IJRRECS/January 2016/Volume-4/Issue-1/5175-5179 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

DESIGNING OF A SECURED DATA CONTROL METHOD FOR CLOUD SYSTEM

N.Vijaya Sunder Sagar[1], Mechineni Sri Sindhu[2]

[1]Assistant Professor & HOD, Dept of CSE, Ashoka Institute of Engineering and Technology, Malkapur, Hyderabad, T.S, India

[2]M.Tech Student, Dept of CSE, Ashoka Institute of Engineering and Technology, Malkapur, Hyderabad, T.S, India

ABSTRACT:

We make a consideration of method of data access system within multiple authority cloud storage. In our work we employ a technique of data access control that is intended for multiple-authority storage systems. In the process of cipher text-Policy based encryption there is an authority that is liable for managing of attributes as well as key distribution. We make study on revocable multiple authorities based cipher text-Policy based encryption which is functional to design method of data access control. We apply revocable method as basic method to construct effective as well as protected data access control method for multiple authority cloud systems. In this system user secret key is not associated to owner key, so that each of the user's needs to hold single secret key from every authority rather than numerous secret keys that are connected to numerous owners.

Keywords: Cipher text-Policy based encryption, Multiple authority, Data access, Cloud storage.

1. INTRODUCTION:

Multiple authority based encryption is appropriate for cloud storage since users might hold attributes that are provided by numerous authorities moreover data owners might share data by usage of access policy described over attributes. It is not easy for

applying of multiple authority based cipher text-Policy based encryption methods in the direction of multiple-authority storage systems due to attribute revocation difficulty [1]. In multiple-authority storage systems user attributes are altered with dynamism. In these storage systems we assume that certificate authority is wholly trustworthy in system. In our work we implement a method of data access control that is intended for multiple-authority storage systems. This method is a significant and resourceful data access control method for cloud systems, where there are numerous authorities that co-exist and every authority provides attributes separately. Cipher text-Policy based encryption process is an essential technique for managing of data access within cloud storage systems, as it provides access control to data owner on policies of access. On the other hand, it is tricky to apply traditional methods of cipher text-Policy based encryption for accessing of data for systems of cloud storage due to the problem of attribute revocation [2][3]. We make modification to the scheme and make it more realistic towards cloud storage systems, where the owners of data are not concerned in generation of key hence we recommend a revocable multiple authority based cipher text-Policy based encryption which is functional to design method of data access control.

2. METHODOLOGY:

We suggest a revocable multiple authority based cipher text-Policy based encryption which is functional to design method of data access control. This technique is a significant and resourceful data access control method for cloud systems, where there are numerous authorities that co-exist and every authority provides attributes separately. For understanding data access controls for multiple authority storage systems, most important issue is construction of fundamental revocable multiple authority procedure. Our proposal does not involve server that is to be entirely reliable, since key update is imposed by means of each attribute authority not server. We divide functionality of authority to global certificate authority as well as multiple attribute authorities. When server is not semi-reliable in a number of scenarios, our method can assurance backward security. We apply revocable scheme as fundamental method to build effective as well as protected data access control method for multiple authority cloud systems. In the

system user secret key is not associated to owner key, so that each of the user's needs to hold single secret key from every authority rather than numerous secret keys that are connected to various owners. Our proposed revocation technique resourcefully achieves forward security along with backward security. We get better competence of attribute revocation technique and in our revocation technique, only cipher-texts that are connected with revoked attribute has to be restructured, while in other technique the entire cipher-texts that are connected by means of any attribute from authority have to be modernized. In proposed method of attribute revocation, key and cipher-text are updated by means of using similar update key, rather than generation of update information for every cipher-text, so that owners are not necessary to store up every random number that is produced throughout encryption process [4]. Cipher text-Policy based encryption process is a capable practice that is considered for accessing of control regarding of encrypted information. There are five various entities within the proposed system such as certificate authority, owners of data, attribute authorities, cloud server as well as data consumers.

