Computers and Electrical Engineering 000 (2017) 1–13

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Identity-based non-repudiable dynamic provable data possession in cloud storage☆

Feng Wang[a,b], Li Xu[a,*], Huaqun Wang[c], Zhide Chen[a]

[a] Fujian Provincial Key Laboratory of Network Security and Cryptology, School of Mathematics and Computer Science, Fujian Normal University, Fuzhou, Fujian, 350117, China
[b] College of Mathematics and Physics, Fujian Provincial Key Laboratory of Big Data Mining and Applications (Fujian University of Technology), Fujian University of Technology, Fuzhou, Fujian, 350118, China
[c] Jiangsu Key Laboratory of Big Data Security & Intelligent Processing, School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, 210023, China

ARTICLE INFO

Article history:
Received 29 November 2016
Revised 23 September 2017
Accepted 25 September 2017
Available online xxx

Keywords:
Wearable device
Index logic table
Cloud storage
Identity-based non-repudiable dynamic provable data possession

ABSTRACT

In cloud-assisted wearable devices, how to protect the integrity of data stored in the cloud is a hot issue. For the scenes where clients are dishonest, we study the non-repudiable dynamic provable data possession schemes, and find that existing dynamic structures are not suitable for non-repudiable dynamic provable data possession schemes. The Merkle hash tree must be combined with timestamps to construct non-repudiable dynamic provable data possession schemes. This will cause the synchronization problem, and map-version tables cannot resist delete-insert attacks. Therefore, we propose a monotonic dynamic structure, i.e., index logic table. Then, we construct an identity based non-repudiable dynamic provable data possession scheme for cloud storage by using index logic tables. The proposed scheme not only resists the hash value stored attack, the delete-insert attack, and the tampering cloud returned value attack, but also avoids the synchronization problem. Furthermore, the proposed scheme has lower computation cost and storage cost in the dynamic operation process.

1. Introduction

Nowadays, wearable technology can be considered as a massive global business. Many major industrial companies have seen the opportunities from it, such as Google, Samsung, Nike, Sony, etc. [1]. However, wearable devices are still limited to computation capabilities and communication resources [2,3]. So, remote cloud server can be used to establish interactions for remote data storage services and communicating among themselves through it, which is called the cloud assisted wearable device [2]. However, there are some security challenges [4] in cloud assisted wearable device, such as privacy-preserving data aggregation, dynamical integrity assurance, non-repudiation, etc.

As for cloud storage, based on its low-cost, scalable, location-independent service, it has become more and more popular. In cloud storage, the data owners (clients) outsource their data in cloud service provider (CSP) such as Google Drive and Amazon S3 etc. However, without the controlling of their data, the cloud storage has some potential security risks [5] such as data privacy, data integrity, data recovery vulnerability, improper media sanitization, and data back, etc. Therefore, how

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. Debiao He.

* Corresponding author.
E-mail address: xuli@fjnu.edu.cn (L. Xu).

https://doi.org/10.1016/j.compeleceng.2017.09.025
0045-7906/© 2017 Published by Elsevier Ltd.

to protect the data integrity of cloud storage becomes a hot issue for researchers. In cloud assisted wearable device, the wearable device users have the same concern too.

Generally, there are two methods for protecting data integrity on cloud storage. Ateniese et al. [6] proposed the provable data possession (PDP) model in 2007. In their model, the verifier can check integrity of remote data with a high probability without fetching back the data. Shacham and Waters [7] presented the proof of retrievability (POR) model in 2008. In their model, if the cloud service provider passed the verifier's audit, the verifier can extract the data. In our work, we focus on PDP model.

Following Ateniese et al.'s [6] work, Ateniese et al. [8] proposed dynamic PDP model and gave a concrete scheme without insert operation. Erway et al. [9] proposed a full-dynamic PDP scheme based on the authenticated flip table. After that, many dynamic PDP schemes are proposed. Most of them are based on the rank-based authentication skip list [10] or Merkle hash tree (*MHT*) [11]. Note that the client must compute lots of hash values for updating their data in rank-based authentication skip list or *MHT* based dynamic PDP schemes, which have a high computational cost. Therefore, some map-version table (*MVT*) based dynamic PDP schemes [12–14] were proposed. Furthermore, Shen et al. [15] proposed a dynamic structure consisted of a doubly linked info table and a location array to reduce computational and communication costs. However, Ni et al. [16] pointed out that Kang and Jia's scheme [14] cannot resist tampering cloud returned value attack, which is described in Section 6.1.3 in detail. We find that Barsoum and Hasan's scheme [13] cannot resist delete-insert attack, which is described in Section 2.4 in detail.

