ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

DATA DYNAMICS USED FOR STORAGE SPACE IN CLOUD COMPUTING

Mrs.K.Geetha[1], Dr. Ananthi Sheshasayee[2]

Research Scholar, Dept. of CS, University of Madras, Chennai, Tamilnadu, India[1]

Research Supervisor & Associate Professor, Dept. of CS, University of Madras, Tamilnadu, India[2]

Abstract: Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. This work studies the problem of ensuring the reliability of data storage in Cloud Computing. In particular, we consider the task of allowing a Third party assessor, on behalf of the cloud client, to verify the reliability of the dynamic data stored in the cloud. The introduction of Third party assessor eliminates the involvement of the client through the assessing of whether his data stored in the cloud is indeed together, which can be important in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation, such as block modification, insertion and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only.

While prior works on ensure isolated data reliability often lacks the support of either public review capability or dynamic data operations, this work achieves both. We first identify the difficulties and possible protection problems of through extensions with fully dynamic data updates from prior works and then show how to construct the seamless combination of these two most important features in our procedure design.

Keywords: Third party assessor, data storage, storage services, dynamic data operations.

I. INTRODUCTION

Cloud computing is Internet ("cloud") based on development and use of computer technology ("computing").It is a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the internet. Users need not have knowledge of, expertise in, or control over the technology infrastructure "in the cloud". There are many types of public cloud computing:

Infrastructure as a Service (IaaS)

Platform as a Service (PaaS)

Software as a Service (SaaS)

Network as a Service (NaaS)

Storage as a Service (STaaS)

Security as a Service (SECaaS)

Data as a Service (DaaS)

Several trends are opening up the time of Cloud Computing, which is an Internet-based progress and use of computer skill. The ever cheaper and more controlling processors, together with the “software as a service” (SaaS) computing structural design, are transforming data centers into pools of computing service on a massive range. The growing network bandwidth and reliable however flexible network relations make it even possible that clients can now give to high quality services from data and software that reside only on isolated data centers. Even though envisioned as a promising service platform for the Internet, this new data storage prototype in “Cloud” brings about many demanding propose issues which have reflective authority on the protection and show of the general structure. One of the prime concerns with cloud data storage is that of data reliability confirmation at untreated servers.

The storage service provider, which experiences Byzantine failures occasionally, may decide to hide the data errors from the clients for the benefit of their own. What is more serious is that for saving money and storage space the service provider might neglect to keep or intentionally delete not often accessed data files which go to an regular client. Consider the great size of the outsourced electronic data and the client’s prohibited supply capacity, the center of the problem can be general as how can the client find an efficient way to do review reliability verifications without the local copy of data files.

A.THIRD PARTY ASSESSOR

The verification schemes with public analysis ability any Third party assessor in control of the public key can act as a verifier. We assume that Third party assessor is balanced while the server is untrusted. The clients may interact with the cloud servers to access or retrieve their pre-stored data. The client may regularly perform block-level operations on the data files. The most general forms of these operations in this paper are modification, insertion, and deletion.

II. EXISTING WORK

Schemes presented before fall into two categories: private assessment capability and public assessment capability. Private assessment capability can achieve higher scheme efficiency, public assessment capability allows anyone, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no confidential in sequence.

Background of isolated data storage mainly focuses on fixed data files and the importance of this dynamic data updates has received limited attention.

Direct extension of the current provable data possession or proof of irretrievability schemes to support data dynamics may lead to security loopholes.

III. PROPOSED WORK

Public auditing system of data storage security in Cloud Computing, and propose a protocol supporting for fully dynamic data operations, especially to support block insertion, which is missing in most existing schemes. Supports scalable and efficient public auditing in Cloud Computing. Also achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the Third party assessor. Security of our proposed construction and justify the performance of our scheme through concrete implementation.

IV. LITERATURE REVIEW

A. COMPACT PROOFS OF RETRIEVABILITY, HOVAV SHACHAM, BRENT WATERS

In a proof-of-retrievability system, a data storage center must prove to a verifier that he is actually storing all of a client's data. The central challenge is to build systems that are both efficient and provably secure that is, it should be possible to extract the client's data from any prover that passes a verification check. In this paper, we give the first proof-of-retrievability schemes with full proofs of security against arbitrary adversaries in the strongest model, that of Juels and Kaliski. Our first scheme, built from BLS signatures and secure in the random oracle model, has the shortest query and response of any proof-of-retrievability with public verifiability. Our second scheme, which builds elegantly on pseudorandom functions (PRFs) and is secure in the standard model, has the shortest response of any proof-of-retrievability scheme with private verifiability (but a longer query). Both schemes rely on homomorphic properties to aggregate a proof into one small authenticator value.

B. DEPENDABLE AND SECURE SENSOR DATA STORAGE WITH DYNAMIC INTEGRITY ASSURANCE, QIAN WANG,DEOARTMENT OF ECE AND KUI REN WENJING,DEPARTMENT OF ECE AND LOU YANCHAO ZHANG, DEPARTMENT OF ECE

Recently, distributed data storage has gained increasing popularity for efficient and robust data management in wireless sensor networks (WSNs). But the distributed architecture also makes it challenging to build a highly secure and dependable yet lightweight data storage system. On the one hand, sensor data are subject to not only Byzantine failures, but also dynamic pollution attacks, as along the time the adversary may modify/pollute the stored data by compromising individual sensors. On the other hand, the resource-constrained nature of WSNs precludes the applicability of heavyweight security designs. To address the challenges, we propose a novel dependable and secure datastorage scheme with dynamic integrity assurance in this paper. Based on the principle of secret sharing and erasure coding, we first propose a hybrid share generation and distribution scheme to achieve reliable and fault-tolerant initial data storage by providing redundancy for original data components. To further dynamically ensure the integrity of the distributed data shares, we then propose an efficient data integrity verification scheme exploiting the technique of algebraic signatures. The proposed scheme enables individual sensors to verify in one protocol execution all the pertaining data shares simultaneously in the absence of the original data. Extensive security and performance analysis shows that the proposed schemes have strong resistance against various attacks and are practical for WSNs.

