IJRRECS/June 2014/Volume-2/Issue-6/2385-2390 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

SHELTERED DATA ALLOTMENT FOR VIBRANT GROUPS IN CLOUD ENVIRONMENT

S.Swathi[1], Narsimha Banothu[2]

[1]M.Tech Student, Dept of CSE, Holy Mary Institute of Technology & Science, Bogaram(V), Keesara(M), R.R.Dist., India

[2]Associate Professor, Dept of CSE, Holy Mary Institute of Technology & Science, Bogaram(V), Keesara(M), R.R.Dist., India

ABSTRACT:

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. A cloud provider put forward numerous services that can possibly profit its customers, such as quick access to their data, scalability, pay-for-use, data storage, data recovery and defend against various hackers, on-demand protection controls. Cloud service providers should make sure the protection of their customers' data. Efficient methods which permit on-demand data accuracy confirmation on behalf of cloud users have to be considered in order to attain the assurances of cloud data integrity and accessibility and apply the excellence of cloud storage service. To accomplish secure data sharing for vibrant groups in the cloud, we suppose to merge the group signature and encryption methods of dynamic broadcast. A secure scheme of multi-owner data sharing known as Mona which is intended for dynamic group in the cloud was proposed in which a novel user can unswervingly decrypt the stored files in the cloud earlier than his contribution.

Keywords: Cloud computing, Cloud service provider, Multi-owner data sharing, Mona.

1. INTRODUCTION:

Cloud computing is the long dreamed visualization of computing as a benefit, where cloud customers can tenuously store their data into the cloud so as to get pleasure from the high quality networks, servers. A

cloud provider put forward numerous services that can possibly profit its customers, such as quick access to their data, scalability, pay-for-use, data storage, data recovery and defend against various hackers, on-demand protection controls [4]. Along with the extensive eagerness on cloud computing, on the other hand, anxiety on data security with cloud storage are arising due to unpredictability of the service and malicious attacks from hackers. Identity privacy is one of the generally noteworthy obstacles for the wide consumption of cloud computing. Unrestricted identity privacy may possibly sustain the abuse of confidentiality [8]. 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 [1]. 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. Efficient methods which permit on-demand data accuracy confirmation on behalf of cloud users have to be considered in order to attain the assurances of cloud data integrity and accessibility and apply the excellence of cloud storage service [11].

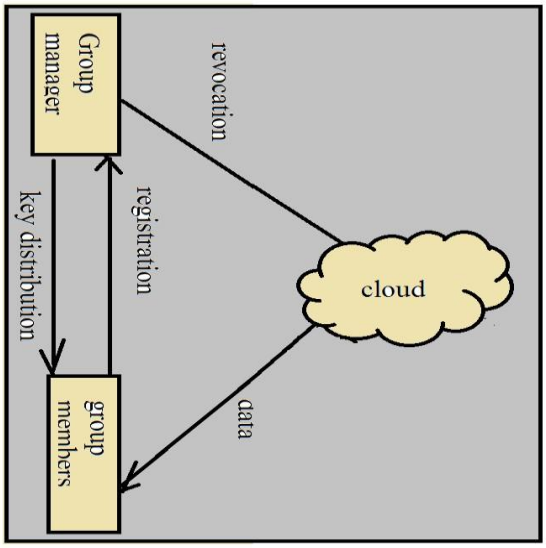

Fig1: An overview of system model.

2. METHODOLOGY:

The 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. 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 [3]. A cloud provider put forward numerous services that can possibly profit its

customers, such as quick access to their data, scalability, pay-for-use, data storage, data recovery and defend against various hackers, on-demand protection controls [14]. The cloud server will not delete maliciously or adjust user information due to the protection of schemes of data auditing but will attempt to become skilled at the content of the stored information and the identities of cloud users [9]. Group manager acquires charge of parameters of system generation, user revocation, and edifying the genuine identity of a dispute data possessor. The manager of the group is acted by means of the administrator of the company as a result, the group manager was assumed to be completely trusted by the other parties [7] [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. The membership of group is energetically changed, because of the staff acceptance and the participation of new employee in the company. A secure scheme of multi-owner data sharing known as Mona which is intended for dynamic group in the cloud was proposed [2]. In the scheme of Mona any user in the group can possibly store up and allocate data files with others by means of the cloud. 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. The intricacy of encryption and dimension of cipher texts are autonomous with the numeral of revoked users in the system [15]. The computation transparency of users intended for the operations of encryption and the size of the cipher text are steady and autonomous of the revocation users. It is supposed to merge the group signature and encryption methods of dynamic broadcast towards accomplishing secure data sharing for vibrant groups in the cloud. To defend the privacy from the revoked users in the encryption scheme dynamic broadcast, each user has to calculate parameters of revocation which outcomes in that mutually the working out overhead of the encryption and the extent of the cipher text augment with the revoked users' number [5] [12]. The group manager works out the parameters of revocation and formulates the result openly accessible by means of transferring those into the cloud and such a design can considerably decrease the computation transparency of users in the direction of encrypting files and the cipher

text extent. User revocation is carried out by the group manager by means of a list of public available revocation that is based on which group members can possibly encrypt their data files and make sure the privacy against the revoked users [6] [10]. To accumulate a data file in the cloud, a member of group performs the operations such as getting the list of revocation from the cloud. The member sends the identity of group as an appeal to the cloud. Verifying the legality of the list of received revocation. Checking of initially whether the marked date is new. File which is stored in the cloud can be removed by means of the group manager.

3. RESULTS:

Comparison on computation outlay of clients intended for operations o data generation among Mona and the system that openly using the scheme of original dynamic broadcast encryption were performed. It is without problems observed that the cost of computation in Mona 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.

4. CONCLUSION:

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. Cloud service providers should make sure the protection of their customers' data. Well-organized methods which permit on-demand data accuracy confirmation on behalf of cloud users have to be considered in order to attain the assurances of cloud data integrity and accessibility and apply the excellence of cloud storage service. A secure scheme of multi-owner data sharing known as Mona which is intended for dynamic group in the cloud was proposed in which a novel user can unswervingly decrypt the stored files in the cloud earlier than his contribution. 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. Comparison on computation outlay of clients intended for operations o data

generation among Mona and the system that openly using the scheme of original dynamic broadcast encryption were performed. It is without problems observed that the cost of computation in Mona is inappropriate to the number of revoked users.

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.