A Review on Secure Auditing with Multiuser Data Sharing for Regenerating-Code-Based Cloud Storage

Name: Miss.Raut Snehal B.
ME Computer,
Computer Engineering Department
Mail-id: snehal.pawase4@gmail.com

Guide: Prof.S. K. Sonkar
ME Computer,
Computer Engineering Department
Mail-id: sonkar83@gmail.com

Abstract

Cloud storage provides different kind of services to the end user such as, remotely stored maintained, managed and backup user data. Security and privacy are the major issues for remote data storage. A secure user applies access policy control mechanism to preserve the sensitivity of data. In access control mechanism, there exist ABE i.e. Attribute Encryption scheme for encryption of data. To identify whether outsourced data is corrupted or not as it is critical issue to add fault tolerance to the cloud storage. Also integrity auditing and failure reparation to the cloud storage is difficult. Regenerating codes technique gets more popularity due their lower repair bandwidth and it provides fault tolerance. In previous methods of regenerating coded data that provides private auditing may required data owner to stay continuously online to manage auditing, repairing, etc. which is impossible and infancy task. To address problem of failed authenticators in the absence of data owners, existing approach introduced a proxy. Proxy have right to regenerate authenticators. Moreover, to release data owners from online burden a novel public verifiable authenticator is generated by a couple of keys and can be regenerated using partial keys. In this research we contribute ourselves to provide multiuser data sharing in cloud. A semi-trusted proxy will get rights from the data owner to validate their data, to maintain data repairing of authenticators and coded blocks.

Keywords: *Cloud storage, regenerating codes, public audit, privacy preserving, authenticator regeneration, proxy, privileged, provable secure.*

I.INTRODUCTION

Cloud computing provide various capabilities to the users and enterprises for storing and processing their data in third party centers. In cloud storage, digital is stored in logical pools. It gains more and more popularity among business and daily life due to its on-demand outsourcing service. Multiple benefits provide relief of burden for data storage, management, maintenance, universal data access with independent location etc. User can upload files on cloud that could be accessed over internet from different computer, tablet, and smart phones by same or other users after authentication is provided [1]. Different multiple approaches are existed to deal integrity of outsourced data. POR i.e. proof of retrievability is suggested in [2]. In POR, data storage center convinces that he is actually storing all clients' data. BLS signature and random oracle model has shortest query and response of POR with public variability. Another scheme is PRF' i.e. pseudo random functions is secure in the standard model has shortest response of PRF scheme with private variability. To aggregate a proof into one small authenticator value both of these schemes depend on homomorphic properties. But the problem is these schemes are only for single server scenario. In [3], author O. R. Begam, T. Manjula, T. Bharath Manohar et al. discussed about PDP i.e. provable data possession. PDP ensures the integrity of data in storage outsourcing for multi-clouds with replication, erasure codes, more recently, regenerating codes. Erasure coding technique achieve both data integrity and deduplication in cloud environment which uploads customer's data in encrypted form and allows for integrity auditing and secure deduplication directly on encrypted data. There exists a problem of integrity verification in regenerating code based cloud storage when cloud suffers from failure and loses of its data. Therefore, Henry C. H. Chen and Patrick P. C. Lee proposed a proxy based system in [4] for multiple cloud storage known as NCCloud. It aims to achieve cost effective repair for a permanent single cloud failure. They proposed F-MSR (functional minimum storage regenerating code) to maintain double fault tolerance and storage space cost. This system only designed for private audit, only data owner is allowed for verification of integrity and repairing of faulty servers. Auditing scheme discussed in [5], required large size of outsourced data as well as capability user's constraints resource. In this scheme task of auditing and reparation can be formidable and expensive for the users. B. Chen, R. Curtmola, G. Ateniese, and R. Burns proposed remote data checking scheme in [6], which required user to stay always online. Therefore it implies its adoption practice.

In this research work we are focusing on the problem of integrity verification in regenerating code based cloud storage. In this TPA will get the privileges from data owner to validate their data, so that data owner doesn't have to stay online continuously. Furthermore, as a part of our contribution, an efficient user revocation with their identity privacy as well as multiuser data sharing in cloud environment can also be provided.

II. RELATED WORK

In this section we are going to discussed related work of previously existed systems. In this we make analysis of existing techniques of privacy auditing and regenrating code based cloud storage.

A. Provable Data Possession(PDP)and Proof of Retrievability(POR)

Provable data possession allows users to stored their data on untusted cloud server o make verification of sever that it possess original data that without accessing it[2]. It provides anticipation proofs for third party store files. To generate proof PDP allows to access minimum portion of file to generate proofs. RSA based Homorphic verification tags allows to verify data possession without retrieving original file data. Another is proof of retrievability i.e. POR allows to back-up services to generate compressed form of proof for verifier to retrive target file. Generally, PDP and POR proposed for single server scenario[3]. The concept of symmetric key cryptography is unsuitable for third-party verification. PDP technique allows outsourcing of dynamic data such as PDP efficiently supports functionalities, i.e. block modifi- cation, deletion and append[4]. In[14] proposed PDP model minimizes the accessess of file block, computations on the client side and server side interactions. The homomorphic verifiable tags allows the data possession without accessing original copy of data.

B. Data Integrity Protection

Major problem in integrity verification is regenerating –code based cloud storage. In[5], regenerating-code based cloud storage is introduced specially with functional repair mechanism. Distributed storage represents the redundancy in incresed reliability. Functional repairing is a problem multicasting from source to an absolute number of receivers over perfect graph. Same kind of study made by B.Chen and G. Ateniese in[6]. To generate regenerating code strategy they extended single server CPOR scheme. Author Henry C. H. Chen and Patrick P. C. Lee proposed FMSR-DIP for data integrity protection. This scheme is mainly designed for private auditing only owner of the data can verify integrity of data and repair it[7]. This technique integrates NCCloud with DIP modules to imnplement FMSR-DIP. The auditing and repairing task is expensive and imposing. The limitations are much overcomed in [14], by utilising storage space and also user don’t want to perform too many operations on their outsourced data to retrive it.

