ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Survey on Enabling Privacy for Secure Cloud Storage by Batch Auditing

Alluri Uday Kumar[*1], Rajeev Bilagi[2]

[*1] M.tech Computer Science, [2]Associate Professor, Sapthagiri College of Engineering, Bangalore, India

udaysce01@gmail.com

Abstract

The Cloud computing is a newest technology which Provides various services through internet. Where users can remotely store their data into the cloud, User can upload their data on cloud and can access those data anytime anywhere without any additional burden. The User doesn't have to worry about storage and maintenance of cloud data. But as data is stored at the remote place how users will get the confirmation about stored data. Hence Cloud data storage should have some mechanism which will specify storage correctness and integrity of data stored on a cloud. Thus, enabling public Auditability for cloud data storage security is of critical importance so that users can resort to an external audit party Third Party Auditor (TPA) to check the integrity of outsourced data when needed. Here the TPA can perform batch auditing, handling multiple audit on a single time so it reduces computation overhead. The Technique of bilinear aggregate signature is used to achieve batch auditing .The public key based homomorphic authenticator and uniquely integrate it with random mask technique to enable privacy for cloud data storage.

Keywords: TPA,CSP, Privacy, Batch Auditing.

Introduction

Cloud computing has been envisioned as the next-generation information technology (IT)architecture for enterprises, Due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location in-dependent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. Cloud computing is used by many IT industries now a days as a new technology. It also gives flexibility to the user, no need to manage the information stored in cloud storage, whenever user puts their data in the cloud it allows user to access all applications and document from anywhere in the world.

While Cloud makes all these advantages, it brings some security threats towards user's data. Cloud Service Provider (CSP) are separate entities, data outsourcing is actually relinquishining user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, since the infrastructure are much more powerful and reliable then personal computing devices, they are still facing both internal and external threats for data integrity [1,2].Secondly, there exist some motivations were CSP behave unfaithfully towards the users regarding the status of their data on the cloud. For Examples, CSP by discarding the data that has not been accessed rarely [3].Outsourcing data to the cloud is more attractive economically for long-term large-scale data storage, it does offer immediately any guarantee on data integrity and availability. It has to be addressed properly, If not then it will impede the successful deployment of the cloud architecture.

To ensure Data security protection traditional cryptographic primitives cannot be adopted directly .For integrity verification simply downloading all the data is not an effective solution due to the expensiveness in input output and transmission cost across the network [4].Moreover, the over head of using cloud storage should be minimized, such that user does not need to perform too many operations to use the data. For Easier management, it is desirable that the cloud server only entertains verification request from a single designated party. To ensure the integrity and to save the users online burden ,it is of critical importance to enable public auditing for cloud data storage , so the user resort to independent third party auditor (TPA) to audit the outsourced data whenever needed. The (TPA) will check integrity of all the data stored in the cloud on behalf of users, provides an easy way for users to ensure the correctness of their storage. Cloud service providers

ISSN: 2277-9655
Impact Factor: 1.852

are more beneficial from the audit results of TPA to improve their cloud based service platform.

To ensure data integrity, recently public checking has been proposed, which allows an external party to verify the correctness of remotely stored .However many schemes [5][6] do not consider privacy protection of users data against external auditors which reveal user data information to the auditors. To protect privacy, the users, who own the data, rely on TPA for storage security of their data, they do not want this auditing process to introduce new vulnerabilities of unauthorized leakage of data towards their data security [7].Before outsourcing data the data has to be encrypted to mitigate privacy of data. To address these problems, this approach utilizes the technique of public key based homomorphic linear authenticator (HLA), which allows TPA to perform the auditing without demanding local copy of data and thus it reduces communication and computation overhead as compared with other approaches. Also HLA is integrated with random masking, the protocol ensures that TPA could not learn anything about the content of the data stored in the cloud server during the auditing process.

Related Work

G.Ateniese et al. [5] are the first to consider public auditability in their defined ―provable data possession‖ (PDP) model for ensuring possession of data files on untrusted storages. It allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. This scheme utilizes the RSA-based homomorphic authenticators for auditing outsourced data and suggests randomly sampling a few blocks of the file. However, the public auditability in this scheme demands the linear combination of sampled blocks exposed to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the auditor.

