Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Protecting Privacy While Enforcing Attribute Based ACPs in Cloud Computing

Pinninti Sushma
B.Tech Student,
Depatment of CSE,
TKR College of Engineering & Technology.

Dr.A.Suresh Rao, MTech, Ph.D,
Professor &HoD,
Depatment of CSE,
TKR College of Engineering & Technology.

B.Jaya Lakshmi
Assistant Professor,
Depatment of CSE,
TKR College of Engineering & Technology.

Abstract:

Cloud computing is typically defined as a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services — such as servers, storage and applications — are delivered to an organization's computers and devices through the Internet.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.

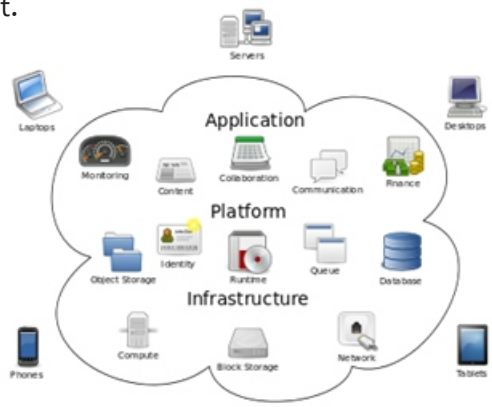
The major problems of this approach include establishing Decomposing Access Control Polices, delegated access control for the encrypted data, proof of ownership allow storage server to check a user data ownership based on hash value and the access rights from users when they are no longer authorized 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:

Privacy, Cloud computing, data sharing, policy decomposition, privacy preserving, access control, Two layer encryption

Introduction:

In a cloud computing system, there's a significant workload shift. Local computers no longer have to do all the heavy lifting when it comes to running applications. The network of computers that make up the cloud handles them instead. Hardware and software demands on the user's side decrease. The only thing the user's computer needs to be able to run is the cloud computing system's interface software, which can be as simple as a Web browser, and the cloud's network takes care of the rest.



Cloud Computing

The National Institute of Standards and Technology's definition of cloud computing identifies "five essential characteristics":On-demand self-service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.Broad network access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations). Resource pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Rapid elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear unlimited and can be appropriated in any quantity at any time.Measured service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Related Work:

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. MohamadNabeel 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 privacypreserving 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.NesrineKaaniche, 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.

EXISTING SYSTEM:

Many organizations have today ACPs regulating which users can access which data; these ACPs are often expressed in terms of the properties of the users, referred to as identity attributes, using access control languages such as XACML. Such an approach, referred to as attribute based access control (ABAC), supports fine-grained access control which is crucial for high-assurance data security and privacy. Supporting ABAC over encrypted data is a critical requirement in order to utilize cloud storage services for selective data sharing among different users. Notice that often user identity attributes encode private information and should thus is strongly protected from the cloud, very much as the data themselves.

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

Approaches based on encryption have been proposed for fine-grained access control over encrypted data. Those approaches group data items based on ACPs and encrypt each group with a different symmetric key. Users then are given only the keys for the data items they are allowed to access. Extensions to reduce the number of keys that need to be distributed to the users have been proposed exploiting hierarchical and other relationships among data items

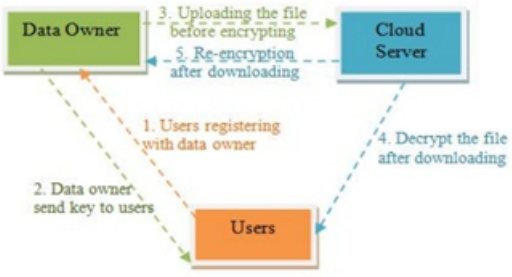
DISADVANTAGES OF EXISTING SYSTEM:

- As the data owner does not keep a copy of the data, when ever user dynamics changes, the data owner needs to download and decrypt the data, re-encrypt it with the new keys, and upload the encrypted data. The user dynamics refers to the operation of adding or revoking users. Notice also that this process must be applied to all the data items encrypted with the same key. This is inefficient when the data set to be re-encrypted is large.

- In order to issue the new keys to the users, the data owner needs to establish private communication channels with the users.

- The privacy of the identity attributes of the users is not taken into account. Therefore the cloud can learn sensitive information about the users and their organization.

