IJRRECS/June 2015/Volume-3/Issue-6/4186-4190 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

IMPLEMENTATION OF EFFECTIVE APPROACH FOR ACCESSING OF DATA IN CLOUD SYSTEM

SK.Munni[1], G.V.Koti Reddy[2]

[1]M.Tech Student, Dept of CSE, Holy Mary Institute of Technology & Science, Hyderabad, T.S, India

[2]Assistant Professor, Dept of CSE, Holy Mary Institute of Technology & Science, Hyderabad, T.S, India

ABSTRACT:

Cloud storage is main provision of cloud computing that provides quite a lot of services for data owners to host their information in cloud system. For multi-authority cloud storage systems to intend the data access control proposal, most important challenging issue is to build fundamental revocable multi-authority cipher text-policy attribute-based encryption protocol. For multi-authority cloud storage, we design a well-organized as well as revocable data access control proposal where there are numerous authorities co-exist and every authority is proficient to provide attributes autonomously. Our attribute revocation means is capable in the sense that it sustains a lesser amount of communication cost as well as computation cost, and is safe in the intellect that it can attain both backward security as well as forward security. It does not necessitate server to be totally trustworthy, since key update is imposed by every attribute authority. Our proposal assures backward security, although the server is not semi-trusted in number of situations. In our novel attribute revocation method, only cipher-texts that are related with revoked attribute requirements to be reorganized.

Keywords: Cloud computing, Attribute-based encryption, Multi-authority, Cloud storage, Attribute authority.

1. INTRODUCTION:

As a result of untrustworthy cloud servers, accessing control of data turn out to be a challenging problem in the systems of cloud storage. Since cloud server cannot be completely reliable by owners of data, they can no longer depend on servers to execute access control [1]. We design a well-

organized as well as revocable data access control proposal for multi-authority cloud storage, where there are numerous authorities co-exist and every authority is proficient to provide attributes autonomously. We suggest a revocable multi-authority cipher text-Policy attribute-based encryption method and apply it as the fundamental techniques to aim data access control system which can capably reach both forward security as well as backward security. Cipher text-Policy Attribute-based Encryption one of most appropriate expertise intended for data access control within cloud storage systems, since it grants data owner additional direct control on access policies. There are two categories of cipher text-policy attribute-based encryption systems such as single-authority CP-ABE where the entire attributes are supervised by means of a single authority, and in the situation of multi-authority CP-ABE in which attribute are from unrelated domains and are supervised by separate authorities. In multi-authority system of cloud storage user attribute is changed with dynamism. Multi-authority CP-ABE is further suitable for data access control concerning cloud storage systems, since users might hold attributes that are issued by numerous authorities and data owners might share data by means of access policy that is defined above attributes from several authorities [2][3]. On the other hand it is tricky to apply multi-authority CP-ABE systems towards multi-authority cloud storage systems as a result of attribute revocation difficulty.

2. METHODOLOGY:

In Cipher text-Policy Attribute-based Encryption, there is an authority that is dependable for attribute management as well as key distribution. Our proposal does not necessitate server to be totally trustworthy, since key update is imposed by every attribute authority. Although the server is not semi-trusted in a number of situations, our proposal can still assurance backward security. To intend the data access control proposal for multi-authority cloud storage systems, most important challenging issue is to build fundamental revocable multi-authority cipher text-policy attribute-based encryption protocol. We apply our projected revocable multi-authority cipher text-policy attribute-based encryption scheme as fundamental techniques to build protected data access control system for multi-authority cloud systems. We change

structure of the method and build it more realistic towards cloud storage systems, in which holders of data are not concerned in the key generation. We recover the effectiveness of the attribute revocation system. In our novel attribute revocation method, only cipher-texts that are related with revoked attribute requirements to be reorganized. In our novel attribute revocation means, both key as well as cipher-text can be modernized by means of using identical update key, rather than requiring owner to produce update information for every cipher-text, so that owners are not necessary to accumulate each random number that is generated throughout the encryption. The expressiveness of access control system was improved where we get rid of restriction that each attribute can come out at most once within a cipher-text.

