IJRRECS/March 2014/Volume-2/Issue-3/2086-2091 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

PROTECTED DATA DISTRIBUTION FOR CONVINCING GROUPS IN CLOUD ENVIRONMENT

D.Sujatha[1], J.Venkatesh[2]

[1]M.Tech Student, Dept of CSE, Bandari Srinivas Institute of Technology, Chevella, R.R Dist., A.P, India

[2]Assistant Professor, Dept of CSE, Bandari Srinivas Institute of Technology, Chevella, R.R Dist., A.P, India

ABSTRACT:

By means of concentrating memory, bandwidth and processing cloud computing permits for additional resourceful computing and to preserve the data the internet was used by the technology. Cloud is kind of centralized database where numerous clients accumulate their data, recover data and possibly adjust data and it is a representation where user is made available services by Cloud Service Provider on the basis of pay per use. To accomplish secure data sharing for vibrant groups in the cloud, we suppose to merge the group signature and encryption methods of dynamic broadcast. Without the assurance of identity privacy, users may possibly be reluctant to connect in the systems of cloud computing because their genuine identities could be effortlessly disclosed to the providers of cloud and attackers. Mona, a secure scheme of multi-owner data sharing is intended for dynamic group in the cloud and it is effortlessly observed that the cost of computation is inappropriate to the number of revoked users. The computation outlay of the cloud is deemed satisfactory, still when the revoked user's number is huge.

Keywords: Multi-owner data sharing, Mona, Cloud, Dynamic broadcast.

1. INTRODUCTION:

Broad range of the internal and external pressures for data reliability exists even though the cloud infrastructures are considerably more dominant and consistent than personal computing strategies. Even if the utilization of cloud computing has rapidly improved; the safety of cloud computing is still considered the most important issue in the environment of cloud

computing. Designing a competent and secure scheme of data sharing intended for groups in the cloud is not an uncomplicated mission because of the subsequent tricky issues such as: identity privacy is one of the generally noteworthy obstacles for the wide consumption of cloud computing [4]. Unrestricted identity privacy may possibly sustain the abuse of confidentiality. The scheme of group signature facilitates users to anonymously make use of the resources of cloud, and the technique of dynamic broadcast encryption allows owners of data to steadily contribute their data files with others together with novel joining users. Cryptographic storage system that facilitates sheltered file sharing on untrusted servers, known as Plutus was proposed. By means of dividing files into file groups in addition to encrypting each file group by means of a key of unique file-block, the owner of the data owner can contribute to the file groups by means of others all the way through delivering the equivalent lockbox key, where the key of lockbox is applied to encrypt the keys of file-block [8]. It brings about an intense key distribution transparency intended for large-scale file sharing. Moreover, the key of file-block requests to be updated and dispersed yet again for a user revocation. Files that are stored on the untrusted server comprises of two parts such as file metadata in addition to file data. The file metadata entails the access control data together with a series of blocks of encrypted key, each of which is encrypted under the authorized user public key [1]. The size of the file metadata is comparative to the authorized user's number. The user revocation in the system is an intractable concern in particular for large-scale sharing, in view of the fact that the file metadata desires to be updated.

2. METHODOLOGY:

The scheme of group signature facilitates users to anonymously make use of the resources of cloud, and the technique of dynamic broadcast encryption allows owners of data to steadily contribute their data files with others together with novel joining users [11]. Mona, a secure scheme of multi-owner data sharing is intended for dynamic group in the cloud. It is effortlessly observed that the cost of computation in Mona is inappropriate to the number of revoked users. The technique of Mona offers exceptional features such as: Any user in the group can possibly store up and allocate data files with others by means of the cloud [3]. The intricacy of encryption and dimension

