International Journal of Science Engineering and Advance Technology

Security Analysis And Perform Extensive Simulations To Demonstrate The Efficiency Of Mona For Data Sharing In The Cloud

1 M.Vamsi Krishna, 2 **Dr.K.V.V.S.Narayana Murthy, 3T.Satya swaroop**
Dept. of CSE, Chaitanya Institute of Science & Tech., Madhavapatnam, Kakinada. E.g.dt, AP, India

Abstract:
Sharing data in a multi-owner manner while conserving data and identity privacy from an untrusted cloud is still a challenging issue due to the regular change of the membership. In this paper we propose a secure multi-owner data sharing scheme named Mona for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption methods any cloud user can anonymously share data with others. In the meantime the storage overhead and encryption computation cost of our method are autonomous with the number of revoked users. In addition we analyze the security of our scheme with rigorous proofs and reveal the competence of our scheme in experiments. Sharing group resource among cloud users is a major problem so cloud computing provides a reasonable and efficient solution. Due to frequent change of membership sharing data in a multi-owner manner to an untrusted cloud is still a challenging issue.

Keywords: Cloud computing, data sharing, privacy-preserving, access control, dynamic groups.

Introduction:

In cloud computing the cloud service providers(CSPs) such as Amazon are capable to deliver various services to cloud users with the assistance of powerful data enters. By migrating the local data management systems into cloud server's users can enjoy high-quality services and hoard significant investments on their local infrastructures. Regrettably designing a competent and protected data sharing scheme for groups in the cloud is not an easy task owing to the following challenging issues. First identity privacy is one of the most significant impediment for the wide exploitation of cloud computing. Second it is extremely recommended that any member in a group should be able to completely enjoy the data storing and sharing services provided by the cloud which is defined as the multiple-owner manner. Groups are usually dynamic in practice e.g. new staff participation and current employee revocation in a company. The changes of membership make secure data sharing tremendously complicated. On one hand the unidentified system challenges new granted users to learn the content of data files stored before their participation as it is not possible for new granted users to contact with anonymous data owners and get the corresponding decryption keys.

Related Work:

By separating files into file groups and encrypting each file group with a unique file-block key the data owner can contribute to the file groups with others through delivering the corresponding lockbox key where the lockbox key is used to encrypt the file-block keys. Though it brings about a heavy key distribution overhead for large-scale file sharing. Furthermore the file-block key needs to be updated and dispersed again for a user revocation. Any user in the group can store and share data files with others by the cloud. The encryption difficulty and size of cipher text sare independent with the number of revoked users in the system. User revocation can be attained without updating the private keys of the remaining users. A new user can directly decrypt the files store up in the cloud before his participation. We can scrutinize that how to securely share data files in a multiple-owner manner for dynamic groups while preserving identity privacy from an untrusted cloud remains to be a challenging issue.

Existing Method:

Lu et al. proposed a secure attribution plan based on the cipher text-policy attribute-based encryption technique which authorizes any member in a group to share data with others. On the other hand the subject of user revocation is not addressed in their scheme. Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. Unfortunately the single owner method holds back the acceptance of their scheme into the case where any user is granted to store and share data. Data owners store the encrypted data files in untrusted storage and assign the equivalent decryption keys only to authorized users. Thus unauthorized users as well as storage servers cannot learn the content of the data files as they have no information of the decryption keys. Though the problems of user contribution and revocation in these methods are

linearly growing with the number of data owners and the number of revoked users respectively.

Disadvantages:

It is particularly recommended that any member in a group should be clever to entirely enjoy the data storing and sharing services provided by the cloud which is defined as the multiple-owner manner. Compared with the single-owner manner where only the group manager can store and adjust data in the cloud the multiple-owner manner is suppler in practical applications. Identity privacy is one of the most vital complexity for the wide use of cloud computing. Without the declaration of identity privacy users may be unwilling to connect in cloud computing systems since their genuine identities could be easily revealed to cloud providers and attackers. On the other hand incompetent identity privacy may carry upon you the neglect of privacy.

Proposed Method:

We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud.

Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners.

Attribute based encryption technique new granted users can directly decrypt data files and uploaded before their participation without contacting with data owners.

User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users.

The size and computation overhead of encryption are constant and independent with the number of revoked users.

It provides secure and privacy-preserving access control to users.

Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.