C. PRIVACY-PRESERVING AUDIT AND EXTRACTION OF DIGITAL CONTENTS, MEHUL A. SHAH RAM SWAMINATHAN MARY BAKER

A growing number of online services, such as Google, Yahoo!, and Amazon, are starting to charge users for their storage. Customers often use these services to store valuable data such as email, family photos and videos, and disk backups. Today, a customer must entirely trust such external services to maintain the integrity of hosted data and return it intact. Unfortunately, no service is infallible. To make storage services accountable for data loss, we present protocols that allow a thirdparty auditor to periodically verify the data stored by a service and assist in returning the data intact to the customer. Most importantly, our protocols are privacy-preserving, in that they never reveal the data contents to the auditor. Our solution removes the burden of verification from the customer, alleviates both the customer's and storage service's fear of data leakage, and provides a method for independent arbitration of data retention contracts.

D. REMOTE INTEGRITY CHECK WITH DISHONEST STORAGE SERVER, EE-CHIEN CHANG, JIA XU

We are interested in this problem: a verifier, with a small and reliable storage, wants to periodically check whether a remote server is keeping a large ¯le x. A dishonest server, by adapting the challenges and responses, tries to discard partial information of x and yet evades detection. Besides the security requirements, there are considerations on communication, storage size and computation time. Juels et al. [10] gave a security model for Proof of Retrievability (POR) system. The model imposes a requirement that the original x can be recovered from multiple challenges-responses. Such requirement is not necessary in our problem. Hence, we propose an alternative security model for Remote Integrity Check (RIC). We study a few schemes and analyze their efficiency and security. In particular, we prove the security of a proposed scheme HENC. This scheme can be deployed as a POR system and it also serves as an example of an effective POR system whose \extraction" is not verifiable. We also propose a combination of the RSA-based scheme by Filho et al. [7] and the ECC-based authenticator by Naor et al. [12], which achieves good asymptotic performance. This scheme is not a POR system and seems to be a secure RIC. In-so-far, all schemes that have been proven secure can also be adopted as POR systems. This brings out the question of whether there are fundamental differences between the two models. To highlight the differences, we introduce a notion, trap-door compression that captures a property on compressibility.

V. READ-THROUGH THE DATA RELIABILITY

The client will give the input like key generation; this is run by the client. It takes as input security parameter, and returns the output as public key and private key.

Run by the client, it takes as input private key and a data block D which is an ordered collection of blocks, and outputs the signature set, which is an ordered collection of signatures.

Run by the server, It takes as input data D, its signatures. It outputs a data reliability proof P for the blocks specified.

Run by the Third party assessor upon receipt of the proof P. It takes as input the public key, and the proof P returned from the server, and outputs TRUE if the reliability of the file is verified as correct.

VI. CLIENT AND THIRD PARTY ASSESSOR

An article, which has great data files to be stored in the cloud and relies on the cloud for data protection and calculation, can be any character clients. Third party assessor which has expertise and capabilities that clients do not have, is trusted to assess cloud storage services on behalf of the clients upon request. users do not necessarily have the time, feasibility or resources to monitor their data online, they can assign the data auditing tasks to an optional trusted third party assessor of their respective choices. To strongly begin such a third party assessor, any possible outflow of user's outsourced data towards third party assessor through the auditing protocol should be prohibited. Third party assessor should not learn user's data content through the delegated data auditing.

VII. ACTIVE DATA PROCESS WITH RELIABILITY DECLARATION

The overtly and competently hold entire active data process including data alteration, data inclusion and data removal for cloud data storage. The file F and the signature have previously been generated and correctly stored at server. The root metadata has been signed by the client and stored at the cloud server, so that anyone who has the client's public key can confront the correctness of data storage.

VIII. CONCLUSION

To ensure cloud data storage protection, it is significant to permit a third party assessor to estimate the service feature from an intention. Public assessment capability also allows clients to assign the reliability confirmation tasks, while they themselves can be defective or not be able to obligate essential calculation proceeds performing constant confirmation.

The problem of providing concurrent public assessment capability and data dynamics for isolated data reliability proves in Cloud Computing has been handled to achieve efficient data dynamics.

REFERENCES

[1] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of retrievability: Theory and implementation," Cryptology ePrint Archive, Report 2008/175, 2008.
[2] A. Juels and B. S. Kaliski, Jr., "Pors: proofs of retrievability for large files," in Proc. of CCS'07. New York, NY, USA: ACM, 2007, pp. 584–597.
[3] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008.
[4]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. New York, NY, USA: ACM, 2007, pp. 598–609.
[5]A. Oprea, M. K. Reiter, and K. Yang, "Space-efficient block storage integrity," in Proc. of NDSS'05, San Diego, CA, USA, 2005.
[6] E.-C. Chang and J. Xu, "Remote integrity check with dishonest storage server," in Proc. of ESORICS'08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 223–237.
[7]H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of ASIACRYPT'08. Melbourne, Australia: Springer-Verlag, 2008, pp. 90–107.
[8]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: Springer- Verlag, 2009, pp. 355–370.