Privacy Preserving Audit Of Data Storage In Cloud

G. Pravallika ¹, P. Chakradhar², A. Rajyalakshmi³, Ch. Anil Babu⁴

¹#1 M.TECH Scholar, RCEC, Eluru
²#3 M.TECH Scholar, VEC, Kavali
³#2 Associate Professor, RCEC, Eluru
⁴#4 Associate Professor, RISE, Ongole

ABSTRACT:

Cloud computing is the deliverance of computing as a service rather than a product. It gives shared resources, information to computers, softwares and other devices over a set of connections. Cloud computing is the extended vision of computing as a service, where data owners can tenuously store their data in the cloud to enjoy on-demand high-quality applications and services from a public pool of configurable total resources. While data outsourcing mitigates the owners of the load of local data storage and preservation, it also reduces their physical control of storage dependability and security, which conventionally has been expected by both enterprises and individuals with high service-level requirements. In order to make possible quick use of cloud data storage service and get back security declarations with outsourced data reliability, well-organized methods that facilitate on-demand data accuracy verification on behalf of cloud data holders have to be designed. The proposed technique publicly auditable cloud data storage is capable to help this emerging cloud economy become fully recognized. With public audit ability, a trusted person with proficiency and abilities data owners do not acquire can be delegated as an outside audit party to review the risk of outsourced data when required. Such an auditing service not only assists save data owners’ computation resources but also provides a apparent yet cost-effective method for data owners to gain trust in the cloud. We describe move toward and system necessities that should be brought into thought, and the challenges that need to be resolved for such publicly auditable secure cloud storage service to become a reality.

Index Terms: Multiparty access control, Social network, Policy specification and management,

1. INTRODUCTION

Cloud computing has been imagined as the next generation architecture of the IT enterprise due to its long list of extraordinary advantages in IT: on demand self-service, everywhere network access, rapid resource elasticity, location independent resource pooling, usage-based pricing, and transference of risk. One fundamental feature of this new computing model is that data is being centralized or outsourced into the cloud. From the data owner’s perspective, including both individuals and IT enterprises, storing data distantly in a cloud in a flexible on-demand manner brings appealing benefits: assistance of the burden of storage management, universal data access with autonomous geographical locations, and prevention of capital expenditure on software, hardware, personnel maintenance etc. While cloud computing makes these advantages more attractive than ever, it also takes new and challenging security threats to the outsourced data. So cloud services providers (CSP) are taken apart administrative entities, data outsourcing actually give up the owner’s very important control over the fortune of their data. As a consequence, the correctness of the data in the cloud is put at risk due to the following reasons.
Although the infrastructures beneath the cloud are much more authoritative and dependable than personal computing devices, they still face a wide range of both external and internal threats to data integrity. Outages and security violations of significant cloud services become visible from time to time. Amazon S3’s current Downtime, Gmail’s mass email deletion incident, and Apple Mobile Me’s post-launch downtime are all such examples.

Second, for benefits of their own, there are various incentives for Cloud Service Providers to perform unfaithfully toward cloud customers concerning the status of their outsourced information. That include Cloud Service Providers, for economic reasons, reclaiming storage by removal data that has not been or is rarely accessed or even thrashing data loss incidents to preserve a standing.

Data owners no longer physically possess the storage of their data; conventional cryptographic primitives for the purpose of data security protection cannot be directly adopted. Simply downloading the data for its reliability authentication is not a practical solution due to the high cost of input and output and broadcast transversely the network. Besides, it is often inadequate to distinguish data corruption only when accessing the data, as it does not give correctness guarantee for un accessed data and might be too late to recover the data loss or damage. Assuming the large size of the outsourced data and the owner’s constrained resource ability, the tasks of auditing the data correctness in a cloud environment can be frightening and expensive for data owners. In addition from the system usability point of view, data owners should be capable to just use cloud storage as if it is local, without disturbing about the need to verify its integrity. So to fully ensure data security and save data owners’ computation resources, we suggest enabling publicly auditable cloud storage services, where data owners can alternative to an external third party auditor (TPA) to verify the outsourced data when needed. Third party auditing presents a crystal clear yet cost-effective method for establishing trust among data owner and cloud server. Based on the audit result from a TPA, the unconfinned audit report would not only help owners to evaluate the risk of their subscribed cloud data services, but also be helpful for the cloud service supplier to improve their cloud based service platform. Enabling public risk auditing protocols will play a significant role for this nascent cloud economy to become fully recognized; where data owners will need ways to assess risk and gain trust in the cloud.
development of public audit ability for existing cloud data storage services. The data owners are currently not complicated enough to demand risk evaluation; on the other hand, existing commercial cloud vendors do not offer such a third party auditing interface to support a public auditing service. This object is intended as a call for action, aiming to inspire further research on reliable cloud storage services and enable public auditing services to become a authenticity. We start by suggestive of a set of systematically and cryptographically desirable properties that should apply to practical consumption for securing the cloud storage on behalf of data owners. A set of building blocks, including recently developed cryptographic primitives to ensure these strong security properties, which could appearance the basis of a publicly auditable secure cloud data storage system.

