Data Auditing System for Efficient Monitoring Of Data in Cloud Computing

D.Dhayalan[1]
MCA (Ph.D.), Vel Tech Multi Tech
Dr.Rangarajan Dr.Sakunthala Engineering
College
Chennai, India
dhayalan.moorthy@rediffmail.com

Manjot Kaur[2]
MCA, Vel Tech Multi Tech Dr.Rangarajan
Dr.Sakunthala Engineering College
Chennai, India
manjot1010khalsa@gmail.com

***Abstract*—This Cloud storage is a model of networked enterprise storage where data is stored in virtualized pools of storage which are generally hosted by third parties. It moves the application software and databases to the centralized large data centres, where the management of the data and services may not be fully trustworthy. We here study the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a third party auditor (TPA), for the cloud client, to verify the integrity of the dynamic data that is stored in the cloud. The TPA works on behalf for the cloud client. By utilizing public key based homomorphic authenticator with random masking privacy preserving public auditing can be achieved. The signature and scheduling policies is used to achieve multiple batch-auditing, for reducing the computation overhead. The new scheme further supports secure and efficient dynamic operations on data blocks, operations such as data update, delete append.**

Keywords--Third Party Auditor (TPA), Boneh–Lynn–Shacham, Bilinear aggregate signature, Batch auditing.

I. INTRODUCTION

Cloud computing is a general term for anything that involves delivering hosted services over the internet. Cloud services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Cloud storage services may be accessed through a web service application programming interface (API) or by API applications that utilize such as Web-based content management cloud desktop storage, a cloud storage gateway. It is sold on demand, typically by the minute or the hour. The advantage of cloud is cost savings. Security is a problem here which cannot be easily adopted by crypting techniques. There are instances where the cloud service provider may hide the data corruptions to maintain the repute [1]. To avoid such instances, we introduce an effective third party auditor (TPA) to audit the user's outsourced data when needed. The security is achieved by signing the data blocks in data files. The security is achieved by signing the data blocks in data files. Signing for the data blocks are done using BLS algorithm. TPA performs the auditing task for each user i.e. single auditing. This increases the auditing time and computation overhead. The technique of Bilinear Aggregate Signature is used to achieve batch auditing i.e.) multiple auditing tasks instantaneously. Earlier auditing was performed only for static data.

Our contribution in this paper is summarized as follows:
•We provide a privacy preserving auditing

• Protocol. E.g. our scheme supports an external auditor to audit the user's outsourced data without learning knowledge on the data content.

• Our scheme supports dynamic operations on data blocks i.e. data update, data append and data delete, which is a best error correct method.

A. Characteristics

Cloud computing is cost-effective. Here, cost is significantly reduced as early expense and recurring expenses are much lower than traditional computing. Maintenance cost is reduced as a third party maintains everything from running the cloud to storing data. The Cloud is characterized by features such as platform, location and device independency, which is now easily available and affordable. Some of the most important characteristics are,

1. On-Demand Self Service

A consumer has separate provision of computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider.

2. *Broad Network Access*

Broadband network access capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms.

3. *Resource Pooling*

The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction.

4. Measured Service

Cloud systems automatically control and optimize resource use, by leveraging a metering capability at some level of abstraction appropriate to the type of service, resource usage can be depending on that.

5. Selection of Provider

A good service provider is the key to good service. So, it is imperative to select the right service provider's cloud computing has taken hold; there are six major benefits that have become clear,

(1) Anywhere/Anytime Access
(2)Collaboration among users -cloud represents an environment in which users can develop software based services and from which they can deliver them.
(3) Storage as a universal service.
(4) Cost benefits - the cloud promises to deliver computing power and services at a lower cost.

6. System Design

Cloud computing components are classified as

a) Cloud User (CU).
b) Cloud Service provider (CSP)
c) Cloud server (CS)

B Third Party Auditor

The third party auditor (TPA), who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes. The users may resort to TPA for ensuring the storage security of their outsourced data, while hoping to keep their data private from TPA. Mostly, the CS may decide to hide the data corruptions caused by server hacks. We assume the TPA, who is in the business of auditing, is reliable and independent, and thus has no incentive to collude with either the CS or the users during the auditing process. TPA should be able to efficiently audit the cloud data storage without local copy of data and without bringing in additional on-line burden to cloud users [3].

The Cloud Computing model of computing is a distributed application structure that partitions tasks or workloads between the providers of a resource or service, called Cloud servers (CS), and service requesters (CR), are called clients [3]. Over and over again clients and servers communicate over a computer network on separate hardware, but often both client and server might reside in the same system called host system.

