AN SECURE THE DATA IN CLOUD BY USING PRIVATE AUDITING SCHEME

C.Sneha[1], C.Suriya[2], S.Anisharaj[3], Ms.S.Indhumathi[4],
Department of Information Technology,
Bharathiyar Institute of Engineering for Women,Deviyakurichi,Salem.

ABSTRACT:

To protect data using cloud storage as much as possible such that a user does not need to perform too many operations to data. In particular, users may not want to go through the complexity in verifying and reparation. Regenerating codes have gained popularity due to their lower bandwidth whileproviding fault tolerance and data integrity. In Existing system checking methods for regenerating-coded data only provide public auditing, requiring data owners to stay online and handle auditing, as well as repairing, which is not practical. We propose a private auditing scheme for the regenerating-code-based cloud storage. To find out the regeneration problem of failed authenticators in the absence of data owners, we preface a proxy, into the traditional private auditing system model. We design a public verifiable authentication, which is generated by a private keys and can be regenerated using secret keys. In this scheme can completely release the instaled difficulty in holders. To ensure the integrity of dynamic data stored in the cloud, external Third Party Auditor (TPA) is acquainted in a cloud infrastructure.

I. INTRODUCTION:

All the of status privateers is one of the most powerful restriction for the wide deployment of cloud computing. Here not land the guaranteed of identity privacy user may be an willing to append in cloud computing systems because their real identities scan be easily disclose to cloud providers and attackers. On the other hand its unreserved identity privacy might contract the abuse of privacy for example the misconduct staff could deceive others on the company to sharing false files without being traceable. Therefore, traceability and which are enables the TPA to expose the real identity of a user's are also highly desirable. Second, it is highly recommended that any member in the groups should able to fully enjoy the data storing as well as sharing services provided by the cloud which are defined as the multiple owner. Compare with the single owner manner where only the group manager could store and modify data in the cloud, the multiple owner manners are more flexible in practical applications. More concretely, each users in the groups are able to not only read data and also modify his or her part of data in the entire data file shared to the company. The changes of membership makes secure data sharing extremely problematic. On one hand, the anonymous systems can challenges modern granted users can learn the content of data files stored before their cooperation, because it is not possible for new granted users to contact with anonymous data holder and access the corresponding decryption keys. On the other hand the efficient membership repeal mechanism without updating the classified keys. Many security schemes for data sharing on untrusted servers had been proposed. In these approaches, data owners are able to store the encrypted data files in mistrustful storage with distributed the

corresponding decryption keys are only to authorized users. Thus, unauthorized users as well as storage servers couldn't learn the comfortable data files because they don't have knowledge of the decryption keys. However, the complexity of user participation and repeal in these schemes are linearly increasing with the numbers of data owners as well as the number of revoked users, respectively. By setting the group with a single attribute, we proposed a secure provenance scheme is established on the cipher text policy attribute established encryption technique, which are allows any member in a group to share data with others. However, the issue of user revocations are not addressed in their scheme.

II.PROBLEM STATEMENT

2.1 EXISTING SYSTEM

In previous system the data correction, failing tolerance is occur in data integrity together to data retrieve. Remote checking methods are needed to data owners in online. The overhead of using cloud storage should be minimized as much as possible such that a user does not must to perform too many operations to their outsourced data. In particular, users may not want to go through the elaboration in verifying and reparation. In the public auditing scheme the bandwidth is reduced and fault tolerance is occur. The regenerating code are first introduced by Dimakis for distributed storage to compressed the bandwidth. The perfect tradeoff curve the minimum bandwidth regenerating point which represent the operating point with the least available repair bandwidth.Ateniese*et al.,* stated the model for Provable Data Possession (PDP) to ensure the possess of a file at untrusted storages . The public key based homomorphic tags are utilized for auditing the user's data file. In spite of ,the pre-computation of the tags imposes heavy computation overhead that can be pricey for an absolute file. In their subsequent work in 2008, PDP scheme used symmetric key based cryptography. This method shows a lower-overhead than their previous advanced scheme and also allows for block updates, deletions and appends to the reserved file. This scheme focuses only on the single server scenario and does not provide the assurance of data availability against server defects and thus left both the distributed scenario and data error recovery issues unexplored. Jules et al., illustrates a "proof of retrievability" (PoR)form, where spot-checking and error-correcting codes arerecycled to guarantee both "possession" and "retrievability" of data files remote achieve service system. It propose a solution that provide security and regeneration and retains benefits offered by each techniques.

2.2 DISADVANTAGES OF EXISTING SYSTEM

→ To fully secure the data integrity and save the users' computation resources as well as online burden.

→ Both of them are designed for private audit, only the data holder is allowed to verify the integrity and repair the faulty servers.

→ Considering the large size of the expanded data and the user's constrained resource capability, the tasks of auditing and renewal in\the cloud can be terrible and expensive for the customers.

