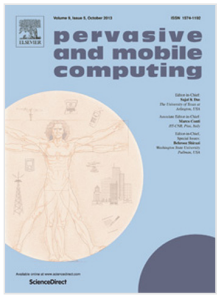
Accepted Manuscript



Achieving fully privacy-preserving private range queries over outsourced cloud data

Yao Shen, Wei Yang, Lu Li, Liusheng Huang

PII: S1574-1192(16)30279-6
DOI: http://dx.doi.org/10.1016/j.pmcj.2017.04.008
Reference: PMCJ 832

To appear in: *Pervasive and Mobile Computing*

Received date: 18 October 2016
Revised date: 22 February 2017
Accepted date: 25 April 2017

Please cite this article as: Y. Shen, W. Yang, L. Li, L. Huang, Achieving fully privacy-preserving private range queries over outsourced cloud data, *Pervasive and Mobile Computing* (2017), http://dx.doi.org/10.1016/j.pmcj.2017.04.008

Achieving Fully Privacy-Preserving Private Range Queries over Outsourced Cloud Data

Yao Shen[a,b,*], Wei Yang[a,b], Lu Li[c], Liusheng Huang[a,b]

[a]*School of Computer Science and Technology, USTC, China*
[b]*Suzhou Institute for Advanced Study, USTC, China*
[c]*School of Computer Science, Yancheng Teachers University, China*

Abstract

With the prevalence of cloud computing, data owners are motivated to outsource their databases to the cloud server. However, to preserve data privacy, sensitive private data have to be encrypted before outsourcing, which makes data utilization a very challenging task. Existing work either focus on keyword searches and single-dimensional range query, or suffer from inadequate security guarantees and inefficiency. In this paper, we consider the problem of multidimensional private range queries over encrypted cloud data. To solve the problem, we systematically establish a set of privacy requirements for multidimensional private range queries, and propose a multidimensional private range query (MPRQ) framework based on private block retrieval (PBR), in which data owners keep the query private from the cloud server. To achieve both efficiency and privacy goals, we present an efficient and fully privacy-preserving private range query (PPRQ) protocol by using batch codes and multiplication avoiding technique. To our best knowledge, PPRQ is the first to protect the query, access pattern and single-dimensional privacy simultaneously while achieving efficient range queries. Moreover, PPRQ is secure in the sense of cryptography against semi-honest adversaries. Experiments on real-world datasets show that the computation and communication overhead of PPRQ is modest.

Keywords: Cloud computing, Multidimensional range query,

*Corresponding author
Email address: shenyao@mail.ustc.edu.cn (Yao Shen)