Privacy Preserving Delegated Access Control in Public Clouds with Two Layer Encryption

[1]Suresh Sakhare,[2]Sunil Shinde,[3]Chetan Dongaonkar,[4]Nayna Sonawane

[1]Student,[2]Student ,[3]Student,[4]Student
[1]Computer and Science Engineering,
[1]PDEA'S College of Engineering, Pune, India

***Abstract*— Cloud computing is a rising computing technology. It permits users, store their data, knowledge or information remotly.The purpose of this paper is to secure access control scheme for public clouds. We present a "Privacy Preserving Two Layer Encryption Access control in Public Clouds", Which provides more security and privacy as compare to the tradition approaches. Current approaches to enforce access management polices(ACPs) on outsourced data using selected encryption require organizations to manages all keys and encryptions and upload encrypted data on the remote storage. Such type of approaches incur high communications and the computation cost to manage keys and encryptions whenever user make changes. To solving this problem by delegating as much of the Access Control enforcement responsibilities as possible to the cloud while reducing the information exposure risk due to colluding users and Cloud.**

***IndexTerms*— Access Control, Anonymous Data, Cloud Computing, Privacy preserving, Two layer encryption.**

I. INTRODUCTION

Cloud competing share data through third party cloud service provider has never been more economical and easier. cloud computing is more popular and play important role in our life. Cloud computing bring users with many benefits such as the relief of the storage and flexible data access. they can motivate users to store their local data into the cloud and defend the privacy of users. they can combining set of existing and new techniques from research area such as Service-Oriented Architectures (SOA) and virtualization. most of the organization perform access management polices.(ACPs) suggests that which users will access that information or records. these access management policies expressed within the terms of user property is known as identity attribute by victimization access management language like XACML. control is often based on security-relevant properties of users referrers the identity attributes, the role of user in organization and project on which user are working. These access control process are called as the attribute based access control (ABAC) systems. attribute-based access control (ABAC),supports fine grained access control for data security and privacy.

Approaches based on encryption have been proposed for fine-grained access control over encrypted data [2]and[3].as shown in fig.1,those approaches based on ACPs and encrypted with different symmetric key. User are given only keys for data items are allowed to access, as Extensions reduce number of keys that need distributed to the users proposed exploiting hierarchical and the other relationships data items. Such approaches have several limitations.

II. TRADITIONAL APPROACH

Privacy and Security propose major concerns in acquisition of cloud technologies for data storage. An approach to solve these concerns is use of Encryption. Where as encryption assures confidentiality of the data against the Cloud, use of conventional encryption approaches isn't sufficient to support enforcement of fine-grained organization Access Control Policies(ACP).Many organizations having today Access Control Policies regulating which users can be access which data, These Acp's are often intended in terms of properties of users which referred to as identity attributes, access control languages such like XACML. Such type of approach , referred as attribute-based-access-control(ABSC), to support fine grained access-control which is crucial for high assurance data privacy and security. To supporting ABAC over encrypted data is critical need in order to utilize cloud storage service's for selected data sharing among different users. Inform that often user identity attributes encode private information and thus should be strongly secure from the Cloud. Approaches based on encryption have been proposed for fine grained access control over encrypted data.

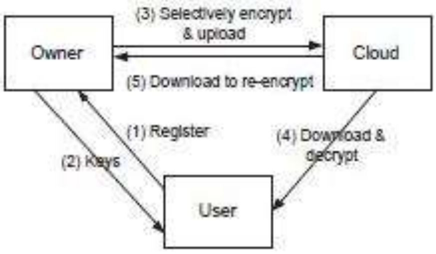


Fig. 1: Traditional approach

As shown in fig. those approaches group data items based upon ACP's and encrypt each group with a different symmetric key, Users then are given only the key for the data items they are allowed to access. Extension to minimize the number of keys that need to distributed to the users have proposed exploiting hierarchical and other relationship among data items. So such approaches however several limitations. As per the data owner does not keep copy of the data whenever the user dynamic or ACP's change the data owner requirement to download and then decrypt data, upload the encrypted data by reencryting it with the new keys. This process must be applied to all the data items encrypted with the same key. This inefficient when data set to be re-encrypted is large. Issue the new keys to user the data owner needs to be establish private communication line with the users. The security and privacy of the identity attributes of users isn’t taken into account. Because of this the Cloud can learn sensitive data about the users and their organization. Recent introduced approaches based on broadcast key management(4),(5),(6) address some of the above limitations. We referred to these approaches as "Single Layer Encryption(SLE) approach, like previous approaches, they need the data owner to enforce Access Control through encryption performed at the data owner. However unlike previous approaches Single Layer Encryption assures the privacy.

1)The data owner does not keep a copy of data as whenever the user dynamics change. the owner download and decrypt the data.re-encrypt the new keys and upload the encrypted data. Notice this process must be applied to all data items encrypted with same key. This is the data set re-encrypted is large.

