International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 20 Issue 2 – FEBRUARY 2016.

SECURE DATA STORAGE IN CLOUD USING CODE REGENERATION AND PUBLIC AUDITION

S.Pavithra

M.Tech Information Technology, Vivekananda College of Engineering for Women, Tiruchengode-637205

***Abstract*--Data integrity maintenance is the major objective in cloud storage. It includes audition using TPA for unauthorized access. The data of the users will be stored in public and private areas of the cloud. So that, only public cloud data will be accessed by user and private cloud will remain more secure. Once any unauthorized modification is made, the original data in the private cloud will be retrieved from the cloud server and will be returned to the user. Every data stored in the cloud will be generated with a Hash value using the Merkle Hash Tree technique. So modification in content will make changes in the Hash value of the document as well. The proxy also performs signature delegation work by generating private and public key for every user using OEAP Algorithm so that the security will be maintained. This scenario is implemented in a multi owner environment in which one document will be accessed by user groups. In this context, the access limit should be properly maintained so that no user of other group should be allowed to modify a particular group's data. Also, if any modifications made to that data will be identified by the proxy and the user is revoked.**

***Index Terms – Cloud storage, code regeneration, public audition, Dynamic Multi Owner*.**

I. INTRODUCTION

Cloud computing is documented as an alternative to traditional information technology due to its intrinsic resource sharing with low maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon and others are able to distribute different services to cloud users with the assist of authoritative data centers. By shifting the local data management systems into cloud servers and users may enjoy high quality services and save significant investments on their limited infrastructures. One of the most essential services is offered by cloud providers was data storage. Let's consider a limited data application the company allows its staffs in the same group or department to store and shared files in the cloud. By utilizing the cloud that the staffs could be completely released from the troublesome local data storehouse and maintenance. However, it is also posing a significant risk to the confidentiality of those stored files. Specifically the cloud servers are managed by cloud providers is not fully trusted by users while the data files stored in the cloud might be confidential and sensitive such as business plans. To preserve data privacy is the primary solution for encrypted data files and then uploaded the encrypted data into the cloud. Unfortunately, the designing of the efficient and secure data sharing scheme for groups in the clouds is not an easy task due to the following challenging issues. First of all identity the privacy is being one of the most significant restriction for the wide deployment of cloud computing. Here not holding the guaranteed of identity privacy user may be unwilling to append in cloud computing systems because their real identities can be easily disclose to cloud providers and also attackers. On the other hand its unconditional identity privacy might incur the abuse of privacy for example the misconduct staff could deceive others on the company to sharing false files without being traceable. Therefore, traceability 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 manner. 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 user in the groups is able to not only read data and also modify his or her part of the data in the entire data file shared with the company.

Last but not the least so that groups are normally dynamic in practice, e.g., new staff cooperation and current employee's revocation in the company. The changes of membership make secure data sharing extremely problematic. On one hand, the anonymous systems can challenge 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 owners and access the corresponding decryption keys. On the other hand the efficient membership repeal mechanism without updating the classified keys of the remaining users has also desire to minimize the complexity of key management. 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 content of the data files because they don't have knowledge of the decryption keys.

However, the complexity of user participation and repeal in these schemes is 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 in the cipher text policy attribute established encryption technique, which allows any member in a group to share data with others. However, the issue of user revocations is not addressed in their scheme. We presented a scalable and fine grained data access control scheme on cloud computing based on the key policy attributes based on by encryption technique with the implementation of the Proxy Server. Unfortunately, the single owner manner hinders the adoption of theirs scheme into the case, where all users are granted to store and share data. Hence we are implementing a group based Data owner system.

II. BACKGROUND

The entire previous auditing scheme is implemented only in a single owner environment and also the owner should always be available in online. Bilinear Pairing Map technique is used for comparing the data and finding unauthorized changes in which no block verification is allowed. CPOR (Compact Proofs of Retrievability) algorithm is implemented for retrieving the data from the cloud. Without the permission of owner the original data will not be retrieved and regenerated back to the modified data. It takes more amount of time and also increases burden the data owner.

III. SECURE DATA STORAGE IN CLOUD

To protect the data integrity and save the data owners computation resources as well as online burden, a secure data storage in the cloud using code regeneration and public audition scheme is proposed for the dynamic multi owner environment, in which the data integrity checking and renewal are implemented by an auditor and a semi trusted proxy separately. This scheme is the first to allow secure data storage in cloud. The contents are masked during the initial phase to avoid leakage of the original data. This method is insubstantial and does not introduce any burden to the TPA or proxy server. The proxy server releases data owners from online burden for the renewal of corrupted blocks. The unauthorized action done by any group member can be found and revoked by the proxy.

To make the scenario easier to follow, this technique is explained with an example description: The staffs (i.e., cloud users) first generate their public and private keys, and then hand over the authenticator regeneration to a proxy (a cluster or powerful workstation provided by the company) by sharing partial private key. After producing encoded blocks and authenticators, the staffs upload and distribute them to the cloud servers. Since that the staffs will be frequently off-line, the company employs a trusted third party (the TPA) to interact with the cloud and perform periodical verification on the staffs' data blocks in a sampling mode. Once some data corruption is detected, the proxy is informed, it will act on behalf of the staffs to regenerate the data blocks as well as corresponding authenticators in a more secure approach. A group of staffs can work under a same project and they can be in one group to access and modify the files.

