IJRRECS/November 2015/Volume-3/Issue-11/4960-4964 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

PUBLIC KEY BASED TRUSTED ANALYSER FOR STORING SENSITIVE DATA OVER CLOUD

Nalla Chaitanya[1], Ch.Subba Reddy[2], T.Shesagiri[3]

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

[2]Assistant Professor, Dept of CSE, Joginpally BR Engineering College, Hyderabad, T.S, India

[3]Associate Professor, Dept of CSE, Joginpally BR Engineering College, Hyderabad, T.S, India

ABSTRACT:

In our work, protocol of Mona was used for sharing of data security in cloud computing environment was studied. Heading towards managing of data security for vibrant groups within the cloud, group signature as well as dynamic broadcast encryption was combined. A great deal of strategies concerning security was put forward for sharing of data on untrustworthy servers. For preserving confidentiality of data, the fundamental solution is to encrypt data files, and subsequently upload encrypted data into the cloud. The introduced protocol for sharing of data security in is an effective multi-owner scheme of data sharing which implies that any user within the group distributes data by untrustworthy cloud strongly. In the scalable system, any user within the group shares data files by the cloud; achieving of user revocation without updating of user private keys; new user decrypt the cloud files earlier than his participation; size of cipher texts are self-reliant with revoked users. It supports effective groups resourcefully and novel approved users can decrypt data files uploaded earlier than their participation devoid of contacting with owners of data.

Keywords: Cloud computing, Data security, Cipher texts, Encryption.

1. INTRODUCTION:

While the data files that are stored in cloud might be confidential, servers of cloud handled by cloud contributor are not absolutely reliable by users. In practical applications, when measured by single-owner means in which only group manager stores and alter data within cloud, multiple-owner approach is more flexible. For maintaining privacy of data, the fundamental solution is to encrypt data files, and subsequently upload encrypted data into the cloud. For the extensive usage of cloud system, privacy of identity is one of most important obstruction. Providers of cloud service within cloud system distribute a variety of services to cloud users by means of prevailing data centres. Storing of data was considered as the major essential services provided by cloud providers [1]. By means of setting a group by means of a single attribute, Lu etal projected an effective provenance system based on the basis of cipher text-policy attribute-based encryption that permits any member within a group to distribute data with others on the other hand; the issue of user revocation is not tackled in their scheme. Quite a lot of strategies concerning security were put forward for sharing of data on untrustworthy servers. In these methods, owners of the data store the encrypted data files within untrustworthy storage and allocate equivalent decryption keys towards authorized users [2][3]. Mechanism of effective membership revocation devoid of updating of secret keys of remaining users is also needed to reduce the complication of key management.

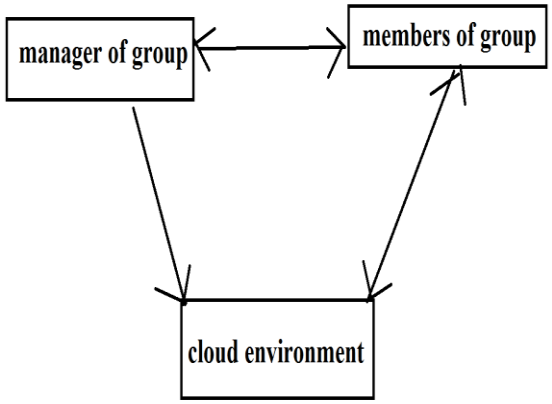

Fig1: overall System.

2. METHODOLOGY:

The perception of group signature scheme was introduced by Chaum and van Heyst that allows any group member sign messages while maintenance of the identity secret from verifiers. Approach of group signature permits users to utilize cloud resources anonymously. Selected group manager can make known identity of the signature's originator during the occurrence of dispute, denotes traceability. The strategy

