IJARES/June 2015/Volume-3/Issue-6/1941-1945 **ISSN 2347- 9337**

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN ENGINEERING AND SCIENCE

AN EFFECTIVE SCHEMING OF A DESIGN FOR SHARING OF DATA IN CLOUD SYSTEM

Pachimadla Banuchandar[1], L.Praveen Kumar[2]

[1]M.Tech Student, Dept of CSE, TRR College of Engineering, Hyderabad, T.S, India

[2]Associate Professor, Dept of CSE, TRR College of Engineering, Hyderabad, T.S, India

ABSTRACT:

A variety of techniques with reference to security for sharing of data on untrustworthy servers were introduced in literature. Broadcast encryption technique allows conveying encrypted information towards a set of users in order that simply a privileged subset of users can decrypt data. A group signature process authorizes any member of group to notice messages while maintenance of identity secret from verifiers. Consideration of a secure as well as efficient data sharing system for groups within the cloud is not an effortless task because of several issues. In our work we suggest an effective and novel secure multi-owner data sharing system which implies that any user within the group can securely distribute data with others by untrustworthy cloud. When evaluated with scheme of single-owner in which only the group manager can accumulate and change data in cloud, multiple-owner mode is additionally flexible in convenient applications. To carry out a successful data sharing for active groups in cloud, we look forward to merge the group signature as well as dynamic broadcast encryption methods. The new arrangement of Mona was introduced for active groups within cloud system and it is a multi-owner data sharing system.

Keywords: Broadcast encryption, Group signature, Multi-owner, Mona, Data sharing, Cloud, and Single-owner.

1. INTRODUCTION:

Cloud system is implemented by means of cloud service providers and they offer plentiful storage services. But the system of cloud cannot be completely trusted some times by users as the cloud service providers are expected to be outside of the trusted domain of cloud users [1]. One of the most basic services that are offered by providers of cloud system is data storage. For preservation of data privacy, the most important solution is encryption of data files, and subsequently uploading the encrypted information into the cloud system. Various techniques concerning security for sharing of data on untrustworthy servers were introduced in literature. In these techniques, owners of the data make storage of encrypted data files in untrustworthy storage and allocate equivalent decryption keys to authorized users. As a result, unauthorized users in addition to storage servers cannot gain knowledge of content of data files since they have no information of decryption keys. By means of low maintenance, cloud computing structure provides a reasonably priced and resourceful solution for sharing of group resources among the users of cloud [2][3]. However sharing of data within a multi-owner approach while preservation of data as well as identity privacy from an untrustworthy cloud is still a demanding issue, is to be handled due to the frequent change of membership. Broadcast encryption facilitates a broadcaster to convey encrypted information towards a set of users in order that simply a privileged subset of users can decrypt data. Dynamic broadcast encryption moreover permits group manager to dynamically take account of novel members while preservation of earlier computed information. The notion of group signatures was initially introduced by Chaum as well as van Heyst. A group signature method permits any member of group to notice messages while maintenance of identity secret from verifiers. An efficient membership revocation system devoid of updating secret keys of remaining users is moreover desirable to reduce difficulty of key management. In our work we put forward an effective and novel secure multi-owner data sharing system which implies that any user within the group can securely distribute data with others by untrusted cloud. The novel system of Mona was introduced for active groups within cloud system and it is a multi-owner data sharing system. By means of leveraging techniques

of group signature as well as dynamic broadcast encryption, any user within the cloud system can anonymously allocate data with others.

