Future Generation Computer Systems 52 (2015) 86–94

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Towards secure and reliable cloud storage against data re-outsourcing☆

Tao Jiang [a], Xiaofeng Chen [a,*], Jin Li [b], Duncan S. Wong [c], Jianfeng Ma [a], Joseph K. Liu [d]

[a] State Key Laboratory of Integrated Service Networks (ISN), Xidian University, PR China
[b] School of Computer Science, Guangzhou University, PR China
[c] Department of Computer Science, City University of Hong Kong, Hong Kong
[d] Institute for Infocomm Research, Singapore

HIGHLIGHTS

- We propose a scheme to prevent CSPs from re-outsourcing their clients' data.
- We explore the economic server collusion problem among cloud storage services.
- Our scheme is efficient where a client does not need to download all its data.

ARTICLE INFO

Article history:
Received 30 June 2014
Received in revised form
26 September 2014
Accepted 10 November 2014
Available online 21 November 2014

Keywords:
Cloud storage
Economical server collusion
Storage security
Probabilistic scheme

ABSTRACT

To increase the profit, a semi-trusted cloud service provider may outsource the files of its client to some low expensive cloud service providers, which may violate the wishes of cloud users and impair their legitimate rights and interests. In this paper, a probabilistic challenge–response scheme is proposed to prove that users' files are available and stored in a specified cloud server. In our scheme, common cloud infrastructure with some reasonable limits, such as rational economic security model, semi-collusion security model and response time bound, are exploited to resist the collusion of cloud servers. These limits guarantee that a malicious cloud service provider could not conduct a t-round communication in a limited time. The security and performance analysis demonstrate that our scheme provides strong incentives against an economically rational cloud service provider from re-outsourcing its clients' data to some other cloud providers.

1. Introduction

Cloud computing provides a low-cost, scalable, location-independent infrastructure for data management and storage. Many individuals and organizations outsource their data to remote Cloud Storage Providers (CSPs) seeking to reduce the maintenance cost and the burden of large local data storage. The CSPs offer paid storage space on its infrastructure to store customers' data. The rapid adoption of cloud services and increasing volumes of data stored at remote servers need new techniques for saving disk space and network bandwidth and efficiently proving the situation of files stored in remote cloud servers. Since the CSPs, storing the client's files, are not necessarily trusted in cloud storage system, efficient and secure schemes should be built to constrain their malicious activities.

For sensitive data, legitimate concerns are necessary when using cloud storage services. The failure of cloud storage server at Amazon results in the permanent loss of customer data [1]. Also, there are a variety of economical and legal restrictions that may compel a customer to choose to store data in a specific cloud storage provider. For example, many companies are willing to store their sensitive data in the same cloud storage server and many privacy laws in Nova Scotia, British Columbia, Australia and EU [2] require personal data stored within a political border or other nations with comparable protections. Further, the cross server deduplication will greatly reduce the storage overhead of cloud servers, which will reduce the costs of the service providers and enhance their competitiveness. However, the data deduplication

☆ This document is a collaborative effort.

* Corresponding author.
E-mail addresses: jiangt2009@gmail.com (T. Jiang), xfchen@xidian.edu.cn (X. Chen), lijin@gzhu.edu.cn (J. Li), duncan@cityu.edu.hk (D.S. Wong), jfma@xidian.edu.cn (J. Ma), ksliu@i2r.a-star.edu.sg (J.K. Liu).
URL: http://ste.xidian.edu.cn/cxf/index.html (X. Chen).

http://dx.doi.org/10.1016/j.future.2014.11.002
0167-739X/

may violate the intention of users and undermine the interests of them. Therefore, we see that it is necessary to constrain the activity of the CSPs and verify that their activity meets the storage obligations. Since the clients data is stored in a remote server without a local copy, it is very difficult to provide transparency to the users that their sensitive data is correctly handled by the cloud provider. We need to use challenge–response scheme to provide an efficient method to prove the malicious storage re-outsourcing activity. However, the existing challenge–response scheme could not provide a proof that the data of clients stored in a semi-trusted remote cloud storage is not re-outsourced in the economical server collusion network model [3,4].

In this paper, we demonstrate that it is possible to design a challenge–response protocol which imposes a strong incentive onto the cloud providers to store their clients' data at rest. In particular, we present a probabilistic challenge–response scheme where semi-collusion bound, communication and computation bound and response time bound are adopted. A malicious cloud server S who has re-outsourced its client data to some other cloud server S' should conduct a t-round communication with S' to generate a correct response. If t is large enough, the malicious server could not generate the response in time even if with unlimited computation power. It is demonstrated that our scheme is secure under cryptography assumption and our analysis shows that as long as the designed communication round t is large enough, TIMER scheme will provide a strong incentive for the rational economic cloud providers to store the data of their clients in their storage servers.

