IJRRECS/June 2015/Volume-3/Issue-6/3932-3936 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

ASSURING OF SECURE DATA TOWARDS OWNERS WITHIN CLOUD STORAGE SYSTEM

K.Divyasri[1], A.Radha Rani[2]

[1]M.Tech Student, Dept of CSE, Malla Reddy Engineering College for Women, Hyderabad, T.S, India

[2]Associate Professor, Dept of CSE, Malla Reddy Engineering College for Women, Hyderabad, T.S, India

ABSTRACT:

Cipher text-Policy ABE (CP-ABE) is resourcefully designed in support of access control concerning encrypted data. It is considered as one of the major appropriate technologies in support of controlling of data access within cloud storage systems, since it provides the data owner additional direct control above access policies. The revocable multi-authority CPABE is a capable technique, which can be functional in any distant storage systems as well as online social networks. We put forward a revocable scheme of multiauthority CP-ABE structure that can support capable attribute revocation. Our scheme does not necessitate server to be completely trusted, since key update is imposed by every attribute authority not server. Although the server is not semi-trusted in several scenarios, our schemes can still assurance backward security and moreover projected structure is well-organized and incurs less computation outlay, and is safe and accomplishes backward security as well as forward security. In our novel attribute revocation method, only ciphertexts that are connected with revoked attribute needs to be modernized.

Keywords: Multi-authority CPABE, Revocation, Semi-trusted, Attribute authority, Encryption.

1. INTRODUCTION:

To attain revocation above attribute level, a number of attribute revocation schemes concerning re-encryption-based were projected by means of relying on a reliable server. Established attribute revocation techniques are no more appropriate for cloud storage systems since cloud server was not completely trustworthy by owners of data [1]. Generally multi-authority CP-ABE is suitable for access control concerning systems of cloud storage, since users might hold attributes that are issued by numerous authorities and data owners might share the data by means of access policy over attributes. However multi-authority methods concerning CP-ABE cannot be directly functional towards data access control meant for Multi-authority storage systems because of attribute revocation. In our work, we put forward a revocable scheme of multiauthority CP-ABE structure that can support capable attribute revocation. The projected structure is well-organized and incurs less computation outlay, and is safe and accomplishes backward security as well as forward security. Our scheme does not necessitate server to be completely trusted, since key update is imposed by every attribute authority not server [2]. Although the server is not semi-trusted in several scenarios, our schemes can still assurance backward security.

2. METHODOLOGY:

Since data owners do not trust cloud servers completely, they do not depend on servers for performing access control. Cipher text-Policy ABE is efficiently designed in support of access control concerning encrypted data. Ciphertext-Policy Attribute-based Encryption is considered as one of the major appropriate technologies in support of controlling of data access within cloud storage systems, since it provides the data owner additional direct control above access policies. In CP-ABE method, there is an authority that is accountable in support of key distribution as well attribute management attribute management. In cloud storage of multi-authority systems, attributes of user are altered dynamically. A user might be entitled several new attributes and his authorization of data access has to be changed. The revocable multi-authority CPABE is a capable technique, which can be functional in any distant storage systems as well as online social networks. In our novel attribute revocation method, only ciphertexts that are connected with revoked

attribute needs to be modernized. In our novel attribute revocation system, key and ciphertext are updated by means of similar update key, rather than requiring owner to generate and update information in support of every ciphertext, such that owners are not necessary to accumulate each random number that is generated during encryption process. Our scheme does not necessitate server to be completely trusted, since key update is imposed by every attribute authority not server. In the storage systems of Multi-authority cloud, the assumptions were made such as: The certificate authority is completely trusted within system and it will not collude with any user; however it has to be prohibited from decrypting any cipher texts by itself. Each attribute authority is trustworthy but can be corrupted by adversary [3][4]. The server is curious however honest and it is curious in relation to the content of encrypted data or else received message, but will carry out accurately the task that was assigned by each attribute authority. Every user is fraudulent and might collude to get hold of unlawful access to data. Multi-authority methods relating to CP-ABE cannot be directly efficient in the direction of data access control meant for Multi-authority storage systems because of attribute revocation.

