IJARES/July 2015/Volume-3/Issue-7/1981-1985 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

SCHEMING OF EFFICIENT ACCESS CONTROL SYSTEM IN CLOUD ENVIRONMENT

N.Vijaya Sunder Sagar[1], M.Nagesh[2], B.Goutham[3], Guntoju Shiva Prasad[4]

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

[2,3]Assistant Professor, Dept of CSE, Ashoka Institute of Engineering and Technology, Hyderabad, T.S, India

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

ABSTRACT:

Cipher text-Policy Attribute-based Encryption is considered as most appropriate technologies in support of data access control within cloud storage systems, since it provides control on access policies. In the system of CP-ABE, there is an authority that is accountable for attribute supervision as well as key distribution. Multi-authority CP-ABE is more suitable for data access control concerning cloud storage systems, since users might hold attributes issued by numerous authorities and data owners might moreover distribute the data by means of access policy described over attributes from several authorities. In our work, we put forward a revocable multi-authority CP-ABE system, where a resourceful as well as secure revocation means is projected to work out attribute revocation within the system. Existing attribute revocation means moreover rely on a trustworthy server or lack of effectiveness, they are not appropriate for dealing with the attribute revocation difficulty in data access control in multi-authority systems of cloud storage. The projected scheme does not necessitate the server to be completely trusted, since the key update is imposed by attribute authority. Though the server is not semi-trusted in several scenarios, projected system still assurances the backward security.

Keywords: Cloud storage, Revocation, Cipher text-Policy Attribute-based Encryption, Multi-authority CP-ABE.

1. INTRODUCTION:

To attain revocation on attribute level, several reencryption-based methods of attribute revocation methods are projected by means of relying on a trustworthy server [1]. Cloud server cannot be completely trusted by data owners, consequently conventional attribute revocation methods are no longer appropriate for the systems of cloud storage. Cipher text-Policy Attribute-Based Encryption is a promise method that is intended for access control of encrypted data. Multi-authority CP-ABE is additionally suitable for access control of cloud storage systems, since users might hold attributes issued by numerous authorities and data owners might allocate the data by means of access policy defined over attributes from dissimilar authorities. Due to the difficulty of attribute revocation, multi-authority CP-ABE systems cannot be directly practical to data access control. To design data access control system for multi-authority cloud storage systems, the most important challenging concern is to build the fundamental Revocable Multi-authority CP-ABE protocol. In our work, we put forward a revocable multi-authority CP-ABE system, where a resourceful as well as secure revocation means is projected to work out attribute revocation within the system. The projected scheme does not necessitate the server to be completely trusted, since the key update is imposed by attribute authority [2][3]. Though the server is not semi-trusted in several scenarios, projected system still assurances the backward security. Revocable multi-authority CP-ABE scheme was projected as the fundamental techniques to build the expressive and secure data access control system for multi-authority cloud storage systems.

2. METHODOLOGY:

Cipher text-Policy Attribute-based Encryption is considered as most appropriate technologies in support of data access control within cloud storage systems, since it provides control on access policies. CP-ABE systems re two types such as single-authority CP-ABE where the entire attributes are managed by a particular authority, and multi-authority CP-ABE in which attributes are from various domains and managed by dissimilar authorities. In CP-ABE system, there is an authority that is accountable for attribute supervision as well as key distribution. Multi-authority CP-ABE is more suitable for data access control concerning cloud storage systems, since

users might hold attributes issued by numerous authorities and data owners might moreover distribute the data by means of access policy described over attributes from several authorities. In multi-authority systems of cloud storage, users' attributes can be transformed dynamically. Cloud server cannot be completely trusted by data owners, they can no longer depend on servers to perform access control. Existing attribute revocation means moreover rely on a trustworthy server or lack of effectiveness, they are not appropriate for dealing with the attribute revocation difficulty in data access control in multi-authority systems of cloud storage [4]. In our work, we put forward a revocable multi-authority CP-ABE system, where a resourceful as well as secure revocation means is projected to work out attribute revocation within the system. In novel attribute revocation means, only the cipher-texts that connected with revoked attribute needs are to be updated. In new attribute revocation technique, key as well as the cipher-text are updated by means of the similar update key, rather than requiring owner to make update information for every cipher text, with the intention that owners are not necessary to accumulate each random number generated during the encryption. To design data access control system for multi-authority cloud storage systems, the most important challenging concern is to build the fundamental Revocable Multi-authority CP-ABE protocol.

