IJRRECS/November 2015/Volume-3/Issue-11/4970-4974 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

A SECURE MODEL FOR PROTECTING A SENSITIVE DATA OVER SECURE REVOCATION OF DATA

P.Sarika[1], T.Shesagiri[2]

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

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

ABSTRACT:

We introduce an effective approach on the basis of two layers of encryption functional to each data item that is uploaded towards the cloud. Complementary from the approach of single layer encryption the Owner as well as the Cloud cooperatively implements access control policies by carrying out two encryptions on each data item. Approach of two layer encryption is not novel; on the other hand, the ways we carry out coarse as well as fine grained encryption is new and make available an improved solution than established solutions on the basis of two layer of encryption. Fine grained access control was maintained by attribute based access control which is critical for high-assurance data protection and confidentiality. System of single layer encryption addresses a several limitations of earlier approaches; it still necessitates the data owner to implement the entire access control policies by fine-grained encryption. Since outer layer encryption is carried out at cloud, no data transmission is necessary among data owner as well as the cloud. In the introduced two layer encryption method, the data owner carry out a coarse grained encryption above the data to guarantee the privacy of data from the cloud. System of two encryptions cooperatively put into practice policies of access control while users have to carry out two decryptions to access the data.

Keywords: Cloud, Single layer encryption, Fine-grained encryption.

1. INTRODUCTION:

In recent times, approaches on the basis of broadcast key management tackle several limitations and referred these approaches as single layer encryption. Contrasting from earlier approaches, single layer encryption guarantees confidentiality of the users and maintain fine-grained access control policies. While single layer encryption addresses a number of limitations of earlier approaches, it still necessitates the data owner to implement the entire access control policies by fine-grained encryption. In our work, we put forward a novel approach which is on the basis of two layers of encryption functional to each data item that is uploaded towards the cloud. Encryption based techniques were introduced for access control of fine-grained data. This comforts the privacy of data against cloud, usage of established encryption approaches is not enough to maintain enforcement of fine-grained access control policies [1]. Different from single layer encryption approach the owner as well as the cloud cooperatively implements access control policies by carrying out two encryptions on each data item. An essential concern in two layer encryption approach is distribution of encryptions among Owner as well as Cloud and the proposal is not new; in contrast the ways we carry out coarse as well as fine grained encryption is new and make available an improved solution than established solutions on the basis of two layers of encryption. Two layer enforcement permits to decrease load on Owner and delegate access control enforcement to the Cloud [2][3].

2. METHODOLOGY:

To delegate enforcing of access control as promising to cloud, one desires to decompose access control policy such that data owner supervises lowest number of attribute conditions that promises privacy of data from cloud. The two layer encryption have to be carried out such that data owner initially encrypts data on the basis of one set of sub access control policies. Demanding issue in the approach of two layers of encryption is decomposing of access control policies with the intention that fine-grained attribute based access control enforcement is delegated to cloud while confidentiality of identity attributes of users and privacy of data are assured. The two encryptions collectively implement the access control policies while users have to carry out two decryptions to access the data. In two layer

encryption the data owner carry out a coarse grained encryption above the data to guarantee the privacy of data from the cloud. Cloud executes fine-grained encryption above encrypted data hat is provided by data owner on the basis of access control policies provided by the data owner. The two layer encryption approach has numerous advantages. When user dynamics alters, only outer layer of encryption desires to be updated. As outer layer encryption is carried out at cloud, no data transmission is necessary among data owner as well as the cloud. Both the data owner as well as cloud service makes use of a broadcast key management system whereby actual keys do not require to be dispersed to the users. Users are particular for one or more secrets which permit them to obtain the genuine symmetric keys for decrypting the data [4]. Identity provider issues identity tokens towards users on the basis of their identity attributes. The Owner decomposes each access control policies into at most two sub access control policies such that Owner implements the least number of attributes to guarantee privacy of data from the Cloud. As Cloud carries out access control implementing encryption, it merely re-encrypts the affected information devoid of involvement of the Owner. Users record their identity tokens to hold secrets for decrypting data that are supposed to access. The Owner initially encrypts data on basis of Owner's sub access control policies to conceal content from Cloud and subsequently uploads them all along with the public information. Users download encrypted information from Cloud and decrypt data by means of the derived keys.