of cipher texts are autonomous with the numeral of revoked users in the system. The revocation of user can possibly be attained devoid of updating the keys of private of the enduring users. A novel user can unswervingly decrypt the stored files in the cloud earlier than his contribution. model of system comprises three dissimilar entities such as the cloud, a manager of the group and huge number of group members which is shown in fig1 [6] [14]. Cloud is controlled by means of cloud service providers and makes available services of priced abundant storage. The cloud is not completely trusted with users in view of the fact that the cloud service providers are very probable to be outside of the trusted domain of the cloud users. Group manager acquires charge of parameters of system generation, user revocation, and edifying the genuine identity of a dispute data possessor [9] [13]. The members of the Group are a set of registered users that will accumulate their private information into the server of the cloud and contribute them with others in the group. To estimate the performance of the cloud in Mona, its computation expenditure was tested to act in response to the operations of various client requests together with file generation, file deletion and file access [7]. The main design goals of the proposed system together with access control, data confidentiality, efficiency and anonymity and traceability are described as follows: Access control: The necessity of access control is twofold. Initially, group members are talented to make use of the cloud resource for the operations of data. Subsequently, users of unauthorized cannot access the resource of cloud at any moment, and revoked users will be incompetent of using the cloud yet again once they are revoked [2] [15]. Data confidentiality: Data confidentiality necessitates that the users of unauthorized together with the cloud are incompetent of learning the content of the accumulated information. A significant and challenging concern intended for data privacy is to preserve its accessibility for active groups. Specifically, novel users have to decrypt the data accumulated in the cloud earlier than their contribution, and revoked users are not capable to decrypt the information moved into the cloud subsequent to the revocation. Anonymity and traceability: Anonymity assurances that members of group can right to use the cloud devoid of revealing the authentic identity [12]. Even though anonymity corresponds to an effectual fortification for user identity, it

also creates a possible inside attack threat to the system. An inside attacker may possibly accumulate and contribute to an untruthful information to derive considerable benefit. Thus, to undertake the inside attack, the manager of group should have the aptitude to make known the authentic identities of owners of the data. Efficiency: Any member of the group can accumulate and contribute to data files with others within the group by means of the cloud [5]. User revocation can be accomplished devoid of connecting the remaining users. The outstanding users do not require updating their confidential keys or operations of reencryption. Novel granted users can gain knowledge of content of data files accumulated earlier than his participation devoid of contacting with the owner of the data [10].

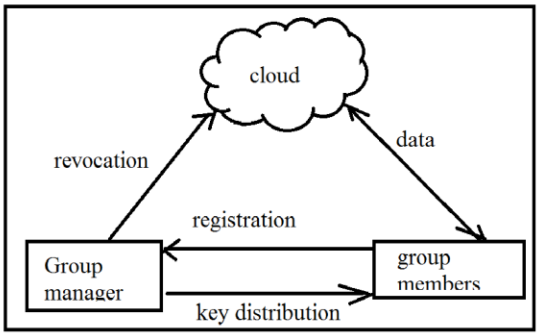

Fig1: An overview of system model

3. RESULTS:

Mona, a secure scheme of multi-owner data sharing is intended for dynamic group in the cloud and it is effortlessly observed that the cost of computation is inappropriate to the number of revoked users. The computation outlay of the cloud is deemed satisfactory, still when the revoked user's number is huge. For the reason that the cloud only entails signatures of group and revocation verifications to makes sure the legitimacy of the requestor intended for all operations. It is worth noting that the cost of computation is autonomous with the dimension of the requested file intended for access and the operations of deletion, in view of the fact that the size of signed message is steady. To estimate the performance of the cloud in Mona, its computation expenditure was tested to act in response to the operations of various client requests together with file generation, file deletion and file access.

4. CONCLUSION:

Mona, a secure scheme of multi-owner data sharing is intended for dynamic group in the cloud and offers exceptional features such as: any user in the group can possibly store up and allocate data files with others by means of the cloud. The intricacy of encryption and dimension of cipher texts are autonomous with the numeral of revoked users in the system. The revocation of user

can possibly be attained devoid of updating the keys of private of the enduring users. A novel user can unswervingly decrypt the stored files in the cloud earlier than his contribution. To accomplish secure data sharing for vibrant groups in the cloud, we suppose to merge the group signature and encryption methods of dynamic broadcast. It is worth noting that the cost of computation is autonomous with the dimension of the requested file intended for access and the operations of deletion, in view of the fact that the size of signed message is steady. To estimate the performance of the cloud in Mona, its computation expenditure was tested to act in response to the operations of various client requests together with file generation, file deletion and file access.

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] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[3] 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.

[4] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[5] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[6] 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.

[7] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[8] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[9] 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.

[10] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[11] D. Pointcheval and J. Stern, "Security Arguments for DigitalSignatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.

[12] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

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

[14] 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.

[15] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp. 514-532, 2001.