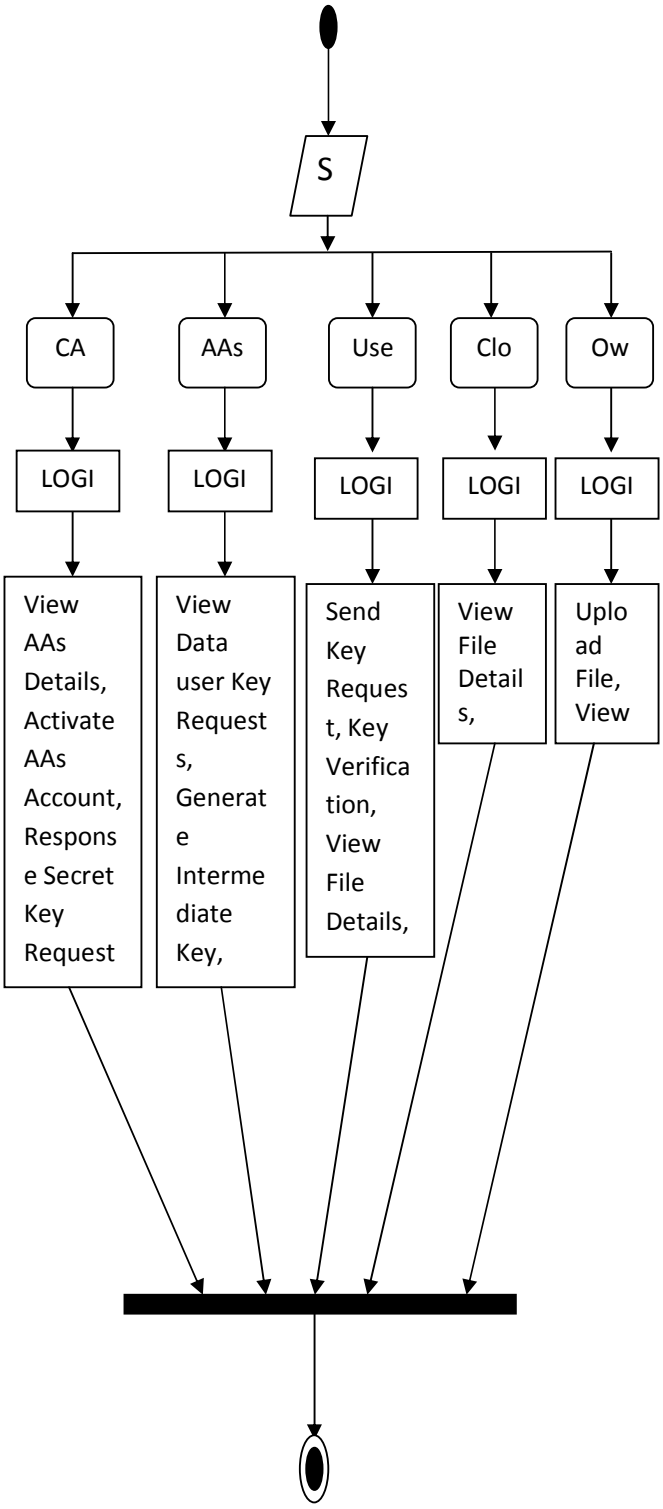


SEQUENCE DIAGRAM:



ACTIVITY DIAGRAM:

Activity diagrams are graphical representations of workflows of stepwise activities, In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system.



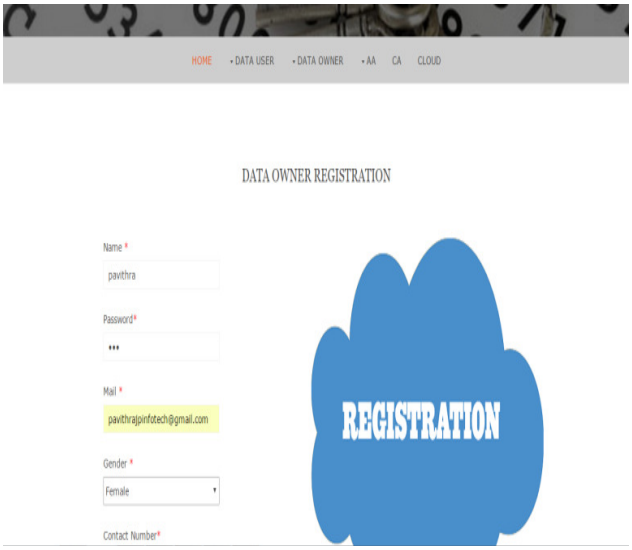
ADVANTAGES:

