International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July 2016

Affording Greater Privacy in Cloud Storage Auditing with Random Masking Technique

[1] N.Venkatesh Naik, india_v2020@yahoo.com, [2] D.Priyanka
Department of Computer Science & Engineering
Sree Visvesvaraya Institute of Technology & Science, Mahabubnagar, Telangana, India.

Abstract: As data is energetically modernized in today's world, the existing remote integrity checking methods which served as persistence for static data can no longer be enforced to authenticate the integrity of dynamic data in the cloud. Auditing is an important service to verify the data in the cloud. Most of the auditing protocols are based on the assumption that the client's secret key for auditing is secure. The security is not fully achieved, because of the low security parameters of the client. The task is very difficult for users with constrained computing resources. The advantage of cloud computing are those users can use the cloud storage as if it is local. For providing integrity to the data that stored in cloud, users can enable public auditability for cloud storage. Users can recourse to a third party auditor to check the correctness of their outsourced data and no need to worry about their data integrity. For operative auditing TPA should not introduce any vulnerability. That is user need privacy from the TPA. The auditing method uses homomorphic encryption with random masking technique which provides greater privacy. This paper is based on a secure cloud storage system supporting privacy preserving public auditing.

Keywords: Cloud computing, Auditing, Batch signature, Client Key Exposure, Cloud storage auditing, Multicast authentication etc.

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 privacy protection of data is an important aspect of cloud storage auditing. It is used to reduce the computational burden of the client. The third party auditor is introduced to help the client to periodically check the integrity of data in cloud. Auditing protocols are for the privacy of data in cloud. 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 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 block less 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.

1. RELATED WORK

Some existing remote integrity checking methods can only serve for static archive data and thus cannot be applied to the auditing service since the data in the cloud can be dynamically updated. Thus, an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. The design of an auditing framework for cloud storage systems and propose an efficient and privacy-preserving auditing protocol. Then, we extend our auditing protocol to support the data dynamic operations, which is efficient and provably secure in the random oracle model. We further extend our auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer. While auditing, the secret key of the client could be exposed which would lead 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.

Problem Statement:

The Key exposure resilience in the storage auditing protocol is not fully supported in the existing system this mechanism is used to detect any dishonest, such as deleting or modifying some client's data that is stored in the cloud in previous time periods can all be detected, even if the cloud gets the clients current secret key for cloud storage auditing.

Auditing protocols can also support dynamic data operations. Other aspects, such as proxy auditing, user revocation and eliminating certificate management in cloud storage auditing have also been studied. Though many research works about cloud storage auditing have been done in recent years, a critical security problem exposure problem for cloud storage auditing, has remained unexplored in previous researches. While all existing protocols focus on the faults or dishonesty of the cloud, they have overlooked the possible weak sense of security and/or low security settings at the client.

2. IMPLEMENTATION

The cloud data storage service involving three different parts, as shown in Fig. 1: the cloud user who stores has large amount of data in the cloud; the Cloud Server provides data storage service and has computation resources and storage space, the third-party auditor which has the responsibility to notify the user about the integrity of the data files stored in the cloud server by performing the important auditing task. Cloud users depend on the Cloud Server for cloud data storage and data maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes. Users no longer have their data locally. So it is very important for the users to ensure that the integrity of their data is properly maintained. Users cannot perform the correctness verification of data because it causes additional online burden and storage overhead.

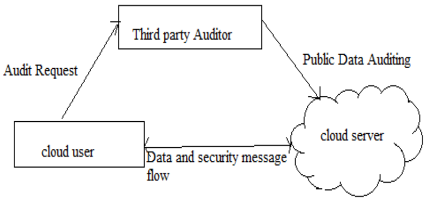

Fig1: Architecture of Public Auditing in Cloud Server

To fully ensure the data correctness and for avoiding additional online burden, it is very important to enable public auditing for cloud data storage. Here users may resort to an independent third party auditor (TPA) to audit the outsourced data whenever needed. The TPA who has the capabilities that can check the integrity of all the data stored in the cloud server which provides an efficient method for the users to ensure their storage integrity in the cloud. Auditing will help users to assess the risk of their cloud data services.

