IJRRECS/June 2015/Volume-3/Issue-6/4176-4180 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

STRATEGY FOR RELIABLE DATA DISTRIBUTION ON VARIABLE CLOUD SERVERS

C.Harsha Vardhini[1], G.Bhanu Prasad[2]

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

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

ABSTRACT:

For managing of data privacy, the most basic solution is encryption of data files, and subsequently uploading of encrypted data into cloud. A resourceful data access control method was set up in cloud computing that is based on method of key policy attribute-based encryption. In our work to work out the challenges of existing solutions, Mona which is an efficient approach of multi-owner data sharing schemed for dynamic groups in the cloud was put forward. When compared with single-owner method where only group manager alters data in the cloud, multiple-owner method is additionally flexible in realistic applications. Mona scheme supports energetic groups efficiently and in particular, novel granted users can decrypt data files that are uploaded prior to their participation devoid of contacting with data owners. Multi-owner data sharing method means that any user within the group shares data efficiently with others by means of untrusted cloud. The most important goals of projected system include access control, confidentiality of data, efficiency, anonymity as well as traceability. To attain efficient data sharing intended for active groups in cloud, group signature as well as dynamic broadcast encryption methods are combined. Group signature permits users to anonymously utilize the assets of cloud, and dynamic broadcast encryption permits owners of data to share their data files securely with other users.

Keywords: Data privacy, Multi-owner, Data owners, Mona, Data sharing, Group signature.

1. INTRODUCTION:

The cloud service providers convey a variety of services towards cloud users by means of influential data centers and mainly offer data storage as the fundamental service [1]. Cloud providers managing the cloud servers are not dependable by users whereas the data files that are stored in the cloud may perhaps be confidential. Quite a lot of security schemes were intended for sharing of data on untrusted servers and in them, the owners of data stores the data files that are encrypted in untrusted storage and allocates the equivalent decryption keys to approved users. By means of placing a group by a single attribute, a protected provenance method which is based on ciphertext-policy attribute-based encryption was projected that permits any member in a group for sharing of data with others. An efficient data access control method was set up in cloud computing that is based on method of key policy attribute-based encryption. Unfortunately, single owner manner obstructs the implementation of their scheme, where any user is approved to share information. In our work to work out the challenges of existing solutions, Mona which is an efficient approach of multi-owner data sharing schemed for dynamic groups in the cloud was put forward [2][3]. The most important goals of projected system include access control, confidentiality of data, efficiency, anonymity as well as traceability. Mona scheme supports energetic groups efficiently and in particular, novel granted users can decrypt data files that are uploaded prior to their participation devoid of contacting with data owners.

2. CHALLENGES FOR DESIGNING DATA SHARING APPROACH IN CLOUD SYSTEM:

By means of migrating systems of local data management into cloud servers, users can benefit from expert services and accumulate important investments on their confined infrastructures. Designing a secure system of data sharing for groups that are located in cloud is not a simple mission due to issues such as: one of the major important obstacles for the extensive consumption of cloud computing is identity privacy. Devoid of assuring identity privacy, users may possibly be reluctant to connect in cloud computing systems since their actual identities might be simply revealed to attackers. Any member within a group was

mostly recommended to benefit from services of data storing as well as sharing that is provided by the cloud, in a multiple-owner approach. When compared with single-owner method where only group manager alters data in the cloud, multiple-owner method is additionally flexible in realistic applications. Unauthorized users in addition to storage servers cannot find out data files content because they contain no knowledge concerning decryption keys. In our work to work out the challenges of existing solutions, Mona which is an efficient approach of multi-owner data sharing schemed for dynamic groups in the cloud was put forward. To attain efficient data sharing intended for active groups in cloud, group signature as well as dynamic broadcast encryption methods are combined. Multi-owner data sharing method means that any user within the group shares data efficiently with others by means of untrusted cloud. Privacy-preserving access control was provided to users, which assures any member in a group to utilize cloud resources anonymously. Actual identities concerning data owners were revealed by group manager during the occurrence of disputes [4]. Achieving of user revocation is through a unique revocation list devoid of updating secret keys of left behind users. The computation transparency of encryption is stable and autonomous with number of revoked users.

