ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

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

[1] Divya, [2] C.Anuradha
[1] Student, M.Tech, Department of CSE, BIST, BIHER, Chennai.
[2] Assistant Professor, Department of CSE, BIST, BIHER, Chennai.

Abstract: ***Data access control is a challenging problem for the public Cloud storage system. Ciphertext policy attribute encryption (CP-ABE) has been adopted as a promising technology Provides flexible, fine-grained and secure data access control Cloud storage with honest and curious cloud server. However, In the existing CP-ABE scenario, the single attribute permissions You must perform time-consuming user legitimacy validation Secret key distribution, resulting in a single point Performance bottlenecks when using CP-ABE Large cloud storage systems. The user may stay in Waiting for the queue to obtain its key for a long time, resulting in inefficient system. Although multiple permissions these have proposed access control programs The program still cannot overcome the shortcomings of the single point Bottlenecks and inefficiencies due to every fact. The authorities still independently manage disjoint attribute sets..***

I. INTRODUCTION

In single-authority schemes, the only authority must verify the legitimacy of users' attributes before generating secret keys for them. As the access control system is associated with data security, and the only credential a user possess is his/her secret key associated with his/her attributes, the process of key issuing must be cautious. However, in the real world, the attributes are diverse.

The process to verify/assign attributes to users is usually difficult so that it normally employs administrators to manually handle the verification, as has mentioned, that the authenticity of registered data must be achieved by out-of-band (mostly manual) means. To make a careful decision, the unavoidable participation of human beings makes the verification time consuming, which causes a single-point bottleneck. Especially, for a large system, there are always large numbers of users requesting secret keys.

In single-authority schemes, the only authority must verify the legitimacy of users' attributes before generating secret keys for them. As the access control system is associated
with data security, and the only credential a user possess is his/her secret key associated with his/her attributes, the process of key issuing must be cautious. However, in the real world, the attributes are diverse. For example, to verify whether a user is able to drive may need an authority to give him/her a test to prove that he/she can drive.

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.

II. RELATED WORK

The same problem also exists due to the fact that multiple authorities separately maintain disjoint attribute subsets and issue secret keys associated with users' attributes within their own administration domain. Each authority performs the verification and secret key generation as a whole in the secret key distribution

The single authority does in single authority schemes. Therefore, the single-point performance bottleneck still exists in such multi-authority schemes.

In single-authority schemes, the only authority must verify the legitimacy of users' attributes before generating secret keys for them. As the access control system is associated with data security, and the only credential a user possess is his/her secret key associated with his/her attributes, the process of key issuing must be cautious. However, in the real world, the attributes are diverse. The disadvantages are the following:

- 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.
- Although existing CP-ABE access control schemes have a lot of attractive features, they are neither robust nor efficient in key generation
- 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.

III. FRAMEWORK

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.

Inspired by the heterogeneous architecture with single *CA* and multiple *RA*s, 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 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. 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. The advantages of the proposed system are the following:

- We conducted detailed security and performance analysis to verify that our scheme is secure and efficient.
- we propose a robust and efficient heterogeneous framework with single *CA*(Central Authority) and multiple *AA*s (Attribute Authorities) for public cloud storage
- It is able to independently complete the user legitimacy verification, while *CA* is only responsible for computational tasks.

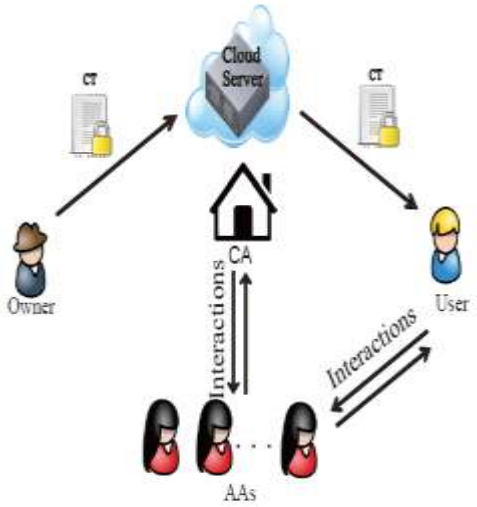
- We reconstruct the CP-ABE scheme to fit our proposed framework and propose a robust and high-efficient access control scheme, meanwhile the scheme still preserves the fine granularity, flexibility and security features of CPABE

- Our scheme includes an auditing mechanism that helps the system trace an *AA*'s misbehavior on user's legitimacy verification

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 3, Issue 4, April 2018

IV. IMPLEMENTATION

ARCHITECTURE DIAGRAM



MODULES

- DATA OWNER
- DATAUSER
- ATTRIBUTE AUTHORITY
- CENTRAL AUTHORITY

DATA OWNER

Data owner register and login by using their username and password while data owner registration cloud server send public key to data owner mail id now the public key send to data owner .data owner upload the file to the cloud in encryption format along with the user view key and public key the keys also send like encryption format .Data user register and login by using their username and password key send to data user id Data user send the key request to Attribute authority finally attribute authority generate the file view key and file download key to the data user mailed the two different key are using for download the file if the key is wrong the user consider as a attacker the file will not download

ATTRIBUTE AUTHORITY

Attribute authority register their details into the registration page key send to mail id the attribute authority activated by the Central authority If AA is not activated AA is doesn't login after activated by CA then i will do further process AA able to see all data user, Data owner and File details AA send key to the user id based on the user request now user get the download key from his/her registered mail id.

CENTRAL AUTHORITY

CA able to see AA details CA check the all AA details compare with the DAta USer details If the AA And DAtauser is same CA consider that Arribute authority as a attacker or hacker

CLOUD SERVER

Cloud server view all data owner and Data user file upload and download details Now the user enter the two diffetent keys for download and view the file cloud view upload and download file details.

V. CONCLUSION

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] P. Mell and T. Grance, "The NIST definition of cloud computing," *National Institute of Standards and Technology Gaithersburg*, 2011.
[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 on Computer 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 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, pp. 568–588