IJARES/July 2015/Volume-3/Issue-7/2037-2041 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

A PROPOSAL FOR ASSURING CONFIDENTIALITY OF USER DATA IN CLOUD SYSTEM

K.Ruben Raju[1], K.Pradeep Reddy[2], M.Parimala[3]

[1]Assistant Professor, Dept of CSE, Tirumala Engineering College, Hyderabad, T.S, India

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

[3]Associate Professor & HOD, Dept of CSE, Tirumala Engineering College, Hyderabad, T.S, India

ABSTRACT:

In the recent times, attribute based access control mainly manages fine-grained access control which is considered as an important issue for assuring of data security. For reducing transparency at data owners, while promising data privacy from cloud system, we suggest an innovative approach that is on the basis of two layers of encryption that is applicable to each data item that is uploaded to cloud. The idea of projected system is not novel but the implementation of coarse as well as fine grained encryption is new and makes an enhanced solution than the earlier works based on the methods of two layers of encryption. A demanding problem concerning the proposed method of two layers of encryption is decomposing of access control policies and simultaneously assuring of privacy of identity attributes of users as well as data confidentiality. In proposed system as outer layer encryption acts upon cloud, no data transmission is necessary among data owner as well as cloud.

Keywords: Attribute based access control, Two layers of encryption, Fine-grained access control, Identity attributes, Cloud system, Data confidentiality.

1. INTRODUCTION:

There are several approaches that have been introduced in literature on the basis of encryption for managing of fine grained access on encrypted data. Generally fine-grained access control permits implementation of selected accession towards the content on the basis of specifications of expressive policy [1]. For data storage, the most important issues regarding the implementation of cloud expertise are security as well as privacy. The techniques of encryption usually makes sure regarding the data confidentiality against cloud, however usage of earlier approaches of encryption were not enough to manage enforcing of fine-grained policies of access control. In the modern times, the techniques that are projected on the basis of broadcast key management deal with some of the issues regarding approaches that are based on encryption and these refer to single layer encryption techniques. Similar to earlier techniques, single layer encryption techniques necessitates implementation of access control all the way through encryption that is performed at data owner. Differing from earlier works, single layer encryption techniques makes sure regarding user privacy and mainly supports fine-grained policies of access control. In our work, we put forward an innovative approach that is on the basis of two layers of encryption that is applicable to each data item that is uploaded to cloud. In this system, data owner in addition to cloud service exploit a proposal of broadcast key management whereby actual keys do not require to be distributed towards users. The two encryptions collectively execute access control policies since users have to execute two decryptions for accessing of the data [2]. Our proposed system is on the basis of privacy preserving attribute basis key management that defend user privacy while implementing attribute basis access control policies. In the proposed system of two layer encryption, data owner carries out coarse grained encryption above data for assuring data confidentiality from cloud.

2. METHODOLOGY:

While single layer encryption techniques handle some of the limitations of earlier works, however these methods necessitate implementation of entire access control policies by means of fine-grained encryption. Techniques of broadcast encryption were introduced for solving problem of encrypting a message and

broadcasting it to subset of users within a system. The simple scheme of broadcast encryption consists of message encryption for each of the privileged user and later broadcasting of the entire encrypted messages. For reducing the overhead at data owners, while promising data privacy from cloud system, we put forward an innovative approach that is on the basis of two layers of encryption that is applicable to each data item that is uploaded to cloud. In our proposed method, data owner carries out coarse-grained encryption, while cloud carries out fine-grained encryption on owner encrypted data that is offered by data owner on basis of access control policies offered by owner of data. The concept of proposed system is not novel but the implementation of coarse as well as fine grained encryption is new and makes an enhanced solution than the earlier works based on the methods of two layers of encryption. Our scheme is on basis of privacy preserving attribute basis key management that defend user privacy while implementing attribute basis access control policies. In our method, users are offered secrets for deriving actual symmetric keys for decrypting of data. The proposed two layer enforcement permits one to decrease load on owner and assigns access control duties towards cloud which provides an improved means for handling of data updates, within cloud [3]. A demanding issue regarding the proposed method of two layers of encryption is decomposing of access control policies and simultaneously assuring of privacy of identity attributes of users as well as data confidentiality. In the proposed method, when dynamics of user alters, then simply outer layer of encryption should be updated.

