International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967
Volume 2 , Issue 1(Jan-Feb 2015), PP361-363

Security Preserving Access Control Mechanism in Public Clouds.

Shubhangi Repale[1], Priyanka Petkar[2] , Prajakta Patil[3], Pratiksha Yadav[4], Vaishali Shinde[5]

[1 2 3 4 5] *(Department of Computer Engg. , JSPM's Rajarshi Shahu College of Engineering, Tathawade / Savitribai Phule Pune University, India)*

Abstract :- Fine-grained access control mechanisms on secure data in the cloud are based on encryption of the data in fine-grained approach. In these approaches, owners of the data in cloud encrypt the data before uploading them on the cloud and re-encrypt the data whenever user credentials change. A better approach should be used that delegates the enforcement of fine-grained access control to the cloud, minimizing overhead at the data owners. Also assure data confidentiality from the cloud. Our technique is based on two layers of encryption that targets such requirement. In the proposed approach, the data owner performs a coarse-grained encryption, while the cloud performs a fine-grained encryption on the owner encrypted data. A challenge is to decompose access control policies (ACPs) such that the two layer encryption can be made. We also utilize an efficient group key management scheme that supports communicative ACPs. Our system assures the confidentiality of the data and preserves the privacy of users' data from the cloud while delegating most of the access control enforcement to the cloud.

Keywords: - Access Control, Cloud Computing, Encryption, Identity, Policy Decomposition

I. INTRODUCTION

Security and privacy represent major concerns in the adoption of cloud technologies for data storage. An approach to moderate these concerns is the use of encryption. However, whereas encryption protects the confidentiality of the data against the cloud, it is not sufficient to enforce organizational access control policies (ACPs). Numerous organizations have ACPs regulating which users can access which data[1]. An important problem in public cloud is how to selectively share documents based on fine-grained attribute-based access control policies (ACPs). An approach is to encrypt documents satisfying different policies with different keys using a public key cryptosystem such as attribute-based encryption, and proxy re-encryption.

II. RELATED WORK

Two layer encryption analysis provides a better way to handle data updates and dynamic changes [3]. In this work a secure collaboration application needs, flexible attribute based system and distributed group key management. This work proposes a novel key management scheme allow users whose attributes satisfy a certain policy to derive the group key and supports rekeying operation when the group changes due to joins or leaves of group members by [3]. This works provides a distributed group key management and rekeying operations. [2] Approaches based on encryption have been proposed for fine-grained access control over encrypted data. As shown in Fig 1, 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 distributed users have been proposed exploiting hierarchical and other relationships among data items. Such approaches however have several limitations.

As the data owner does not keep a copy of the data, whenever the user dynamics or policies change, the data owner needs to download and decrypt the data, re-encrypt it with the new keys, and upload the encrypted data. In this work recent group key management system used and reduce the cost of re-encryption by introducing two layer encryption. The approach preserves the confidentiality of the data and the user privacy from the cloud, while delegating most of the access control enforcement to the cloud. Further, in order to reduce the cost of re-encryption required whenever the access control policies changes, our approach uses incremental encryption techniques [2].

