International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 30th December 2017. Link :
http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-13

Title: Distributed Concurrent Independent Acccess to Encrypted Cloud Data.

Volume 06, Issue 13, Page No: 264 - 269.

Paper Authors

*** GUNTUPALLI PADMA, A LATHA.**

* Dept of CSE, St.Mary's Women's Engineering College.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

DISTRIBUTED CONCURRENT INDEPENDENT ACCCESS TO ENCRYPTED CLOUD DATA

***GUNTUPALLI PADMA, **A LATHA**

*PG Scholar, Dept of CSE, St.Mary'sWomen's Engineering College, Budampadu, Guntur

**Associate Professor, Dept of CSE, St.Mary'sWomen's Engineering College, Budampadu, Guntur

ABSTRACT —

Users can added various files in the form of text, image, audio, video etc. through the program by using encryption algorithm so that it can be stored on cloud. Thus we can secure data on a cloud. Due to this efficiency is increase and data will be secure on the cloud. Recently, some research considers the problem of secure and efficient public data integrity auditing for shared dynamic data. But this scheme is not secure against collusion of cloud storage server. An efficient public integrity auditing with a secured group user revocation based on vector commitment and group user revocation. A distributed key generation algorithm is used to generate authenticated user passwords across multiple servers and eliminate single point failures. This scheme supports the public checking and efficient user revocation and also provides confidentiality, efficiency and traceability of secure group user revocation. A homomorphic encryption algorithm is also used forcreating unique id for the users. In this system, we purpose a novel public verify technique for the integrity of shared data with efficient user revocation in a mind. By applicability idea of proxy re-signatures. It grant the cloud to re-sign blocks on favor of existing users during the revocation, so that existing users do not need to download and re-sign blocks by themselves. In a public verify , it always able to audit the integrity of shared data without the fetching of whole data from the cloud, even if some part of shared data has been re-sign by cloud. This mechanism is able to support batch auditing by verifying multiple auditing task simultaneously. Experimental results shows that our mechanism can significantly improve the efficiency of user revocation.

Keywords — Cloud Computing, User Revocation, Public Integrity Auditing, Encryption.

1. INTRODUCTION

cloud computing security or, more simply, cloud security is an involving sub domain of computer security, network security and more broadly information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, application and the associated infrastructure of cloud computing. Organizations use the cloud in a variety of different service models (SAAS, PAAS, and IAAS) and deployment models (Private, Public, Hybrid, and Community). Cloud Security problems are coming from Loss of control, Lack of trust (mechanisms), Multi- tendency. Cloud Security is security principles applied to protect data, applications and infrastructure associated within the Cloud Computing technology. Cloud security is important for increasing usage of Cloud Services in non-traditional sector, growing adoption of Cloud Services in government departments, rise in Cloud Service-specific Attacks, Growing usage of Cloud Services of Critical Data Storage. sharing and low support, offers an improved misuse of assets. In cloud processing, cloud administration suppliers offer an idea of unending storage room for customers to host data [1]. It can help customers to diminish their monetary straightforwardness of data administrations by exchanging the neighborhood administration's framework into cloud servers. Then again, security worry turns into the fundamental disadvantage as we now outsource the capacity of data, which is potentially

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

agreeable, to cloud suppliers. To take care of data privacy, a general move towards is to encrypt data documents before the customers transfer the encrypted data into the cloud [2]. Unfortunately, it is hard to outline a safe and effective data sharing plan, particularly for dynamic groups in the cloud. cloud service provider(CSPs), which will enhance the capacity impediment of asset oblige nearby gadgets. As of late, some business cloud storage services, for example, the basic stockpiling service(S3) [1] on-line information reinforcement services of Amazon and some down to earth cloud based software Google Drive [2], Dropbox [3], Mozy [4], Bitcasa [5] and Memopal [6], have been manufactured for cloud application. Since the cloud servers may give back an invalid result in some cases, for example, server hardware/software disappointment, human upkeep and pernicious assault [7],[8] new structures of affirmation of information honesty and availability are required to ensure the security and protection of cloud client's information. For giving the respectability and accessibility of remote cloud store, a few arrangements [9], [10], [11] and their variations [12], [13],[14], [15], have been proposed. In these arrangements, when a plan bolsters information alteration, we call it element plan, generally static one (or restricted element plan, if a plan could just effectively bolster some predetermined operation, for example, affix). A plan is freely obvious implies that the information uprightness check can be performed by information proprietors, as well as by any outsider evaluator. Then again, the dynamic plans above spotlight on the situations where there is an information proprietor what's more, just the information proprietor could change the information. To apply vector commitment plan [17] over the database, at that point we influence the Asymmetric Group Key Agreement (AGKA) [18] and bunch marks [19] to bolster ciphertext information base overhaul among bunch clients and effective gathering client denial separately. In particular, the gathering client utilizes the AGKA convention to encrypt/decrypt the offer database, which will promise that a client in the gathering will be capable to encrypt/decrypt a message from some other gathering clients. The gathering mark will keep the intrigue of cloud and denied bunch clients, where the information proprietor will join in the client disavowal stage and couldn't disavow the information that last altered by the revoked client.

