ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

A Survey on Delegated Access Control in Public Cloud

V.Karthik[1], K.S.Arvind[2]

PG Scholar, Dept. of Computer Science and Engineering, Kalaignar Karunanidhi Institute of Technology, Coimbatore, TamilNadu, India[1]

Assistant Professor, Dept. of Computer Science and Engineering, Kalaignar Karunanidhi Institute of Technology, Coimbatore, TamilNadu, India[2]

ABSTRACT: Cloud computing, as an emerging computing standard. Cloud computing enables users to remotely store their data in a cloud and also benefit from services on-demand. With rapid development of cloud computing, more enterprises will outsource their sensitive data for sharing in a cloud. To maintain the shared data confidential against untrusted cloud service providers (CSPs), a natural way is to store only the encrypted data in a cloud. The major problems of this approach include establishing Decomposing Access Control Polices, delegated access control for the encrypted data, proof of ownership allow storage server to check a user data ownership based on hash value and the access rights from users when they are no longer authorized to access the encrypted data. In the proposed approach the privacy of users is protected while enforcing attribute based ACPs and utilizing the two layer of encryption reduce the overhead at Owner, opposed to unauthorized access to data and to any data leak during sharing process, providing levels of access control verification.

KEYWORDS: cloud computing; TLE; policy decomposition; privacy preserving; access control

I. INTRODUCTION

In adoption of cloud technology for storage environment represents major concerns in the part of security and privacy. Here we need to assure the confidentiality of the user's data and protect the privacy of the user. The Traditional Encryption Approach is not sufficient for assure the confidentiality of records from the cloud server. Nowadays most of the organization perform access control polices (ACPs) means "which users can access which data or records"*;* these access control policies can be expressed in the terms of user property, called as identity attribute by using access control language like XACML. Such an approach, called as Attribute Based Access Control (ABAC) support fine-grained access control which is necessary for high-assurance data security and secrecy

Fine Grained Access Control: Fine grained access control is the ability to resolve who can access individual data items and attributes. Fine grained access control allows one to implement selective access to the content based on policy specification. These system make possible yielding differential access rights to a set of users and allow exibility in specify the access rights of individual users only. Several methods are known for implementing fine grained access control.

Delegation: Delegation is a method of transmission access rights to a user. Delegation may occur in two forms: administrative delegation and user delegation. An administrative delegation allows an administrative user to assign access rights to a user and does not (necessarily) require that the administrative user possesses the ability to use the access right. A user delegation allows a user to allocate a subset of his available rights to 2 another user. However, a user delegation operation requires that the user performing the delegation must possess the ability to use the access right. Furthermore, we believe that an administrative delegation operation is often long-lived and more durable (permanent) than a user delegation operation that is short-lived (temporary) and intended for a specific purpose.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

II. LITERATURE SURVEY

Mohamed Nabeel and Elisa Bertino, proposed a paper [1] "**Privacy preserving delegated access control in public cloud**", these afford efficient group key management scheme that supports expressive ACPs. It assures the confidentiality of the data and preserves the privacy of users from the cloud while delegating most of the access control enforcement to the cloud. Here two layer encryption is performed, one by data owner and another one by cloud. Under our approach, the data owner performs a coarse-grained encryption, where cloud performs a fine-grained encryption on top of the owner encrypted data. A major issue is how to decompose access control policies (ACPs) such that the two layer encryption can be performed. Our approach is based on a privacy preserving attribute based key management scheme that protect the privacy of users while enforcing attribute based ACPs. Here decomposing the ACPs and utilize the two layer of encryption decrease the transparency at the Owner.

Mohamad Nabeel Dept. of Computer Science., Purdue Univ., West Lafayette, IN, USA, proposed a paper [2] "**Privacy preserving delegated access control in the storage as a service model**". Here a new approach for delegating privacy-preserving fine-grained access enforcement to the cloud. The approach is based on a recent key management scheme that allows users whose attributes satisfy a certain policy to derive the data encryption keys only for the content they are allowed to access from the cloud. His approach preserves the confidentiality of the data and the user privacy from the cloud, where delegating most of the access control enforcement to the cloud. Additionally, in order to reduce the cost of re-encryption required whenever the access control policies changes, these approach uses incremental encryption techniques.

