International Journal of Scientific Research in Computer Science and Engineering
Vol.4, Issue.4, pp.16-19, August (2016)

Review Paper

E-ISSN:2320-7639

Key Exposure Resilience for Cloud Storage Auditing

J.S. Ande[1*], A.S. Kumar[2], A.V. Kumar[3]

[1]Dept. of CSE, Sanketika Vidya Parishad Engineering College, Visakhapatnam, India
[2]Dept. of CSE, Sanketika Vidya Parishad Engineering College, Visakhapatnam, India
[3]Dept. of CSE, Sanketika Vidya Parishad Engineering College, Visakhapatnam, India

Corresponding Author: sudhakar1007.ande@gmail.com

Available online at www.isroset.org

Received: Jul/06/2016, Revised: Jul/14/2016, Accepted: Aug/20/2016, Published: Aug/30/2016

Abstract— Never days data is dynamically updated, the existing remote integrity examine the methods which served as a reason for static data can no longer be impose to authenticate the integrity of dynamic data in the cloud. In this scenario, cloud storage auditing carries an efficient and secure dynamic auditing protocol which pulls a confidence to the data owners that their data is correctly stored in the cloud. The existing auditing protocols assume that the secret key of the client is very secure while in reality, it is not. Therefore, to overcome these fault, this paper launches an idea of lessening the client's secret key revelation. In this paper, we suggest a system where de-duplication strategy of data is taking on and it will verify the duplicity of data and eliminate the redundant one using MD5 hashing. Also, it uses tile bitmap method wherein it will identify 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 bitma

I. INTRODUCTION

Cloud Computing conveys us a path by which we can easily get access to all the applications as utilities world wide on the internet. It also helps us to create any application or customize and set up the same. Initially we will see 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 allow services over network, i.e., on public networks or on private networks, i.e., WAN, LAN or VPN. Frequent applications such as e-mail, video or audio conferencing, customer relationship management (CRM), all run in a cloud [1]. Cloud Computing basically means manipulation, configuration and ability to access the applications online over the internet. Its prime benefit is that it offers data storage and reduces cost which is beneficial for a huge number of end users all across the world. The most worrying concern about cloud computing is its security and privacy [2]. Considering the whole data management and infrastructure management in cloud is done by a third-party, it is always a fascinating task to handover the data as it is not reliable. Yet, the cloud computing vendors make sure many more secure password safe guarded 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 been stored uniformly and maintained which is made available to end users over a huge scale network. The end users access data from each and every part of the world. Storage outsourcing into the cloud is very much cost favorable and also helps in intricacy of huge scale data storage for long term use [3]. So even if any kind of interruption occurs locally at the client's site, the data which has been uploaded in the cloud will be available for access for which the client can download later., such a service is also cleaning out data owner's authorized control over the future of their data, which they have traditionally forecasted with high service-level requirements. Also, the huge amount of data in the cloud and owner's limited computational capabilities further makes the task of storage auditing in a cloud environment is expensive and even discourage for individual clients [4]. 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 ability and capabilities that users do not possess, also it can systematically check the integrity of the overall data stored in the cloud on favor of the users, which provides a much more easier and reliable way for the users to make sure 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 problem since the data can be forged too, which if produced would be unseen to the client. So, in order to maintain the authenticity of the data and to minimize the burden of reckoning and exchanging information in the auditing protocols, Homomorphic Linear Authenticator (HLA) technique was studied which allows the auditor to verify the genuineness of the data in the cloud without

fetching the whole data [5]. This is also described as block less verification. Several cloud storage auditing protocols likewise have been suggested on the basis of this technique. Few of the auditing protocols have been suggested which supports data dynamic operations like addition, deletion and modification.

While auditing, the secret key of the client could be revealed which would leads to forging of the data later when the client requests for the same. Key revelation 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 revelation 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 kind of 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 relevant is a vital problem in cloud storage and various procedures were adopted.