- They are either unable or inefficient in supporting fine-grained ABAC policies.



Traditional Encryption Approach

PROPOSED SYSTEM:

In this paper, we propose a new approach to address this shortcoming. The approach is based on two layers of encryption applied to each data item uploaded to the cloud. Under this approach, referred to as two layer encryption (TLE), the data owner performs a coarse grained encryption over the data in order to assure the confidentiality of the data from the cloud. Then the cloud performs fine grained encryption over the encrypted data provided by the data owner based on the ACPs provided by the data owner. It should be noted that the idea of two layer encryption is not new. However, the way we perform coarse and fine grained encryption is novel and provides a better solution than existing solutions based on two layers of encryption. We elaborate in details on the differences between our approach and existing solutions in the related work section.

Hybrid Encryption Approach

A challenging issue in the TLE approach is how to decompose the ACPs so that fine-grained ABAC enforcement can be delegated to the cloud while at the same time the privacy of the identity attributes of the users and confidentiality of the data are assured. In order to delegate as much access control enforcement as possible to the cloud, one needs to decompose the ACPs such that the data owner manages minimum number of attribute conditions in those ACPs that assures the confidentiality of data from the cloud. Each ACP should be decomposed to two sub ACPs such that the conjunction of the two sub ACPs result in the original ACP. The two layer encryption should be performed such that the data owner first encrypts the data based on one set of sub ACPs and the cloud re-encrypts the encrypted data using the other set of ACPs. The two encryptions together enforce the ACP as users should perform two decryptions to access the data.

ADVANTAGES OF PROPOSED SYSTEM:

The TLE approach has many advantages.

- When user dynamics changes, only the outer layer of the encryption needs to be updated. Since the outer layer encryption is performed at the cloud, no data transmission is required between the data owner and the cloud.

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

• Further, both the data owner and the cloud service utilize a broadcast key management whereby the actual keys do not need to be distributed to the users.

• Instead, users are given one or more secrets which allow them to derive the actual symmetric keys for decrypting the data.

TWO LAYER ENCRYPTION METHOD:

Identity token providence: IdPs issue identity tokens to Users based on their identity attributes.Policy decomposition: The Owner decomposes each ACP into at most two sub ACPs such that the Owner enforces the minimum number of attributes to assure confidentiality of data from the Cloud. It is important to make sure that the decomposed ACPs are consistent so that the sub ACPs together moves the original ACPs. The Owner enforces the confidentiality related sub ACPs and the Cloud enforces the remaining sub ACPs.Identity token registration: Users register their identity tokens in order to obtain secrets to decrypt the data that they are allowed to access. Users register only those identity tokens related to the Owner's sub ACPs and register the remaining identity tokens with the Cloud in a privacy preserving manner. It should be noted that the Cloud does not learn the identity attributes of Users during this phase.

Data encryption and uploading: The Owner encrypts the data based on the Owner's sub ACPs in order to hide the content from the Cloud and then uploads them along with the public information generated by the keygen algorithm and the remaining sub ACPs to the Cloud. It in turn allows data encryption based on the keys generated using its own algorithm. Note that the Keys at the Cloud takes the secrets issued to Users and the sub ACPs given by the Owner into consideration to generate keys. Data downloading and decryption: Users download encrypted data from the Cloud and decrypt the data using the derived keys. The users decrypt the data twice.

CONCLUSION:

In this paper, we present a unique method for privacy preserving of data storage in multi-cloud environment. It also provides several advancements in cloud computing due to its technical capabilities.

The feature work may also involves load-balancing in multi-cloud environment for maximum storage and accuracy for various users. Cloud computing is a growing paradigm as an enabling technology to deliver on-demand and elastic storage and computing capabilities, while removing the ownership need for hardware. But several privacy and security act demand strong protection of the cloud users, which in turn increases the complexity to develop privacy-preserving cloud services. The privacy preserving using delegated access control in multi-cloud delivers the critical capabilities required for a robust, cost-effective, and secure cloud security implementation.

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. NesrineKaaniche, 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.

Volume No:1, Issue No:1 (June-2015)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

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. 13thACM 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. SmithaSundareswaran, 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 JianWeng "Attribute- Based Encryption with Verifiable Outsourced Decryption" 2013.