International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 15
May 2018

A Robust and Auditable Data Access Control using CP-ABE for Multiple Attribute Authorities Cloud Storage System

SHAIK MALINA & MR. I PHANI KUMAR
1PG Scholar, Dept of CSE, VelagaNageswaraRao College Of Engineering, Ponnur(Post),Ponnur(Md)Guntur(D.T), Andhra Pradesh
2Assoc Professor, Dept of CSE, VelagaNageswaraRao College Of Engineering, Ponnur(Post),Ponnur(Md)Guntur(D.T)A. Andhra Pradesh

ABSTRACT

Data access control is a challenging issue in public cloud storage systems. Ciphertext-Policy Attribute-Based Encryption (CP-ABE) has been maintain as a assuring technique to provide flexible, fine-grained and secure data access control for cloud storage with honest-but-interested cloud servers. However, in the existing CP-ABE schemes, the single attribute authority must execute the time-consuming user authority verification and secret key sharing, and hence it results in single-point performance congestion when a CP-ABE scheme is maintain in large-scale cloud storage system. Users may be fastening in the waiting queue for a long period to obtain their secret keys, thereby resulting in low-efficiency of the system. Although multi-authority access control schemes have been proposed, these schemes still cannot overcome the drawbacks of single-point congestion and low efficiency, due to the fact that each of the authorities still indivally manages a disjoint attribute set.In this project, I proposed a novel heterogeneous framework to remove the problem of single-point performance congestion and provide a more efficient access control scheme with an auditing mechanism. We implement Our framework employs multiple attribute authorities to share the load of user authority verification. And we use RC4 algorithm ,It requires a secure exchange of a shared key. Meanwhile, in our scheme, aCA (Central Authority) is introduced to generate secret keys for authority verified users. Unlike other multi-authority access control schemes, each of the authorities in our scheme manages the whole attribute set individually. To increase security, I also propose an auditing mechanism to detect which AA (Attribute Authority) has incorrectly or maliciously performed the authority verification procedure. Analysis shows that our system not only assurance the security requirements but also makes great performance increase on key generation.

1. 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. Despite the mentioned benefits, this paradigm also brings forth new challenges on data access

control, which is a critical issue to ensure data security. 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. 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.

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. Thus he/she can get an attribute key associated with driving ability . To deal with the verification of various attributes, the user may be required to be present to confirm them. Furthermore, 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. large system, there are always large numbers of users requesting secret keys. 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. Furthermore, in multi-authority schemes, 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.

The 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 straightforward idea hard to meet the security requirement of access control for public cloud storage. Our recent work, TMACS, is a threshold multi-authority CP-ABE access control scheme for public cloud storage, where multiple authorities jointly manage uniform attribute set.

II.Related work

Cryptographic techniques are well applied to access control for cloud storage system.[3]The data owners encrypt files by using the symmetric encryption approach with content keys and then use every user's public key to encrypt the content keys.Attribute-based Encryption (ABE) is a promising technique that is very suitable for access control of encrypted data.In CP-ABE schemes,[1] there is always a secret key(SK) used to generate attribute private keys, we introduce(t, n) threshold secret sharing into our scheme to share the secret key among authorities. In existing access control systems for public cloud storage, there brings a single-point bottleneck on both security and performance against the single authority for any specific attribute.[1]By introducing the combining of (t;n) threshold secret sharing and multi-authority CP-ABE scheme we propose multi- authority access control system in public cloud storage, in which multiple authorities jointly manage a uniform attribute set. By combining the traditional multi-authority scheme with ours, we construct a hybrid one, which can satisfy the scenario of attributes coming from different authorities which can solve single point bottleneck problem and provide security.

MODULE

1.CertificateAuthority: Certificate Authority is responsible for the construction of the system by setting up system parameters and attribute public key(PK) of each attribute in whole attribute set.

2.**Attribute authority**: Attribute authority focuses on the attribute management and key generation. AA jointly manages the whole attribute set , any one of the AA can not assign users secrete key alone for the master key is shared by AA.

3. Data Owner: Owner encrypts his/her file and define access about who can get access to his/her data. 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 attribute public key gained from CA .

4. Data Consumer: In this module, Users are having authentication and security to access the detail which is presented in the system. Before accessing the details user should have the account in that otherwise they should register first. CA can assign user identity uid and password to data consumer.[1]

5. **Public Cloud Server:**An entity which is managed by cloud server provider to provide data storage services . In cloud data storage , a user store his data in cloud server .In cloud data storage system , user store their data in clouds and no longer possess the data locally. Thus the correctness and availability of the data files being stored on the distributed cloud server must be guaranteed.

5. RESULT ANALYSIS

The above mentioned, information in reality, the tedious procedure of user legitimacy verification is much more complicated than secret key generation. In our scheme, the load of legitimacy verification is shared among multiple AAs, while a much lighter computational task is assigned to the single CA. Thus, the efficiency of key distribution is improved. More Specifically, multiple AAs are standby for the legitimacy verification in the system. When there is a key request, an idle AA is selected by a scheduling algorithm to perform the verification and other AAs are standby to serve the subsequent user requests. the theoretical performance analysis as the following steps. Firstly, we model our system in queueing theory, and then we analyze the state probabilities to obtain the two important factors, the mean failure probability and the average waiting time for users. Finally, to show the significant performance improvement of our proposed RAAC, we compares it with single-AA system. It's important to note that, the comparison between RAAC and multi-authority systems is similar, since each authority independently manages.

CONCLUSION

This paper, we proposed a new framework, named RAAC, A detailed report algorithms to retrieve best keyword cover was presented. Best keyword cover query aims to recover spatial objects with respect to user's requirement. Algorithms are used to find answer to such query. a disjoint attribute subset. When a user requests secret keys with regard to one certain attribute subset, he/she has to go to the only and exclusive authority that issues secret keys with that attribute subset. 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 ofthe 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.

REFERENCE:

[1] 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.

[2] Z. Fu, X. Sun, S. Ji, and G. Xie, "Towards efficientcontent-aware search over encrypted outsourced data incloud," inin Proceedings of 2016 IEEE Conference onComputerCommunications (INFOCOM 2016). IEEE, 2016, pp. 1–9.

[3] K. Xue and P. Hong, "A dynamic secure group sharing framework in public cloud computing,"IEEE Transac-tions on Cloud Computing, vol. 2, no. 4, pp. 459–470,2016.

[4] 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. 778–788,2015.

[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, 2016.

[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," inProceedings of 2015IEEE Global Communications Conference (GLOBECOM2015). IEEE, 2015, pp. 1–6.

Author's Profiles

Shaik Malina
pursing M. Tech in Computer Science and Engineering from VelagaNageswaraRao College Of Engineering in 2018, respectively.
malina.shaik30@gmail.com
9666247103

I.PHANI KUMAR received M.Tech in Computer Science He is currently working as Assoc. Professor And HOD, Dept of C.S.E, VelagaNageswaraRao College Of EngineeringCollege,Ponnur(Post),Ponnu

r(Md)Guntur(D.T), Andhra Pradesh,
A.P, and India.
phankumari@gmail.com
9110323715