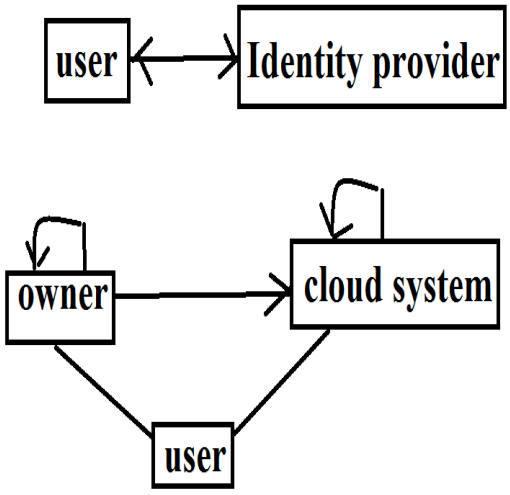

Fig1: Two Layer Encryption approach

3. OVERVIEW OF TWO LAYER ENCRYPTION APPROACH:

As the Cloud is not trustworthy for the privacy of outsourced data, Owner has to encrypt and upload the encrypted data towards the cloud. Consequently, for Cloud implementation of authorization policies by encryption and keep away from the process

of re-encryption by possessor, data might have to be encrypted to contain two encryption layers. Two layer encryption technology concepts as shown in fig1is not innovative; on the other hand, the ways we carry out coarse as well as fine grained encryption is new and make available an improved solution than established solutions on the basis of two layers of encryption. Two encryption layers are known as inner encryption layer which guarantees the privacy of data regarding the Cloud and is produced by the Owner as well as outer encryption later which are for fine-grained approval for managing access towards the data by means of users and are produced by the Cloud. The two layer encryption approach consists of Owner, User, identity provider as well as Cloud [5]. To entrust implementing of access control as promising to cloud, one desires to decompose access control policy such that data owner supervises lowest number of attribute conditions that promises privacy of data from cloud. Contrasting from single layer encryption approach the Owner as well as the Cloud cooperatively implements access control policies by carrying out two encryptions. Attribute based access control maintains fine-grained access control which is critical for high-assurance data protection and confidentiality. This permits to decrease load on Owner and delegate access control enforcement to the Cloud. An essential concern in two layer encryption approach is distribution of encryptions among Owner as well as Cloud. There are two promising extremes such as first approach is for Owner to encrypt the entire data items by means of a single symmetric key and allow Cloud carry out total access control associated encryption. It has the least transparency for Owner since he does not handle any attributes and carry out fine grained access control associated encryption [6]. It has the slightest information disclosure risk due to collusions since fine grained access control is put into effect in initial encryption. It has the uppermost transparency on Owner since Owner has to carry out the similar task at first and later needs to handle identity attributes. It has the uppermost information exposure threat due to collusions among Users as well as the Cloud while one malevolent User reveal Owner's encryption key expose the entire sensitive data towards the Cloud. The second method is for Owner as well as Cloud to carry out total access control associated encryption.

4. CONCLUSION:

Towards implementation of access control towards cloud, one desires to decompose access control policy such that data owner supervises lowest number of attribute conditions that promises privacy of data from cloud. An approach known as two encryption layers consists of inner encryption layer which guarantees the privacy of data regarding the Cloud and is produced by the Owner as well as outer encryption later which are for fine-grained approval for managing access towards the data by means of users and are produced by the Cloud. A necessary issue concerning two layer encryption methods are distribution of encryptions among Owner as well as Cloud. While outer layer encryption is carried out at cloud, no data transmission is necessary among data owner as well as the cloud. The system of two layer enforcement permits to decrease load on Owner and delegate access control enforcement to the Cloud. We set up an effectual approach which is on the basis of two layers of encryption functional to each data item that is uploaded towards the cloud. Introduced system of two layer encryption is not novel; on the other hand, the ways we carry out coarse as well as fine grained encryption is new and make available an improved solution than established solutions on the basis of two layers of encryption.

REFERENCES

[1] 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.

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

[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 Worksharing, ser. CollaborateCom '11, 2011, pp. 172–180.

[4] J. Li and N. Li, "OACerts: Oblivious attribute certificates," IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 4, pp. 340–352, 2006.

[5] T. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in CRYPTO '91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer-Verlag, 1992, pp. 129–140.

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