IJRRECS/August 2015/Volume-3/Issue-8/4586-4590 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN EFFECTIVE SCHEME FOR ACHIEVING SECURITY OF CLOUD STORAGE SYSTEM

Nelapati Jayabhagyam[1], Yenumala Sankara Rao[2]

[1]M.Tech Student, Dept of CSE, ST.Mary's Group of Institutions, Chebrolu, A.P, India

[2]Assistant Professor, Dept of CSE, ST.Mary's Group of Institutions, Chebrolu, A.P, India

ABSTRACT:

Multi-authority process of cipher text based encryption is suitable for managing of data access in storage systems, while users might hold attributes and owners might share data by means of access policy. For control system of data access for storage systems of multiple clouds most important issue is building of basic method of revocable multi-authority process. Because of attribute revocation complexity, multi-authority process of cipher text based encryption cannot be practical towards data access control for multiple storage systems. We present revocable multi-authority process of cipher text based encryption where a resourceful revocation technique to resolve attribute revocation difficulty in system. We modify the proposed framework and make it realistic towards cloud storage systems, where owners are not concerned in key generation.

Keywords: Cipher-text, Cloud storage, Data access, Multi-authority, Access policy, Revocation technique.

1. INTRODUCTION:

Cipher text based encryption is most proper technology that is for controlling of data access in the systems of cloud storage, since it provides owner more control on access policies. It is tricky for direct application of multi-authority process of cipher text based encryption towards storage systems of multiple clouds due to attribute revocation

difficulty. In storage systems of multiple clouds attributes of user can be altered energetically [1]. In our work we present revocable multi-authority process of cipher text based encryption where a resourceful revocation technique to resolve attribute revocation difficulty in system. Our revocable multi-authority process does not need the server to be totally confidential, since key update is imposed by every attribute authority not server. Because of data outsourcing as well as untrustworthy cloud servers, managing of data access turn out to be a demanding issue within cloud systems. Revocable multi-authority process of cipher text based encryption is applied as basic method to design data access control method and attribute revocation technique resourcefully achieves forward safety as well as backward safety. Revocable multi-authority process of cipher text based encryption build protected data access control system for storage systems of multiple clouds. In our proposed technique, only cipher-texts that are associated with revoked attribute requirements are updated and in others cipher-texts that are connected by any attribute from authority has to be updated.

2. METHODOLOGY:

For the reason that cloud server cannot be completely trustworthy by owners, they are not capable to depend on servers to perform access control. Chase projected a multi-authority process of cipher text based encryption but it cannot be useful since there are two main issues such as security issues and revocation issues. Multi-authority process of cipher text based encryption of chase technique allows central authority to decrypt cipher-texts, as it holds master key of system. Chase protocol of multi-authority process of cipher text based encryption does not sustain attribute revocation [2][3]. We present revocable multi-authority process of cipher text based encryption where a resourceful revocation technique to resolve attribute revocation difficulty in system. Our revocable multi-authority process is developed for storage systems of multiple clouds where there are numerous authorities that co-exist and every authority issues attributes separately. Proposed revocable multi-authority process is protected in random oracle representation and is more competent to earlier works. Our procedure does not need the server to be totally confidential, since key update is imposed by every attribute authority not server. We

make transformation of proposed framework and make it realistic towards cloud storage systems, where owners are not concerned in key generation. Our novel cipher text based encryption is applied as basic method to design data access control method and attribute revocation technique resourcefully achieves forward safety as well as backward security. In the proposed system user secret key is not associated to owner key, so that each of the users holds individual key from every authority rather than numerous secret keys that are connected to numerous owners. In our proposed attribute revocation technique, only cipher-texts that are associated with revoked attribute requirements are updated and in others cipher-texts that are connected by any attribute from authority has to be updated. In our proposed attribute revocation technique, key and cipher-text are updated by means of same update key, rather than requiring update information for every cipher-text, so that owners are not necessary to store up each random number that is produced during the process of encryption.