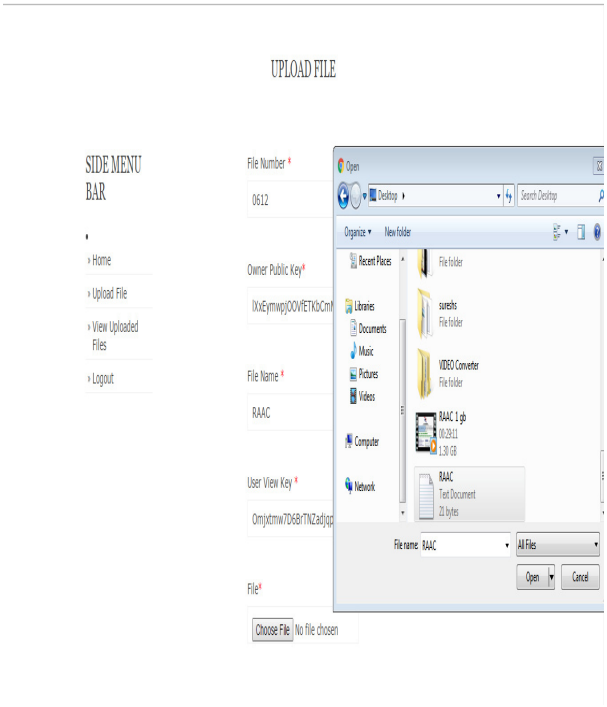
- To address the single-point performance bottleneck of key distribution existed in the existing schemes, we propose a robust and efficient heterogeneous framework with single *CA* (Central Authority) and multiple *AA*s (Attribute Authorities) for public cloud storage.
- The heavy load of user legitimacy verification is shared by multiple *AA*s, each of which manages the universal attribute set and is able to independently complete the user legitimacy verification, while *CA* is only responsible for computational tasks.
- We reconstruct the CP-ABE scheme to fit our proposed framework and propose a robust and high-efficient access control scheme.
- Our scheme includes an auditing mechanism that helps the system trace an *AA*'s misbehavior on user's legitimacy verification.

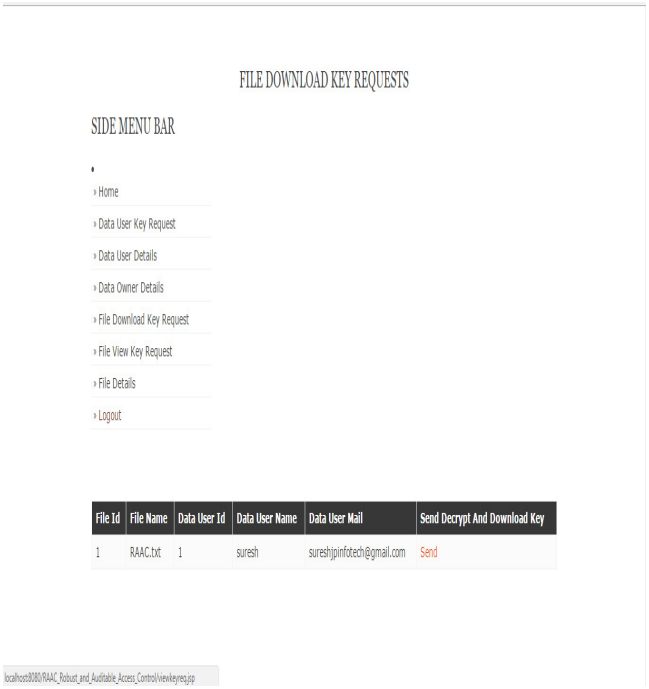
DISADVANTAGES:

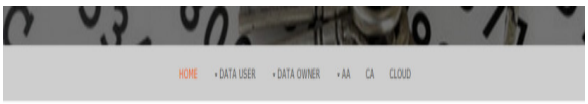
- In Key Generation Distribution phase of RAAC, the communication overhead on CA and AA is obviously larger than others due to the fact that CA must participate in the Key Generation and AA must communicate with CA. The extra overhead is introduced to guarantee the audit ability of AAs, which is worth.
- Furthermore, from the view of users, RAAC gets a better performance than TMACS in Key Generation Distribution phase because the latter one enforces to communicate with authorities. Our RAAC also shows an advantage over DAC-MACS in Encryption and Decryption phase.

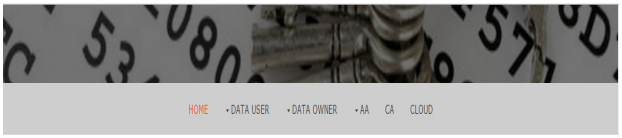
RESULTS:

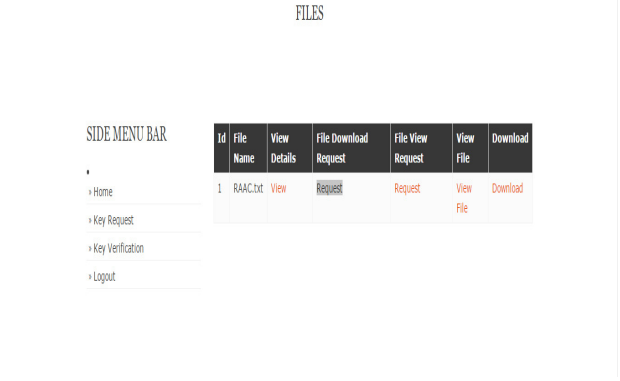












CONCLUSION

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-*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.

REFERENCES

[1] Kaiping Xue, *Senior Member, IEEE,* Yingjie Xue, Jianan Hong, Wei Li, Hao Yue, *Member, IEEE,* David S.L. Wei, *Senior Member, IEEE,* and Peilin Hong, "RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage", IEEE Transactions on Information Forensics and Security, 2017.

[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, "Enabling personalized search over encrypted outsourced data with efficiency improvement," IEEE Transactions on Parallel& Distributed Systems, vol. 27, no. 9, pp. 2546–2559, 2016.

[3] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficient content-aware search over encrypted outsourced data in cloud," in in Proceedings of 2016 IEEE Conference onComputer Communications (INFOCOM 2016). IEEE, 2016, pp. 1–9.

[4] 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.

[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 attribute based 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 time sensitive data in public cloud," in Proceedings of 2015IEEE Global Communications Conference (GLOBECOM2015). 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–EUROCRYPT2011. Springer, 2011, pp. 568–588.

[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, pp. 2895–2903.

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

