IJRRECS/August 2015/Volume-3/Issue-8/4535-4539 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

TOWARDS DESIGNING OF EFFECTIVE DATA ACCESS PROPOSAL BY USAGE OF MULTIPLE-AUTHORITY SYSTEM

A.Divya Bharathi[1], M.Jhansi Lakshmi[2]

[1]M.Tech Student, Dept of CSE, Global Institute Of Engineering and Technology, Hyderabad, T.S, India

[2]Associate Professor & HOD, Dept of CSE, Global Institute Of Engineering and Technology, Hyderabad, T.S, India

ABSTRACT:

The component of cloud storage is a significant service of cloud computing that offers services in support of data owners for hosting of their information within cloud. Because of outsourcing and untrustworthy cloud servers, data access control turns into a challenging issue within cloud storage systems. In our work we recommend a revocable multi authority CTP basis attribute encryption, in which a resourceful as well as protected revocation method solve attribute revocation problem within system. Our system capably attains forward security as well as backward security. When server is not semi trustworthy in a number of scenarios, our system can promise backward security. We apply our proposed system of revocable multi authority CTP basis attribute encryption as fundamental method to put up the expressive and protected data access control system for multi-authority cloud storage systems.

Keywords: Cloud storage, Cloud computing, Outsourcing, Multi-authority, CTP, Attribute based encryption, Data access.

1. INTRODUCTION:

CTP basis Attribute Encryption is one of the important technologies intended for data access control within cloud storage systems, since it gives data owner additional control on access policies. CTP basis Attribute Encryption is of two types such as single-authority basis cipher-text- attribute encryption in which attributes are managed by means of a particular authority, and

multi-authority CTP basis attribute encryption where attributes are managed by means of different authorities [1]. Multi-authority CTP basis attribute encryption is more suitable for data access control regarding cloud storage systems, since users might hold attributes that are issued by multiple authorities and data owners might share data by means of access policy described over attributes from various authorities. In multi-authority systems of cloud storage user attributes are changed with dynamism. In our work we propose a revocable multi authority CTP basis attribute encryption, in which a resourceful as well as protected revocation method solve attribute revocation problem within system. Our attribute revocation means can capably attain forward security as well as backward security. Our proposed scheme does not need server to be completely trusted, since key update is imposed by every attribute authority. When server is not semi-trusted in a number of scenarios, our system can still promise backward security. Hence we apply our revocable multi authority CTP basis attribute encryption as underlying method to put up the expressive and protected data access control system for multi-authority cloud storage systems.

2. METHODOLOGY:

Since cloud server cannot be completely trusted by means of data owners, they no longer depend on servers to perform access control. It is hard to apply conventional CTP basis attribute encryption schemes in the direction of data access control for cloud storage systems due to attribute revocation difficulty [2][3]. We propose a revocable multi-authority CTP basis attribute encryption and make it applicable as fundamental techniques to propose data access control system. It is a suitable technology for managing of data access in cloud storage, since it gives data owners' added control on access policies. We adjust framework of scheme and make it more realistic towards cloud storage systems, where owners are not concerned in key generation. User secret key is not connected to owner's key, so that each user just needs to grasp one secret key from authority rather than numerous secret keys connected to numerous owners. We to a great extent get better effectiveness of attribute revocation means. In our new attribute revocation scheme, only cipher-texts that are connected with revoked attribute has to be updated, while in other schemes all cipher-texts that are connected with any of attribute from

authority have to be updated. Our proposed system does not need server to be completely trusted, since key update is imposed by every attribute authority. When server is not semi-trusted in a number of scenarios, our system can still promise backward security. In our novel attribute revocation system, both key and cipher-text are updated by means of similar update key, rather than requiring owner to produce update information for cipher-text, so that owners are not necessary to accumulate each random number that is generated during encryption.