III. PROPOSED SYSTEM

Many mechanisms trade with the integrity of outsourced data without a local copy have been proposed under different system and security models up to now. The most powerful work among these studies are the PDP (provable data possession) method and POR (proof of retrievability) method, which were basically proposed for the single-server scenario]. Considering that files are usually striped and redundantly saved across multi-servers or multi-clouds, explore integrity verification schemes applicable for such multi-servers or multi-clouds

setting with different redundancy schemes, such as replication, erasure codes, and, more recently, regenerating codes. The main aim of the project is to support dynamic groups efficiently. We produce secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. Christo Ananth et al. [8] discussed about a Secure system to Anonymous Blacklisting. The secure system adds a layer of accountability to any publicly known anonymizing network is proposed. Servers can blacklist misbehaving users while maintaining their privacy and this system shows that how these properties can be attained in a way that is practical, efficient, and sensitive to the needs of both users and services. This work will increase the mainstream acceptance of anonymizing networks such as Tor, which has, thus far, been completely blocked by several services because of users who abuse their anonymity. In future the Nymble system can be extended to support Subnet-based blocking. If a user can obtain multiple addresses, then nymble-based and regular IP-address blocking not supported. In such a situation subnet-based blocking is used. Other resources include email addresses, client puzzles and e-cash, can be used, which could provide more privacy. The system can also enhanced by supporting for varying time periods. Revocation is user is performed if any user make unauthenticated action on any data in the cloud. Also if a data has been modified by the user it will be detected, penalized and the code will be regenerated by the proxy. In this the user revocation is performed by the group manager via a public available revocation list(RL),planed on which group members can encrypt their data files and ensure the confidentiality against the revoked users.Ateniese*et al.*, proposed a new scheme called homomorphic linear authenticators (HLA) where the communicative involvement is self-regulating of customer's file length. It also supports infinite number of verification,but it cannot verify in public. Later,Shacham*etal.*,projected the two POR protocols. The first protocol is designed with BLS signatures and it acquire only the curtest query and response with public verifiability. Both schemes hope the homomorphic property aggregating verification argument into a small value. Shahetal. States that TPA storage should be more believable by encouraging a TPA to get the encrypted data first and then distributing a number of pre-computed symmetric keyed hashes done then cryptic data to the external auditor. Then the auditor verifies both the integrity of the customer's file and the server's ownership with the earlier committed decryption key. This proposed work only deals with the encrypted files and it permits from the stateless auditor and enclosed usage, which may induces online burden to customers when the keyed has sear employed. It suggests a method where dynamic data operations are efficiently done at the block level by applying rank based verification in the cloud servers. Later, Wang et al. related a "BLS based homomorphic authenticator with mutual verifiability" and also means the data dynamics using "Merkle Hash Tree (MHT)" in-order to find out the data integrity in cloud computing.

IV.SYSTEM ARCHITECTURE

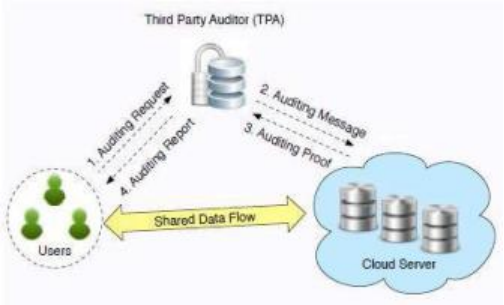

Fig: System Model Build in User, Cloud, Server and TPA

The cloud storage system using many models as given as follows:

Client: The client, who is an individual user and desires to save and retrieve data in their huge amount of data in the cloud.

Cloud Service Provider (CSP): The CSP, who regulate the cloud servers and provides storage as service on its infrastructure to the cloud users based on pay per service basis.

Third Party Auditor (TPA): The checker, who audits cloud data on benefit of the user and also check the storage truth of data reality utilize from the cloud.

V.MODULE

It repose of four modules,

- → Cloud Module.
- → Proxy Server Module.
- → Group Member Module.
- → User Revocation Module

5.1 CLOUD SERVER

A local Cloud which provides priced abundant storage services are been created in this module.The users can upload their developed where the cloud storage can be made secure. The cloud is not fully honorable by users since the CSPs are very likely to be outside of the cloud users trusted domain. Similar to that the cloud server is genuine but curious. That is, the cloud server will notmaliciously delete or repair user data due to the protection of data investigating schemes, but will try to learn the content of the stored data and the identities of cloud users. This essentially means that the owner (client) of the data moves its data to a third party cloud storage server which are supposed to presumably for a fee truly store the data with it and provide it back to the owner whenever required.

