IJRRECS/June 2015/Volume-3/Issue-6/4096-4100 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

EFFECTIVE FUNCTIONING TOWARDS ACCESS CONTROL POLICIES IN CLOUD SYSTEM

K.Sravanthi[1], Dr.Vaka Murali Mohan[2]

[1]M.Tech Student, Dept of CSE, TRR College of Engineering, Hyderabad, T.S, India

[2]Professor, Dept of CSE, TRR College of Engineering, Hyderabad, T.S, India

ABSTRACT:

In recent times, strategies that are on the basis of broadcast key management were introduced to tackle some of the earlier works limitations and these methods are referred as single layer encryption approaches. In our work we suggest a new approach to deal with the earlier works limitations and it is on the basis of two layers of encryption functional to each data item that is uploaded to the cloud. It should be eminent that scheme of two layer encryption is not innovative on the other hand; the way we carry out coarse as well as fine grained encryption is novel and offers an enhanced solution than traditional solutions on the basis of two layers of encryption. The two layer encryption has to be implemented with the intention that the data owner initially encrypts data on the basis of one set of sub access control policies and cloud re-encrypts the encrypted data by means of the other set of access control policies. We describe two encryption layers as inner encryption layer as well as outer encryption layer.

Keywords: Access control policies, Broadcast key management, Encrypted data, Fine grained encryption, Two layer encryption.

1. INTRODUCTION:

Encryption techniques promise the privacy of data against the cloud. However the usage of conventional methods of encryption is not enough to maintain the enforcement of fine-grained organizational policies of access control. Managing of attribute based access control over encrypted data is an important prerequisite to make use of the services of cloud storage for selective data sharing between different users [1]. Methods that are

based on encryption were proposed for fine-grained access control above encrypted data. Security along with privacy corresponds to most important concerns in implementation of cloud technologies in support of data storage. In recent times, approaches based on broadcast key management were introduced to tackle some of the earlier works limitations and these methods are referred as single layer encryption approaches. Like earlier approaches, they necessitate data owner to implement access control all the way through encryption that is performed at the data owner. Contrasting from the earlier approaches, single layer encryption assures confidentiality of users and maintains fine-grained access control policies. As single layer encryption addresses several limitations of earlier approaches, it still necessitates data owner to implement all access control policies by fine-grained encryption, both at first and subsequent tousers are added/revoked [2][3]. These encryption activities were to be performed at owner that hence incurs high communication as well as computation outlay. In our work we put forward a new approach to deal with the earlier works limitations. The approach is on the basis of two layers of encryption functional to each data item that is uploaded to the cloud. It is on the basis of privacy maintenance of attribute based scheme of key management that defends privacy of users although enforcing attribute based access control policies. Under this method of two layer encryption, the data owner carries out a coarse grained encryption above data to promise the privacy of the data from cloud.

2. AN OVERVIEW OF TWO LAYER ENCRYPTION:

It should be distinguished that proposal of two layer encryption is not innovative on the other hand, the way we carry out coarse as well as fine grained encryption is novel and offers an enhanced solution than traditional solutions on the basis of two layers of encryption. A significant issue in two encryption layers approach is how to allocate encryptions among owner as well as cloud. The two encryptions mutually put in force the access control policies as users have to carry out two decryptions to access data. A challenging concern in the two layer encryption approach is how to decompose the access control policies with the intention that fine-grained attribute based access control enforcement can be delegated towards cloud while at same time privacy of

identity attributes of users and secrecy of the data are guaranteed. The two layer encryption has to be carried out so that the data owner initially encrypts data on the basis of one set of sub access control policies and cloud re-encrypts the encrypted data by means of the other set of access control policies. To delegate access control enforcing as capable towards cloud, one desire to decompose access control policies so that data owner supervises least number of attribute conditions in access control policies that assures privacy of data from cloud. Each access control policy has to be decomposed to two sub access control policies so that conjunction of two sub access control policies results in the original access control policy. Two layer of encryption has numerous advantages. During the modification of user dynamics only the outer layer of encryption wishes to be updated. While the outer layer encryption is executed at cloud, none of the data transmission is compulsory among the data owner as well as cloud. Both the data owner as well as cloud service makes use of system of broadcast key management whereby actual keys do not require to be dispersed to users [5]. Instead, users are specified one or additional secrets which permit them to obtain the authentic symmetric keys for decrypting the information.