A. MAC Based Solution

It is mainly used for data authentication. In this method the user upload both the data blocks and calculated MAC of data to Cloud Server and store the user's secret key to Third Party Auditor. The TPA will retrieve data blocks & the secret key is used to check integrity of the data stored on the cloud. In this method of MAC based solution there are mainly two methods to check integrity of data. A first method is upload the data blocks and the MACs of the data to the cloud server and sends the secret key to the TPA. Then the TPA retrieves data blocks with their MACs and checks the integrity of data using secret key. The TPA requires the knowledge of the data blocks for verification. For avoiding the requirement of the data to TPA verification, one may restrict the verification to just consist of equality checking.

B. HLA based solution

Homomorphic linear authentication (HLA) is for privacy of data in cloud server. HLA techniques are used to audit data file from cloud server without retrieving the user's data file. HLA generate verification metadata from the user's data file that authenticate the correctness of a data block. That is authenticator is calculated from the linear combination of data blocks. The user authenticates each block of file by a set of HLAs. Then the TPA sends random set of challenge to the
cloud server. The cloud server sends back its set of authenticator computed from file blocks.

C. Using Extensible authentication protocol

For hierarchical architecture they proposed the method of identity based signature. In this an authentication protocol for cloud computing (APCC) is provided. APCC is more efficient and less complex as compared to other authentication protocols. In this method, for authentication Challenge–handshake authentication protocol (CHAP) is used. When a client requests for any service on the cloud, the Service provider authenticator (SPA) sends the first request for identity of client. The steps are as follows1. SPA sends a CHAP request / challenge to the client when client request for any service to cloud service provider.2. The Client send back CHAP response/ challenges which is calculated by using any hash function.3. SPA compares the value of challenge with the calculated value of its own. SPA sends CHAP success message to the client if they are matched. Cloud computing provides authentication of the client by implementing this EAP CHAP method. Spoofing identity theft, data tempering threat, DOS attack can be prevented by using this method. The data is being transferred between client and cloud server. Asymmetric key encryption (RSA) algorithm is used for more providing more security.

The audit performed by TPA would be effective for the cloud service providers for improving their cloud service [5].For the privacy of data in cloud, the users, who is the owner of the data depends on TPA, the storage security of their data; avoid process of auditing because it introduces additional vulnerabilities of leakage of information causing threat toward their data privacy. By the encryption of data before outsourcing it to cloud is a way to provide privacy which is a concern of data auditing. Encryption is not a complete solution for providing privacy to user's data against third party auditing it is a way to reduce complexity of key management. But there is a chance of leakage of data because of the exposure of key for decryption. Privacy preserving third party auditing protocol is independent to data encryption. For auditing the different TPA is delegated to different user. This problem is addressed by using the technique of public key based homomorphic linear authenticator [7] (or HLA for short), which enables TPA toper form the public auditing without asking the copy of data and thus reduces the communication and computation overhead as compared to the straightforward data auditing approaches. To achieve privacy preserving public auditing the random masking technique is integrated with the homomorphic authenticator. The server's response is masked with randomness generated by a Pseudo Random Function(PRF) from the linear combination of sampled blocks, since random masking is used and therefore cannot derive the user's data content. There is no need to worry how many linear combinations of the same set of file blocks can be collected. Homomorphic authenticator has the algebraic property. Public key based homomorphic authenticator is used in this scheme. Signature aggregation helps for the multi task auditing.

Consider e:G1*G2→Gt be a bilinear map and G1,G2,Gt are multiplicative cyclic groups. Assume g be the generator ofG2.