5.2 PROXY SERVER DEPLOYMENT

Group manager takes gripe of followings,

- → Signature Generation
- → Signature Verification
- → Content Regeneration

A proxy agent acts on behalf of the data owner to regenerate authenticators and data blocks on the servers during the repair procedure. Respect that the data owner is restricted in computational and storage resources compared to other entities and may becomes off-line after the data upload procedure. The proxy, who would always be online,is supposed to be much more powerful than the data holder but less than the cloud servers in terms of computation and memory capacity.

5.3 GROUP MEMBER GENERATION

Group members are a set of registered users that will

1. Cache their private data into the cloud server.

2. Share them with others in the group. The group memberships are dynamics changed, due to the staff resignation and new employee participation in the company. The group member had the ownership of changing the files in the group.

3. Notable in the group can view the files which are uploaded in their group and also modify it. Also each group will have private key and public key in it. The public key is used for viewing the document in the cloud whereas the private is the meant for providing modification rights for an user.

5.4 USER REVOCATION

User revocation is performed by the proxy via a public available RL based on which group member scan encrypt their data files and assure the confidentiality against the revoked users. Noun authorized access to the document is encouraged in the cloud storage. So the data should be provided rights to modify only by the group's own users. Other members cannot modify the content. Once if any user tries to hack the private key of another group and trying to modify this will be detected by the cloud server and the user's account will be revoked by the user. The user could never enter his login again. This function will be performed by the cloud.

VI.CONCLUSION

In this paper, we propose the privacy preserving public auditing mechanism for shared data in the cloud. It involves the hashing technique to achieve the correctness of data over cloud server. Then propose an effective and flexible distributed scheme with certain dynamic data support, including block update, delete, and append. The TPA is able to audit the purity of shared data, yet cannot distinguish who is the signer on each block, which can achieve identity privacy. To support expert handling of multiple auditing tasks, to further explore the technique of bilinear aggregate signature to continue the main result into a multi-user setting TPA can perform multiple auditing tasks simultaneously. A preserving the identity of the sponsor on each block from the third party

auditor and proposed scheme is highly efficient and provably secure.

REFERENCE:

[1] P. Mell and T. Grance, "The NIST definition of cloud computing,"National Institute of Standards and Technology, Tech. Rep., 2009.

[2] Ateniese G, Burns R, Curtmola R, Herring J, Kissner L, Peterson Z,and Song

D, "Provable data possession at untrusted stores," in Proc.of CCS'07. New York, NY, USA: ACM, 2007, pp. 598 609.

[3] Ateniese G, Pietro R.D, Mancini L.V, and Tsudik G, "Scalable and efficient provable data possession," in Proc. of SecureComm'08. New

York, NY, USA: ACM, 2008, pp.1-10.

[4] Bowers K.D, Jules A, and Oprea A, "Proofs of retrievability: Theory

and implementation," Cryptology ePrint

Archive, Report 2008/175,
2008.

[5] Jules A and Kaliski B.S, Jr., "Pors: proofs of retrievability for large files," in

Proc. of CCS'07. New York, NY, USA: ACM, 2007, pp.584–597.

[6] Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, and

Wenjing Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," IEEE Transactions On Cloud Computing, Year 2013.

[7] SadiaMarium, QamarNazir, Aftab Ahmed,SairaAhthasham,MirzaAamirMehmood "Implementation of Eap with RSA for Enhancing The Security of Cloud

Computing," International Journal of Basic and Applied Sciences, 2012, pp. 177-183.

[8] Christo Ananth, A.Regina Mary, V.Poornima, M.Mariammal, N.Persis Saro Bell, "Secure system to Anonymous Blacklisting", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Issue 4,July 2015,pp:6-9

[9] C. Erway, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in ACM Conference on Computer and Communications Security , E. Al-Shaer, S. Jha, and A. D.Keromytis,Eds. ACM, 2009, pp. 213–222.

[10] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp.847–859, 2011.

[11] Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM.IEEE, 2010, pp. 525–533.

[12] J. Walker, M. Kounavis, S. Gueron and

G.Graunke "Recent Contribution to Cryptographic Hash Functions," Intel

Technology Journal, vol-13, issue-2, 2009,pp- 80-95.

[13] S.M. Bellovin, E.K. Rescorla," Deploying a New Hash Function,"presented at first NIST Workshop", 2005.Available at http://www.csrc.nist.gov/pki/HashWorkshop/2005/Oct31_Presentations/Bellovin.new-hash.pdf.

[14] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Dynamic audit services for integrity verification of outsourced storages in clouds," in SAC , W. C. Chu, W. E. Wong, M. J. Palakal, and C.-C. Hung, Eds. ACM, 2011, pp. 1550–1557.

[15] K. Zeng, "Publicly verifiable remote data integrity," in ICICS ,ser.Lecture Notes in Computer Science, L. Chen, M. D. Ryan, and G.Wang, Eds., vol. 5308. Springer, 2008, pp. 419–434.