2. PROPOSED SYSTEM

In proposed system Advanced Encryption Standard (AES) is the best algorithm for secure data storage in this function performs the searching and sorting of the similar data items in the cloud domain. A distributed key generation (DKG) is an encryption process in which multiple parties contribute to the calculation of a shared public and private key set. A Homomorphic Encryption technique is also used in order to increase the integrity of the shared data. The third party auditor can view all the data which is exchanged between cloud users as well as with the cloud server, which is not necessary. TPA will maintain the history of the data users in the cloud and also the actions performed by them.

Group users consist of a data owner and a number of users who are authorized to access and modify thedata by the data owner. The cloud storage server is semi-trusted, who provides data storage services for the group users. TPA could be any entity in the cloud,which will be able to conduct the data integrity of the shared data stored in the cloud server. In our system, the data owner could encrypt and upload its data to the remote cloud storage server. Also, he/she shares the privilege such as access and modify (compile and execute if necessary) to a number of group users.

The TPA could efficiently verify the integrity of the data stored in the cloud storage server, even the data is frequently updated by the group users. The data owner is different from the other group users, he/she could securely revoke a group user when a group user is

found malicious or the contract of the user is expired.

3. Related Work

User Revocation: If a user wishes to revoke from a group their request regarding revocation will be forwarded to the auditor where auditor will check to it and revoke the user from group. The user revocation is secure because only existing users are able to sign the blocks in shared data. even with a re-signing key, the cloud cannot generate a valid signature for an arbitrary block on behalf of an existing user. In addition, after being revoked from the group, a revoked user is no longer in the user list, and can no longer generate valid signatures on shared data.

Group Sharing: Data owner will store their data in the cloud and share the data among the group members. Who upload the data have rights to modify and download their data in the cloud. He can also set rights to other users in his group to edit or download data.

File Upload: File owner allowed uploading data on the cloud either for their private or public use. They act as a Group Manager for the file they upload in cloud. Both the original user and group users are able to access, download and modify shared data. Shared data is divided into a number of blocks. A user in the group can modify a block in shared data by performing an insert, delete or update operation on the block.

File Auditing: If an user edited an data then the auditor will monitor the user and report to the owner about the edited data. The group manager will monitor the changes in the file and if he founds any discrepancy auditor has full rights to revocate from his particular group. The public verifier can audit the integrity of shared data without retrieving the entire data from the cloud, even if some blocks in shared data have been re-signed by the cloud.

Key Distribution: The prerequisite of key transportation is that clients can safely get their private keys from the gathering director with no Certificate Authorities. In other existing plans, this purpose is skilful by expecting that the communication channel is secure, on the other hand, in our plan, we can accomplish it without this solid thought.

Access control: First, collect individuals can make use of the cloud asset for information stockpiling and information sharing. Second, unapproved clients can't get to the cloud asset whenever, and disavowed clients will be unfitted for utilizing the cloud asset again once they are renounced.

Algorithms :AES (Advanced Encryption Standards) : It is an iterative rather than Feistel cipher. This comprises of a series of linked operations, which involve replacing inputs by specific outputs or substitutions and others involve shuffling bits around so called permutations. AES performs all its computations on bytes rather than bits. Hence, AES takes a 128 bit secret key and it will be combined with a plaintext block which is arranged in four columns and four rows for processing as a matrix. This is called cipher text. But in DES, the number of rounds is variable and they depends on the length of the key. AES uses 10 rounds for 128-bit keys, and it takes 9 loops for 10 rounds. Likewise 12 rounds for 192-bit keys with 11 loops for 12 rounds. And finally 14 rounds for 256-bit keys, with 13 loops for 14 rounds. Every round uses a different 128- bit,192-bit and 256-bit round key respectively, which is calculated from the original AES key.

1.Byte Substitution: (Sub Bytes) 16 input

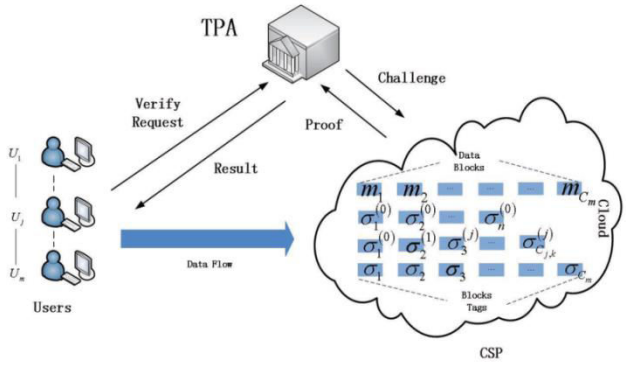
2.Shift rows: Each four rows of the matrix are shifted to the left. Shift is carried out as below-

First row is not shifted.