A public auditing scheme consists of different algorithms (KeyGen, SigGen, GenProof, and Verify Proof). A key generation algorithm KeyGen runs to setup the scheme which is done at the user side. Sig Gen is used by the user to generate verification metadata, which consist of digital signatures. Gen Proof is run by the cloud server to generate a proof of data storage integrity. Verify Proof is run by the TPA to audit or verify the proof. Running a public auditing system consists of two phases, Setup and Audit:

Auditing Based on Batch Signature

Multicast authentication can be used in the cloud environment to protect user from malicious attacks. Data integrity, Data origin authentication, Non repudiation are the security services provided by the multicast authentication. The technique here used is an asymmetric key technique called signature. In normal case, the sender generates a signature for each packet with its private key, which is called signing, and each receiver checks the validity of the signature with the sender's public key, which is called verifying. If the verification succeeds, the receiver knows the packet is authentic .Designing a multicast authentication is a difficult task .Multicast authentication protocol(Multicast Authentication based on Batch Signature)two schemes. The basic scheme (MABS efficient asymmetric cryptographic primitive called batch signature, which encourages the authentication of any number of packets simultaneously with one signature verification, to tackle the efficiency and packet loss problems in general environments.

3.CONCLUSION

The cloud storage auditing with key exposure resilience protocol is used in paper .The user can upload their data in the cloud and they can protect their data by using the Third Party Auditor. The technique used for auditing is homomorphic linear authenticator and random masking. This method guarantees the cloud user that during the efficient auditing process the Third Party Auditor would not learn any details about the content of the file stored on the cloud server. This will eliminates the burden of cloud user from the expensive auditing task and frees the user from the fear about the leakage of outsourced data. Considering TPA concurrently handle multiple audit sessions from different users for their outsourced data files. Further extend the privacy-preserving public auditing protocol into a batch verification scheme Multicast Authentication based on Batch Signature is used where the TPA can perform auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

REFERENCE

[1] G. Ateniese et al., “Provable data possession at untrusted stores,” in Proc. 14th ACM Conf. Comput. Commun.Secur. 2007, pp. 598–609.

[2] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, “Scalable and efficient provable data possession,” in Proc. 4th Int. Conf. Secur.Privacy Commun.Netw.2008, Art. ID 9.

[3] H. Shacham and B. Waters, “Compact Proofs of Retrievability,” Advances in Cryptology-Asiacrypt’08, pp.90-107, 2008.

[4] C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, “Dynamic provable data possession,”.

[5] J. Yu, R. Hao, F. Kong, X. Cheng, J Fan, and Y.Chen, “Forward-Secure Identity-Based Signature: Security Notions and Construction,” Information Sciences, Vol. 181, Iss. 3, pp. 648-660, 2011.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable data possession at untrusted stores .InProc. of CCS’07, (2007), pp. 598-609.

[7] H. Shacham and B. Waters, “Compact proofs of retrievability”,InProc. of ASIACRYPT‘08, vol. 5350, (2008), pp. 90-107.

[8]. V. R. D. P K Deshmukh, “Investigation of tpa for cloud data security, ”International Journal of Scientific and Engineering Research, 2013.

[9]. C. Wang, Q. Wang, K. Ren, and W. Lou, “Towards Secure and Dependable Storage Services in Cloud Computing,” IEEE Trans. Service Computing, vol. 5, no. 2, 220-232, Apr.-June 2012

[10]. 10. R.C. Merkle, “Protocols for Public Key Cryptosystems,” Proc.IEEE Symp. Security and Privacy, 1980.

Authors

N.Venkatesh Naik, working as Assoc.Professor & HOD, Computer Science & Engg. Dept, in Sree Visvesvaraya Institute of Technology & Science, Mahabubnagar,Telangana,India.

D.Priyanka pursing M.Tech in Computer Science & Engineering from Sree Visvesvaraya Institute of Technology & Science, Mahabubnagar, Telangana, India.