2)The new keys to the users as the data owner needs to establish private communication channels with the users.

3)The identity attributes of the users is not taken into there account. Therefore cloud can learn information about the users and organizations.

4)The approach is based on broadcast key management schemes [4],[5]and[6] address. they provide some of the limitations. The approaches as single layer encryption (SLE) approaches. like a previous approaches as they require data owner to enforce access to control through encryption perform at data owner. they unlike previous approaches as SLE assures the privacy of the users and supports fine-grained ACPs.

5)SLE addresses some limitations of previous approaches as it still requires the data owner to enforce all the ACPs by fine-grained encryption both initially and subsequently after users are added or revoked or change. All these encryption activities to be performed at the owner that thus high communication and computation cost.

For example:-

if an ACP changes, the owner must be download from the cloud. as the data covered by this ACPs. generate a new encryption key as re-encrypt the downloaded data with new key. then upload the re-encrypted data to cloud. In this paper, we are 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. this approach as referred two layer encryption(TLE). Data owner performs a coarse grained encryption over data in order to assure the confidentiality of from the cloud. Then the cloud performs fine-grained encryption over the encrypted data provided by owner based on ACPs provided by the owner. It should be noted that the idea of two layer encryption is not new. The way we perform coarse and fine grained encryption is provides abettor solution than existing solutions based on two layers encryption[7].as We can elaborate details on the differences between our approach and existing approach section. A challenging issue in TLE 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 are assured. In order to delegate as much access control enforcement as possible to the cloud needs to decompose ACPs such that the owner manages minimum no. of attribute in those ACPs that assures the data from the cloud. ACP decomposed two sub ACPs such that conjunction of two sub ACPs result is in the original ACPs.The two layer encryption performed such that owner first encrypts the data on one set of sub ACPs.then the cloud re-encrypts the encrypted data.they can use the other set of ACPs.The two encryptions enforce the ACP as users perform two decryptions to access the data.

For example:-

if the ACP is (C1^C2)v(C1^C3).

ACP can be decompose two sub ACPs C1 and C2vC3.

(C1^C2)v(C1^C3) = C1^(C2VC3).

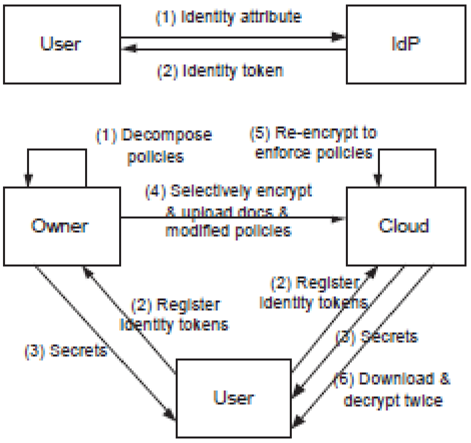
The owner enforces the former by encrypting data for the users. the cloud enforces the latter by re-encrypting owner encrypted data for the users satisfying the latter. Cloud not handle C1 as it cannot decrypt owner encrypted data. that users should be satisfy the original ACP to access the data by performing two decryptions. In this paper we are show problem of decomposing ACPs that owner manage minimum no. of attribute conditions while at same time assuring the data in cloud is NP-complete. We give two optimization algorithms that the find near optimal set of attribute. They can decompose ACP into two sub ACPs. TLE approach are provided many advantages. When the user dynamics changes as only the outer layer of encryption needs updated. the outer layer encryption is on the cloud. no need of transmission between owner and cloud. both owner and the cloud service utilize as the key management scheme[8] where the users are do not disturbed by the actual key. one more advantage users are given one or more secrets to derive the actual symmetric keys for decrypting the data.

.

III. Proposed System 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 The TLE approach has many advantages. When the policy or 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. Further, both the data owner and the cloud service utilize a broadcast key management scheme 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. This two layer enforcement allows one to reduce the load on the Owner and delegates as much access control enforcement duties as possible to the Cloud. Specifically, it provides a better way to handle data updates, user dynamics, and policy changes. The system goes through one additional phase compared to existing approach.

Proposed System architecture


User
(1) Identity attribute
(2) Identity token
IdP
(1) Decompose policies
(5) Re-encrypt to enforce policies
Owner
(4) Selectively encrypt & upload docs & modified policies
Cloud
(2) Register identity tokens
(3) Secrets
(2) Register identity tokens
(3) Secrets
(6) Download & decrypt twice
User

Modules:

The system is proposed to have the following modules along with functional requirements.

1. Identity token issuance
2. Identity token registration
3. Data encryption and uploading
4. Data downloading and decryption
5. Encryption evolution management

Identity token issuance

IdPs are trusted third parties that issue identity tokens to Users based on their identity attributes. It should be noted that IdPs need not be online after they issue identity tokens.