Advantages:

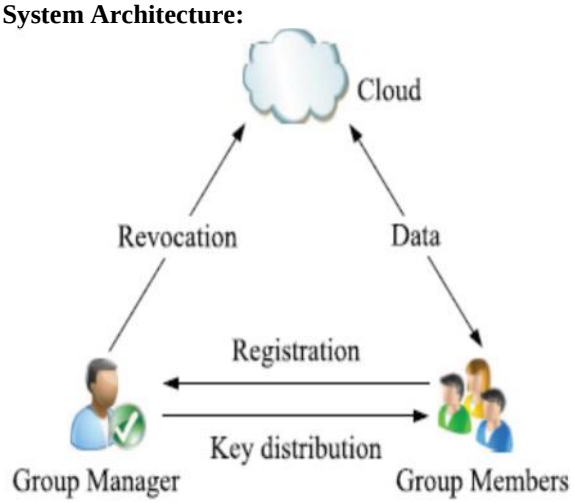
Any user in the group can store and share data files with others by the cloud.

The encryption complexity and size of cipher texts are independent with the number of revoked users in the system.

User revocation can be achieved without updating the private keys of the remaining users.

Efficient sharing of data among different users of different groups by using Mona algorithm.

System Architecture:



Group manager takes charge of system parameters generation, user registration, user revocation and revealing the real identity of a argument data owner. Group members are a set of registered users that will store up their private data into the cloud server and share them with others in the group. Yet the cloud is not completely trusted by users since the CSPs are very possible to be outside of the cloud users' trusted domain. We imagine that the cloud server is honest but curious. That is the cloud server will not unkindly remove or adjust user data due to the protection of data auditing schemes but will attempt to learn the content of the stored data and the identities of cloud users. Cloud is functioned by CSPs and provides priced plentiful storage services.

Implementation:

Cloud Module :

We build up this module where the cloud storage can be made secure. Still the cloud is not completely trusted by users because the CSPs are very likely to be outside of the cloud users' trusted domain. We generate a local Cloud and provide priced plentiful storage services. A like we assume that the cloud server is honest but curious. The cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes but will try to learn the content of the stored data and the identities of cloud users. The users can upload their data in the cloud.

Group Manager Module :

The Group manager is the admin. The group manager has the logs of each and every procedure in the cloud. The group manager is accountable for user registration and also user revocation too. Group manager takes arraign of System parameters generation, User registration, User revocation and revealing the real individuality of a dispute data owner. Therefore we assume that

the group manager is fully trusted by the other parties.

Group Member Module :

The group member has the ownership of varying the files in the group. Whoever in the group can scrutiny the files which are uploaded in their group and can also modify it. Group members are a set of registered users that will store up their private data into the cloud server and share them with others in the group. Note that the group association is vigorously changed due to the staff resignation and new employee participation in the company.

File Security Module :

File stored in the cloud can be removed by either the group manager or the data owner that is the member who uploaded the file into the server. This is encrypting the data file.

Group Signature Module:

In addition the designated group manager can disclose the identity of the signature's originator when a argument occurs which is indicated as traceability.A group signature method permits any member of the group to symbol messages while keeping the identity secret from verifiers.

User Revocation Module :

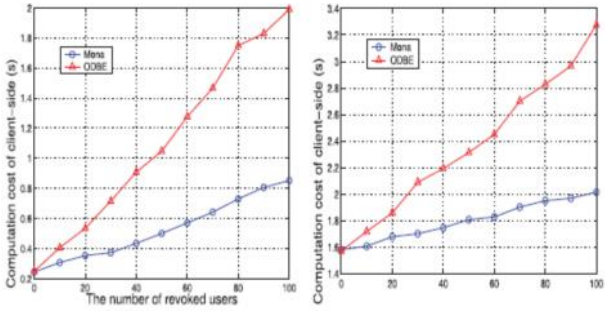
User revocation is carried out by the group manager by means of a public available revocation list (RL) based on which group members can encrypt their data files and make sure the privacy next to the revoked users.

Algorithm Used:

Mona Algorithm :

1. Group manager take charge of secure symmetric encryption algorithm with secret key k. and it will be kept secret as the master key of the group manager.
2. the group manager adds the group user list, which will be used in the traceability phase. After the registration, user i obtains a private key which will be used for group signature generation and file decryption.
3. User revocation is performed by the group manager via a public available revocation list ðRLÞ, based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.
4. Uploading the data into the cloud server and adding the data into the local shared data list maintained by the manager.
5. Group members in different groups sharing data is validated by
6. Group manager based on signature validation.
7. On receiving the data, the cloud first invokes signature generation technique to check its validity. If the algorithm returns true, the group signature is valid; otherwise, the cloud abandons the data.
8. Obtaining the tuple data from his local storage.Invoking signature generation to compute a group signature on data.
9. Sending data and the signature as a deletion request to the cloud.