M. A. Shah, [6] propose allow a TPA to keep online storage honest by first encrypting the data then sending a number of pre-computed symmetric-keyed hashes over the encrypted data to the auditor. The auditor verifies both the integrity of the data file and the server's possession of a previously committed decryption key. The auditor verifies both the integrity of the data file and the server's possession of a previously committed decryption key. This scheme works only for encrypted files and the auditor has to keep state, and suffers from restricted usage, when keyed hashes are used this scheme potentially brings in online burden to users.

Q. Wang et al. [7] propose to combine BLS based homomorphic authenticator with MHT(Merkle Hash Tree) to support both public auditability and fully data dynamics, simultaneously.

A. Jules [8] to assure possession and Retrievability this approach make use of spot-checking and error correcting codes. But this model works only with encrypted data. Some advanced versions of PoR protocols had been proposed in order to guarantees private auditability and these protocols make use of Boneh–Lynn–Shacham (BLS) signatures. But these protocols were not privacy-preserving. Although they describe a straight forward Merkle-tree construction for public PoRs, this approach only works with encrypted data. To preserve online storage secure then comes the TPA based approach. This scheme works only for encrypted files and the auditor has to keep state, and suffers from restricted usage, when keyed hashes are used this scheme potentially brings in online burden to users.

C. Erway [9] developed a skip lists based scheme to enable provable data possession with full dynamics support. However, the verification in these two protocols requires the linear combination of sampled blocks, and thus does not support privacy preserving auditing. While all the above schemes provide methods for efficient auditing and provable assurance on the correctness of remotely stored data, none of them meet all the requirements for privacy preserving public auditing in cloud computing. More importantly, none of these schemes consider batch auditing, which can greatly reduce the computation cost on the TPA when coping with a large number of audit delegations.

C.Wang [10] in this approach a partially dynamic version of the prior PDP scheme, using only symmetric key cryptography but with a bounded number of audits.

Qian Wang [11] in this model the problem is generalized so that the client finds an efficient way to perform periodical integrity verifications without the local copy of data files. If any two users or more users are using a data, one is writing a data while one is reading a data than it may be wrong read by 1 user, so to resolve data inconsistency is become an important task of the data owner and another problem how to trust on TPA is not calculated. If TPA become intruder and pass information of data or deleting a data than how owner know about this problem are not solved that is Integrity and consistency.

ISSN: 2277-9655
Impact Factor: 1.852

Govinda V [12] in this the third party auditor ensures data integrity over out sourced data and proposed digital signature method to protect the privacy and integrity and integrity of outsourced data in cloud environment. TPA check the integrity of data on cloud on the behalf of users, in this solve the previous problem in Enabling public verifiability and data dynamics for storage security in cloud computing and privacy-preserving audit and extraction of digital contents. They generally cannot help recovery for two reasons. First, as mismatch between the stored value and computed value of checksums just means that one of them was modified, but it does not provide information about which of them is legitimate. Stored checksums are also likely to be modified or corrupted. Second, checksums are generally computed using a one-way hash function and data cannot be reconstructed given a checksum value.

Existing System

To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user;
2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.
Problems Associated With existing system are:

- It does offer any guarantee on data integrity and availability to the outsourced on cloud.
- It is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those unaccessed data and might be too late to recover the data loss or damage.
- It does not support batch Auditing.

Proposed System

The figure 1 below represents system model
USER:

An entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations.

CLOUD STORAGE SERVER (CSS):

An entity, which is managed by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain the clients' data.
Advantages of Cloud Storage

- Usability: All cloud storage services have desktop folders for PC's. This allows users to drag and drop files between cloud storage and their local storage.
- Bandwidth: Avoid emailing files to individuals and instead send a web link to recipients through email.
- Accessibility: Stored files can be accessed from anywhere via Internet connection
- Disaster Recovery: It is highly recommended that businesses have an emergency back-up plan ready in the case of an emergency. Cloud storage can be used as a back-up plan by businesses by providing a second copy of important files. These files are stored at a remote location and can be accessed through an internet connection.
- Cost Savings: Businesses and organizations can often reduce annual operating costs by using cloud storage.cloud storage costs about 3 cents per gigabyte to store data internally. Users can see additional cost savings because it does not require internal power to store information remotely.