2. CHALLENGES FOR DESIGNING EFFECTIVE DATA SHARING SYSTEM:

Scheming of a secure and efficient data sharing system for groups within the cloud is not an effortless task because of several issues. The cloud servers that are supervised by the providers of cloud are not completely trusted by users because data files that are stored in the cloud might be sensitive and private. One of the basic difficulties concerning extensive utilization of cloud computing is Identity privacy. Without assurance of identity privacy, users might be reluctant to connect in the systems of cloud computing since their actual identities may possibly be made known to attackers [4]. It is extremely suggested that any member within a group have to be competent to completely benefit from data storing as well as sharing services that are provided by cloud, which describes the approach of multiple-owner. When compared with system of single-owner in which only the group manager can accumulate and change data in cloud, multiple-owner mode is additionally flexible in convenient applications. Groups are usually active in practice. The changes of membership build protected data sharing tremendously tricky. A well-organized membership revocation method devoid of updating secret keys of the remaining users is moreover desirable to reduce difficulty of key management. To resolve the challenges above, we put forward an effective and novel secure multi-owner data sharing system for active groups within cloud system. Mona system will effectively support active groups resourcefully. Particularly, novel users who are granted permission can directly decrypt data files that are uploaded earlier than their participation devoid of contacting with data owners. User revocation can be simply attained all the way through a new revocation list devoid of updating secret keys of remaining users.

The sizes as well as computation overhead of encryption are stable and self-sufficient with number of revoked users.

3. AN OVERVIEW OF PROPOSED MONA SYSTEM:

The cloud system servers that are monitored by the providers of cloud are not completely

trusted by users because data files that are stored in the cloud might be sensitive and confidential. We introduce a novel secure multi-owner data sharing system for active groups within cloud system known as Mona system which will in fact support active groups resourcefully. We imagine a cloud computing structural design which consists of three different entities such as the cloud, a group manager as well as a huge number of group members as shown in fig1. Group members are registered users who store their private information into the cloud server and distribute them to others within the group. Group manager considers generation of system parameters registration of user, user revocation, as well as revealing actual identity of a dispute data owner. The cloud servers that are administered by the providers of cloud are not completely trusted by users because data files that are stored in the cloud might be sensitive and private. To accomplish an effective data sharing for active groups in cloud, we look forward to merge the group signature as well as dynamic broadcast encryption methods [5]. Dynamic broadcast encryption method allows owners of the data to effectively share their data files with others and permits group manager to take account of novel members dynamically while preservation of earlier computed information. A group signature method permits any member of group to anonymously make usage of cloud resources. Each user has to work out revocation parameters to defend confidentiality from revoked users within dynamic scheme of broadcast encryption which results in computation transparency of encryption and size of cipher-text augment with number of revoked users. Heavy overhead as well as large cipher-text size might obstruct implementation of broadcast encryption system to capacity-limited users. To undertake this demanding issue, we permit group manager to work out revocation parameters and make result available by means of migrating them into cloud. Such a proposal can considerably cut the computation transparency of users towards encryption of files and cipher-text size. The computation transparency of users for encryption operations along with cipher-text size is stable and autonomous of the revocation users [6].

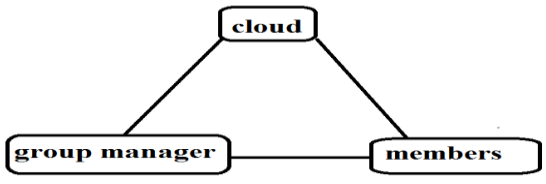

Fig1: An overview of system model.

4. CONCLUSION:

Cloud computing arrangement provides a reasonably priced and resourceful solution for sharing of group resources among the users of cloud. Distribution of data within a multi-owner method while preservation of data as well as identity privacy from an untrustworthy cloud is still a demanding issue is to be handled because of the frequent change of membership. The cloud servers that are controlled by the providers of cloud are not completely trusted by users because data files that are stored in the cloud might be sensitive and private. The technique of broadcast encryption moreover permits group manager to dynamically take account of novel members while preservation of earlier computed information. We suggest an effective and novel secure multi-owner data sharing system which implies that any user within the group can securely distribute data with others by untrustworthy cloud. By leveraging procedures of group signature as well as dynamic broadcast encryption, any user within the cloud system can anonymously allocate data with others. When compared with single-owner system in which only the group manager can accumulate and change data in cloud, multiple-owner mode is additionally flexible in convenient applications.

REFERENCES

[1] 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.

[2] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290 .pdf, 2008.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[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.