3. AN OVERVIEW OF PROPOSED SYSTEM:

Managing of data access is an effective method to make sure data security in the cloud. CTP basis attribute encryption is an appropriate technology for managing of data access in cloud storage, since it gives data owner's added control on access policies. It is hard to apply traditional CTP basis attribute encryption schemes towards data access control for cloud storage systems due to attribute revocation difficulty. In general CTP basis attribute encryption of multi-authority type is more suitable for data access control regarding cloud storage systems. While users might hold attributes that are issued by numerous authorities and data owners might share data by means of access policy described over attributes from various authorities, CTP basis attribute encryption of multi-authority type are more preferred. To attain revocation on attribute level, various re-encryption basis attribute revocation methods are projected by depending on a trusted server [4]. As cloud server cannot be completely trusted by means of data owners, consequently conventional attribute revocation methods are no more appropriate for cloud storage systems. Hence we suggest a revocable multi-authority CTP basis attribute encryption and make it applicable as fundamental techniques to propose data access control system. We apply revocable multi authority CTP basis attribute encryption as underlying method to put up the expressive and protected data access control system for multi-authority cloud storage systems. In the data access control system shown in fig1 in multi-authority cloud storage, there are five types various entities in system such as certificate authority, attribute authorities, data owners, cloud server as well as data consumers. Certificate authority is a total trustworthy

certificate authority within the system that sets up system and accepts registration of users as well as attributes authorities in system. In our method cipher-texts that are connected with revoked attribute has to be updated, while in other schemes all cipher-texts that are connected with any of attribute from authority have to be updated. For each authorized user in system, certificate authority allocates an inclusive exceptional user identity to it and creates a global public key for this user. Certificate authority is not concerned in any attribute management as well as creation of secret keys that are connected with attributes. Every attribute authority is an autonomous attribute authority that is accountable for revoking user's attributes consistent with their role in its domain. Our system does not need server to be completely trusted, since key update is imposed by every attribute authority [5]. In our method, each attribute is connected by means of a single attribute authority however each of it supervises a random number of attributes. Each owner initially divides data into quite a lot of component consistent with logic granularities and encrypts each of the data components by various content keys by usage of symmetric encryption techniques. The owner describes access policies on attributes from numerous attribute authorities and encrypts content keys in policies and later the owner sends encrypted information towards cloud server together with cipher-texts. They do not depend on server to perform data access control however access control occurs inside cryptography [6].

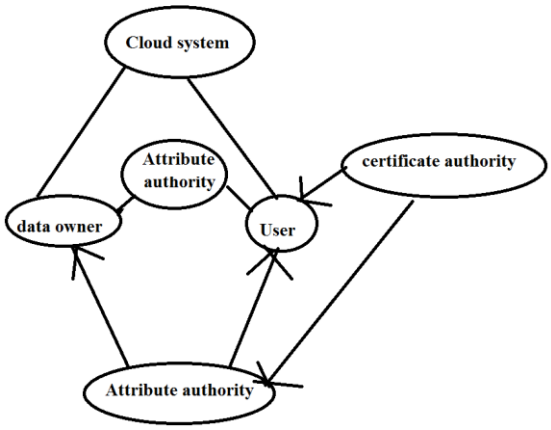

Fig1: An overview of system model.

4. CONCLUSION:

We suggest a revocable multi authority CTP basis attribute encryption, in which a resourceful as well as protected revocation method solve attribute revocation problem within system. Our revocable multi authority CTP basis attribute encryption capably attain forward security as well as backward security and does not need server to be completely trusted, since key update is imposed by every attribute authority. When server is not semi trustworthy in different

situation our system can still promise backward security. We make an application of our revocable multi authority CTP basis attribute encryption as underlying method to put up the expressive and protected data access control system for multi-authority cloud storage systems. We alter structure of scheme and make it more realistic towards cloud storage systems, where owners are not concerned in key generation. In our novel attribute revocation system, only cipher-texts that are connected with revoked attribute has to be updated, while in other schemes all cipher-texts that are connected with any of attribute from authority have to be updated.

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.