IJRRECS/November 2015/Volume-3/Issue-11/4955-4959 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

A COMPETENCE AND COMMUNICATIVE MODEL FOR SECURE DATA ACCESS FOR VARIOUS AUTHORIZED CLOUD STORAGE

Koli Sushmaja[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:

To introduce access control system of data for storage of multi-authority cloud, most significant issue is to build the fundamental revocable multi-authority CP-ABE procedure. We set up a revocable multi-authority CP-ABE means that supports safe attribute revocation. Introduced model of attribute revocation is well-organized in the sense that it sustains less communication as well as computation cost, and is protected in the sense that it can attain backward as well as forward security. An effective method of revocable multi-authority CP-ABE is functional in the direction of online social networks. Multi-authority cipher text-policy attribute-based encryption was practical as fundamental techniques to build expressive as well as protected data access control system for multi-authority cloud storage systems. For achieving revocation on attribute level, several attribute revocation methods of re-encryption based are projected by depending on a trustworthy server. The method of multi-authority CP-ABE is additional benefit for access control of cloud systems, as users may hold attributes that are issued by numerous authorities and the data owners might distribute the data by means of access policy.

Keywords: Attribute revocation, Access control, Cloud storage.

1. INTRODUCTION:

There are single authority cipher text-policy attribute-based encryption and also multi-authority cipher text-policy-ABE. In single cipher text-policy-ABE, single authority manages all attributes and in multi-authority cipher text-policy-ABE different authorities manage different domains [1]. For attaining of revocation on attribute level, a number of attribute revocation schemes of re-encryption-based are projected by depending on a trustworthy server. On the other hand, traditional methods of attribute revocation moreover depend on a trustworthy server or else lack of effectiveness; they are not appropriate for dealing with problem of attribute revocation in data access control within storage systems of multi-authority cloud. In these systems, attributes of user can be altered dynamically. Cipher text-policy attribute-based encryption is an efficient approach for accessing control of encrypted data. In our work, we introduce revocable multi-authority cipher text-policy attribute-based encryption method that supports safe attribute revocation. Revocable multi-authority cipher text-policy attribute-based encryption is an efficient method functional towards online social networks. Projected revocable multi-authority text-policy attribute-based encryption system was functional as fundamental techniques to build expressive as well as protected data access control system for multi-authority cloud storage systems. The introduced strategy does not necessitate the server to be completely trusted, as the key update is implemented by each attribute authority [2][3]. Although server is not semi-trusted in a number of situations, introduced scheme can still assurance backward security.

2. METHODOLOGY:

In novel attribute revocation means, only cipher-texts that are connected with revoked attribute requirements to be updated, all the cipher-texts that connected with any attribute from authority have to be updated [4]. In our novel attribute revocation means, key as well as cipher-text are updated by means of similar update key, in place of requiring owner to produce and bring up to date information for every cipher-text, such that owners are not necessary to accumulate every random number produced during the encryption. Data access control system was considered within multi-authority cloud storage as shown in fig1 consisting of certificate authority, attribute authorities,

owners, cloud server as well as users. System of revocable multi-authority cipher text-policy attribute-based encryption is a well-organized method functional towards online social networks. In introduced scheme, every attribute is connected by a single attribute authority; however each of them manages a random number of attributes. Every attribute authority contains full control over structure of its attributes. The certificate authority is an overall trustworthy certificate authority within the system which sets up system and accepts registration of users. We set up revocable multi-authority cipher text-policy attribute-based encryption means that supports safe attribute revocation. Our model of attribute revocation is well-organized in the sense that it sustains less communication as well as computation cost, and is protected in the sense that it can attain backward as well as forward security. Every attribute authority is an autonomous attribute authority that is accountable for entitling user's attributes in accordance with their role in its domain. The certificate authority accepts the registration of users and attributes authorities within the system. Each user contains an inclusive identity within system and might be entitled a set of attributes which may approach from numerous attribute authorities.