- Second row is shifted to one (byte) position to the left.
- And third row is shifted two positions to the left from right.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

- Fourth row is shifted three positions to the left.
- The resulting is a new matrix consisting of the 16 bytes,
- but shifted with respect to each other.



4. LITERATURE SURVEY

Proofs of Retrievability (PoR), presented by Juels and Kaliski, permit the customer to store a file F on an untrusted server, and later run a productive review convention in which the server demonstrates that (regardless it) has the customer's information [1]. Developments of PoR plans endeavor to minimize the customer and server stockpiling, the correspondence multifaceted nature of a review, and even the quantity of document pieces got to by the server amid the review. In this work, we distinguish a few unique variations of the issue, (for example, limited use versus unbounded-use, learning soundness versus data soundness), and giving almost ideal PoR plans for each of these variations. Our developments either enhance (or sum up) the earlier PoR developments, or give the first known PoR plans with the required properties. Specifically, we formally demonstrate the security of an (advanced) variation of the limited use plan of Juels and Kaliski, without making any improving presumptions on the conduct of the foe. Construct the initially unbounded-use PoR plan where the correspondence many-sided quality is straight in the security parameter and which does not depend on Random Oracles, determining an public query of Shacham and Waters. Assemble the initially limited use plan with data theoretic security. The primary understanding of our work originates from a basic association between PoR plans and the thought of hardness intensification, broadly considered in many-sided quality hypothesis. Specifically, our changes originate from first abstracting a simply data theoretic idea of PoR codes, and after that building almost ideal PoR codes utilizing cutting edge instruments from coding and complexity theory.

Kallahalla et al [2] offered a cryptographic storage system that allow secure data sharing on unreliable servers based on the methods that dividing files into file groups and encrypting each file group with a file-block key. Conversely, the fileblock keys need to be updated and distributed for a user revocation, so, the system had a heavy key distribution overhead. Additional schemes for data sharing on untrusted servers have been proposed in Still, the difficulty of user participation and revocation in these schemes is linearly rising with the number of data owners and the revoked users.

Liu et al [3] ,proposed a secure multi-owner data sharing scheme, named Mona. It is claimed that the scheme can achieve fine-grained access control and revoked users will not be able to access the sharing data again once they are revoked. Conversely, the scheme will easily suffer from the collusion attack by the revoked user and the cloud [13]. The revoked user can use his private key to decrypt the encrypted data file and get the secret data after his revocation by combining with the cloud. In the stage of file access, first of all, the revoked user throws his request to the cloud, then the cloud act in response the corresponding encrypted data file and revocation list to the revoked user without verifications. Next, the revoked user can calculate the decryption key with the help of the attack algorithm. Lastly, this attack can

guide to the revoked users receiving the sharing data and releasing other secrets of legal members.

Zou et al. [4] ,presented a sensible and flexible key management method for trusted joint computing. By leveraging access control polynomial, it is designed to achieve well-organized access control for dynamic groups. Regrettably, the secure way for sharing the private permanent portable secret between the user and the server is not sustain and the private key will be revealed once the personal everlasting portable secret is obtained by the invader/attackers.

5.CONCLUSION

In this paper, we have proposed a new public auditing mechanism for shared data with efficient user revocation in the cloud. When a user in the group is revoked, it allow the semitrusted cloud to re-sign blocks that were signed by the revoked user with proxy re-signatures. Thus, the cloud can improve the efficiency of user revocation and existing users in the group can save a sign cant amount of computation and communication resources during user revocation.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, "Achieving Secure, Scalable, and Finegrained Data Access Control in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010. [5] 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

[6] 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.

[7] B. Waters, "Ciphertext-Policy AttributeBased Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. http://eprint.iacr.org/2008/290.pdf, 2008

[8] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.

[9] 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.

[10] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ci-phertexts or Decryption

Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[11] Zhongma Zhu, Zemin Jiang, Rui Jiang, "The Attack on Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," Proceedings of 2013 International Conference on Information Science and Cloud Computing (ISCC 2013), Guangzhou, Dec.7, 2013, pp. 185-189.

[12] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, December 2013.

[13] Xukai Zou, Yuan-shun Dai, and Elisa Bertino, "A practical and flexible key management mechanism for trusted collaborative computing," INFOCOM 2008, pp. 1211-1219.

[14]. E. Shi, E. Stefanov, and C. Papamanthou, "Practical dynamic proofs of retrievability," in Proc. of ACM CCS 2013, Berlin, Germany, Nov. 2013, pp. 325–336.

Mrs Guntupalli. Padma, Scholar, M.Tech, Department of Computer Science & Engineering, St.Mary's Women's Engineering College, Budampadu, Guntur. .

Mrs A. Latha, Associate Professor, Department of Computer Science & Engineering, St.Mary's Women's Engineering College, Budampadu, Guntur.