2. CLOUD STORAGE ARCHITECTURE AND SECURITY THREATS

2.1. Problem Statement

The architecture consists of four different entities: data owner, user, cloud server (CS), and TPA. Here the Third Party Auditor is the trusted entity that has expertise and capabilities to assess cloud storage security on behalf of a data owner upon demand. Under the cloud model, the data owner may represent either the individual or the endeavor customer, who relies on the cloud server for remote data storage and preservation, and thus is relieved of the load of building and maintaining local storage communications. Some cases cloud data storage services also provide benefits like relative low cost, availability and on demand sharing among a group of trusted users, such as partners in a collaboration team or human resources in the enterprise organization. For effortlessness, we suppose a single writer or many readers scenario applied. Only the data owner can dynamically interact with the CS to update her stored data, while users just have the dispensation of file reading. As the data owner no longer possesses physical control of the data, it is of critical importance to permit the data owner to verify that his data is being correctly stored and maintained in the cloud. Assuming the probably large cost in terms of resources and expertise, the data owner may remedy to a TPA for the data auditing task to ensure the storage security of her data, while hoping to keep the data private from the TPA. We suppose the TPA, who is in the dealing of auditing, is reliable and independent, and has no incentive to scheme with either the CS or the owners during the auditing process. The TPA should be able to efficiently audit the cloud data storage space without local copy of information and without any additional online burden for data owners. Besides, any possible leakage of an owner’s outsourced data toward a TPA through the auditing protocol should be forbidden.

3. DESIRABLE PROPERTIES FOR PUBLIC AUDITING

To enable public auditing for cloud data storage to become a reality and the whole service architecture design should not only be cryptographically well-built, but, more important, be practical from a systematic point of view. We briefly sophisticated a set of suggested desirable properties below that satisfy such a design principle. The in-depth analysis is discussed in the next section. Note that these necessities are ideal goals. They are not necessarily complete yet or even fully achievable in the current stage.

Minimize Auditing Overhead: The overhead imposed on the cloud server by the auditing process must not outweigh its benefits. Such overhead may contain both the I/O cost for data access and the bandwidth cost for data transfer. Any extra online burden on a data owner should also be as low as possible. Ideally, after auditing delegation, the data owner should just enjoy the cloud storage service while being worry free about storage auditing correctness.

Protect Data Privacy: Data privacy protection has forever been an important feature of a service level agreement for cloud storage services. The implementation of a public auditing protocol should not violate the owner’s data privacy. In
another words a TPA should be able to capably audit the cloud data storage without demanding a local copy of data records or even learn the data content.

**Support Data Dynamics:** As a cloud storage service is not just a data warehouse, owners are subject to dynamically updating their data via various application purposes. The design of auditing protocol should incorporate this essential feature of data dynamics in Cloud Computing.

**Support Batch Auditing:** The prevalence of large-scale cloud storage service further demands auditing effectiveness. When receiving multiple auditing mechanisms from different owners’ delegations, a TPA should still be intelligent to handle them in a fast yet cost-effective fashion. This property could essentially enable the scalability of a public auditing service even under a storage cloud with a large number of data owners.

4. **ENSURING CLOUD DATA SECURITY**

Traditional Methods Revisited An easy approach to protect the data integrity would be using conventional cryptographic methods, such as the well-known Message Authentication Codes (MACs). Initially, data owners can locally maintain a small amount of Message Authentication Codes for the data files to be outsourced. Every time the data owner needs to retrieve the file, she can verify the integrity by recalculating the Message Authentication Code of the received data file and comparing it to the locally precomputed value. If the data file is large, a hash tree can be employed, where the leaves are hashes of data blocks and internal nodes are hashes of their children of the tree. The data owner only needs to store the root hash of the tree to authenticate his received data. To avoid retrieving data from the cloud server, a simple improvement to this simple solution can be performed as follows: Before data outsourcing, the owner chooses a set of random MAC keys, precomputed the MACs for the whole data file, and publishes these verification metadata to the TPA. The TPA can each time reveal a secret MAC key to the cloud server and ask for a fresh keyed MAC for comparison. In this way the bandwidth cost for each audit is only at the bit-length level (keys and MACs). Though, a particular drawback is that the number of times a data file can be audited is limited by the number of secret keys that must be fixed a priori, which might introduce an additional online burden to the data owner: Once all possible secret keys are exhausted, the data owner then has to retrieve data from the server in order to recomputed and republish new MACs to the TPA.

![Fig.3: Secure Audit System Architecture](image)

4.1. **Utilizing Homomorphic Authenticators**

To significantly reduce the arbitrarily large communication overhead for public audit ability without introducing any online burden on the data owner, we resort to the homomorphic authenticator technique. Homomorphic authenticators are unforgivable metadata generated from individual data blocks, which can be securely aggregated in such a way to assure a verifier that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator.

4.2. **Protecting Data Privacy**

The reason that linear combination of sampled blocks may potentially expose owner
data information is due to the following fact about basic linear algebra theory: if enough linear grouping of the same blocks are collected, the TPA can simply derive the sampled data content by solving a system of linear equations.

5. CONCLUSION

Cloud computing has been imagined as the next-generation architecture of enterprise IT. In dissimilarity to traditional enterprise IT solutions, where the IT services are under appropriate physical, logical, and personnel controls, cloud computing move about the application software and databases to servers in big data centers on the Internet, where the management of the information and services are not completely dependable. This unique feature raises many new security challenges in areas such as software and data recovery, security, and privacy, as well as legal issues in areas such as regulatory compliance and auditing, all of which have not been implicit. Here focus on cloud data storage security. We first present network architecture for efficiently describing, developing, and evaluating secure data storage problems. We then propose a set of steadily and cryptographically desirable properties for public auditing services of dependable cloud data storage security to turn into dependability. Through in-depth analysis, some existing data storage security building blocks are scrutinized.

6. REFERENCES


Mrs. G. Pravallika pursuing M.Tech CSE in Ramachandra College of Engineering, Eluru under JNTU Kakinada University.

Mr. P. Chakradhar working as Associate Professor in Ramachandra College of Engineering, Eluru. He received M.Tech degree in CSE from Acharya Nagarjuna University.

Mrs. A. Rajyalakshmi pursuing M.Tech CSE in Visvodaya Engineering College, Kavali under JNTU Anantapur University,