In this paper, we present the idea of an effective approach for key exposure resistance using de-duplication and tile bitmap method, which ultimately eases the process by taking input as the user data and performs the operation by using deduplication strategy and tile bitmap method for effective cloud storage [6].

II. PROBLEM STATEMENT

A. The System and Threat Model

Lets consider a cloud data storage service which includes three different entities, as shown in the Figure 1, the cloud user, who has huge amount of data files to be stored in the cloud; the cloud server, which is handled by the cloud service provider to supply data storage service and has significant storage space and computation resources; the third-party auditor, who has skilfulness and abilities that cloud users do not have and is trusted to assess the cloud storage service security and reliability in favor of the user upon request.

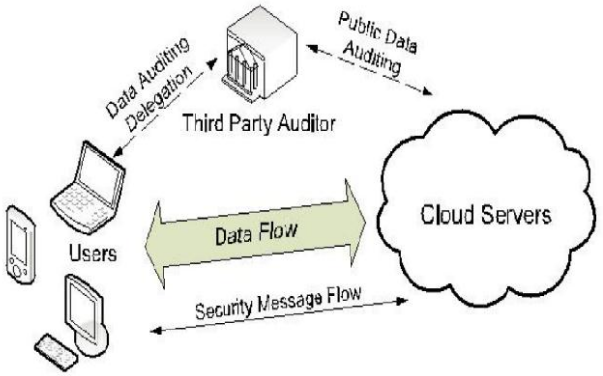

Figure. 1 The architecture of cloud data storage service

Users depend on the Cloud Servers(CS) for cloud data storage and maintenance. As users no longer own their data locally, it is of critical significance for users to make sure that their data are being perfectly stored and maintained. To save the computation resource further the online burden likely brought by the periodic storage correctness verification, cloud users may resort to TPA while expecting to keep their data private from TPA.

Let's assume the data integrity threats against users' data can come from both internal and external attacks at CS. Likewise, CS can be self-interested. For their own benefits, such as to maintain reputation, CS might even decide to hide these data misrepresentation incidents to users. Using third-party auditing service provides a cost-effective method for users to gain trust in cloud. We consider that the TPA, who is in the business of auditing, is reliable and independent. Yet, it may harm the user if the TPA could learn the outsourced data after the audit [7]. Note that in our model, beyond users' reluctance to leak data to TPA, we also assume that cloud servers have no incentives to reveal their hosted data to external parties. Accordingly, we assume that neither CS nor TPA has drive to collude with each other during the auditing process. To authorize the CS to respond to the audit delegated to TPA's, the user can give a certificate on TPA's public key, and all audits from TPA are authenticated against such a certificate. These authentication handshakes are omitted in the following presentation.

B. Design goals

To authorize privacy-preserving public auditing for cloud data storage under the preceding model, our protocol design should attain the following security and performance guarantees: a) Public audit ability: To permit TPA to verify the correctness of the cloud data on demand without retrieving a copy from the whole data or introducing further online burden to the cloud users. b) Storage correctness: To make sure that there exists no cheating cloud server that can pass the TPA's audit without actually storing users' data intact. c) Privacy preserving: To make sure that the TPA cannot derive users' data content from the information collected during the auditing process. d) Batch auditing: To

enable TPA with secure and efficient auditing capability to cope with the multiple auditing delegations from possibly huge number of different users at the same time. e) Light weight: To allow TPA to perform auditing with minimum communication and computation above [8].

III. PUBLIC AUDITING MECHANISM

A public audit scheme consists of four algorithms (KeyGen, SigGen, GenProof and VerifyProof). KeyGen is a key generation algorithm that is executed by the user to the system configuration. SigGen is used by the user to generate verification metadata, which may consist of MAC, signatures, or any other related information to be used for the audit. GenProof is managed by the cloud server to generate a proof of correctness of data storage while VerifyProof is run by the TPA to audit the test from the cloud server. Running a public audit system consists of two phases, Setup and auditing:

Setup: The user initializes the public parameters and secret system by running KeyGen and pre-processes the data• file F using SigGen to generate verification metadata. The user then saves the file data and metadata F check in cloud server, and removes your working copy. As part of the pre-processing, the user can modify the data file F by expanding or including additional metadata to be stored on the server [9].

