Information Sciences 000 (2016) 1–17

Contents lists available at ScienceDirect

Information Sciences

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

Tell me the truth: Practically public authentication for outsourced databases with multi-user modification

Wei Song[a,b,c], Bing Wang[c], Qian Wang[a,*], Zhiyong Peng[a,b], Wenjing Lou[c]

[a] The State Key Laboratory of Software Engineering, Wuhan University, China
[b] School of Computer Science, Wuhan University, China
[c] Department of Computer Science, Virginia Polytechnic Institute and State University, USA

ARTICLE INFO

Article history:
Received 1 January 2016
Revised 12 May 2016
Accepted 11 July 2016
Available online xxx

Keywords:
Outsourced database
Public authentication
Homomorphic verifiable tags

ABSTRACT

With the advent of cloud computing, outsourcing databases to remote cloud servers provide the elastic, flexible and affordable data management services for the Internet users. The cloud users can create, store, access and update the remote outsourced databases just as they are using the database system locally. However, unlike storing data in a fully-controlled local database, storing data in a remote cloud server raises data privacy and security concerns, i.e., the correctness and completeness of the query results. Although some solutions have been proposed to address this problem, they do not scale well when multiple users update the remote outsourced database for two major reasons. First, the existing schemes mainly use the authenticated data structure (ADS) to provide the verification service which incurs expensive computation cost, especially when modifications are made to the database. Second, the data owner has to remain online all the time to participate in generating signatures for the modified data. Consider the fact that the outsourced databases involve lots of heavy multi-user modification operations, the existing solutions are not practical from the efficiency perspective. To address the above concerns, in this paper, we first propose a novel and efficient signature scheme which features additive homomorphic operations. On top of that, we further propose a new and practical mechanism for correctness and completeness verification with the support of multi-user modifications and without requiring an always-online data owner. Finally, we prove the security of our scheme under the well-known Computational Diffie–Hellman assumption and conduct extensive experiments to evaluate the performance of our scheme. The experimental results show that our scheme outperforms the existing solutions.

1. Introduction

In cloud computing, the users and the enterprises can lease the computing and storage resources provided by the powerful cloud service provider. Under this new IT Paradigm, database outsourcing [6] is considered as a prominent service model by providing an elastic, flexible and affordable solution for the organizations and enterprises to maintain their database services. As can be seen in recent years, more and more enterprises begin to move their data management services to the cloud for the easy management and low cost. The successful real-world examples such as Amazon Relational Database

* Corresponding author.
E-mail addresses: songwei@whu.edu.cn (W. Song), bingwang@vt.edu (B. Wang), qianwang@whu.edu.cn (Q. Wang), peng@whu.edu.cn (Z. Peng), vjlou@vt.edu (W. Lou).

http://dx.doi.org/10.1016/j.ins.2016.07.031
0020-0255/

(RDS)[1], Azure[2], and EnterpriseDB[3] enable users around the world to share and update their outsourced data anywhere anytime. While enjoying all the benefits, the users have to worry about their data security and privacy because the outsourced database service providers are often not in the same trusted domain with cloud users. As a result, for the correct utilization of the outsourced data at the cloud, the correctness and completeness of the query results over the outsourced data should be verified from the users' perspective.

To this end, a number of solutions have been proposed based on the various technologies [4,7,8,10–15,17,19,20,22,23,25,26,28] in recent years. However, most of them only consider the cases that the outsourced data is static or updated only by a single data owner. Others [8,17] require the data owner to sign the verification data structures for every modification. This mode requires the data owner to stay online all the time to support multi-user modification. On the other hand, the existing works commonly utilize the authenticated data structures (ADS), which incurs expensive computation cost for every data modification operation. Obviously, such verification approaches do not scale well when the frequency of the data modification operations increases. Given the fact that the outsourced databases involve a large amount of multi-user modification operations, the existing solutions are not practical from the efficiency perspective.

Consider the following application scenario. A supermarket such as Walmart has many branch stores. This supermarket outsources the management of its sales data to the cloud. Each branch store is able to upload and update the sales data stored on the cloud. At the same time, the clients such as the analysts, the managers and so on need to access the sales data contributed by multiple branch stores. However, the cloud is not fully trusted (i.e., it may be malicious or become prey to an external attack). So, the problem is how can the client efficiently and correctly verify the results generated and returned from the cloud, particularly when the outsourced data is modified by multiple users frequently? Therefore, there still lacks a practical correctness and completeness verification method for the outsourced data with multi-user modifications. From the users' perspective, a practical verification scheme should have the following properties:

- **Correctness verification**: The outsourced data stored at the remote server may be polluted by the attackers. But, the cloud server may hide the fact for the economic reasons and its reputation. So, the user should be able to detect the polluted data in the query results returned from the outsourced database server.
- **Completeness verification**: The outsourced database server is not fully trusted. To save the resources, it is possible that the outsourced database server only returns partial results or does not execute the query over the entirely outsourced data at all. The user should be able to detect such misbehavior by verifying the completeness of the query results.
- **The support of multi-user modification**: One of the main advantages of the outsourced database is to allow the multiple online users to share the data. Therefore, the practical integrity verification mechanism should allow the user to efficiently verify the integrity of the query results, even the outsourced data is contributed by the multiple users.
- **Public verification**: To improve the usability of the verification scheme, it should be able to allow anyone in the system to verify the integrity of the query results without storing some meta data locally or retrieving the entire data collection from cloud, even if some outsourced data have been modified and signed by multiple users. In addition, the system should not depend on any special entity, e.g., an always online data owner, to execute the verification.
- **High efficiency**: The user should be able to verify the query results of the outsourced databases with higher communication and computation efficiency than the approach of downloading the outsourced data and executing the query locally.

Keep the above goals in mind, in this work, we propose an efficient signature scheme based on the bilinear map to support the integrity verification of the outsourced databases with multi-user modification. Our solution also supports the public verifiability, in which the authorized user signs the data by its private key after the modification operation. The user then can use the public key to verify the query results even the outsourced data have been modified and signed by multiple users. To efficiently support multi-user modification, the proposed verification scheme is designed to enable the user to independently sign the data without an always-online data owner and/or the third party trusted entity. The main contributions in this paper can be summarized as follows:

- We for the first time propose an efficient and practical scheme to support the public verification of the outsourced databases with multiple writers. Compared with the existing solutions, our scheme is highly efficient, secure and scalable.
- We evaluate the performance of our scheme by numerical analysis, which illustrates that the proposed scheme is indeed an efficient integrity verification solution for outsourced databases. Moreover, we formally prove that the proposed scheme is secure.
- We fully implement a prototype of the proposed scheme and evaluate its performance through the extensive experiments. Our experimental results further validate its effectiveness and efficiency.

The rest of our paper is organized as follows. In the next section, we discuss the related work. We set up the system model in Section 3. Then we introduce several cryptographic primitives used in this paper in Section 4. Section 5 details our signature scheme, based on which the integrity verification mechanism is presented in Section 6. We analyze the perfor-

[1] http://aws.amazon.com/.
[2] http://azure.microsoft.com/.
[3] http://www.enterprisedb.com/.

Please cite this article as: W. Song et al., Tell me the truth: Practically public authentication for outsourced databases with multi-user modification, Information Sciences (2016), http://dx.doi.org/10.1016/j.ins.2016.07.031