Elisa Bertino, Mohamed Nabeel proposed a paper [5] "**Towards attribute based group key management**". Attribute based system permit fine-grained access control among a group of users each identified by a set of attributes. A protected collaborative applications need such flexible attribute based systems for managing and distributing group keys. These system able to support any monotonic access control policy over a set of attributes. When the group changes, the rekeying operations do not affect the private information of existing group members and thus our schemes eliminate the need of establishing expensive private communication channels

Nesrine Kaaniche, Maryline Laurent proposed a paper [6] "**A Secure Client Side Deduplication Scheme in Cloud Storage Environments**", here a new client-side deduplication scheme for securely storing and sharing outsourced data via the public cloud that towards the security and privacy of the public cloud environments. Here originality of proposal system is twofold. First, it ensures better confidentiality towards unauthorized users. Therefore every client compute a per data key to encrypt the data that he intends to store in the cloud. As such, the data access is managed by the data owner. Second, by integrate access privileges in metadata file, an authorized user can decode an encrypted file only with his private key. These solution is also shown to be resistant to unauthorized access to data and to any data disclosure during sharing procedure, given that two levels of access control verification.

III. COMPARISON OF APPROACHES

In this section we compare ABE-based existing approaches as a whole and the two AB-GKM based approaches. A common feature of all these approaches is that they support secure attribute based group communication.

Table 1: Comparison of Approaches

Property	ABE	SLE	TLE
Cryptosystem	Asymmetric	Symmetric	Symmetric
Secure attribute based group management	Yes	Yes	Yes
Efficient revocation	No	Yes	Yes
Delegation of access control	No	No	Yes

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

As shown in Table 1, while ABE-based approaches rely on asymmetric cryptography, our two approaches rely only on symmetric cryptography which is more efficient than the asymmetric cryptography. A key issue in the ABE-based approaches is that they do not support resourceful user revocations unless they use additional attributes. Our schemes address the revocation problem.

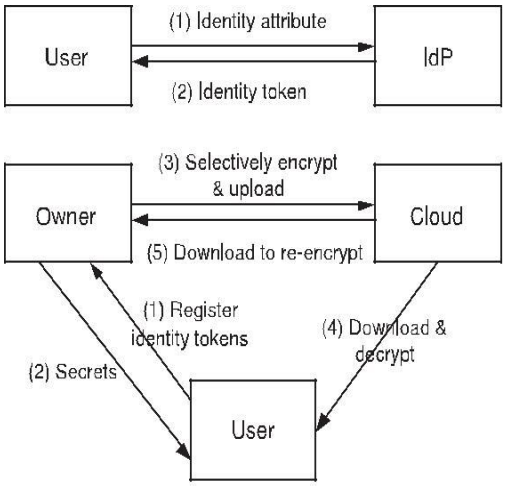

Fig.1 Single Layer Encryption

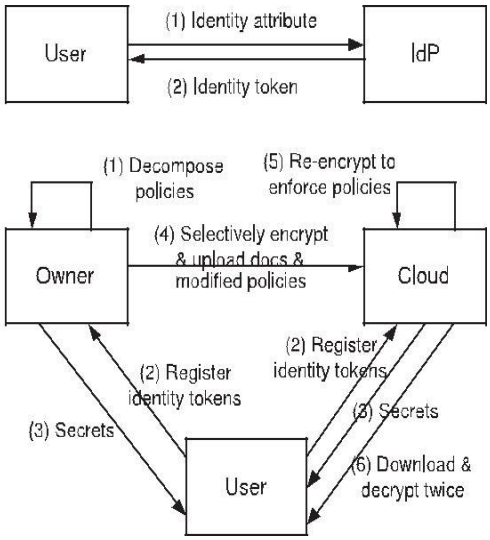

Fig.2 Two Layer Encryption

It should be well-known that the ABE based approaches and our SLE approach (Fig.1) follows the expected data outsourcing scenario by which the data owner manages all users and data before uploading the encrypted data to the cloud, whereas the Two Layer Encryption based approach(Fig.2) provides the advantage of limited management of users and data in the cloud itself while assuring confidentiality of the data and privacy of users. With always increasing user base and large amount of data, while such delegation of user management and access control is becoming very important, it also has tradeoffs in terms of privacy. Compared to the SLE approach, in the TLE approach, the data owner has to expose partial access control policies to the cloud which may allow the cloud to infer some details about the identity attributes of users. It is an interesting topic to investigate how to construct symmetric key based practical solutions to hide the access control policies from the cloud while utilizing the benefits of delegation of control.