Audit: The TPA, in order to ensure that it holds the data file F properly at the time of the audit, cloud server issues• a challenge to the cloud server or audit messages. Cloud server to derive the response message from the verification of data and metadata to run the GenProof, stored in the file function F. TPA to verify the response through VerifyProof then.

Our framework assumes the TPA has been, which is a desirable property managed by our proposed solution. It is easy to extend the above framework to capture a complete audit system state, essentially by splitting metadata verification into two parts that are stored by the TPA and cloud server respectively. Our design assumes no additional property in the data file. If the user wants more resilient error, he / she can always redundantly encoding the first data file, and then use our system with the data file that has the integrated correction codes errors [10].

A. KeyGen Process:

The keygen process will execute between user and cloud server, the user will register to cloud server the user should provide a user secure key that will be represent sk and additionally to that key the cloud server will add a public key to user key pk. By using both secure key and public key cloud server a generates a user security key by applying as KeyGen (sk, pk) [11].

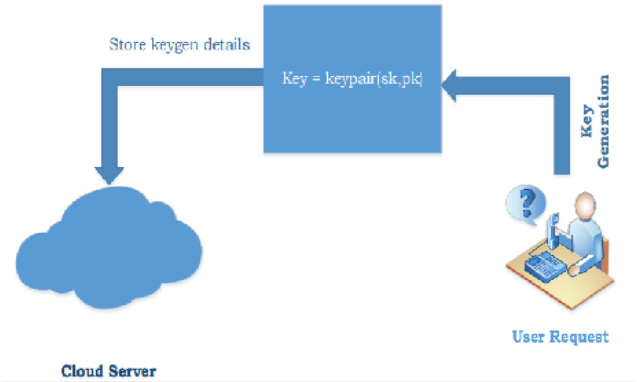

Figure 2. KeyGen Process

B. SigGen Process

The signature generation process will generate between user and cloud server, when a user upload his data to cloud server, the cloud server will give signature of the data by using the data file names as attribute, it will apply SSG(names) [12].

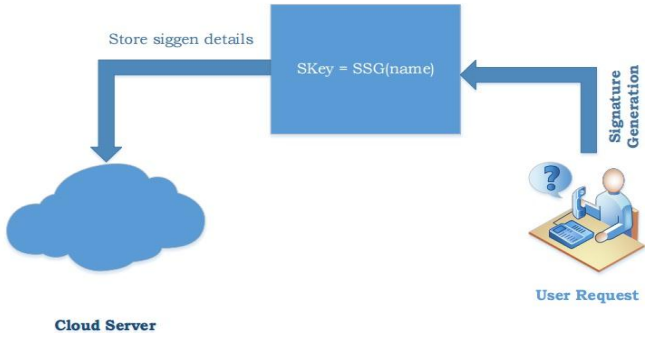

Figure 3. SignGen Process

C. GenProof process

The generation proof is applied by cloud server, the cloud server will collect user data from trusted party auditor, then the cloud server will generate generation proof to that user data by applying challenge chal(fk,vk) the fk will represents a file data key and the vk will attach by the trusted party auditor key to that file this will be useful to trusted party auditor at the time of verification proof [13].

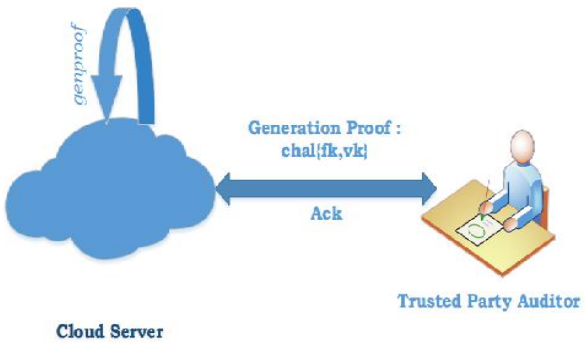

Figure 4. GenProof Process

D. *VerifyProof process*

The verification proof is generated by trusted party auditor, the auditor will collect data of user that should be generated a generation proof by cloud server. The GenProof generated data verify by TPA with matching of vk matching of the data [14].

