ISSN 2395-1621

OPoR: Enabling Proof of Retrievability in Cloud Computing for Secure Data Storage

[#1]Ankita Patil, [#2]Amruta Nerlekar, [#3]Prof. Priyadarshani Kalokhe

[#123]Department of Computer

Savitribai Phule Pune University

[123]Alard College of Engineering and Management Marunji, Pune-411057

ABSTRACT

With cloud storage services, it is ordinary for data to be not only stored in the cloud, but also shared across many users. However, public auditing for such shared data while conserving individuality privacy remains to be an open challenge. In this paper, we propose the first privacy-preserving contrivance that allows public auditing on shared data kept in the cloud. In particular, we deed ring signatures to compute the confirmation material needed to audit the truthfulness of shared data. With our contrivance, the candor of the signer on each slab in shared data is kept private from a third party auditor (TPA), who is still able to openly verify the truth of shared data without recovering the complete file. Our untried results establish the effectiveness and efficiency of our proposed contrivance when auditing shared data.

ARTICLE INFO

Article History

Received: 28th November 2016

Received in revised form :

28th November 2016

Accepted: 30th November 2016

Published online :

2nd December 2016

Index Terms: **Public auditing, privacy-preserving, shared data, cloud computing.**

I. INTRODUCTION

Data outsourcing technique brings with it many advantages. But associated with it are the risks involved.The client cannot physically access the data from the cloud server directly, without clients are either not used by client from a long time. Though, there is a requirement of checking the data periodically for correction purpose, known as data integrity. Here we provide a survey on the different techniques of data integrity. The basic schemes for data integrity in cloud are Provable Data Possession (PDP) knowledge, cloud provider can modify or delete data which and Proof of Retrievability (PoR). These two schemes are the most active area of research in the cloud data integrity field. Cloud computing is an emergent computing exemplification in which IT modality and abilities are provided as services over the Internet while stashing platform and execution details. Auspicious as it is, this exemplification also brings forth new defiance for data safety and privacy when users outsource sentient data for sharing on cloud servers, which are likely outside of the same faithful domain of data owners.

Data access control has been growing in the past thirty years and various systems have been developed to actively implement ne-grained access control [20], which allows exhibition in specifying differential access rights of distinct users. However, traditional access control systems are mostly planned for in house services and depend seriously on the system itself to enforce authorization policies.

Thus, they cannot be germane in cloud computing because users and cloud servers are no longer in the same faithful domain. For the purpose of helping the data owner force access control over data kept on unfaithful cloud servers, a feasible idea would be encrypting data through certain cryptographic primitives but releasing decryption keys only to authorized users. One perilous issue of this branch of tactics is how to achieve the desired security goals without presenting high complexity of key management and data encryption. Existing work resolve this issue either by presenting a per le access control list (ACL) for ne-grained access control, or by sorting les into several groups for efficiency. As the system scales, however, the ACL-based structure would introduce an exceedingly high complexity which could be proportional to the number of system users. The le group based structure, on the other hand, is just able to afford coarse-grained access control of data.

Aiming at providing ne-grained access command over encrypted data, a fresh public key primeval namely attribute-based encryption (ABE) [23] is presented in the cryptographic community, which permits public key-based one-to-many encryption. In ABE system, users' keys and ciphertexts are labeled with sets of descriptive attributes and access policies respectively, and an exact key can decrypt a ciphertext only if the connected attributes and policy are matched.

II. LITERATURE SURVEY

1. H. Li, B. Wang, and B. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in IEEE Transactions on Cloud Computing

A novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. In particular, we exploit ring signatures to compute verification metadata needed to audit the correctness of shared data.

2. Q. Wang, K. Ren, S. Yu, and W. Lou, "Dependable and secure sensor data storage with dynamic integrity assurance," ACM Transactions on Sensor Networks.

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.

3 J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, "Fine-grained access control system based on attribute-based encryption," ESORICS.

The present a generic and efficient solution to implement attribute-based access control system by introducing secure outsourcing techniques into Attribute-based encryption (ABE). More precisely, two cloud service providers (CSPs), namely key generation-cloud service provider (KG-CSP) and decryption-cloud service provider (D-CSP) are introduced to perform the outsourced key-issuing and decryption on behalf of attribute authority and users respectively.

