J Inf Process Syst, Vol.13, No.3, pp.573~589, June 2017
https://doi.org/10.3745/JIPS.04.0034

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

Query with SUM Aggregate Function on Encrypted Floating-Point Numbers in Cloud

Taipeng Zhu*, Xianxia Zou*, and Jiuhui Pan*

Abstract

Cloud computing is an attractive solution that can provide low cost storage and powerful processing capabilities for government agencies or enterprises of small and medium size. Yet the confidentiality of information should be considered by any organization migrating to cloud, which makes the research on relational database system based on encryption schemes to preserve the integrity and confidentiality of data in cloud be an interesting subject. So far there have been various solutions for realizing SQL queries on encrypted data in cloud without decryption in advance, where generally homomorphic encryption algorithm is applied to support queries with aggregate functions or numerical computation. But the existing homomorphic encryption algorithms cannot encrypt floating-point numbers. So in this paper, we present a mechanism to enable the trusted party to encrypt the floating-points by homomorphic encryption algorithm and partial trusty server to perform summation on their ciphertexts without revealing the data itself. In the first step, we encode floating-point numbers to hide the decimal points and the positive or negative signs. Then, the codes of floating-point numbers are encrypted by homomorphic encryption algorithm and stored as sequences in cloud. Finally, we use the data structure of DoubleListTree to implement the aggregate function of SUM and later do some extra processes to accomplish the summation.

Keywords

Coding Scheme, DoubleListTree, Encryption, Floating-Point Numbers, Summation

1. Introduction

Cloud database services, for example Amazon Relational Database Service and Microsoft SQL Azure, are attractive for enterprises to outsource their databases. Enterprises can get started without purchasing their expected future software and employing DBA, hence cloud can reduce the total cost of ownership [1]. However, the main problem is that parts of the data may be sensitive, such as credit card numbers or other personal information. Storing and processing sensitive data on infrastructure that provided by a third party increases the risk of unauthorized disclosure if the infrastructure is compromised by an adversary [2]. A straightforward approach to addressing the security and privacy problem is to encrypt data before they are sent to cloud. However, after being encrypted, a database might not be easily queried. When a database is large, it is not acceptable to decrypt the entire database

Manuscript received July 1, 2016; first revision November 11, 2016; accepted December 14, 2016.
Corresponding Author: Jiuhui Pan (jhpan_126@126.com)
* Dept. of Computer Science, Jinan University, Guangzhou, China (t.p.zhu@outlook.com, tzouxianxia@jnu.edu.cn, jhpan_126@126.com)