3. AN OVERVIEW OF PROPOSED SYSTEM:

We identify that cloud server are not reliable by means of data owners, as a result established attribute revocation techniques are no longer appropriate for cloud systems. Due to unreliable cloud servers, managing of data access turn out to be a demanding issue within cloud systems [4]. We introduce revocable process of cipher text based encryption where a resourceful revocation technique to resolve attribute revocation difficulty in system. The revocable process of cipher text based encryption is a promising system that is practical to remote storage systems. Proposed revocable procedure is protected in random oracle representation and is more competent to earlier works. We change proposed framework and make it practical towards cloud storage systems, where owners are not concerned in key generation. In this technique user secret key is not associated to owner key, so that each of the users holds individual key from every authority rather than numerous secret keys that are connected to numerous owners. Our revocable method is developed for storage systems of multiple clouds where there are numerous authorities that co-exist and every

authority issues attributes independently. Revocable procedure of cipher text based encryption build protected data access control system for storage systems of multiple clouds. In our proposed method, key and cipher text are updated by same update key, to a certain extent than requiring update information for every cipher-text, in order that owners are not necessary to store up each random number that is produced during encryption. A new revocable multi-authority process of cipher text based encryption based on single-authority cipher text based encryption was projected by Lewko and Waters. We extend it towards multiple authority situations and make it revocable. We apply method in Chase's multi-authority process of cipher text based encryption to pack secret keys for same user and put off collusion attack. Chase procedure of multi-authority process of cipher text based encryption does not sustain attribute revocation. Multi-authority procedure of cipher text based encryption of chase technique allows central authority to decrypt cipher-texts, as it holds master key of system. This protocol does not sustain attribute revocation. We separate the functionality of authority as global certificate authority as well as numerous attribute authorities [5]. To solve attribute revocation difficulty, we allocate aversion number for every attribute. When an attribute revocation takes place, only those components that are related to revoked attribute within secret keys and cipher texts has to be updated. When user attribute is revoked from equivalent attribute authority, it makes a novel version key for revoked attribute as well as produces an update key. With update key, the entire users, apart from revoked user, who hold revoked attributes, update its secret key. By means of update key, components that are connected to revoked attribute within cipher text moreover are updated to current version. To get better efficiency, we delegate workload of cipher text update to server by means of using proxy re-encryption technique, so that recently joined user decrypt earlier published data that are encrypted with earlier public keys, when they contain sufficient attributes [6]. By means of updating cipher texts, all users require to hold most recent secret key, to a certain extent than to maintain records on the entire earlier secret keys.

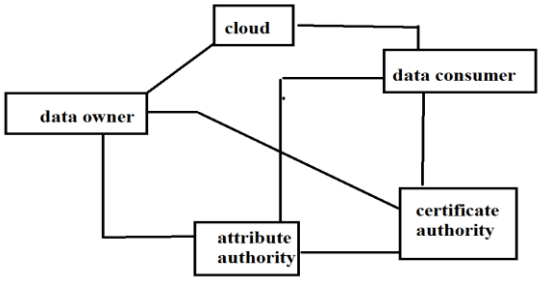

Fig1: Data access control in cloud storage.

4. CONCLUSION:

Cipher text based encryption is most appropriate knowledge for data access within cloud storage. It is not easy to apply traditional methods of cipher text based encryption to manage data access for cloud storage systems due to attribute revocation difficulty. We implement revocable multi-authority process of cipher text based encryption where a resourceful revocation technique to resolve attribute revocation difficulty in system. The proposed multi-authority process of cipher text based encryption build protected data access control system for storage systems of multiple clouds. We make alteration of framework and make it realistic towards cloud storage systems, where owners are not concerned in key generation. Proposed multi-authority process of cipher text based encryption is applied as basic method to design data access control method and attribute revocation technique resourcefully achieves forward safety as well as backward safety.

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] J. Hur and D.K. Noh, ‘‘Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,’’ IEEE Trans. Parallel Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.

[5] 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.

[6] 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.