4. X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms of outsourcing modular exponentiations," ESORICS.

The first outsource-secure and efficient algorithm for simultaneous modular exponentiations. Moreover, we prove that both the algorithms can achieve the desired security notions.

5. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM

Cloud Computing is the long dreamed vision of computing as a utility, 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, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities.

6. Q. Zheng and S. Xu, "Secure and efficient proof of storage with deduplication," in CODASPY.

This "one stone, two birds" phenomenon not only inspired us to propose the novel notion of Proof of Storage with Deduplication (POSD), but also guided us to design a concrete scheme that is provably secure in the Random Oracle model based on the Computational Diffie-Hellman (CDH) assumption.

III. SYSTEM OVERVIEW

We ponder a wireless sensor network with a large number of sensor nodes, each of which has a unique ID and may perform different functionalities. These nodes are deployed tactically into areas of interest and continuously sense the environments. Some of them are prepared with sufficient capacity to store the sensed data locally in a distributed manner for a certain period.

Distributed manner for a sure period. We assume that these nodes have delimited power supply, storage space, and computational capability. Due to the constrained resources, computationally expensive and energy-intensive operations are not auspicious for such systems. In addition, for such a WSN, we also opine that basic security contrivances such as pairwise key establishment between two neighboring nodes are already in place to provide basic communiqué security [Blundo et al. 1992]. However, individual sensors are not consistent since they can undergo random Byzantine failures and be compromised due to a lack of tamper-proof hardware.

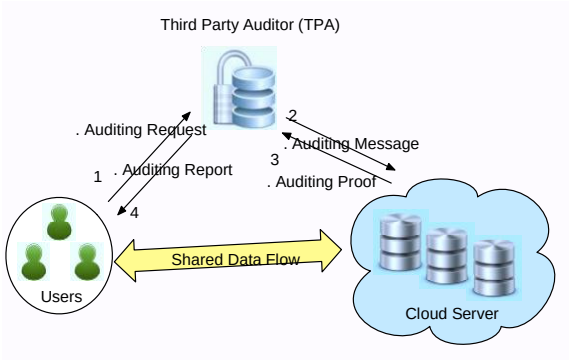

Fig 1. Cloud data storage architecture

In this paper, we only ponder how to audit the integrity of shared data in the cloud with stationary groups. It means the group is pre-defined before shared data is marked in the cloud and the membership of users in the group is not reformed during data sharing. The original user is liable for deciding who is capacitate to share her data before outsourcing data to the cloud. Another interesting problem is how to audit the truthfulness of shared data in the cloud with dynamic groups a new user can be added into the group and a present group member can be revoked during data sharing while still preserving identity privacy.

IV. EXISTING SYSTEMS

The existing structure can simultaneously provide provable security in the enhanced security model and enjoy desirable efficiency, that is, no structure can resist reset attacks while supporting efficient public verifiability and

dynamic data processes simultaneously PoR model is the first to support dynamic update processes and security against reset attack in a verification scheme. The robustness against reset attack ensures that a malicious storing server can never gain any advantage of passing the verification of an incorrectly stored file by resetting the client (or the audit server) in the upload phase. We will see that most of existing PoR structures cannot ensure this strong security for cloud storage.

V. PROPOSED SYSTEMS

We present an efficient verification structure for ensuring remote data integrity in cloud storage. The proposed structure is proved secure against reset attacks in the strengthened security model while supportive efficient public verifiability and dynamic data operations simultaneously proposed a dynamic version of the prior PDP structure. However, the system impose a priori limit on the number of queries and do not support fully dynamic data operations. In Wang et al. considered dynamic data storing in distributed scenario, and the proposed challenge-response protocol can both determine the data realism and locate possible errors. Similar to only considered partial support for dynamic data operation. In they also considered how to save storage space by introducing de duplication in cloud storing. Recently, Zhu et al. announced the provable data possession problem in a cooperative cloud service providers and designed a new remote integrity checking system.