of vibrant broadcast encryption facilitates a broadcaster to broadcast encrypted data towards a set of users with the intention that only advantaged subset of users can decrypt data. It allows owners of data to allocate their data files strongly with others and moreover permits group manager to include novel members while maintaining earlier computed information. In the direction of attaining of data security for vibrant groups within the cloud, group signature as well as dynamic broadcast encryption was combined. In Mona unfortunately, every user has to work out revocation parameters to look after privacy from revoked users in broadcast encryption, where computation precision of encryption and size of cipher text improves with revoked users. In this scheme, any user within the group shares data files by the cloud and achieve user revocation without updating of user private keys. Protocol for sharing of data security in is an effective multi-owner scheme of data sharing which implies that any user within the group distributes data by untrustworthy cloud strongly. The heavy transparency as well as huge cipher text size might obstruct implementation of broadcast encryption to capacity restricted users [4]. The computation transparency of users meant for encryption operations as well as size of cipher text are continuous and autonomous of the revocation users. To deal with this challenging issue, we allow the group manager to workout revocation parameters and formulate result available publicly by migrating them into cloud and such a system considerably decreases computation transparency of users to encrypt files.

3. AN OUTLINE OF PROPOSED SCHEME:

On the other hand; single owner method might obstruct the functioning of applications with situation, where any member within a group has to share data files with others. Unfortunately, single owner manner obstructs implementation of their system into the case, where any user is approved to accumulate and distribute data. Vibrant groups although maintaining of identity privacy from an untrustworthy cloud tuned out to be a challenging topic. In our work, proposal of Mona protocol for sharing of data security in cloud computing environment as shown in fig1 was studied. In the protocol of Mona, any user within the group shares data files by the cloud; achieving of user revocation without updating of user private keys; new user

decrypt the cloud files earlier than his participation; size of cipher texts are self-reliant with revoked users. Effectual membership revocation devoid of updating of secret keys of remaining users is also needed to reduce the complication of key management. Towards attaining of data security for vibrant groups within the cloud, group signature as well as dynamic broadcast encryption was combined. Yu et al. has provided a scalable as well as fine-grained data access control system in cloud system on the basis of key policy attribute-based encryption. Approach of group signature permits users to utilize cloud resources anonymously. The strategy of vibrant broadcast encryption allows owners of data to allocate their data files strongly with others. System of broadcast encryption allows owners of data to allocate their data files strongly with others and moreover permits group manager to include novel members while maintaining earlier computed information [5]. Any member within a group has to share data services that are provided by the cloud, described as multiple-owner manner. The proposal of Mona strategy is an effective multi-owner scheme of data sharing which implies that any user within the group distributes data by untrustworthy cloud strongly. Mona strategy supports effective groups resourcefully and novel approved users can decrypt data files uploaded earlier than their participation devoid of contacting with owners of data. The size as well as computation transparency concerning encryption are autonomous by revoked users. The actual identities of data owners are exposed by group manager during the occurrence of disputes. Secure as well as privacy-preserving access control was provided to users, which assurances that any member within a group makes use of cloud resource [6].

4. CONCLUSION:

Proposal of group signature permits users to utilize cloud resources anonymously and strategy of vibrant broadcast encryption facilitates a broadcaster to broadcast encrypted data towards a set of users with the intention that only advantaged subset of users can decrypt data. In our work, design of Mona protocol for sharing of data security in cloud computing environment was studied. Meant for wide-ranging usage of cloud system, privacy of identity is one of most important obstruction. Strategy of single owner method might obstruct the

functioning of applications with situation, where any member within a group has to share data files with others. In the introduced protocol, any user within the group shares data files by the cloud; achieving of user revocation without updating of user private keys; new user decrypt the cloud files earlier than his participation; size of cipher texts are self-reliant with revoked users. Whichever member within a group has to share data services that are provided by the cloud, described as multiple-owner manner. The strategy of introduced system is an effective multi-owner scheme of data sharing which implies that any user within the group distributes data by untrustworthy cloud strongly. In the strategy of Mona unfortunately, every user has to work out revocation parameters to look after privacy from revoked users in broadcast encryption, where computation precision of encryption and size of cipher text improves with revoked users. To get data security for vibrant groups within the cloud, group signature as well as dynamic broadcast encryption was combined.

REFERENCES

[1] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," http://www.cloudsecurityalliance.org, 2009.

[2] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107, Dec. 2008.

[3] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Service Computing, vol. 5, no. 2, 220-232, Apr.-June 2012.

[5] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. ACM Conf. Computer and Comm. Security (CCS '09), pp. 213-222, 2009.

[6] R.C. Merkle, "Protocols for Public Key Cryptosystems," Proc. IEEE Symp. Security and Privacy, 1980.