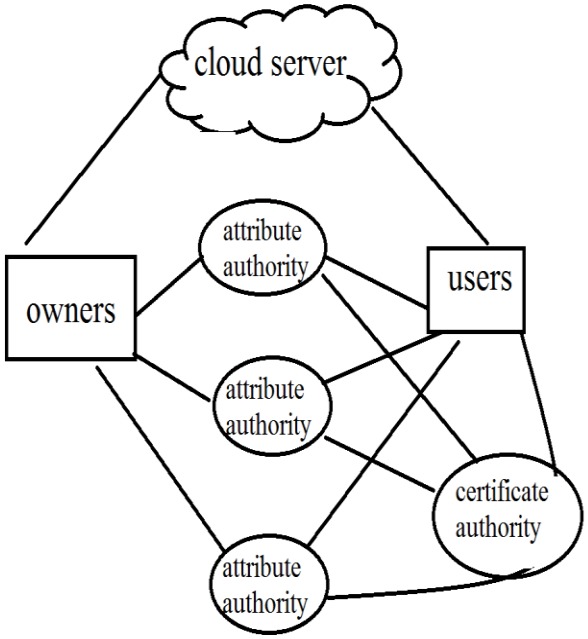

Fig1: Data access control system in multi-authority cloud storage.

3. SYSTEM OF DATA ACCESS CONTROL:

A data access control system was considered in multi-authority cloud storage, as shown in fig1. There are several entities in the system such as a certificate authority, data owners, the cloud server, attribute authorities, as well as data consumers. Certificate authority is a

comprehensive trusted certificate authority within the system which sets up system and recognize the registration of the entire the users and attribute authorities in the system. Every attribute authority is an autonomous attribute authority that is accountable for entitling as well as revoking user's attribute consistent with their role in its domain. Each user contains a global identity within the system and user might be entitled a set of attributes which might come from numerous attribute authorities. In the systems of multi-authority cloud storage systems, we make assumptions such as: Certificate authority is completely trusted in the system and it will not collude with any user, however it should be prohibited from decrypting several cipher-texts by itself. Each attribute authority is trusted however can be corrupted by means of adversary [5][6]. The server is curious however hones and it is curious concerning the content of encrypted data or else the received message, but will carry out accurately task which was assigned by every attribute authority. We put forward a novel revocable multi-authority CP-ABE procedure based on single-authority CP-ABE that is we expand it to multi-authority situation and make it revocable. We separate the functionality of authority into a comprehensive certificate authority) as well as numerous attribute authorities. Certificate authority sets up the system and recognizes the registration of users and attribute authorities within the system. To deal with the protection issue in, as an alternative of using the system exceptional public key to encrypt data, our system requires the entire attribute authorities to make their own public keys as well as uses them to encrypt data mutually with the comprehensive public parameters and this put off the certificate authority in projected system from decrypting the cipher-texts.

4. CONCLUSION:

Cipher text-Policy Attribute-Based Encryption is a promise method that is intended for access control of encrypted data. CP-ABE systems re two types such as single-authority CP-ABE where the entire attributes are managed by a particular authority, and multi-authority CP-ABE in which attributes are from various domains and managed by dissimilar authorities. Multi-authority CP-ABE is additionally suitable for access control of cloud storage systems, since users might hold attributes issued by numerous authorities and data owners might allocate the data by means of

access policy defined over attributes from dissimilar authorities. Existing attribute revocation means moreover rely on a trustworthy server or lack of effectiveness, they are not appropriate for dealing with the attribute revocation difficulty in data access control in multi-authority systems of cloud storage. To design data access control system for multi-authority cloud storage systems, the most important challenging concern is to build the fundamental Revocable Multi-authority CP-ABE protocol. In our work, we put forward a revocable multi-authority CP-ABE system, where a resourceful as well as secure revocation means is projected to work out attribute revocation within the system. The projected scheme does not necessitate the server to be completely trusted, since the key update is imposed by attribute authority. Though the server is not semi-trusted in several scenarios, projected system still assurances the backward security. In novel attribute revocation means, only the cipher-texts that connected with revoked attribute needs are to be updated.

REFERENCES

[1] 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.

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

[3] S. Yu, C. Wang, K. Ren, and W. Lou, ‘‘Attribute Based Data Sharing with Attribute Revocation,’’ in Proc. 5th ACM Symp. Information, Computer and Comm. Security (ASIACCS’10), 2010, pp. 261-270.

[4] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, ‘‘Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption,’’ IEEE Trans. Parallel Distributed Systems, vol. 24, no. 1, pp. 131-143, Jan. 2013.

[5] 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.

[6] 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.