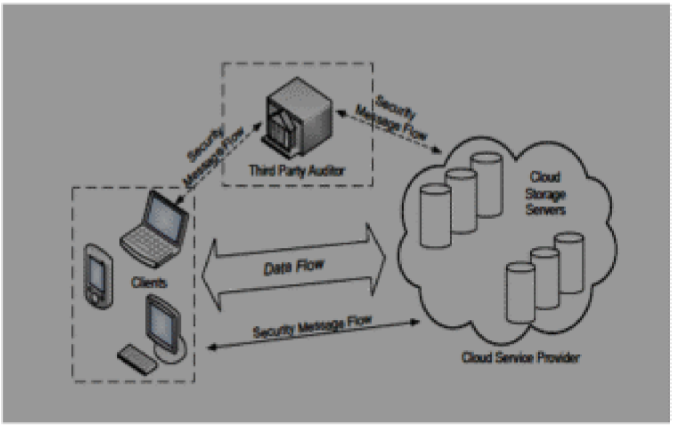


Fig. 1: The architecture of cloud as a storage service.

The figure (1) shows the architecture of Cloud the data flows between the client and cloud service provider and the TPA manages the security message flow between the two.

A client does not share any of its resources, but requests for a server's content or service function. Therefore the Client's initiate communication sessions between servers which await for incoming requests.

II. EXISTING SYSTEM

To introduce an effective third party auditor (TPA) for privacy and security, the following major requirements have to be satisfied: TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data as in earlier systems, and introduce no additional on-line burden to the cloud user(CU). The third party auditing (TPA) process should not bring in any new vulnerability towards user data privacy [1]. They utilized and uniquely combined the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which satisfies all above requirements. This proposed scheme is the first to support scalable, cost efficient public auditing in the Cloud Computing. In particular, this scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA [2]. In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it does not deal with any guarantee on data integrity and data availability.

III. PROPOSED SYSTEM

The proposed system has a scheme enhanced with explicit and efficient dynamic data operations for data storage security in Cloud Computing and it is crucial to consider some dynamic cases, in which a user may wish to perform various block-level operations such update the data, delete and append to modify the data file while maintaining the storage to assure correctness. There is a straightforward way to support the block-level operations is that the user to download all the data from the cloud servers and re-compute the whole parity blocks as well as verification tokens.

A. Update Operation

In cloud data storage, sometimes the user may need to modify some data block(s) stored in the cloud, from its current value Dij to a new one, Dij + Δ Dij. We refer this operation as data update.

B. Delete Operation

Some data blocks needs some updated and for that deletion should be performed from time to time. This delete operation that we consider is a common one, in which user replaces the data block with zero or some special reserved data symbol. From this we can suggest the delete operation is actually a special case of the data update operation, where the original data blocks are to be replaced with zeros or some predetermined special blocks.

C. Append Operation

The user may want to increase the size of his stored data by adding blocks to the data store in the data file, for this we perform the operation append. We foresee that the most frequent append operation in cloud data storage is mass appended, in which the user needs to upload a large number of blocks at a time. Dynamic operations are performed by constructing the matrix, where 0's indicate the blocks we need to change and 1's indicate the unchanged blocks [4].

We need to create a cloud environment where user and TPA along with cloud Server are connected to each other. In public auditing system, the correctness of the data is checked by Keygen, gen proof sagging, and verifies proof algorithms. The technique of bi-linear aggregate signature is used to achieve batch auditing.

4. Construct Public Auditing System

The public auditing system can be constructed in two phases, Setup and Audit. Setup: The user initializes the public and secret parameters of the system by executing KeyGen, and pre-processes the data file (F) by using Signature Gen to generate the verification metadata. The user then store the data file F at the cloud server, and deletes its local copy from the disk, and publishes the verification metadata to TPA for later audit. As a part of pre-processing, the user may alter the data file F by expanding it or including additional metadata to be stored at cloud server.

Audit: The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of the audit. The cloud server will derive the response message from a function of the stored data file (F) by executing GenProof. Using this verification metadata, the TPA verifies the response via two processes known as Verify Proof and Keygen Process.

The Batch signature scheme is proposed which is based on the BLS signature.

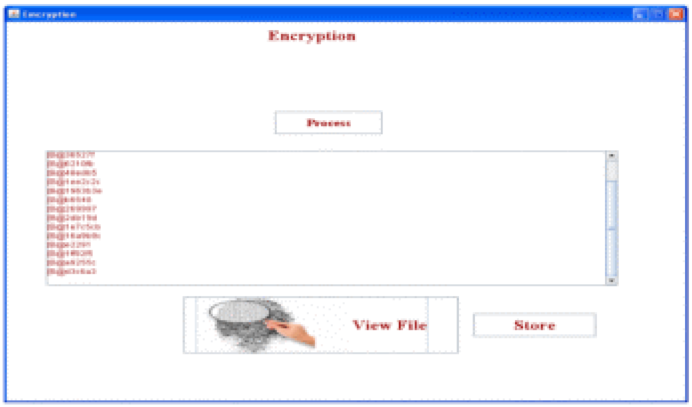


Fig. 2: The data are received by sign on it.

The Figure 2 performs the encryption for the client data with signature (signs) on it.

The BLS signature scheme uses a cryptographic primitive called pairing, which can be defined as a map over two cyclic groupsG1 and G2.

The BLS signature scheme consists of 3 phases,

a) In the key generation phase, a sender chooses a random integer and computes the function. The private key is x and the public key is y.

b) The message is given in the signing phase, the sender first computes the hash function h () and then computes the signature of m.

