Cryptology ePrint Archive: Report 2013/045

Towards Efficient Verifiable SQL Query for Outsourced Dynamic Databases in Cloud

Jiawei Yuan and Shucheng Yu

Abstract: With the rising trend of outsourcing databases to the cloud, it is important to allow clients to securely verify that their queries on the outsourced databases are correctly executed by the cloud. Existing solutions on this issue either suffer from a high communication cost, or introduce too much computational cost on the client side. Besides, so far only four types of SQL queries (i.e., selection query, projection query, join query and weighted sum query) are supported in existing solutions. It still remains challenging to design a verifiable SQL query scheme that introduces affordable storage overhead, communication and computational cost, and supports more SQL queries used in practice.

This paper investigates this problem and proposes an efficient verifiable SQL query scheme for dynamic databases outsourced to the cloud. Our proposed scheme makes several major progresses: 1) it reduces the communication complexity (excluding the query results) to a logarithmic level (i.e., $O(log~n)$, where n is the number of tuples in a table), while existing schemes all have a linear or quadratic complexity; 2) it constrains the computational complexity on the client side, in terms of expensive operations such as exponentiation, to a constant level, which is of linear level in existing schemes; 3) in addition to the queries supported by existing schemes, our proposed scheme also supports more practical query types including polynomial queries of any degrees, variance query and many other linear queries. Our design exploits techniques such as Merkle hash tree and constant size polynomial commitment. We shows the efficiency and scalability of our scheme through extensive numerical analysis. Based on the Strong Diffie-Hellman assumption, the Bilinear Strong Diffie-Hellman assumption and the Computational Diffie-Hellman problem, we show that our scheme is provably secure.

Category / Keywords: Integrity Check, Dynamic Database Outsource, SQL Query, Authenticated Data Structure, Cloud Storage

Publication Info: ACNS13

Date: received 28 Jan 2013, last revised 9 Feb 2013

Contact author: jxyuan at ualr edu

Available formats: PDF | BibTeX Citation

Version: 20130209:084557 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]