EXPERIMENTAL RESULTS:



The computation cost in Mona augments with the number of revoked users as clients necessitate to perform algorithms to calculate the parameter Ar;r and make sure whether the data owner is a revoked user. Besides P1; P2; :::; Pr need to be computed by clients in ODBE. Consequently Mona is still superior to ODBE in terms of computation cost. Comparable to the data generation operation the total computation cost is mainly resolute by the symmetrical decryption operation if the accessed file is large which can be verified.

Conclusion:

We suggest a secure multi-owner data sharing scheme. It entail that any user in the group can firmly share data with others by the untrusted cloud. Our proposed scheme is able to hold up dynamic groups efficiently. Purposely new granted users can directly decrypt data files uploaded before their participation without get in touch with data owners. User revocation can be simply achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are stable and autonomous with the number of revoked users. We make available secure and privacy-preserving access control to users which guarantee any member in a group to anonymously make use of the cloud resource. Furthermore the genuine identities of data owners can be exposed by the group manager when disputes occur. We provide thorough security analysis and perform extensive simulations to reveal the efficiency of our scheme in terms of storage and computation overhead.

References:
[1] 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.
[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc.Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.
[3] 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.
[4] 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.
[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius:Securing Remote Untrusted Storage," Proc. Network and DistributedSystems Security Symp. (NDSS), pp. 131-145, 2003.
[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "ImprovedProxy Re-Encryption Schemes with Applications to SecureDistributed Storage," Proc. Network and Distributed Systems SecuritySymp. (NDSS), pp. 29-43, 2005.
[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: TheEssential of Bread and Butter of Data Forensics in CloudComputing," Proc. ACM Symp. Information, Computer and Comm.Security, pp. 282-292, 2010.
[8] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: AnExpressive, Efficient, and Provably Secure Realization," Proc. Int'lConf. Practice and Theory in Public Key Cryptography Conf. Public KeyCryptography,
http://eprint.iacr.org/2008/290.pdf, 2008.
[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-BasedEncryption for Fine-Grained Access Control of EncryptedData," Proc. ACM Conf. Computer and Comm. Security (CCS),pp. 89-98, 2006.
[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and TracingSchemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf.Advances in Cryptology (CRYPTO), pp. 41-62, 2001.
[11] D. Boneh and M. Franklin, "Identity-Based Encryption from theWeil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology(CRYPTO), pp. 213-229, 2001.
[12] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature,"Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO),pp. 41-55, 2004.
[13] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity BasedEncryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf.Theory and Applications of Cryptographic Techniques (EUROCRYPT),pp. 440-456, 2005.
[14] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully CollusionSecure Dynamic Broadcast Encryption with Constant-Size Ciphertextsor Decryption Keys," Proc. First Int'l Conf. Pairing-Based
Cryptography, pp. 39-59, 2007.
[15] D. Chaum and E. van Heyst,"Group Signatures," Proc. Int'l Conf.Theory and Applications of Cryptographic Techniques (EUROCRYPT),pp. 257-265, 1991.

Authors:

Sri. M. Vamsi krishna, well Known Author and excellent teacher Received M.Tech (AI &R), M.Tech (CS) from Andhra university is working as Professor and HOD, Department of CSE, Chaitanya Institute Science and Technology. He has 13 years of teaching & research experience. He has 20 publications of both national and international conferences /journals. His area of Interest includes AI, Computer Networks, information security, flavors of Unix Operating systems and other advances in computer Applications.

Dr.K.V.V.S.Narayana Murthy M.Tech, Ph.D. Professor of CSE department in Chaitanya Institute of Science & technology. He has 15 years of teaching & research experience to his credit number of publications both national and international conferences /journals. His area of interest includes compiler design, formal languages and automata theory, computer organization.

Mr.T.Satyaswaroop is a student of Chaitanya Institute of Science & Technology, Madhavapatnam, Kakinada Presently he is pursuing his M.Tech [computer science Engineering] from this college and he received B.Tech from Sri Sai Aditya Institute of Science & Technology affiliated to JNT University, Kakinada in the year 2012.His area of interest includes computer networks, cloud computing and object oriented languages, current trends in computer science.