3. AN OVERVIEW OF PROPOSED SCHEME:

Modern techniques for implementing access control policies on outsourced information by means of selected encryption involve managing of encryptions and uploading of encrypted information towards secluded storage. These methods gain high computation cost for managing of keys as well as encryptions when user credentials modify [4]. We put forward an innovative approach that is on the basis of two layers of encryption that is applicable to each data item that is uploaded to cloud and minimizes information exposure risks because of colluding of users as well as cloud. The method of two layer encryption must be implemented such that data owner encrypts

data initially and later cloud re-encrypts encrypted data by means of other set of access control policies. The two encryptions collectively implement access control policies since users have to execute two decryptions for accessing of the data.

In the proposed system while outer layer encryption is acted upon cloud, no data transmission is necessary among data owner as well as cloud. When dynamics of user alters, then simply outer layer of encryption should be updated. Data owner in addition to cloud service exploit a proposal of broadcast key management whereby actual keys do not require to be distributed towards users. Here in our method, users are provided secrets for deriving real symmetric keys for decrypting of data. The proposed system is not novel but the execution of coarse as well as fine grained encryption is new and makes an enhanced solution than the earlier works based on the methods of two layers of encryption. A issue which is the most challenging one regarding proposed method is decomposing of access control policies and simultaneously assuring of privacy of identity attributes of users as well as data privacy. We provide an overview of proposed system for the difficulty of delegated access control towards outsourced. Two layers of encryption technique hold entities of Owner, User, Identity provider as well as Cloud. Single layer encryption techniques necessitate implementation of access control all the way through encryption that is performed at data owner[5]. Different from Single layer encryption techniques, owner and cloud together implement access control policies by implementing two encryptions on every data item and this two layer enforcement permits one to decrease load on Owner and assigns access control duties towards Cloud. It provides an improved means for handling of data updates, within cloud. Our proposed method is on basis of privacy preserving attribute basis key management that defend user privacy while implementing attribute basis access control policies. Two encryption layers consist of inner encryption layer as well as outer encryption layer. Inner encryption layer promises privacy of the data regarding the cloud and is produced by owner [6]. The outer encryption layer is for fine grained approval for controlling access to data by users and is produced by Cloud.

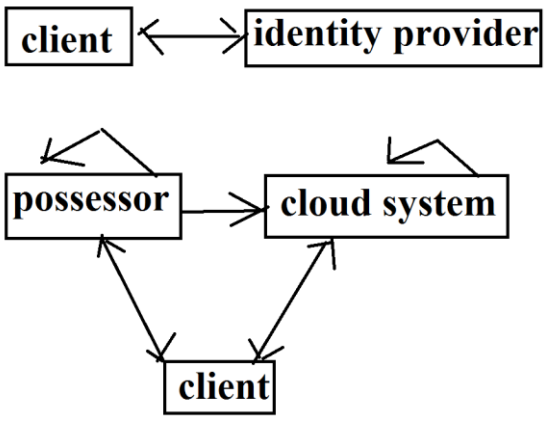

Fig1: Representation of two layer of encryption.

4. CONCLUSION:

Modern techniques for applying access control policies on outsourced information by particular encryption involve managing encrypted information towards secret storage. We suggest a pioneering approach that is on the basis of two layers of encryption that is applicable to each data item that is uploaded to cloud. In system of two layer encryption, data owner achieve coarse grained encryption above data for assuring data confidentiality from cloud. The concept of projected scheme is not novel but the implementation of coarse as well as fine grained encryption is new and makes an enhanced solution than the earlier works based on the methods of two layers of encryption. In our technique, data owner carries out coarse-grained encryption, while cloud carries out fine-grained encryption on owner encrypted data that is offered by data owner on basis of access control policies offered by owner of data. The technique of two layer encryption should be implemented such that data owner encrypts data initially and later cloud re-encrypts encrypted data by means of other set of access control policies.

REFERENCES

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

[2] 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.

[3] 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.

[4] 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.

[5] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext - policy attribute-based encryption," in SP '07: Proceedings of the 2007 IEEE Symposium on Security and Privacy. Washington, DC, USA: IEEE Computer Society, 2007, pp. 321–334.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," ACM Transaction on Information System Security, vol. 9, pp. 1–30, February 2006.