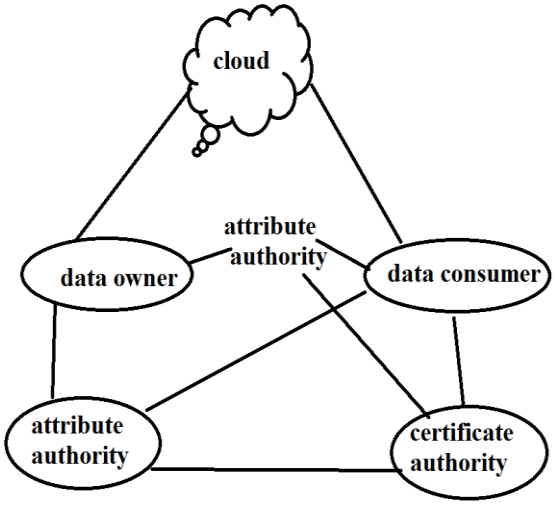

Fig1: Data access control system in multi-authority cloud storage.

3. AN OVERVIEW TOWARDS VARIOUS MODELS IN CLOUD SYSTEM:

We consider data access control system in cloud storage of multi-authority systems were considered shown in fig1 where there are five types of entities within the system such as a certificate authority (CA), data owners, the cloud server, attribute authorities, and data consumers. Every attribute authority is an autonomous attribute authority that is accountable for revoking of attributes of user in accordance with their role or else identity. In our system, each attribute is connected with a single attribute authority, but each attribute

authority can handle a random number of attributes. The projected structure is well-organized and incurs less computation outlay, and is safe and accomplishes backward security as well as forward security. Every attribute authority contains complete control over construction as well as semantics of its attributes. Each attribute authority is accountable for making a public attribute key in support of each attribute it supervises and a secret key in support of every user reflecting attributes. The certificate authority is an overall trusted certificate authority within the system which set up system as well as admitting registration of entire users and attribute authority in the system. For every legal user within the system, the certificate authority allocates an overall exceptional user identity to it and moreover generates a comprehensive public key for user on the other hand; the certificate authority is not concerned in any attribute management as well as creation of secret keys that are connected with attributes [5]. User might be allowed a set of attributes which might approach from numerous attribute authorities. The user will obtain a secret key which is connected with its attributes permitted by equivalent attribute authorities. Every owner initially makes the division of data into quite a few components in relation to logic granularities and encrypts every data component by means of separate content keys by means of techniques of symmetric encryption. The access policies were defined by the owner on attributes from numerous attribute authorities moreover encrypts content keys in the policies. Encrypted data was conveyed by the owner towards the cloud server simultaneously with ciphertexts but they do not depend on the server to perform data access control. Access control takes place inside cryptography specifically only when user's attributes convince access policy which is defined within ciphertext, user is capable to decrypt it as a result users with dissimilar attributes can decrypt distinct content keys and consequently get hold of separate granularities of data from similar information [6].

4. CONCLUSION:

Generally multi-authority CP-ABE is suitable for access control concerning systems of cloud storage, since users might hold attributes that are issued by numerous authorities and data owners might share the data by means of access policy over attributes. In cloud storage of multi-

authority systems, attributes of user are altered dynamically. In our work, we put forward a revocable scheme of multiauthority CP-ABE structure that can support capable attribute revocation. Although the server is not semi-trusted in several scenarios, our schemes can still assurance backward security. The revocable multi-authority CPABE is a capable technique, which can be functional in any distant storage systems as well as online social networks. In our novel attribute revocation method, only ciphertexts that are connected with revoked attribute needs to be modernized. In our novel attribute revocation system, key and ciphertext are updated by means of similar update key, rather than requiring owner to generate and update information in support of every ciphertext, such that owners are not necessary to accumulate each random number that is generated during encryption process. The projected structure is well-organized and incurs less computation outlay, and is safe and accomplishes backward security as well as forward security. It does not necessitate server to be completely trusted, since key update is imposed by every attribute authority not server. In our system, each attribute is connected with a single attribute authority, but each attribute authority can handle a random number of attributes.

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.