III. PROPOSED SYSTEM

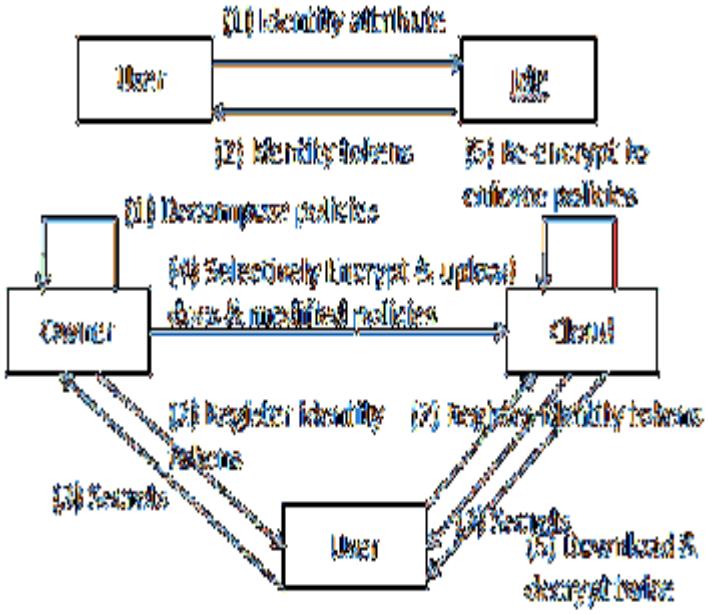

Fig. 1. Two Layer Encryption Approach

We now give a general idea of our solution to the problem of delegated access control to outsourced data in the cloud. The first module identity token issuance comprises of two tasks. In the first task, the user login with user-id and password and the server will generate key for two step authentication based on their identity attribute and mail to user. The second module encrypts the data and uploads on the cloud. Data owners are in blame of encrypting the data before uploading them on the cloud that is fine grained encryption and re-encrypting the data that is coarse grained encryption whenever user credentials change. The third module identity token registration where users register to owner to get token and register the identity token in order to obtain secrets to decrypt the data that they are approved right to use. Users register only those identity tokens related to the owner's sub ACPs and register the left over identity tokens with the Cloud in a privacy preserving method.

The users download encrypted data from the Cloud and decrypt the data using the derived keys. Users decrypt double to first remove the encryption layer added by the cloud and then by the owner. As access control is imposed through encryption, users can decrypt only those data for which they have compelling secrets. The fourth module encryption evolution management, over time user credentials may change. Further, previously encrypted data may go through numerous updates. In such situations, data previously encrypted must be re-encrypted with a new key. As the Cloud performs the access control enforcing encryption, it simply re encrypts the pretentious data without the involvement of the Owner.

3.1 Policy decomposition

In the single layer encryption approach, the Owner obtains a high communication and computation overhead since it has to manage all the authorizations when user dynamics change. To increase the performance, if the access control related encryption is somehow delegated to the Cloud, the Owner can be freed from the responsibility of managing authorizations through re-encryption. The Cloud is not trusted for the confidentiality of the outsourced data. So the Owner has to initially encrypt the data and upload the encrypted data to the cloud.

Therefore, in order for the Cloud to allow enforcing authorization policies through encryption and avoiding re-encryption by the Owner, the data may have to be encrypted again to have two encryption layers. Using the policy decomposition, the Owner decomposes each ACP into two sub ACPs. The Owner carries out the minimum number of attributes to assure confidentiality of data from the Cloud. The policy decomposition produces two sets of sub ACPs, for the owner and other for the cloud[1].

3.2 Privacy Preserving Attribute Based Group Key Management

BGKM (Broadcast Group Key Management) scheme is special type of Group Key Management scheme where private communication channels are not used and rekey operation is performed in single broadcasting. In BGKM scheme private keys are not given to the users. Instead users are given a secret. Secret is combined with public information. From that actual private keys are obtained. This scheme require a private communication only once for initial secret sharing. In such scheme, change of public information does not affect secrets of existing users. The subsequent rekeying operations are performed using one broadcast message.

IV. CONCLUSION

Thus our technique is based on two layers of encryption that targets such requirement. In the proposed approach, the data owner performs a coarse-grained encryption, while the cloud performs a fine-grained encryption on the owner encrypted data. A challenge is to decompose access control policies (ACPs) such that the two layer encryption can be made. We also utilize an efficient group key management scheme that supports communicative ACPs. Our system assures the confidentiality of the data and preserves the privacy of user's data from the cloud while delegating most of the access control enforcement to the cloud.

V. ACKNOWLEDGEMENT

We would like to acknowledge the guidance of Prof. V. D. Shinde for her insightful support and inspiration throughout the various stages of this paper. We sincerely appreciate the help and advice given by her which went a long way in helping us understanding the key concept of this paper.

REFERENCES

[1] Mohamed Nabeel, Elisa Bertino Fellow, Privacy preserving delegated access control in public clouds, IEEE.

[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, 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 Works haring, ser. Collaborate Com '11, 2011, pp. 172–180.*

[4] M. Nabeel, N. Shang, and E. Bertino, Privacy preserving policy based content sharing in public clouds, IEEE Transactions on Knowledge and Data Engineering, 2012.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, *in CCS '06: Proceedings of the 13th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2006, pp. 89–98*.

[6] X. Liang, Z. Cao, H. Lin, and J. Shao, Attribute based proxy re-encryption with delegating capabilities, *in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security, ser. ASIACCS '09*. New York, NY, USA: ACM, 2009, pp. 276–286.

[7] M. Nabeel and E. Bertino, Attribute based group key management, IEEE Transactions on Dependable and Secure Computing, 2012

[8] Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah, Encryption Efficiency Analysis and Security Evaluation of RC6 Block Cipher for Digital Images, *World Academy of Science, Engineering and Technology International Journal of Computer, Information Science and Engineering Vol:1 No:2, 2007*

[9] 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.