IV. CONCLUSION

Current technologies for uploading the encrypted data incurs high cost because it manages all keys. Whenever user credentials changes therefore burden on the owner to manage all keys. To reduce the overhead of the data owner, we proposed a two layer encryption based approach to solve the problem of delegated access control and reduce the burden on the data owner. Here decompose of Access Control Polics is done on the cloud, so that owner has to handle minimum number of attribute conditions. We showed that the policy decomposition problem is NP-Complete and provided estimate algorithms. Based on the decomposed Access Control Policies, we proposed a novel approach to privacy preserving fine-grained delegated access control to data in public clouds environment. Here our approach is based on a privacy preserving attribute based key management scheme that protects the privacy of users while enforcing attribute based Access Control Polices. This proposal is shown to support data deduplication, as it employs an preverification of data subsistence, in cloud servers which is helpful for saving bandwidth. Thus the proposed system provides better security and privacy of the user's data and incurs low communication cost when compared to the existing system. Thus, the approach is based on a privacy preserving attribute based key management scheme that protects the privacy of users while enforcing attribute based Access Control Polices.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

REFERENCES

1. M. Nabeel and E. Bertino, "Privacy preserving delegated access control in public cloud," in IEEE Transactions on Knowledge and Data Engineering, 2014.
2. M. Nabeel and E. Bertino, "Privacy preserving delegated access control in the storage as a service model" in IEEE International Conference on Information Reuse and Integration (IRI), 2012.
3. M. Nabeel and E. Bertino, "Privacy preserving policy based content sharing in public clouds,"In IEEE Transactions on Knowledge and Data Engineering, 2012.
4. M. Nabeel, E. Bertino, M. Kantarcioglu, and B. M. Thuraisingham, "Towards privacy preserving access control in the cloud," in Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications and Work sharing, ser. Collaborate Com '11, 2011, pp. 172–180.
5. M. Nabeel and E. Bertino, "Towards attribute based group key management," in Proceedings of the 18th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2011.
6. Nesrine Kaaniche, Maryline Laurent," A Secure Client Side Deduplication Scheme in Cloud Storage Environments" 6th International Conference on new Technologies, Mobility and Security year 2014.
7. D. Harnik, B. Pinkas, and A. Shulman-Peleg. Side channels in cloud services: Deduplication in cloud storage. IEEE Security And Privacy, 8(6):40–47, 2010.
8. A.Fiat and M. Naor, "Broadcast Encryption," Proc. 13th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '93), pp. 480-491, 1994.
9. D. Hankerson, A. J. Menezes, and S. Vanstone. Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.
10. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attri-bute-Based Encryption," Proc. IEEE Symp. Security and Privacy (SP '07), pp. 321-334, 2007.
11. E. Bertino and E. Ferrari, "Secure and Selective Dissemination of XML Documents," ACM Trans. Information and System Security, vol. 5, no. 3, pp. 290-321, 2002.
12. J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious Trans-fer with Access Control," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), pp. 131-140, 2009.
13. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), PP 89-98, 2006.
14. J. Xu, E.-C. Chang, and J. Zhou. Weak leakage-resilient client-side deduplication of encrypted data in cloud storage. In Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security, ASIA CCS '13, pages 195–206, New York, NY, USA, 2013. ACM.
15. R. C. Merkle. A digital signature based on a conventional encryption function. In A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, CRYPTO '87, pages 369–378, London, UK, UK, 1988. Springer-Verlag.
16. R. C. Merkle. A digital signature based on a conventional encryption function. In A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, CRYPTO '87, pages 369–378, London, UK, UK, 1988. Springer-Verlag.
17. Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin, "Ensuring Distributed Accountability for Data Sharing in the Cloud" March 2012.
18. Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng "Attribute- Based Encryption with Verifiable Outsourced Decryption" 2013.

BIOGRAPHY

V.Karthik is a PG Scholar of Kalaignar Karunanidhi Institute of Technology, Coimbatore. He received B.E Computer Science and Engineering Degree in Hindusthan Institute of Technology, Coimbatore. He is doing Project in the field of Cloud Computing (Cloud Security).

Mr.Arvind K.S is working as Assistant Professor in Kalaingnar Karunanidhi Institute of Technology. He had received his Bachelor of Technology from Pondicherry University, Master of Engineering from Anna University Chennai and currently pursuing Research in Anna University Chennai. His field of Research is Cloud Computing and Information Security.