VI. SECURITY MODEL

Shacham and Waters planned a security model for PoR system in [3]. Generally, the checking structure is secure if (i) there exists no efficient algorithm that can fraud the verifier with non-negligible probability; (ii) there exists a omnibus time extractor that can recover the original data file by carrying out multiple challenges responses. Under the description of a PoR system, the client periodically challenges the storage server to guarantee the correctness of the cloud data and the original files can be recovered by interacting with the server. The explanations of correctness and soundness was given in the structure is correct if the verification algorithm accepts when interacting with the valid prover (e.g., the server returns a valid response) and it is sound if any duplicitous server that convinces the client that is storing the data file is actually storing that file.

Note that in the "game" between the adversary and the subscriber, the adversary has chockfull ingress to the information kept in the server, i.e., the adversary plays the preface of the prover (server). In the confirmation process, the goal of adversary is to fraud the client, i.e., trying to generate valid responses and permit the data verification without being detected. Our security model has subtle but crucial modification from that of the prior works. Though some earlier works also considered the architecture with two servers, our structure achieves the outsourcing of the tag generation. Thus, the new structure also requires to prevent the cloud audit server from generating invalid tags for the client's files kept in the cloud storage server. The certification from the cloud servers is used in the new system to achieve this security requirement. In order to successfully perform the authentication while achieving blockless, the server should take over the job of computing. Due to this creation, our security model differs from that of the original PoR in both the verification and the data updating process. Specifically, in our scheme tags should be authenticated by the client (prover) in every protocol execution other than calculated or pre-stored by the client.

Besides, our PoR model is the first to support dynamic update operations and security against reset invasion in a verification scheme. The robustness against reset invasion ensures that a malicious storage server can never increase any advantage of passing the verification of an imperfectly stored file by resetting the client (or the audit server) in the upload phase. We will see that most of existing PoR schemes cannot ensure this strong security for cloud storage.

VII. CONCLUSION

We propose two outsource-secure and efficient algorithms for modular exponentiations and simultaneous modular exponentiations, which are the most basic and expensive operations in many discrete-logarithm cryptosystems. Compared with the algorithm [33], the proposed algorithm is superior in both efficiency and check ability.

In this paper, we have designed a protocol for outsourcing of MIC to a malicious cloud. We have shown that the proposed protocol simultaneously fulfills the goals of correctness, security (input/output privacy), robust cheating resistance, and high efficiency. With MIC already well rooted in scientific and engineering fields, the proposed protocol can be deployed individually or serve as a primitive building block, based on which some higher level secure outsourcing protocols are constructed. We also introduced a Monte Carlo verification algorithm to handle result verification. Its superiority in designing inexpensive.

We motivated the need of the cloud storage notion we call proof of storage with de duplication or POSD, to fulfill data integrity and duplication simultaneously. We also presented an efficient POSD scheme, which is proven secure in the Random Oracle model based on the Computational Diffie Hellman assumption. Compared with the PDP/POR/POW schemes, which cannot achieve one of the two goals, our scheme is as efficient as theirs. scheme is as efficient as theirs. One interesting future work is to remove the random oracle in the protocol without jeopardizing performance. Another is to seek a different design methodology for such protocols so as to achieve even substantially better performance.

REFERENCES

[1] H. Li, B. Wang, and B. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," in IEEE Transactions on Cloud Computing, 2014, pp. vol. 2, no. 1, 43–56.

[2] Q. Wang, K. Ren, S. Yu, and W. Lou, "Dependable and secure sensor data storage with dynamic integrity assurance," ACM Transactions on Sensor Networks, vol. 8, no. 1, pp. 9:1–9:24, Aug. 2011. [Online]. Available:http: //doi.acm.org/10.1145/1993042.1993051.

[3] J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, "Fine-grained access control system based on attribute-based encryption," ESORICS, 2013

[4] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms of outsourcing modular exponentiations," ESORICS, pp. 541–556, 2012.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, 2010, pp. 525–533.

[6] Q. Zheng and S. Xu, "Secure and efficient proof of storage with deduplication," in CODASPY, 2012, pp. 1–12.

[7] X. Lei, X. Liao, T. Huang, H. Li, and C. Hu, "Outsourcing large matrix inversion computation to a public cloud,," in IEEE Transactions on Cloud Computing, 2013, pp. vol. 1, no. 1.

