ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Privacy inPublic Auditing for Secure Cloud Storage

[I]P.Nagajothi, [II]Mr. R.Baskar
[I]Assistant Professor/CSE Department, K.S.Rangasamy College of Technology, India
[II]PG Student, K.S.Rangasamy College of Technology, Tiruchengode, India

Abstract
Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection.cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. To further extend the result to enable the TPA to perform audits for multiple users simultaneously and efficiently.

Keywords
TPA.Constrained,Arbitration,Delegation,Lightweight,Aggravation

I. 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 independent resource pooling, rapid resource elasticity, usage-based pricing and transfer- ence of risk [2]. While cloud computing makes these advantages more appealing than ever, it also brings new and challenging security threats toward users' outsourced data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing 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, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity [4]. Examples of outages and security breaches of noteworthy cloud services appear from time to time [5], [6], [7].In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. Besides, 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.

Considering the large size of the outsourced data and the user's constrained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for the cloud users [2]. Moreover, the overhead of using cloud storage should be minimized as much as possible, such that a user does not need to perform too many operations to use the data (in additional to retrieving the data). In particular, users may not want to go through the complexity in verifying the data integrity. Besides, there may be more than one user accesses the same cloud storage, say in an enterprise setting. For easier management, it is desirable that cloud only entertains verification request from a single designated party. Data storage, so that users may resort to an independent third-party auditor (TPA) to audit the outsourced data when needed. The TPA, who has expertise and capabilities that users do not, can periodically check the integrity of all the data stored in the cloud on behalf to ensure their storage correctness in the cloud. Moreover, in addition to help users to evaluate the risk of their subscribed cloud data services, the audit result from TPA would also be beneficial for the cloud service providers to improve their cloud-based service platform, and even serve for indepen- dent arbitration purposes. In a word, enabling public auditing services will play an important role for this nascent cloud economy to become fully established, where users will need ways to assess risk and gain trust in the cloud..

To the best of knowledge, scheme is the first to support scalable and efficient privacy-preserving public storage auditing in cloud. Specifically, scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner.

To Prove the security and justify the performance of proposed schemes through concrete experiments and comparisons with the state of the art. The rest of the paper is organized as follows:Itintroduces the system and threat model, and design goals.

II. Problem Statement

The System and Threat Model storage service involving three different entities, as illustrate the cloud user, who has large amount of data files to be stored in the cloud; the cloud server, which is managed by the cloud service provider to provide data storage service and has significant storage

1. Public auditability: to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users.
2. Storage correctness: to ensure that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users' data intact.
3. Privacy preserving: to ensure that the TPA cannot derive users' data content from the information collected during the auditing process.
4. Batch auditing: to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously.
5. Lightweight: to allow TPA to perform auditing with minimum

communication and computation overhead.

III. The Proposed Schemes

Public auditing scheme which provides a complete outsourcing solution of data—not only the data itself, but also its integrity checking. After introducing notations and brief preliminaries, To start from an overview of public auditing system and discuss two straightforward schemes and their demerits. Then, present main scheme and show how to extent main scheme to support batch auditing for the TPA upon delegations from multiple users.

Parameters of the system by executing KeyGen, and preprocesses the data file F by using SigGen to generate the verification metadata. The user then stores the data file F and the verification metadata at the cloud server, and deletes its local copy. As part of preprocessing, the user may alter the data file by expanding it or including additional metadata to be stored at 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 a response message by executing Gen Proof using F and its verification metadata as inputs. The TPA then verifies the response via Verify Proof. framework assumes that the TPA is stateless, i.e., TPA does not need to maintain and update state between audits, which is a desirable property especially in the public auditing system [1]. Note that it is easy to extend the framework above to capture a stateful auditing system, essentially by splitting the verification metadata into two parts which are stored by the TPA and the cloud server, respectively. Design does not assume any additional property on the data file. If the user wants to have more error resilience, he can first redundantly encodes the data file and then uses system with the data that has error- correcting codes integrated.

IV. Evaluation

Security Analysis evaluate the security of the proposed scheme by analyzing its fulfillment of the security guarantee described in namely, the storage correctness and privacy- preserving property. To start from the single user case, where main result is originated. Then, to show the security guarantee of batch auditing for the TPA in multiuser setting.

Storage Correctness Guarantee :To prove that the cloud server cannot generate valid response for the TPA without faithfully storing the data, If the cloud server passes the Audit phase, it must indeed possess the specified data intact as it is. Proof. To show that there exists an extractor of in the random oracle model. With valid theorem follows from.

Suppose that extractor can rewind a cloud server in the execution of the protocol to the point just before the challenge his given. Now, the extractor sets

The result shows that even when the number of invalid responses exceeds 18 percent of the total batch size, the performance of batch auditing can still be safely concluded as more preferable than the straightforward individual auditing. Note that the random distribution of invalid responses within the collection is nearly the worst case for batch auditing. If invalid responses are grouped together, even better results can be expected.

V. Conclusion

Proposing and bricking privacy-preserving public auditing system for data storage security in cloud comput- ing. It 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, further extend privacy-preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that schemes are provably secure and highly efficient.Thepreliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of design on both the cloud and the auditor side.

References

[1] *QinLiu, Chiu C. Tan, Jie Wu and Fellow (2013) "Privacy in public auditing for secure cloud storage" IEEE Transactions On Parallel and Distributed Systems, Vol 20, No.10, pp-1-11.*

[2] *Michael Mitzenmacher(2012) "Compressed Bloom Filters" IEEE Transactions on networking,Vol 10, No.5, pp-604-612.*

[3] *JunbeomHur(2013) "Improving Security and Efficiency in Attribute-Based Data Sharing" IEEE Transactions On Knowledge And Data Engineering, Vol 25, No.10, pp-2271-2282.*

[4] *Fang Hao, MuraliKodialam, T. V. Lakshman and Haoyu Song(2012) "Fast Dynamic Multiple-Set Membership Testing Using Combinatorial Bloom Filters" IEEE Transactions on networking,Vol 20, No.1, pp-295-304.*

[5] *Xun Yi, Elisa Bertino, JaideepVaidya, and Chaoping Xing "Private Searching on Streaming Data Based on Keyword Frequency" IEEE Transactions On Depedable And Secure Computing" Vol 20, No.5, pp-1-14.*

[6] *Shucheng Yu, Cong Wang, KuiRen† and Wenjing Lou "Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing" IEEE Transactions On Parallel and Distributed Systems, Vol 20, No.8, pp-1-9.*

[7] *Ning Cao, Cong Wang, Ming Liy, KuiRen and Wenjing Lou "Privacy-Preserving Multi-keyword Ranked Search over Encrypted Cloud Data" IEEE Transactions On Parallel and Distributed Systems, Vol 20, No.10, pp-1-11.*