THIRD PARTY AUDITOR (TPA):

An entity, which 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. Consider the existence of a semi-trusted CS as does. Namely, in most of time it behaves properly and does not deviate from the prescribed protocol execution. However, during providing the cloud data storage based services, for their own benefits the CS might neglect to keep or deliberately delete rarely accessed data files which belong to ordinary cloud users. Moreover, the CS may decide to hide the data corruptions caused by server hacks or Byzantine failures to maintain reputation.
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. Communicate over a computer network on separate hardware, but both client and server may reside in the same system. A server machine is a host that is running one or more server programs which share their resources with clients. A client does not share any of

ISSN: 2277-9655
Impact Factor: 1.852

its resources, but requests a server's content or service function. Clients therefore initiate communication sessions with servers which await incoming requests. Third Party Auditor is kind of inspector. There are two categories: private auditability and public auditability. Although private auditability can achieve higher efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would help owners to evaluate the risk of their subscribed cloud data services, and it will also be beneficial to the cloud service provider to improve their cloud based service platform. Hence TPA will help data owner to make sure that his data are safe in the cloud and management of data will be easy and less burdening to data owner.

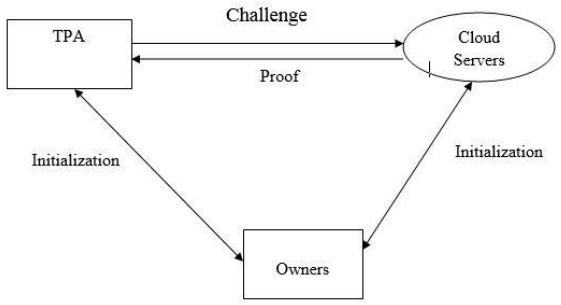

Fig 1. Proposed System

There are four algorithms which can be used in a public auditing scheme (KeyGeneration, SigGeneration, GenrateProof, and VeriProof).

- KeyGeneration: the key generation algorithm that is run by the user to setup the scheme.
- SigGeneration: used by the user to generate verification metadata, this may consist of MAC, signatures or other information used for auditing.
- GenrateProof: run by the cloud server to generate a proof of data storage correctness.
- VeriProof: run by the TPA to audit the proof from the cloud server.

Conclusion

In this paper, a discussion on various approaches for Enabling Privacy for cloud data storage by batch auditing. Cloud computing security is a major issue that needs to be considered. Using TPA, to verify the correctness and integrity of data stored on a cloud. It uses public key based homomorphic linear authentication (HLA) protocol with random masking to enable privacy, it achieved zero knowledge privacy through random masking technique. It supports batch auditing where TPA will handle multiple users request at the same time which reduces communication and computation overhead. It uses bilinear signature to achieve batch auditing. Here Enabling Privacy for cloud storage by batch auditing has been introduced with bilinear aggregate signature for secure cloud Storage.

Reference

[1] *M. Arrington, "Gmail disaster: Reports of mass email deletions," Online at http://www.techcrunch.com/2006/12/28/gmail-disasterreports-of-mass-email-deletions/*

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

[3] *G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,Z. Peterson, and D. Song, "Provable data possession at untrustedstores," in Proc. of CCS'07, Alexandria, VA, October2007, pp. 598–609.*

[4] *A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October2007, pp. 584–597.*

[5] *G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson and D. Song, "Provable data possession at untrusted stores," in Proc. of CCS'07, 2007, pp. 598–609.*

[6] *M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.*

[7] *Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, ―Enabling public verifiability and data dynamics for storage security in cloud computing,‖ in Proc. of ESORICS'09,Saint Malo, France, Sep. 2009.*

[8] *A. Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for large files," in Proc. of CCS'07, October 2007, pp. 584–597.*

[9] *C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic provable data ossession," in Proc. of CCS'09, 2009, pp. 213–222.*

ISSN: 2277-9655
Impact Factor: 1.852

[10] *C. Wang, K. Ren, W. Lou, and J. Li, "Towards publicly auditable secure cloud data storage services," IEEE Network Magazine, vol. 24, no. 4, pp. 19–24, 2010.*

[11] *Qian Wang and Cong Wang and Kui Ren, Wenjing Lou, Jin Li "Enabling Public Auditability And Data Dynamics For Storage Security in Cloud Computing" in IEEE transactions on parallel and distributed systems, 2011, vol. 22, no. 5.*

[12] *Govinda V, and Gurunathaprasad, H Sathshkumar,"Third Party Auditing For Security Data Storage in cloud through digital signature using RSA" IJASATR, 2012, issue 2,vol-4, Issn 2249-9954.*