Contributions. In general, there are several theoretical and practical contributions in our works:

- We are among the first to explore the economic server collusion security model in cloud storage services. In this model, a semi-trusted server may re-outsource the clients data to some servers with low expense to increase its profit, which will lead to some potential problems in cloud storage.
- We are among the first to propose a probabilistic challenge–response scheme whose security is dependent not only on cryptographic assumption but also on the network delay in cloud storage. Our construction indicates that the accurate measuring and controlling the network delay are important in challenge–response protocols against server collusion.
- We introduce a semi-collusion bound in the server collusion model, in which a server will collude with some other servers to deceive its clients. However, the server will not conduct a full signature delegation and share its secret key with its conspirator in the collusion. The semi-collusion bound is important in both theoretical adversary model construction and practical collusion with economically rational participants.

2. Related work

Provable Data Possession: To protect the availability of the clients' files stored in remote data storage server, Ateniese et al. [5] proposed a formalized model called Provable Data Possession (PDP). Unlike the low efficiency deterministic schemes [6–8] and probability scheme [9], PDP could efficiently check whether the clients' files stored in remote server have been tampered or deleted with very high probability. Several variations of their proposed scheme, such as static PDP schemes [10–12] and limited dynamic or dynamic schemes [13,14], are proposed to achieve efficient proof of remote data availability.

Secure Deduplication: Conducting deduplication will reduce the data storage burden and maintenance cost, which can promote price reductions of data storage service and enhance the competition of CSPs. Recent researches on storage deduplication [15,16] showed that deduplication achieves a higher level of scalability, availability, and durability. However, Harnik et al. [17] pointed out that client-side deduplication introduces security problems that an attacker is able to get the entire file from the server by learning just a small piece of the hash value about the file. Therefore, Halevi et al. [18] proposed a scheme called Proofs of Ownership (PoWs), where a client proves to the server that it actually holds a copy of the file and not just some short information about it based on Merkle trees [19] and specific encodings.

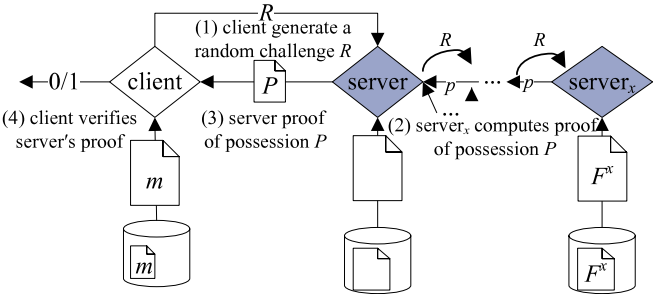

Fig. 1. The storage re-outsourcing in the challenge–response provable data possession scheme with server collusion.

Location Sensitive Services: In data storage system, users' data is important for some location sensitive services. Some schemes [20,21] proposed to use semi-trusted landmarks to provide geolocation solutions for data storage. Also, to provide the security against the colluding of adversaries, hidden landmarks are used in geolocation system [22] in wireless networks. Bowers et al. [1] proposed an hourglass scheme to verify a cloud storage service provider is duplicate data from multiple drives through the measurements of network delay. Gondree and Peterson [23] proposed a provable data geolocation and they detect the network delay of different distances and they point that their system could be built on any exiting PDP scheme.

The PDP relevant solutions are proposed to realize efficient data availability check on remote data storage servers. The data storage deduplication relevant solution PoWs is proposed to protect against an attacker from gaining access to potentially huge files of other users based on a very small amount of side information. However, all these schemes focus on the authentication of data integrity and availability problems between clients and servers, which could not prevent a semi-trusted server from re-outsourcing clients' data to some other servers to save its storage space or increase its profit. Such behavior may reduce the security and availability guarantee of clients' data and the benefit of the clients may be violated in this situation.

3. Data re-outsourcing problem

In this section, we first model the economic server collusion in cloud storage service when the servers providing cloud storage service are semi-trusted. Then, we analyze the potential problems that may occur in this situation.

3.1. Economical server collusion

We assume that all the cloud storage providers, driven by interests, are semi-trusted and they are motivated to increase the income from the clients and reduce the expense for their service. Therefore, it is reasonable to construct an economical server collusion security model in which a server colludes with some other servers and conducts storage re-outsourcing activity privately as shown in Fig. 1.

A client offloads its file F and stores it in a remote CSP to reduce the storage and management cost. However, the CSP may re-outsource the client's file to some less expensive CSPs for its own benefit. In this situation, the CSP will not need to store the