3. INTRODUCTION TO NOVEL REVOCABLE MULTIAUTHORITY CP-ABE SYSTEM:

For the access control of cloud systems, multi-authority cipher text-policy attribute-based encryption is additional benefit since users might hold attributes that are issued by numerous authorities and the data owners might distribute the data by means of access policy [5]. To recommend the data access control system for multi-authority cloud storage schemes, the most important demanding issue is to build the fundamental revocable multi-authority cipher text-policy attribute-based encryption process. Authority was separated into a global certificate authority as well as numerous attribute authorities. The certificate authority accepts user registration and attributes authorities within the system. It allocates a global user identity towards each user as well as a global authority identity to each attribute authority within the system. Since user identity is globally exceptional in the system, secret keys that are issued by several attribute authority for similar user identity can be tied mutually for decryption. In the

projected system, each attribute is connected by a single attribute authority; however each of them manages a random number of attributes. To work out attribute revocation difficulty, aversion number for each attribute was assigned. When an attribute revocation takes place, only those components connected with revoked attribute within secret keys as well as cipher-texts should be updated. When a user attribute is revoked from its equivalent attribute authority, it produces a novel version key for revoked attribute and produces an update key. A novel revocable multi-authority cipher text-policy attribute-based encryption on basis of single-authority cipher text-policy attribute-based encryption was projected by Lewko and Waters and later it was extended to multi-authority situation and makes it revocable. With update key, all users, apart from the revoked user, who hold revoked attributes can bring up to date its secret key. By means of the update key, components connected with revoked attribute in cipher-text can moreover be updated to current version. To deal with protection issue rather than using system unique public key towards encrypting data, our system necessitates the entire attribute authorities to produce their individual public keys and employs them to encrypt data mutually with comprehensive public parameters that put off certificate authority in our system from decrypting the cipher-texts [6]. To get better the effectiveness, workload of cipher-text update was delegated towards server by means of proxy re-encryption means, so that newly joined user is moreover capable to decrypt earlier published data, which are encrypted with earlier public keys, if they have adequate attributes. By means of bringing up to date cipher-texts, the entire users require to hold only most recent secret key, to a certain extent than keeping records on earlier secret keys.

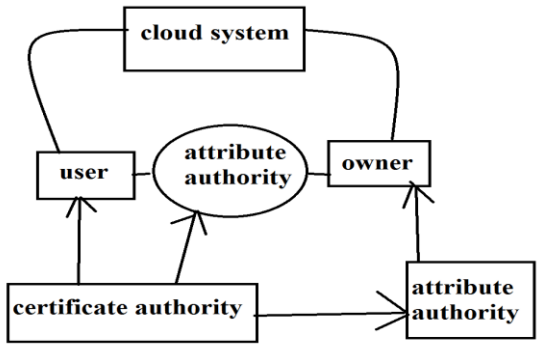

Fig1: system representation of data access control.

4. CONCLUSION:

We have commenced revocable multi-authority cipher text-policy attribute-based encryption technique that supports safe attribute revocation. Introduced system of revocable multi-authority cipher text-policy attribute-based encryption system was

functional as fundamental techniques to build expressive as well as protected data access control system for multi-authority cloud storage systems. To suggest data access control system in support of multi-authority cloud storage schemes, the most important demanding issue is to build the fundamental revocable multi-authority cipher text-policy attribute-based encryption procedure. Our representation of attribute revocation is ordered in the sense that it sustains less communication as well as computation cost, and is protected in the sense that it can attain backward as well as forward security. In effective system of attribute revocation means, only cipher-texts that are connected with revoked attribute requirements to be updated, all the cipher-texts that connected with any attribute from authority have to be updated. In the technique of multi-authority CP-ABE different authorities manage different domains. In storage systems of multi-authority cloud, attributes of user can be altered dynamically. Data access control approach was considered within multi-authority cloud storage, consisting of certificate authority, attribute authorities, owners, cloud server as well as users. Dealing of protection issue to a certain extent than using system unique public key towards encrypting data, our system necessitates the entire attribute authorities to produce their individual public keys and employs them to encrypt data.

REFERENCES

[1] B. Waters, ‘‘Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,’’ in Proc. 4th Int’l Conf. Practice and Theory in Public Key Cryptography (PKC’11), 2011, pp. 53-70.

[2] V. Goyal, A. Jain,O. Pandey, andA. Sahai, ‘‘Bounded Ciphertext Policy Attribute Based Encryption,’’ in Proc. 35th Int’l Colloquium on Automata, Languages, and Programming (ICALP’08), 2008, pp. 579-591.

[3] A.B. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B.Waters, ‘‘Fully Secure Functional Encryption: Attribute-Based Encryption
and (Hierarchical) Inner Product Encryption,’’ in Proc. Advances in Cryptology-EUROCRYPT’10, 2010, pp. 62-91.

[4] 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.

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

[6] 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.