IJRRECS/May 2014/Volume-2/Issue-5/2317-2322 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

PROVISION OF SECURE DATA AMONG USERS IN CLOUD SYSTEM

Porika Sagar[1], Dr.B.Vijayakumar[2]

[1]M.Tech Student, Dept of CSE, St.Martin's Engineering College, Kompally, Hyderabad, A.P, India

[2]Professor & HOD, Dept of CSE, St.Martin's Engineering College, Kompally, Hyderabad, A.P, India

ABSTRACT:

As cloud service providers are very probable to be exterior of trustworthy domain of cloud users, cloud is not completely trusted with users. Preserving accessibility for active groups is significant and challenging concern intended for data privacy. Since tricky issues such as distinctiveness and privacy is one of the generally noteworthy obstacles for wide consumption of cloud computing, a competent and secure scheme construction of data sharing within the cloud projected for groups is not an uncomplicated mission. Any member of the group can accumulate and contribute to data files with others within the group by efficiency of cloud. For dynamic group in the cloud protected data system, multi-owner data sharing is intended and outlay of computation is inappropriate to the number of revoked users. To accomplish secure data sharing, merging of group signature and encryption methods of dynamic broadcast for vibrant groups in the cloud was performed. The most important design goals of protected data system are access managing, effectiveness, data discretion, ambiguity and traceability. Protected scheme of multi-owner data sharing is intended 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 for dynamic group in cloud. Group signature facilitates users to anonymously make use of the resources of cloud. Members of group can have right to use the cloud devoid of revealing the authentic identity and anonymity assurances.

Keywords: Cloud system, Anonymity, Data sharing, Multi-owner, Encryption, Vibrant groups.

1. INTRODUCTION:

By means of encryption of attribute-based user is capable to encrypt a data file and other decrypt the data which is encrypted by using their attribute keys. A protected attribution scheme, based on group signatures and techniques of ciphertext-policy attribute-based encryption, was set up [4]. Key of group signature and an attribute key are the keys which are comprised by user. To accumulate and allocate data files with others manner of single owner may possibly obstruct functioning of applications with the circumstances, where any member within a group has to be allowed. Besides updating of user secret key cloud servers attain user revocation, manager entrusts tasks of data file reencryption. With the intention that a user can simply decrypt a cipher-text providing the attributes of the data file convincing access structure, manager of the group assigns an access construction and the equivalent secret key [8]. Random key is additionally encrypted with an attribute set; the owner of the data makes use of a random key to encrypt a file. To gain knowledge of the decryption keys of the entire encrypted blocks attack of collusion between the untrusted server and any revoked malicious user is commenced. Server makes use of proxy cryptography for the access control to unswervingly re-encrypt the proper key of content from the master public key towards an approved user's public key [1]. Owner of data encrypts blocks of content which are additionally encrypted under a master public key by exceptional and symmetric content keys. As file metadata desires to be updated the user revocation in the system is an intractable concern. Under the authorized user public key with a series of blocks of encrypted key the file metadata entails the access control data together [11]. Size of the file metadata is comparative to the authorized users in particular for large-scale sharing. File metadata in addition to file data are the two files which are stored on untrusted server. Key of file-block requests to be updated and dispersed for a user revocation for large-scale file sharing; it brings about an intense key distribution transparency [16]. Data owner can contribute to the file groups by means of others all the way through delivering the equivalent lockbox key, by a key of unique file-block, where key of lockbox is applied to encrypt the keys of file-block [3]. Cryptographic storage that facilitates sheltered file sharing on untrusted servers

was set up. Scheme of group signature facilitates users to anonymously make use of resources of cloud and technique of dynamic broadcast encryption allows owners of data to steadily contribute their data files with others together with novel joining users [14]. Within the cloud a competent and secure scheme construction of data sharing which is projected for groups is not an uncomplicated mission since subsequent tricky issues such as distinctiveness privacy is one of the generally noteworthy obstacles for the wide consumption of cloud computing.