C.Public Auditing

Author C.Wang introduced privacy preserving public auditing system to provide data security in[8]. A homomorphic linear authenticator and random masking provides assurity that the TPA cannot learn any content form the original data copy at the time of auditing process. It reduced the user burden from tedious and expensive auditing task. TPA concurrently handles the multiple sessions from different users to outsourced their data. Whereas, in[9] public auditing for shared data with efficient user revocation is proposed by B. Wang, B.Li and Hui Li. The idea of proxy resignatures permits cloud to resign blocks on behalf of existing users at the time of user revocation.Idea of proxy resignature supports batch auditing by making verification of multiple auditing task. MuR-DPA is next version proxy resignature which incorporates authorised data structure based on Merkle tree[10]. Merkel hash tree can be referred as MR-MHT. In this the level of nodes are generated as top-down manner whereas, replica blocks are organised into same sub-tree of replica. MuR-DPA suports dynamic data updates and verification updates. It provides security against dishonest cloud service providers. However, with these all benefits there is a problem of proof size which depend upon the size of dataset. The concept of short signature is based on weil pairing[11], mainly signatures based discreate logs i.e. on DSA required two elements. BLS signatures have ability to generate number of secret keys which is verify publically. With the help of linear subspaces regeneration of codes, authenticators can computed efficiently. The concept of Extract repair and functional repair used to regenerate corrupted blocks. Functional corrupted block represents the newly generated blocks from multiple corrupted blocks with higher probability[5].

D.Regenerating Codes

At very first, Alexandros G. Dimakis, P. Brighten Godfrey, Yunnan Wu, introduced the concept of regenerating codes for distributed storage to save and repair bandwidth[12]. It determines the information that comunicates to repair the failure of an encoded systems as well as noticed the tradeoff between storage and repair bandwidth. MBR is minimum bandwidth regenrating to represents the operation point with minimum storage regenerating(MSR), it corresponds to minimum storage cost. Random linear network coding mechanism is introduced in[13]. This model can achieve the capacity given by max-flow and min-cut bound in multicast and multiscore networks. Distributed random linear network programming can effectively minimises the correlated sources within network. It generalises the result of Slepian–Wolf coding. DMRDPC is “Distributed Multiple Replicas Data Possession Checking” . This scheme validates the availability of data and integrity in the cloud environment. This scheme finds the optimal spanning tree in complete bidirectional directed graph. Therefore, optimal spanning binary tree can be used to enhance communication efficiency by optimizing partial order of multiple scheduling replicas data possession cheking.

In[15],author Yves Deswarte, Jean-Jacques Quisquater proposed two types of methods for remote file integrity cheking. In first method based on multiple challenges and precomputed returns for each file to be varified. The responses being evaluated by server is guaranteed by the fact that a challenge is never reused before reboot of the server.

III. CONCLUSION

In this review paper we have studied existing techniques of privacy-preserving public auditing for regenerating-code-based cloud storage. There exists a problem of remote data integrity checking, integrity verification in regenerating code based cloud storage when cloud suffers from failure and loses of its data. Previously data owner have to always stay online to keep storage available and verifiable after malicious corruption. It is infeasible task in which data owner cannot stay online at every movement hence we determined that there is need of semi-trusted entity to maintain reparation of encoded blocks and authenticators. From literature survey analysis we found solution such as semi-trusted (TPA) proxy to handle reparation of authenticators and coded blocks.

VI.REFERENCES

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores,” in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS ’07. New York, NY, USA: ACM, 2007, pp. 598– 609.

[2] Juels and B. S. Kaliski Jr, “Pors: Proofs of retrievability for large files,” in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 584–597.

[3] 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 netowrks. ACM, 2008, p. 9

[4] 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.

[5] 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.

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

[7] 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.

[8] Boyang Wang, Baochun Li ,“Panda: Public Auditing for Shared Data with Efficient User Revocation in the Cloud”, IEEE Transactions on cloud computing

[9] Chang Liu, Rajiv Ranjan, Chi Yang, Xuyun Zhang, Lizhe Wang ,“MuR-DPA: Top-down Levelled Multi-replica Merkle Hash Tree Based Secure Public Auditing for Dynamic Big Data Storage on Cloud”, IEEE Transactions on computers

[10] Boneh, B. Lynn, and H. Shacham, “Short signatures from the weil pairing,” Journal of Cryptology, vol. 17, no. 4, pp. 297–319, 2004

[11] A.G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, “Network coding for distributed storage systems,” Information Theory, IEEE Transactions on, vol. 56, no. 9, pp. 4539–4551, 2010.

[12] T. Ho, M. Medard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and ´ B. Leong, “A random linear network coding approach to multicast,” Information Theory, IEEE Transactions on, vol. 52, no. 10, pp. 4413– 4430, 2006.

[13] 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 netowrks. ACM, 2008, p. 9.

[14] J. He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, "Distributed data possession checking for securing multiple replicas in geographicallydispersed clouds," Journal of Computer and System Sciences, vol. 78, no. 5, pp. 1345–1358, 2012.

[15] Y. Deswarte, J.-J. Quisquater, and A. Sa¨ıdane, "Remote integrity checking," in Integrity and Internal Control in Information Systems VI. Springer, 2004, pp. 1–11.