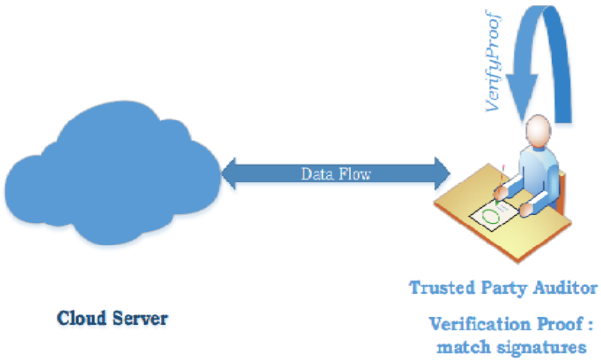

Figure 5. VerifyProof Process

IV. CONCLUSION

In this paper, we propose a privacy-preserving public auditing system for data storage security in Cloud Computing. We utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

REFERENCES

[1]. S.L.Mewada, U.K. Singh, P. Sharma, "*Security Enhancement in Cloud Computing (CC)*", International Journal of Scientific Research in Computer Science and Engineering, Vol.1, Issue.1, pp.31-37, 2013.

[2]. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "*Above the clouds: A berkeley view of cloud computing*," University of California, Berkeley, pp.1-28, 2009.

[3]. S. Ayyub, D. Roy, "*Cloud Computing Characteristics and Security Issues*", International Journal of Computer Sciences and Engineering, Vol.1, Issue.4, pp.18-22, 2013.

[4]. J. Kincaid, "*MediaMax/TheLinkup Closes Its Doors*," from www.techcrunch.com, US, pp.1-2,2008.

[5]. Amazon.com, "*Amazon s3 availability event: July 20, 2008*," Online at http://status.aws.amazon.com/s3-20080720.html, 2008.

[6]. S. Wilson, "*Appengine outage*", Online at http://www. cio-weblog.com/50226711/appengine outage.php, June 2008.

[7]. B. Krebs, "*Payment Processor Breach May Be Largest Ever"*, Online at http://voices.washingtonpost.com/securityfix/ 2009/01/payment processor breach may b.html, Jan. 2009.

[8]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song, "*Provable data possession at untrusted stores*" Provable data possession at untrusted stores, Proceedings of the 14th ACM conference on Computer and communications security, Virginia, pp.598-609, 2007.

[9]. M. A. Shah, R. Swaminathan, M. Baker, "*Privacypreserving audit and extraction of digital contents*", Cryptology ePrint Archive Report, Vol.2008, pp.1-21, 2008.

[10]. Q. Wang, C. Wang, J. Li, K. Ren, W. Lou, "*Enabling public verifiability and data dynamics for storage security in cloud computing"*, LNCS Springer, vol.5789, pp.355–370, 2009.

[11]. A. Juels, J. Burton S. Kaliski, "*Pors: Proofs of retrievability for large files*", Proceedings of the 14th ACM conference on Computer and communications security, NewYork, pp.584–597, 2007..

[12]. E. Thomas, R. Puttini, M. Zaigham, "Book of *Cloud Computing: Concepts, Technology & Architecture"*, Prentice Hall, NewJersey, pp.1-528, 2013..

[13]. H. Shacham and B. Waters, "*Compact proofs of retrievability*", in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.

[14]. M. A. Shah, M. Baker, J. C. Mogul, R. Swaminathan, "*Auditing to keep online storage services honest*", Proceeding HOTOS'07 Proceedings of the 11th USENIX workshop on Hot topics in operating systems, SanDiego, pp.1-6, 2007.