3. CONSIDERING OF DATA ACCESS CONTROL STRUCTURE IN CLOUD STORAGE:

In our work we put forward a revocable method of multi-authority cipher text-Policy attribute-based encryption method, to solve attribute revocation difficulty in the system. Our attribute revocation means is capable in the sense that it sustains a lesser amount of communication cost as well as computation cost, and is safe in the intellect that it can attain both backward security as well as forward security. To attain revocation on attribute level, a number of re-encryption based attribute revocation methods are projected by means of depending on a trustworthy server [4]. As cloud server cannot be completely trustworthy by data owners, consequently conventional attribute revocation schemes are no longer appropriate for cloud systems. We believe a data access control scheme in multi-authority cloud storage, as shown in fig1 consisting of entities such as certificate authority, attribute authorities, data owners, cloud server as well as data consumers. Each user has an inclusive identity during the system and he might be allowed a set of attributes which may possibly come from numerous attribute authorities. He will obtain a secret key connected with attributes permitted by equivalent attribute authorities. Our proposal does not necessitate server to be totally trustworthy, since key update is imposed by every attribute authority. Every attribute authority is a self-determining attribute authority that is accountable for allowing and revoking user's attributes

consistent with their role in its domain. In our system, each attribute is connected with a single attribute authority, but each of it can supervise a random number of attributes. Every attribute authority has complete control above structure and semantics of its attributes. The certificate authority is an inclusive trustworthy certificate authority within the system that sets up system and recognizes registration of the entire users and attributes authorities within the system. For every legal user within the system, the certificate authority allocates an inclusive exceptional user identity to it and moreover produces a public key for this user. Certificate authority is not concerned in any attribute managing and making of secret keys that are connected with attributes. Each attribute authority is accountable for producing a public attribute key in support of each attribute it supervises and a secret key for every user reflecting attributes [5]. Each owner initially divides the data into quite a few components in proportion to logic granularities and encrypts each data module with distinct content keys by means of symmetric encryption methods. The access control takes place within the cryptography. Users with dissimilar attributes can decrypt several numbers of content keys and consequently gets hold of different granularities of data from the similar data [6].

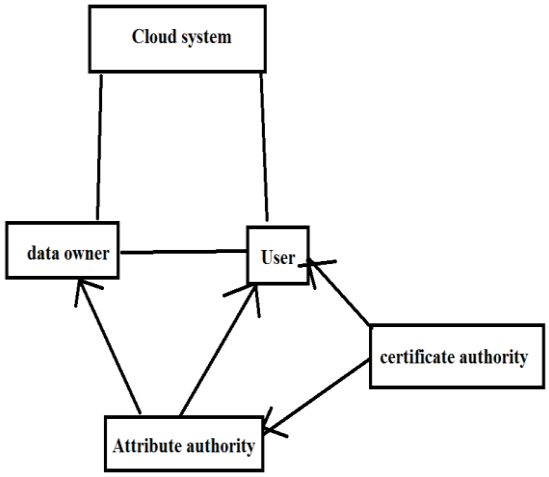

Fig1: view of system model.

4. CONCLUSION:

Within cloud systems cipher text-policy attribute-based encryption which is the most appropriate expertise intended for data access control, since it grants data owner additional direct control on access policies. For cloud systems while cloud server cannot be completely trustworthy by data owners, consequently conventional attribute revocation schemes are no longer appropriate. For multi-authority cloud storage we plan an efficient as well as revocable data access control proposal, where there are numerous authorities co-exist and every authority is proficient to provide attributes autonomously. As key

update is imposed by every attribute authority our proposal does not necessitate server to be totally trustworthy. Attribute revocation means is competent in the sense that it sustains a lesser amount of communication cost as well as computation cost, and is safe in the intellect that it can attain both backward security as well as forward security. While server is not semi-trusted in a number of situations, our proposal can still assurance backward security. Key as well as cipher-text can be modernized in our novel attribute revocation means, by means of using identical update key, rather than requiring owner to produce update information for every cipher-text. Within a cipher-text the expressiveness of access control system was improved where we get rid of restriction that each attribute can come out at most once.

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.