Chapter 7.15
Ensuring Correctness, Completeness, and Freshness for Outsourced Tree-Indexed Data

Tran Khanh Dang
National University of Ho Chi Minh City, Vietnam

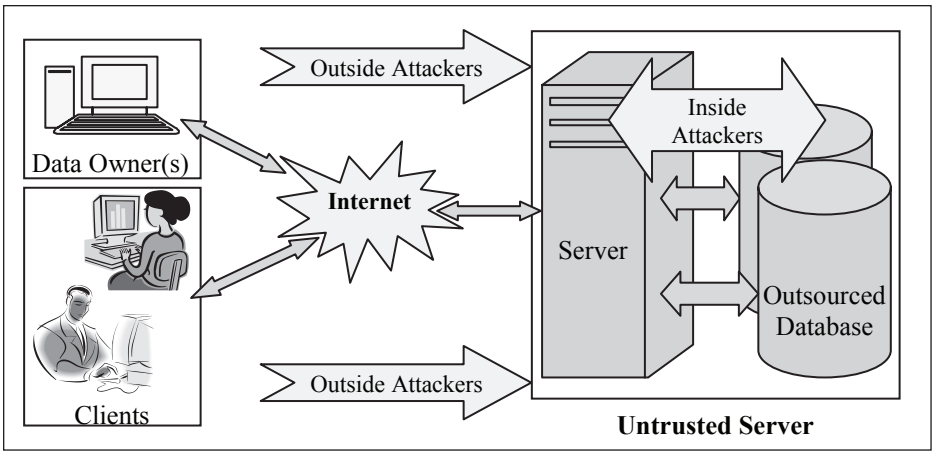
ABSTRACT

In an outsourced database service model, query assurance takes an important role among well-known security issues. To the best of our knowledge, however, none of the existing research work has dealt with ensuring the query assurance for outsourced tree-indexed data. To address this issue, the system must prove authenticity and data integrity, completeness, and freshness guarantees for the result set. These objectives imply that data in the result set is originated from the actual data owner and has not been tampered with; the server did not omit any tuples matching the query conditions; and the result set was generated with respect to the most recent snapshot of the database. In this paper, we propose a vanguard solution to provide query assurance for outsourced tree-indexed data on untrusted servers with high query assurance and at reasonable costs. Experimental results with real datasets confirm the effciency of our approach and theoretical analyses.

INTRODUCTION

Outsourcing database services is emerging as an important new trend thanks to continued growth of the Internet and advances in the networking technology. Organizations outsource their data management needs to an external service provider, thereby freeing them to concentrate on their core business. In this outsourced database service (ODBS) model, organizations rely on the premises of external service providers, which include hardware, software, and manpower, for the storage and retrieval management of their data, and they operate other business applications via the Internet without having to maintain applications *in-house*. Figure 1 depicts key "actors" in

Figure 1. The ODBS model and security threats at the server side



the most general and complicated ODBS model (Mykletun, Narasimha, & Tsudik, 2004),[1] where multiple data owners (say, separate departments of an organization) outsource their data to a certain database server (which may be untrusted) and allow users (may be other departments, partners of the organization, or even themselves) to access the outsourced data. This service model is a recent and important manifestation of the outsourcing trend of different information technology services. As we can see, however, among issues needing to be addressed in order to make this model reality, security-related issues must be of crucial concern due to the fact that the server may be untrusted, and both data as well as users' queries can now be exposed to the server and hackers/malicious users (corresponding to inside and outside attackers as shown in Figure 1, respectively). This means that, in this ODBS model, apart from secure network communication channels and other necessary security procedures at the user side (Axelrod, 2004), efficient and effective solutions to security threats inside the server are indispensable. We discuss in more detail these server-side security-related issues below.

Security Issues in the ODBS Model

Since a service provider is typically not fully trusted, the ODBS model raises numerous interesting research challenges related to security issues. First of all, because the life-blood of every organization is the information stored in its databases, making outsourced data confidential is therefore one of the foremost challenges in this model. In addition, privacy-related concerns must also be taken into account due to their important role in real-world applications.[2] Not less importantly, in order to make the outsourced database service viable and really applicable, the query result must also be proven qualified. This means the system has to provide users with some means to verify the query assurance claims of the service provider. Overall, most crucial security-related research questions in the ODBS model relate to the below issues:

- **Data confidentiality:** Outsiders and the server's operators (database administrator–DBA) cannot see the user's outsourced data contents in any cases (even as the user's queries are performed on the server).