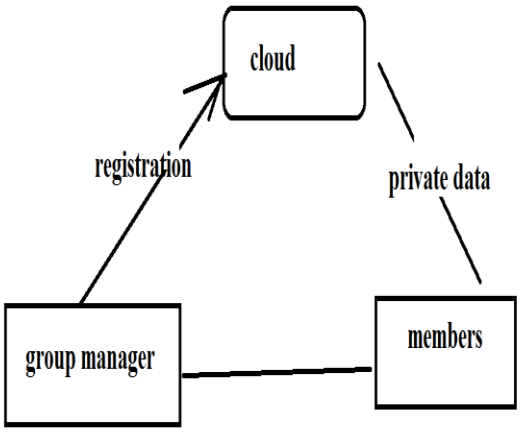

Fig1: An overview of system model.

3. CONSIDERATION OF COMPUTING DESIGN:

Cloud computing design was considered by merging with an example that a company utilizes a cloud to make possible its staffs within the same group for sharing of their files. For managing of data privacy, the most basic solution is encryption of data files, and subsequently uploading of encrypted data into cloud. The system representation consists of different entities as cloud, group manager and a huge number of group members' shown in fig1. Cloud is controlled by providers of cloud and offers priced

abundant services. Cloud providers managing the cloud servers are not dependable by users whereas the data files that are stored in the cloud may perhaps be confidential. Group manager considers generation of system parameters, registration and revocation of user, and exposes actual identity of data owner. Group member's stores and share their confidential data which is in cloud server with others within the group. The most important goals of projected system include access control, confidentiality of data, efficiency, anonymity as well as traceability. Confidentiality of data necessitates that unauthorized users with cloud are incompetent of learning stored data content. An essential issue for data confidentiality is to continue its accessibility for dynamic groups. Anonymity assurances that group member's access cloud devoid of revealing actual identity. Even though anonymity symbolizes an effectual protection for user identity, it moreover causes a possible inside attack hazard to system [5]. Any group member storing and sharing of data files with others in group by cloud describes efficiency. User revocation is attained devoid of involving remaining users. The prerequisites of access control are twofold such as group members uses cloud resource for operations of data initially and secondly, unlawful users cannot access cloud resource at any instance, and revoked users are lacking ability utilize cloud once more after they are revoked. To attain efficient data sharing intended for active groups in cloud, group signature as well as dynamic broadcast encryption methods are combined. Group signature permits users to anonymously utilize the assets of cloud, and dynamic broadcast encryption permits owners of data to share their data files securely with other users. Group manager computes revocation parameters and make result to public accessible by means of migrating them into cloud and such a design can drastically decrease the computation transparency of users to encrypt files as well as size of ciphertext. Computation overhead of user intended for encryption procedures and the cipher text size are steady and autonomous of revocation users [6].

4. CONCLUSION:

By means of migrating systems of local data management into cloud servers, users can benefit from expert services and accumulate important investments on their confined infrastructures. Designing a secure system of

data sharing for groups that are located in cloud is not a simple mission. When compared with single-owner method where only group manager alters data in the cloud, multiple-owner method is additionally flexible in realistic applications. Multi-owner data sharing method means that any user within the group shares data efficiently with others by means of untrusted cloud. An efficient data access control method was set up in cloud computing that is based on method of key policy attribute-based encryption. In our work to work out the challenges of existing solutions, Mona which is an efficient approach of multi-owner data sharing schemed for dynamic groups in the cloud was put forward. Mona scheme supports energetic groups efficiently and in particular, novel granted users can decrypt data files that are uploaded prior to their participation devoid of contacting with data owners. Privacy-preserving access control was provided to users, which assures any member in a group to utilize cloud resources anonymously. Cloud is controlled by providers of cloud and offers priced abundant services. Cloud providers managing the cloud servers are not dependable by users whereas the data files that are stored in the cloud may perhaps be confidential. The most important goals of projected system include access control, confidentiality of data, efficiency, anonymity as well as traceability.

REFERENCES

[1] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[3] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[4] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.

[5] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[6] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.