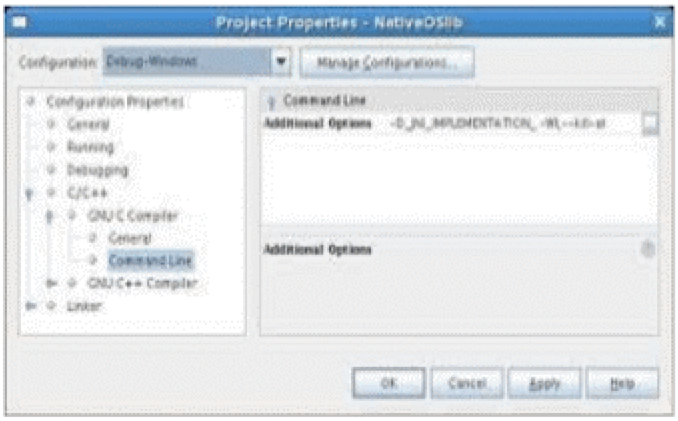
c) In the verification phase, the receiver first computes and then checks the data. In case the verification is successful, then the message m is authentic.

Merits:

- Very short signature can be generated.
- It can solve communication overhead.

5. Privacy-Preserving Public Auditing Scheme

The privacy preserving public auditing scheme uniquely integrates the homomorphic authenticator which enables TPA to accomplish the auditing without demanding the local copy of data and thus significantly reduces the communication and computation overhead as compared to the other data auditing approaches with random masking technique. We use our protocol where the linear Combination of sampled blocks in the server's response is masked with randomness generated by a pseudo random function (PRF).With new techniques as random masking, the TPA has no longer all the necessary information to build up a correct group of linear equations and therefore cannot derive the user's data content. Further so due to the algebraic property of the homomorphic authenticator, the validation of the block authenticator pairs will not be affected by the randomness generated from a PRF.



Configuration: Debug-Windows

Additional Options -D_JNI_IMPLEMENTATION_ -Wl,--kill-at

Additional Options

Fig. 3: User performs the dynamic operations.

The figure 3 describes user performing the dynamic operations such as data update, delete and append.

6. *Multiple Batch Auditing*

TPA may concurrently handle multiple auditing delegations upon different users' requests. It is a difficult and tedious task for an individual. Given K auditing delegations on K distinct data files from K different users, it is more advantageous for TPA to batch these multiple tasks together and audit at one time [5]. We also propose the technique of bilinear aggregate signature, which at a time can support the aggregation of multiple signatures by distinct signer for aggregating distinct messages into a single signature and thus provides efficient verification for the authenticity of all messages. We can now aggregate K verification equations into one equation by using the Signature aggregation and bilinear properties and thus the concurrent auditing of multiple tasks can be achieved.

7. *Multiple Batch Auditing Using Block-Level Operations*

We enhance the scheme with explicitly and efficiently handle dynamic data operations public auditing system of data storage security in Cloud Computing. For a user to perform few block-level operations such as update, append and delete the data blocks from a data file while the maintaining the data storage assurance is by downloading all the data from the cloud servers and re-computed the whole parity blocks as well as the verification tokens. And also check the integrity of outsourced data whenever needed. This proposed work studies the problem of ensuring the integrity of data storage in Cloud computing. We take account of the task of allowing a third party auditor (TPA), on behalf of the cloud client, to validate the integrity of the dynamic data stored in the cloud servers. We utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system. It supports scalable and efficient public auditing in the Cloud Computing.

The technique of signature and scheduling policies is used to achieve batch auditing, where the Third party Auditor (TPA) can perform multiple auditing tasks at one time. The data in the cloud is dynamic and it does not remain static now.

Unlike most prior works, the new scheme further supports secure and efficient dynamic operations on data blocks stored in the cloud, including: data update, delete and append.

IV. CONCLUSION

The public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, it considers the task of allowing a third party auditor (TPA) verifies the integrity of the dynamic data on behalf of the cloud client. It utilizes and uniquely combines the key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system and thus support an d efficient public auditing in the Cloud.

REFERENCES

[1] A. L. Ferrara, M. Greeny, S.Hohenberger, M. Pedersen (2009), "Practical short signature batch verification", in proceedings of CT-RSA, volume 5473 of LNCS. Springer- Verlag, pp. 309–324.

[2] Cong Wang, Qian Wang, KuiRen, Wenjing Lou (2010),"Privacy Preserving Public Auditing for Data Storage Security in Cloud Computing".

[3] M.A.Shah, R.Swaminathan, M. Baker (2008), "Privacy preserving audit and extraction of digital contents", Cryptology ePrint Archive.

[4] [Online] Available: Amazon.com, "Amazon s3 availability event: (2008)," Online at http://status.aws.amazon.com/ s3-20080720.html.

[5] P. Mell, T. Grance, (2009) "Draft nits working definition of cloud computing," Referenced on June 3rd 2009 Onli