A Survey Paper on Cloud Storage Auditing with Key Exposure Resistance

Sneha Singha[1], **S. D. Satav**[2]

[1]M.E (Computer) Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007

[2]Assistant Professor (Computer) Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, India. Savitribai Phule Pune University, Pune, Maharashtra, India -411007

Abstract: ***As data is dynamically updated in today's world, the existing remote integrity checking methods which served as a purpose for static data can no longer be enforced to authenticate the integrity of dynamic data in the cloud. In this scenario, cloud storage auditing conveys an efficient and secure dynamic auditing protocol which draws a confidence to the data owners that their data is correctly stored in the cloud. The present auditing protocols assume that the secret key of the client is very secure while in reality, it is not. Thus, to overcome these flaws, this paper introduces an idea of lessening the client's secret key disclosure. In this paper, we propose a system where de-duplication strategy of data is adopted and it will check the duplicacy of data and eliminate the redundant one using MD5 hashing. Also, it uses tile bitmap method wherein it will check the previous and the current versions of the data to ease the auditor's workload and to make the system more efficient.***

Keywords: Data storage, cloud storage auditing, de-duplication, cloud computation, key-exposure resistance, tile bitmap

1. Introduction

Cloud Computing delivers us a path by which we can easily get access to all the applications as utilities worldwide on the internet. Also, it helps us to create any application or customize and configure the same. Firstly we will see as to what a cloud means. Cloud refers to a network of applications. In other words, we can say that cloud is something, which is remotely located. Cloud grants services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Many applications such as e-mail, video or audio conferencing, customer relationship management (CRM), all run in cloud. Cloud Computing basically means manipulation, configuration and ability to access the applications online on internet. Its prime benefit is that it offers data storage and reduces cost which is beneficial for a large number of end users all across the world.

The most bothering concern about cloud computing is its security and privacy. Since the whole data management and infrastructure management in cloud is done by a third-party, it is always a compelling task to handover the data as it is not trusted. However, the cloud computing vendors ensure many more secure password protected accounts, as a result of which any sign of security violation would lead to loss of clients and businesses.

Cloud storage is a model where data is stored uniformly and maintained which is made available to end users over a large scale network. The end users access data from each and every part of the world. Storage outsourcing into the cloud is very much cost beneficial and also assists in intricacy of large-scale data storage for long term use. So even if any kind of disruption occurs locally at the client's site, the data which has been uploaded in the cloud will be available for access which the client can download later. Meanwhile, such a service is also wiping out data owner's legitimate control over the future of their data, which they have traditionally forecasted with high service-level requirements. Also, the large amount of data in the cloud and owner's limited computational capabilities further makes the task of storage auditing in a cloud environment expensive and even dismaying for individual clients. Clients will hesitate to store data in cloud if it is a matter of their data security and integrity.

For this reason, the Third Party Auditor (TPA) was introduced which is nothing but a software which plays an important role in auditing the integrity and privacy of the data. The TPA, is nothing but a third party software which has the expertise and capabilities that users do not possess, also it can periodically check the integrity of the overall data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud.

Cloud Storage Auditing is basically a scenario where the Third Party Auditor (TPA) audits or checks the integrity of the data in the cloud to see if any unauthorized person or organization has modified the data in any way since the data has been stored in the cloud. This was a major issue since the data can be forged too, which if produced would be invisible to the client. So, in order to maintain the authenticity of the data and to lessen the burden of reckoning and exchanging information in auditing protocols, Homomorphic Linear Authenticator (HLA) technique was studied which permits the auditor to verify the genuineness of the data in the cloud without fetching the whole data. This is also termed as blockless verification. Several cloud storage auditing protocols likewise have been proposed on the basis of this technique. Few auditing protocols have been proposed which supports data dynamic operations like addition, deletion and modification.

While auditing, the secret key of the client could be exposed which would leads to forging of the data later when the client requests for the same. Key exposure could happen due to several reasons:

1) Key management- Key management is a process which is done by the client. In case any fault occurs and if the client is using a cheap software-based key management, then key exposure is possible.
2) Internet based security attacks- Suppose if a client downloads any data or file and if that it contains malicious program, then it may infect the system. This allows the hackers to easily access any confidential data.
3) Trading with hackers- It can happen that cloud also earns incentives by trading with the concerned hackers. In this process, the cloud can get the client's data and forge the authenticator by regenerating false data or by hiding data loss. Thus, dealing with key exposure is a vital issue in cloud storage and various methodologies were adopted which we will discuss in section 2.

In this paper, we present the idea of an effective approach for key exposure resistance using de-duplication and tile bitmap method, which eventually eases the process by taking input as the user data and performs the operation by using de-duplication strategy and tile bitmap method for effective cloud storage. For further proceeding of the paper, section 2 is dedicated for literature survey and related work. Section 3 is for conclusion and future scope.

2. Literature Survey

As the previous section reveals various methodologies for enabling cloud storage auditing, but still there is a huge gap to meet the perfection. So, as a step towards this, this paper tried to grab many concepts so that a new and efficient system can be proposed. The detailed studies are as follows.

In [1], a thorough survey of various methods of cloud storage auditing is performed. Few existent methods have been analyzed and the challenged faced have been described in order to make an efficient protocol. When we store the data, the different version of the data is also stored uniformly. Thus, for the minimization of storage overhead, [2] “delta encoding” was adopted wherein the differences between the versions was noted. A specific type of delta encoding, skip delta encoding was adopted to optimize the added cost of storing and retrieving the data.