3.1 Regeneration model

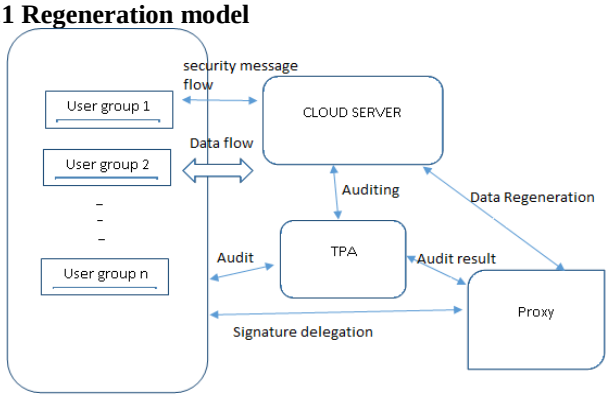

Fig 1: Regeneration System model

The system model for Secure data storage is shown in Fig 1.., which involves four entities: *the group of data owners*, stores their data in the cloud; *the cloud*, which are managed by the cloud service provider, provide storage service and have considerable computational resources; *the third party auditor*(TPA), who has knowledge and capabilities to carry out public audits on the coded data in the cloud, the TPA is trusted and its audit result is impartial for both data owners and cloud servers; and *a semi trusted proxy agent*, acts on behalf of the data owner to restore the data blocks during the repair procedure. Notice that the data owner is restricted in computational and storage resources compared to cloud and may become off-line after the data upload procedure. The proxy, who would always be online, is supposed to be much more powerful than the data owner but less than the cloud servers in terms of computation and memory capacity. To save resources as well as the online burden the data owners resort to the TPA for integrity verification and delegate the reparation to the proxy.

3.2 User Logs

Group members are a set of registered users that will

1. Store their private data into the cloud server and
2. Share them with others in the group.

This module maintains the user's details in it. The group membership is dynamically changed, due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. All the users in the group can view the files which are uploaded in their group and also can 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 a user.

3.3 User and Data maintenance

The registered users and data will be maintained using a cloud server. A local Cloud which provides priced abundant storage services are been created in this module. The users can upload their data in the cloud. This module can be

developed where the cloud storage can be made secure. The cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to that the cloud server is honest but curious. That is, 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. This essentially means that the owner (client) of the data moves its data to a third party cloud storage server which is supposed to - presumably for a fee - faithfully store the data with it and provide it back to the owner whenever required.

The cloud server provides privilege to generate secure multi-owner data sharing scheme called MONA. It implies that any user in the group can securely share data with others by the cloud. This 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 but within the group.

3.4 Authentication and Signature Generation

This module makes the following functions

1. Signature Generation,
2. Signature Verification,
3. 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. Notice 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 owner but less than the cloud servers in terms of computation and memory capacity. To save resources as well as the online burden potentially brought by the periodic auditing and accidental repairing, the data owners resort to the TPA for integrity verification and delegate the reparation to the proxy. Considering that the data owner cannot always stay online in practice, in order to keep the storage available and verifiable after a malicious corruption, it introduces a semi-trusted proxy into the system model and provides a privilege for the proxy to handle the reparation of the coded blocks and authenticators. It generates signature using OAEP based key delegation which provides unique private and public key for each group registered in the cloud. So the users can access the document provided by its own group only. The users can view other group's document using private key of the other groups. If he modifies other group content he will be revoked by the cloud server.

3.5 User Revocation and file regeneration

User revocation is performed by the proxy via a public available RL based on which group members can encrypt their data files and guarantee the privacy against the revoked users. No unauthorized 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 server. Also if content is modified by unauthorized user it will be rollback to its original state by the cloud server.

IV. CONCLUSION

A public investigating scheme that which can be used for regenerating code over the cloud storage system, where the data owners are privileged to delegate TPA for their data validity checking for keep the original data privacy opposition to the TPA has been proposed. No data owners can always stay in online so in order to keep the storage available and verifiable after a malicious corruption and a semi trusted proxy is introduced into the system model that which can be used to provide a privilege for the proxy to handle the reparation of the coded blocks and authenticators. More number of users can handle the files as it's defined with group. This scheme is provable secure and highly efficient.

Not only in text data, regeneration system is planned to appeal for audio and video data by generating transformation of data and then comparing the data will modification. Number of techniques like DWT, WSQ algorithms can be used for this. To design collusion resistant proxy re-signature schemes while also supporting public auditing (i.e., blockless verifiability and non-malleability) remains to be seen. Essentially, since collusion-resistant proxy re-signature schemes generally have two levels of signatures, where the two levels of signatures are in different forms and need to be verified differently, achieving blockless verifiability on both of the two levels of signatures and verifying them together in a public auditing mechanism is challenging which will be considered in future.

REFERENCES

[1] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote data checking for network coding-based distributed storage systems," in *Proceedings of the 2010 ACM workshop on Cloud computing security workshop*. ACM, 2010, pp. 31–42.

[2] H. Chen and P. Lee, "Enabling data integrity protection in regenerating-coding-based cloud storage: Theory and implementation," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 25, no. 2, pp. 407–416, Feb 2014.

[3] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 24, no. 9, pp. 1717–1726, 2013.

[4] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 12, pp. 2231–2244, 2012.

[5] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," *Proceedings of the IEEE*, vol. 99, no. 3, pp. 476–489, 2011.

[6] H. Shacham and B. Waters, "Compact proofs of retrievability," in *Advances in Cryptology-ASIACRYPT 2008*. Springer, 2008, pp. 90– 107.

[7] Y. Hu, H. C. Chen, P. P. Lee, and Y. Tang, "Nccloud: Applying network coding for the storage repair in a cloud-of-clouds," in *USENIX FAST*, 2012.

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–9.

[9] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession," in *Proceedings of the 4th international conference on Security and privacy in communication networks*. ACM, 2008, p. 9.

[10] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosen message attacks," *SIAM Journal of Computing*, vol. 17, no. 2, pp. 281–308, 1988.