

Privacy Preserving Public Auditing in Secured Cloud Storage



Computer Science

KEYWORDS : Third party Auditor(TPA),Block Authentication Code (BAC),Cloud Computing

Mr.V.Sajeev

Department of Computer Science and Engineering,Nehru Institute of Technology,Coimbatore

Mrs.R.Gowthamani

Department of Computer Science and Engineering,Nehru Institute of Technology,Coimbatore

ABSTRACT

Cloud computing is the long dreamed vision where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, the burden of local data storage and maintenance can be relieved from users. Thus, enabling public audit ability 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. To 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 separate copy of data as local, 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. In this paper we propose a system of auditing using BAC(Block Authentication Code)

1. INTRODUCTION

Several trends are opening up the era of Cloud Computing, is an Internet-based development and use of computer technology. The more powerful processors, together with the software as service(SaaS) computing architecture, are transforming different data centers into pools of computing service. The increasing network bandwidth and reliable, flexible network connections make it possible that users can subscribe high quality services from data and software that reside exclusively on remote data centers. Moving data into cloud offers great convenience to users since they don't have to care about the complexities of hardware management. Data to be stored remotely into the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, data access with geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc

While these advantages of using clouds are unarguable, due to the opaqueness of the Cloud—as separate administrative entities, the internal operational details of cloud service providers (CSP) may not be known by users. The correctness of the data which is using in the cloud is being put at risk due to the different stated reasons. First of all, although infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing lot of both internal and external threats for data integrity. Secondly, for the benefits of its own, there exist various motivations for cloud service providers to behave unfaithfully towards the cloud users regarding the status of their outsourced data. Examples are cloud service providers, for monetary reasons, reclaiming the storage by discarding data that has not been or rarely accessed, or even hiding data loss of incidents so as to maintain a reputation. To enable privacy-preserving public auditing for cloud data storage under the previously mentioned model, our protocol design should have to achieve the following security and performance guarantee

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 on-line burden to the cloud users.

Storage correctness: This ensures that there exists no cheating cloud server that can pass the audit from TPA without indeed storing user's data intact.

Privacy-preserving: to ensure that there exists no way for TPA to derive user's data content from the information collected during the auditing process.

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.

Lightweight: to allow TPA to perform auditing with minimum communication and computation overhead.

Considering the large size of the outsourced data and the user's constrained resource capability, the ability to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users. Therefore, to fully ensure the data security and save the cloud user's computation resources, it is of utmost importance to enable public auditability for cloud data storage so that the users may route to a third party auditor (TPA), who has expertise and capabilities that the users do not, audit the outsourced data when needed. To provide the public auditing system of data storage security in Cloud Computing and provide a privacy preserving auditing protocol, i.e., this scheme supports an external auditor to audit user's outsourced data in the cloud without learning knowledge on the data content.

To the best of our knowledge, our scheme is the first to support scalable and 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.

We prove the security and we justify the performance of our proposed schemes through concrete experiments and comparisons with the state-of-the-art.

2. ARCHITECTURE

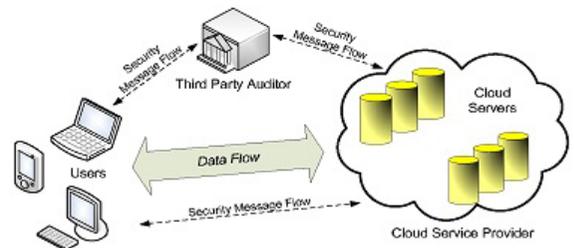


Fig1: Architecture of cloud data storage.

3. RELATED WORK

Ensuring Data Storage Security in Cloud Computing(Cong Wang, Qian Wang, and Kui Ren)

Several security challenges in ensuring data storage security in large cloud systems

Privacy Preserving Auditing and Extraction of Digital Contents(Mehul A. Shah, Ram Swaminathan, Mary Baker)

Several protocols are presented that allow third party auditor to periodically verify the data stored by a service and assist in returning data intact to the customer.

Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing(Qian Wang, Cong Wang, Jin Li, Kui Ren, and Wenjing Lou)

The Merkle Hash Tree Algorithm is used for the auditing.

4. PROPOSED MODEL

We propose a BAC (Block Authentication Code) for data transparent. It will overcome the existing system. That is BAC is generating the authentication code and data block is called as authentication unit. Working flow of data is: At the sender side, the authentication information BAC is generated based on a selected hash function with the packet content and a commonly agreed key as the input. Based on the value of each bit (0/1) of BAC, some packets are scheduled to be sent out with additional delays. At the receiver side, the receiver extracts the embedded BAC based on the relative packet delay and compares the extracted BAC with the BAC generated based on the received content for authentication. The following schemes are proceed in our proposed system. They are, BAC generation, BAC embedding/ BAC extraction and BAC authentication.

5. PROPOSED ALGORITHM:

To present our scheme, we use the following notations:

1. The stream packets are clustered to blocks, denoted as block[i], with b packets in each block, where $0 < i < \lfloor \text{total packet number} / b \rfloor$. Padding is used when necessary to generate the last block.
2. The length (in terms of bits) of the BAC for each data block is n.
3. A hash function, denoted as $H(X)$, is a one-way hash, using an algorithm such as MD5 or SHA .
4. X,Y represent the concatenation of X with Y.
5. A secret key k is only known to the communicating parties.
6. The origin of the data stream can be identified by a flag, which is f bits, where $0 \leq f \leq n$.

ADVANTAGES OF PROPOSED MODEL

- Resource sharing is considered for data transmission.
- High security level.
- Batch Auditing can be performed.

6. SYSTEM DESIGN

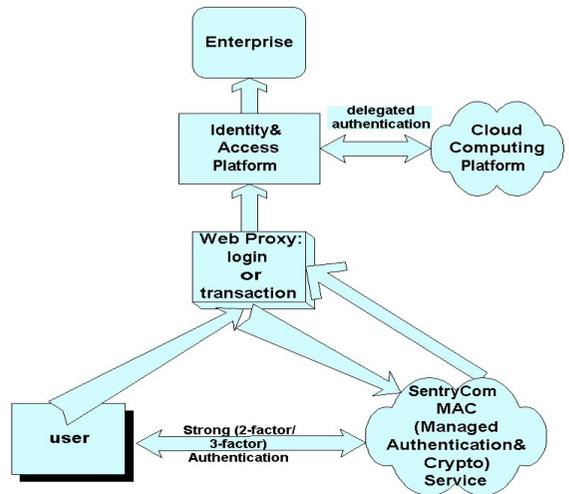


Fig 2: System Design

7. RESULT AND ANALYSIS

The auditing using BAC increases the security level of the system. The TPA can perform auditing without demanding the local copy of the data. Also the batch auditing is also possible.

8. CONCLUSION

In this paper, we propose a privacy-preserving public auditing system for data storage security in Cloud Computing, where TPA can perform the storage auditing without demanding the local copy of data. We utilize the BAC authentication code generator. Using data blocks, authentication procedure is done and reduces the time delay. We further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple auditing tasks in a batch manner, i.e., simultaneously. Extensive security and performance analysis shows that the proposed schemes are provably secure and highly efficient. We believe all these advantages of the proposed schemes will shed light on economies of scale for Cloud Computing.

REFERENCE

The main references are international journals and proceedings. All references should be to the most pertinent and up-to-date sources. References are written in Vancouver style. Please use a consistent format for references – see examples below: || [1] H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in Proc. of NDSS'01, 2001 | . || [2] P. D. McDaniel and A. Prakash, "Methods and limitations of security policy reconciliation," in Proc. of SP'02, 2002 | || [3] J. Anderson, "Computer Security Technology Planning Study," Air Force Electronic Systems Division, Report ESD-TR-73-51, 1972, <http://seclab.cs.ucdavis.edu/projects/history/>. || [4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Scalable secure file sharing on untrusted storage," in Proc. of FAST'03, 2003. || [5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. of NDSS'03, 2003. || [6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. of NDSS'05, 2005. 2006.