K. Yang et al.[3] introduced a framework for auditing data storage in the cloud and also proposed an efficient privacy-preserving auditing protocol. Furthermore, it was extended to support dynamic operations like addition, deletion or modification of data. [4]explains the method of auditing the service dynamically to verify the integrity of a non trustable and outsourced storage on the basis of fragment structure, random sampling, and index-hash table, which also supported updates to the data outsourced and anomaly detection time to time.

In [5], the authors have tried to improve the existing proof of storage models by using Merkle Hash Tree (MHT) construction for block tag authentication. In [6], the authors have presented two provably-secure PDP schemes which are more efficient than the aforementioned solutions, even when compared with schemes that achieve weaker guarantees. Furthermore, [7] extends the previous work on data possession proofs by the Multiple Replica Provable Data Possession (MR-PDP) for a single copy of a file in a client/server storage system.

[8]introduces a mechanism of storage integrity auditing which permits the end users to compute the cost along with achieving fast data error localization, i.e it identifies if any server misbehaves. However, for an efficient auditing, a much more secure cloud storage system was proposed which supported privacy-preserving public auditing and the results were extended so that TPA could perform audits for multiple users at the same time and also execute it efficiently. Thus, in all the above works the cloud storage auditing is tried to make more efficient in various ways.

As we all are already aware that the public key and the secret key play an important role in the encryption and the decryption of the data. If the secret key is exposed, it may lead to data forging and can get in hands of any unauthorized user. [9] narrates an idea of public key encryption which uses the concept of Binary Tree Encryption (BTE) wherein there is a master public key associated with the tree. Every node has a corresponding secret key and to encrypt a message destined for a particular node, one uses both public key and the name of the target node. The ciphertext which comes as a result can then be decrypted using the secret key of the target node.

Now, atleast one secret key is used to sign the message in the current time-period and then obtain the secret key for the next time-period. As in the typical signature scheme, the public key is stable for all time-periods. A verification scheme checks both the validity of the signature and its time-period [10]. The signature scheme is forward secure because it might happen that signature can be forged for the previous time period even if it has the current secret key.

As we discussed regarding the encryption of the keys, [11] introduced the concept of key-insulated security whose aim was to lessen the damage caused by secret key exposure. This was needed as usually cryptographic computations are performed on insecure devices. Thus, in this paper model has been proposed wherein the secret key stored on the insecure device are refreshed at various time periods along with a physically secure device which already possess the master key. In this way, the authors have construct a (t,N)-key-insulated encryption scheme based on any (standard) public key encryption scheme.

3. Conclusion

As this complete paper narrates the different methodologies on enabling cloud storage auditing with key exposure resilience, but none of the methodologies seems to be perfect. So, this survey paper as a bit proposes a method of an effective key exposure resistance where we adopt the de-duplication strategy of data. Moreover, it will check the duplicacy of data and eliminate the redundant one using MD5 hashing algorithm. After the public and private keys are generated, it uses tile bitmap method wherein it will check the previous and the current versions of the data to ease the auditor's workload and to make the system more efficient.

References

[1] K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and opportunities," *World Wide Web*, vol. 15, no. 4, pp. 409-428, 2012.

[2] B. Chen and R. Curtmola, "Auditable Version Control Systems," *2014 Network and Distributed System Security Symposium*, 2014.

[3] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *IEEE Trans. Parallel and Distributed Systems*, Vol. 24, No. 9, pp. 1717-1726, 2013.

[4] Y. Zhu, H.G. Ahn, H. Hu, S.S. Yau, H.J. An, and C.J. Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," *IEEE Trans. on Services Computing*, vol. 6, no. 2, pp. 409-428, 2013.

[5] 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 and Distributed Systems*, vol. 22, no. 5, pp. 847-859, May 2011.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," *Proc. 14th ACM Conf. Computer and Comm. Security*, pp. 598-609, 2007.

[7] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MRPPDP: Multiple-Replica Provable Data Possession," *Proc.28th IEEE International Conference on Distributed Computing Systems*, pp. 411-420, 2008.

[8] C. Wang, S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," *IEEE Trans. Computers*, Vol. 62, No. 2, pp. 362-375, 2013.

[9] R. Canetti, S. Halevi and J. Katz, "A forward-secure public-key encryption scheme," *Advances in Cryptology- EUROCRYPT'03*, pp. 255-271, 2003.

[10] F. Hu, C.H. Wu and J.D. Irwin, "A new forward secure signature scheme using bilinear maps," *Cryptology ePrint Archive*, Report 2003/188, 2003.

[11] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Key-insulated public key cryptosystems," *Advances in Cryptology-Eurocrypt'02*, pp. 65-82, 2002.

Author Profile

Sneha Singha, is currently pursuing M.E (CSE) from Department of Computer Engineering, Jayawantrao Sawant College of Engineering, Pune, MAH, India. She received her B.E (CSE) degree from Shree Rayeshwar Institute of Engineering and Information Technology, Goa University, India. Her research interests include Cloud computing and Network security.

Asst Prof. Sandip Satav, received the M.E (CSE/IT) degree from Department of Computer Engineering, Vishwakarma Institute of Technology, Pune, MAH, India in 2004. He is currently working as Asst. Professor with Department of Information Technology, Jayawantrao Sawant College of Engineering, Pune, MAH, India. His research interests include Image Processing, Networking.