2. METHODOLOGY:

With the numeral of revoked users in the system intricacy of encryption and dimension of cipher texts are autonomous. Protected scheme of multi-owner data sharing is intended 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 for dynamic group in cloud [13]. A novel user can unswervingly decrypt the stored files. Cloud, a manager of the group and huge number of group members represents the model of system as shown in fig1. To act in response to the operations of various client requests together with file creation file erasure and file admission, performance of the cloud in protected data system and its computation expenditure was tested [9]. In the group, members of the group will accumulate their private information and distribute them among others. By the manager of the group charge of parameters of system creation, user revocation, and enlightening the genuine identity of a dispute data possessor are acquired. Cloud is controlled and makes available services of priced abundant storage by means of cloud service provider [7]. Cloud is not completely trusted with users as cloud service providers are very probable to be exterior of the trustworthy domain of the cloud users. Revocation of user can possibly be attained devoid of updating the keys of private of the enduring users. Intricacy of encryption and dimension of cipher texts are autonomous with numeral of revoked users in the system [2]. Protected data system offers exceptional features as any user in the group can possibly store up and allocate data files with others by means of cloud. For dynamic group in the cloud protected data system, multi-owner data sharing is intended and outlay of computation is inappropriate to the number of revoked users [15]. Dynamic

broadcast encryption allows owners of data to steadily contribute their data files with others together with novel joining users who can gain knowledge of the content of data files accumulated earlier than his participation devoid of contacting with the owner of the data [12]. Group signature facilitates users to anonymously make use of the resources of cloud. By outstanding users, updating of their confidential keys or operations of reencryption is not requiring. Any member of the group can accumulate and contribute to data files with others within the group by efficiency of cloud. To make known the authentic identities of owners of the data to undertake the inside attack, manager of group should have the ability. An inside attacker may possibly accumulate and contribute to an untruthful information to derive considerable benefit [5]. Even though anonymity corresponds to an effectual fortification, for user identity a possible inside attack threat was created to the system. Members of group can have right to use the cloud devoid of revealing the authentic identity and anonymity assurances. Subsequent to the revocation, novel users have to decrypt the information that is accumulated in cloud earlier than their contribution, and revoked users are not capable to decrypt the information moved into the cloud [10]. Significant and challenging concern intended for data privacy is preserving its accessibility for active groups. To learn the content of the accumulated information, data discretion necessitates that the users of unauthorized together with the cloud are lacking ability. Users of unauthorized cannot access the resource of cloud and revoked users will be incompetent of using the cloud [6]. For the operations of data, at first the members of the group are talented to make use of the cloud resource. The most important design goals of protected data system are access managing, effectiveness, data discretion, ambiguity and traceability.

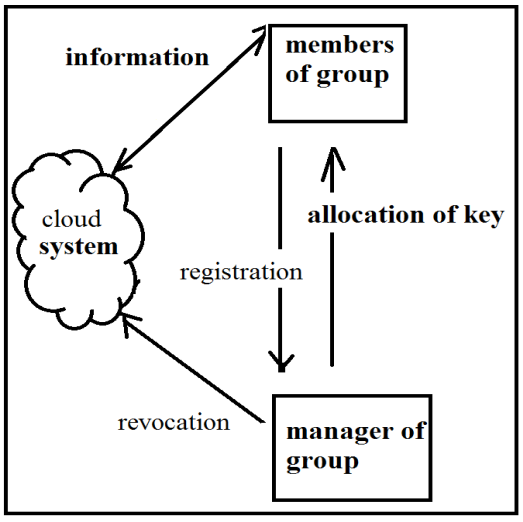

Fig1: An overview of system model.

3. RESULTS:

In response to the operations of various client requests together with file generation, computation expenditure of protected data system was tested to perform for file deletion and file access. With dimension of the requested file intended for access with operations of deletion it is worth noting that expenditure of computation is autonomous, while the size of signed message is steady. Authenticity of the requestor was made sure by revocation verifications and signatures of group. Cloud is deemed satisfactory while revoked user's number is huge the computation outlay. Sheltered scheme of multi-owner data sharing is intended for dynamic group in the cloud protected data system and cost of computation is inappropriate to the number of revoked users.

4. CONCLUSION:

To act in response to the operations of various client requests together with file generation, file deletion and file access, performance of the cloud in protected data system and its computation expenditure was tested. With dimension of the requested file intended for access and the operations of deletion, cost of computation is autonomous given that size of signed message is balanced. Novel user can unswervingly decrypt the stored files in cloud earlier than his contribution. To accomplish secure data sharing, we suppose to merge the group signature and encryption methods of dynamic broadcast for vibrant groups in the cloud. Devoid of updating the keys of private of the enduring users, revocation of user can possibly be attained. Owner of data encrypts blocks of content which are additionally encrypted under a master public key by exceptional and symmetric content keys.

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.

[16] "Mona: Secure Multi-Owner Data Sharingfor Dynamic Groups in the Cloud", Xuefeng Liu, Yuqing Zhang, , Boyang Wang, and Jingbo Yan, 2013.