3. AN OVERVIEW OF PROPOSED SYSTEM:

There are five various entities within multiple authority cloud storage system such as certificate authority, owners of data, attribute authorities, cloud server as well as data consumers. Each attribute authority is trustworthy still can be corrupted by means of adversary. The server is curious regarding content of encrypted data or else received message however will carry out accurately task that is allocated by means of each of the attribute authority. In multiple-authority storage systems we assume that certificate authority is wholly trustworthy in system. In these systems user attributes are altered with dynamism and will not collude by any user, however it has to be prohibited from decrypting any cipher-texts [5]. For scheming of method of data access controls for multiple authority storage systems, most important issue is construction of fundamental revocable multiple authority procedure. We study data access control technique that is intended for multiple-authority storage systems and it is resourceful for cloud systems, where there are numerous authorities that co-exist and every authority provides attributes separately. Chase has proposed a multiple

authority based cipher text-Policy based encryption procedure; on the other hand, it cannot be applied as fundamental techniques due to two most important reasons. First is the security issue: Chase's multiple authority based cipher text-Policy based encryption procedure permit central authority for decryption of cipher-texts, while it holds systems master key. Second is the issue of Revocation: Chase's procedure does not manage attribute revocation. We propose revocable protocol on basis of single-authority cipher text-Policy based encryption and was extended towards multi authority situation and make it revocable. We make the proposed scheme more realistic towards cloud storage systems, where the owners of data are not concerned in generation of key hence we recommend a revocable multiple authority based cipher text-Policy based encryption which is functional to design method of data access control. For managing of security issue rather than usage of system public key towards encrypt data, proposed system necessitate each and every attribute authority for generating their public keys and make use of them for data encryption by means of global public parameters which put off certificate authority in proposed system from decrypting cipher texts. Our method does not involve server that is to be entirely reliable, since key update is imposed by means of each attribute authority not server. We utilize the proposed method in Chase's method of multiple authority based cipher text-Policy based encryption to pack secret keys that are generated by several authorities for similar user and put off collusion attack. We separate functionality of authority to global certificate authority as well as multiple attribute authorities [6]. The certificate authorities set up system and recognize user registration as well as attribute authority within system.

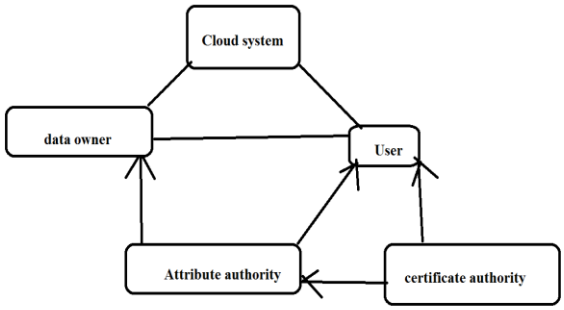

Fig1: Representation of system model.

4. CONCLUSION:

We suggest a revocable multiple authority based cipher text-Policy based encryption which is functional to design method of data access control. In this structure user secret

key is not associated to owner key, so that each of the user's needs to hold single secret key from every authority rather than numerous secret keys that are connected to numerous owners. We apply revocable method as fundamental method to build effective as well as protected data access control method for multiple authority cloud systems. Cloud storage is an important concept of data access service that set up a vast challenge for managing of data access. Multiple authority based cipher text-Policy based encryption is suitable for accessing of data for cloud storage. Our proposed method does not involve server that is to be entirely reliable, since key update is imposed by means of each attribute authority not server. We consider of method of data access system within multiple authority cloud storage and for scheming of method of data access controls for multiple authority storage systems, most important issue is construction of fundamental revocable multiple authority procedure.

REFERENCES

[1] M. Chase, ''Multi-Authority Attribute Based Encryption,'' in Proc. 4th Theory of Cryptography Conf. Theory of Cryptography (TCC'07), 2007, pp. 515-534.

[2] M. Chase and S.S.M. Chow, ''Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,'' in Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), 2009, pp. 121-130.

[3] A.B. Lewko and B. Waters, ''Decentralizing Attribute-Based Encryption,'' in Proc. Advances in Cryptology-EUROCRYPT'11, 2011, pp. 568-588.

[4] S. Jahid, P. Mittal, and N. Borisov, ''Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation,'' in Proc. 6th ACM Symp. Information, Computer and Comm. Security (ASIACCS'11), 2011, pp. 411-415.

[5] S. Ruj, A. Nayak, and I. Stojmenovic, ''DACC: Distributed Access Control in Clouds,'' in Proc. 10th IEEE Int'l Conf. TrustCom, 2011, pp. 91-98.

[6] K. Yang and X. Jia, ''Attribute-Based Access Control for Multi-Authority Systems in Cloud Storage,'' in Proc. 32th IEEE Int'l Conf. Distributed Computing Systems (ICDCS'12), 2012, pp. 1-10.