Identity token registration

Users register their token to obtain secrets in order to later decrypt the data they are allowed to access. Users register their tokens related to the attribute conditions in ACC with the Owner, and the rest of the identity tokens related to the attribute conditions in ACB/ACC with the Cloud. When Users register with the Owner, the Owner issues them two sets of secrets for the attribute conditions in ACC that are also present in the sub ACPs in ACPB Cloud. The Owner keeps one set and gives the other set to the Cloud. Two different sets are used in order to prevent the Cloud from decrypting the Owner encrypted data.

Data encryption and uploading

The Owner first 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 AB-GKM::KeyGen algorithm and the remaining sub ACPs to the Cloud. The Cloud in turn encrypts the data based on the keys generated using its own AB-GKM::KeyGen algorithm. Note that the AB-GKM::KeyGen 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 twice to access the data. First, the Cloud generated public information tuple is used to derive the OLE key and then the Owner generated public information tuple is used to derive the ILE key using the AB-GKM::KeyDer algorithm. These two keys allow a User to decrypt a data item only if the User satisfies the original ACP applied to the data item.

Encryption Evolution Management

Over time, either ACPs or user credentials may change. Further, already encrypted data may go through frequent updates. In such situations, data already encrypted must be re-encrypted with a new key. As the Cloud performs the access control enforcing encryption, it simply re-encrypts the affected data without the intervention of the Owner.

IV. Conclusion

Current approaches to enforce ACPs on outsourced data using selective encryption require organizations to manage all keys and encryptions and upload the encrypted data to the remote storage. Such approaches incur high communication and computation cost to manage keys and encryptions whenever user credentials change. In this paper, we proposed a two layer encryption based approach to solve this problem by delegating as much of the access control enforcement responsibilities as possible to the Cloud while minimizing the information exposure risks due to colluding Users and Cloud. A key problem in this regard is how to decompose ACPs so that the Owner has to handle a minimum number of attribute conditions while hiding the content from the Cloud. We showed that the policy decomposition problem is NP-Complete and provided approximation algorithms. Based on the decomposed ACPs, we proposed a novel approach to privacy preserving fine-grained delegated access control to data in public clouds. Our approach is based on a privacy preserving attribute based key management scheme that protects the privacy of users while enforcing attribute based ACPs. As the experimental results show, decomposing the ACPs and utilizing the two layer of encryption reduce the overhead at the Owner. As future work, we plan to investigate the alternative choices for the TLE approach further. We also plan to further reduce the computational cost by exploiting partial relationships among ACPs.

References

[1] G.Ateniese, R. Burns, R.urtmola, J.Herring, L. Kissner, Z. Peterson, and D.Song, "Deduplication in cloud storage using side channels in cloud services," Oct 2008.

[2] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of

Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[3] K. D. Bowers, A. Juels, and A. Oprea, "Hail: A high-availability and integrity layer for cloud storage," in Proc. Of CCS'09, 2009, pp. 187-198.

[4] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[5] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int"l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[6] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[7]] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int"lCryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[8] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[9] X.Liu,B.Wang,Y.Zhang, and J.Yan,"Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,"IEEE Computer Society,vol. 24,no. 6,June. 2013.

[10] M. Nabeel and E. Bertino, "Privacy preserving delegated access control in the storage as a service model," in *EEE International Conference on Information Reuse and Integration (IRI)*, 2012.

[11] E. Bertino and E. Ferrari, "Secure and selective dissemination of XML documents," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 3, pp. 290–331, 2002.

[12] G. Miklau and D. Suciu, "Controlling access to published data using cryptography," in *VLDB '2003: Proceedings of the 29th international conference on Very large data bases*. VLDB Endowment, 2003, pp. 898–909.

[13] N. Shang, M. Nabeel, F. Paci, and E. Bertino, "A privacy-preserving approach to policy-based content dissemination," in *ICDE '10: Proceedings of the 2010 IEEE 26th International Conference on Data Engineering*, 2010.

[14] 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 Worksharing*, ser. CollaborateCom "11, 2011, pp. 172–180. [15]M.Nabeel,N.Shang,andE.Bertino,"Privacypreservingpolicy based content sharing inpublic clouds," *IEEE Transactions on Knowledge and Data Engineering*, 2012. 14

[16] S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in *Proceedings of the 33rdInternationalConferenceonVeryLarge DataBases*, ser.VLDB "07. VLDB Endowment, 2007, pp. 123–134. [8] 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.

[17] A. Fiat and M. Naor, "Broadcast encryption," in *Proceedings of the 13th Annual International Cryptology Conference on Advances inCryptology*,ser.CRYPTO "93. London, UK:Springer-Verlag, 1994, pp. 480–491.

[118] D. Naor, M. Naor, and J. B. Lotspiech, "Revocation and tracing schemes for stateless receivers," in *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, ser. CRYPTO "01. London, UK: Springer-Verlag, 2001, pp. 41–62.