All the schemes mentioned above are based on the hypothesis that the clients are honest, i.e., these schemes protect clients from the cloud service provider's misbehavior, but do not protect cloud service provider from the clients' misbehavior. For example, if a client didn't update his/her data stored in cloud, he/she insisted that he/she had updated the data, and claimed for compensation because that the client claimed that the cloud server had lost his/her outsourced data, the existed schemes cannot solve this dispute. Mo et al. [17] proposed non-repudiable PDP to protect the cloud service provider's benefits in 2014. In their scheme, they designed a dynamic non-repudiable PDP based on Merkle hash tree combined with timestamp. Wang et al. [18] proposed a RSA based non-repudiable PDP scheme based on Pedersen commitment function. In their scheme, the client needs to compute an additional commitment for every block, which incurs a high computational cost.

In cloud storage service, only the clients who have purchased the cloud storage service are allowed to upload data to the cloud server. So, when a client wants to upload data, the cloud server must check the public key certificate of the client to ensure the client has purchased the cloud storage service. In order to eliminate the complicated certificate management, Wang et al. [19] proposed identity based provable data possession (ID-PDP) scheme in 2014. Wang [20] and Wang et al. [21] extend Wang et al.'s scheme [19] into distributed multicloud storage and proxy-oriented cloud storage respectively. Liu et al. [22] pointed out that Wang's scheme [20] cannot resist hash value stored attack, which is described in Section 6.1.1 in detail. At the same time, Ming and Wang [23] pointed out that Wang's scheme [20] cannot resist tampering cloud returned value attack, which is described in Section 6.1.3 in detail. However, most of the existing ID-PDP schemes are static.

Therefore, we focus on the scenes that the clients are dishonest by using identity based cryptography, monotonic dynamic structure index logic table (*ILT*) and Diffie-Hellman key agreement [24]. Then, we propose an identity-based non-repudiable dynamic provable data possession (ID-NR-DPDP) for cloud storage. The main contributions are described below.

First, we point out that the existed dynamic structures are not suitable for non-repudiable dynamic PDP scheme. The *MHT* should combine with timestamp to construct non-repudiable dynamic PDP scheme, which will cause synchronization problem, and *MVT* is vulnerable to delete-insert attack.

Second, we propose the notion of monotonic dynamic structure for non-repudiable dynamic PDP scheme. We also design a concrete monotonic dynamic structure, i.e., *ILT*.

Third, we extend the identity based PDP scheme to identity-based dynamic non-repudiable PDP scheme.

Final, we use monotonic dynamic structure *ILT* to resist delete-insert attack and avoid synchronization problem. We use Diffie-Hellman key agreement to resist tampering cloud returned value attack. Furthermore, our proposed scheme can resist hash value stored attack, and has more effective dynamic operation both in computation cost and storage space.

The rest of the paper is organized as follows. Section 2 introduces the preliminaries, including bilinear pairing, Diffie–Hellman key agreement [24], Galindo and Garcia's identity-based signature [25], Merkle hash tree (*MHT*), and map-version table (*MVT*). We propose the structure of ID-NR-DPDP in Section 3 and monotonic dynamic structure in Section 4. Concrete structure of our identity-based dynamic non-repudiable PDP scheme is given in Section 5. The analysis of security and efficiency are given in Section 6. Our conclusions are described in Section 7.

2. Preliminaries

In this section, we review bilinear pairing [26], Diffie–Hellman key agreement [24], Galindo and Garcia's identity-based signature [25], Merkle hash tree (*MHT*) [11,27], and map-version table [12–14], respectively.

2.1. Bilinear pairing

Let G_1 be an additive group (for example, elliptic curve [28–30] group) with the prime order q, and G_2 be a multiplicative group with the same order, and P be a generator of G_1. The map $e: G_1 \times G_1 \rightarrow G_2$ is named bilinear pairing [26] if the following three properties are satisfied.

Please cite this article as: F. Wang et al., Identity-based non-repudiable dynamic provable data possession in cloud storage, Computers and Electrical Engineering (2017), https://doi.org/10.1016/j.compeleceng.2017.09.025