3. AN OVERVIEW OF SOLUTION TO OUTSOURCED DATA IN CLOUD SYSTEM:

Broadcast encryption was commenced to resolve difficulty of how to resourcefully encrypt a message and broadcast it towards a subset of users within a system. Two layer encryption systems comprises of entities such as Owner, User, Identity provider as well as Cloud. Our method is on the basis of privacy preserving attribute based scheme of key management that defends privacy of users although enforcing attribute based access control policies. Two layer of enforcement permit one to decrease the load on Owner and delegates as much access control enforcement duties as promising towards the Cloud. It offers an enhanced means to hold data updates, as well as user dynamics change. In order for Cloud to permit to impose authorization policies all the way through encryption and avoid re-encryption by Owner, the data might have to be encrypted once more to contain two encryption layers. We call two encryption layers as inner encryption layer as well as outer encryption layer. Inner encryption

layer assures the privacy of data regarding Cloud and is generated by Owner. The outer encryption layer is for fine-grained approval for managing access to the data by users and is generated by means of Cloud. The two layer encryption has to be carried out so that the data owner initially encrypts data on the basis of one set of sub access control policies and cloud re-encrypts the encrypted data by means of the other set of access control policies. A significant issue in two encryption layers approach is how to allocate encryptions among owner as well as cloud. The two encryptions commonly put in force the access control policies as users have to carry out two decryptions to access data. There are two promising extremes in which the initial approach is for Owner to encrypt all data items by means of a particular symmetric key and allow Cloud carry out complete access control associated encryption. The second method is for the Owner as well as Cloud to carry out complete access control associated encryption twice [4]. The first method has slightest overhead for Owner since Owner does not handle any attributes and perform fine grained access control associated encryption. On the other hand it has the uppermost information exposure risk because of collusions among Users and Cloud since one malicious User revealing Owner's encryption key depicts all sensitive information to the Cloud. The second method contains least information exposure risk because of collusions since fine grained access control is imposed in the first encryption. The Two layer encryption approach decrease transparency that is incurred by Owner during first encryption in addition to succeeding re-encryptions. In this two layer encryption the Owner holds only the smallest set of attribute conditions and the majority of key management tasks are carried out by means of the Cloud [6].

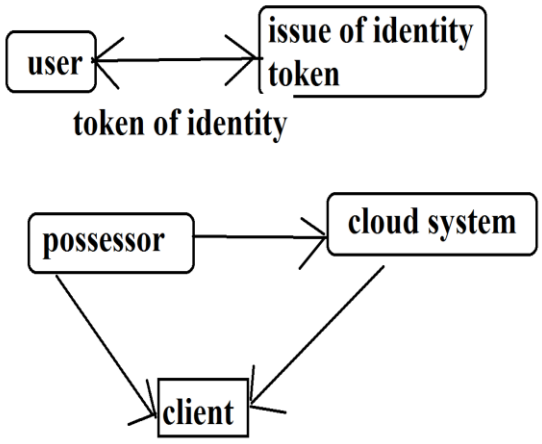

Fig1: Representation of two layer of encryption

4. CONCLUSION:

Complementary from previous approaches, single layer encryption assures confidentiality of users and maintains fine-

grained access control policies. In our work we suggest a new approach on the basis of two layers of encryption functional to each data item that is uploaded to the cloud. Proposed system of two layer encryption is not innovative on the other hand; the way we carry out coarse as well as fine grained encryption is novel and offers an enhanced solution than traditional solutions on the basis of two layers of encryption. A important issue regarding two layer encryption approach is how to decompose the access control policies with the intention that fine-grained attribute based access control enforcement can be delegated towards cloud while at same time privacy of identity attributes of users and secrecy of the data are guaranteed. Our procedure is on source of privacy preserving attribute based scheme of key management that defends privacy of users although enforcing attribute based access control policies. Two encryption layers such as inner encryption layer as well as outer encryption layer were present in proposed system. Two layer of enforcement authorize one to reduce the load on Owner and delegates as much access control enforcement duties as promising towards the Cloud. It recommends an improved means to hold data updates, as well as user dynamics change.

REFERENCES

[1] 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 33rd International Conference on Very Large Data Bases, ser. VLDB '07. VLDB Endowment, 2007, pp. 123–134.

[2] 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.

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

[4] J. Camenisch, M. Dubovitskaya, and G. Neven, "Oblivious transfer with access control," in CCS '09: Proceedings of the 16th CM conference on Computer and communications security. New York, NY, USA: ACM, 2009, pp. 131–140.

[5] K. P. N. Puttaswamy, C. Kruegel, and B. Y. Zhao, "Silverline: toward data confidentiality in storage-intensive cloud applications," in Proceedings of the 2nd ACM Symposium on Cloud Computing, ser. SOCC '11. New York, NY, USA: ACM, 2011, pp. 10:1–10:13.

[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Eurocrypt 2005, LNCS 3494. Springer-Verlag, 2005, pp. 457– 473.