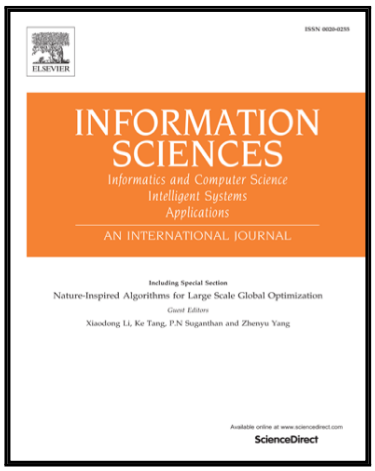

Enabling Verifiable Multiple Keywords Search over Encrypted Cloud Data

Yinbin Miao, Jian Weng, Ximeng Liu, Kim-Kwang Raymond Choo, Zhiquan Liu, Hongwei Li

PII: S0020-0255(18)30514-0
DOI: 10.1016/j.ins.2018.06.066
Reference: INS 13759

To appear in: *Information Sciences*

Received date: 16 November 2017
Revised date: 28 June 2018
Accepted date: 30 June 2018

Please cite this article as: Yinbin Miao, Jian Weng, Ximeng Liu, Kim-Kwang Raymond Choo, Zhiquan Liu, Hongwei Li, Enabling Verifiable Multiple Keywords Search over Encrypted Cloud Data, *Information Sciences* (2018), doi: 10.1016/j.ins.2018.06.066

Enabling Verifiable Multiple Keywords Search over Encrypted Cloud Data

Yinbin Miao[a,b], Jian Weng[c], Ximeng Liu[d], Kim-Kwang Raymond Choo[e], Zhiquan Liu[c,*], Hongwei Li[f]

[a]*Department of Cyber Engineering, Xidian University, Xi'an 710071, China*
[b]*Key Laboratory of Optical Communication and Networks, Chongqing 4000565, China*
[c]*College of Information Science and Technology, College of Cyber Security, Jinan University, Guangzhou 510632, China*
[d]*Department of Information Systems, Singapore Management University, 80 Stamford Road, Singapore*
[e]*Department of Information Systems and Cyber Security, The University of Texas at San Antonio, San Antonio, TX 78249 USA*
[f]*Department of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 610051, China*

Abstract

Searchable Encryption (SE) enables a user to search over encrypted data, such as data stored in a remote cloud server. Existing certificate-, identity-, and attribute-based SE schemes suffer from certificate management or key escrow limitations. Furthermore, the semi-honest-but-curious cloud may conduct partial search operations and return a fraction of the search results (i.e., incomplete results) in order to reduce costs. In this paper, we present a secure cryptographic primitive, Verifiable Multiple Keywords Search (VMKS) over ciphertexts, which leverages the Identity-Based Encryption (IBE) and certificateless signature techniques. The VMKS scheme allows the user to verify the correctness of search results and avoids both certificate management or key escrow limitations. We then demonstrate the security of proposed VMKS scheme (i.e., the scheme achieves both ciphertext indistinguishability and signature unforgeability). We also use a real-world dataset to evaluate its feasibility and efficiency.

Keywords: Searchable encryption, certificate management, key escrow, ciphertexts indistinguishability, signatures unforgeability

1. Introduction

During the outsourcing of data (e.g. text, image, video) to a remote cloud service provider, data owners (individuals and organizations) generally encrypt their (sensitive) data in order to ensure data confidentiality [7, 20, 24, 27, 37, 38, 36, 40]. In addition, some organizations may need to ensure that they are compliant with the relevant industry regulations and privacy requirements (e.g. the new European Union's General Data Protection Regulation).

Despite the benefits of encrypting the data prior to outsourcing, searching over encrypted data (and dataset) remains a challenge. Searchable encryption (SE) was designed to allow users to securely search over ciphertexts, based on pre-defined keywords, and selectively retrieve files of interest [29, 1, 25, 26]. Examples of SE schemes include public key encryption with keyword search (PEKS), and the latter can be broadly categorize into certificate-based keyword search [5, 3] and identity (or attribute)-based keyword search [43, 32] schemes. In certificate-based keyword search schemes, the data owner shares his/her data by encrypting them with a specific data user's public key. The key limitation is certificate management, as one needs to verify the certificates and public keys via the certificate management system. In other words, scalability can be a challenge in practice. The key limitation with identity (or attribute)-based keyword search schemes is key escrow, since the trusted authority center can decrypt any ciphertext in the system.

A number of researchers have attempted to address such limitations. For example, the keyword search scheme presented in [42] was designed to mitigate limitations in most existing SE schemes, such as those of [12, 16, 13]. However, the keyword search scheme presented in [42] assumes that the cloud is honest-but-curious, in the sense that the cloud service provider will faithfully follow the established protocols but at the same time, it is curious to deduce valuable information. Such an assumption is usually insufficient in practical applications, since the cloud may be financially motivated to return incomplete search results (e.g. to minimize computation and bandwidth resources). Therefore, we consider a semi-honest-but-curious cloud [2], which executes a fraction of the requested search operations and returns incomplete search results in practice. We then provide a result verification mechanism to guarantee the accuracy of the search results by appending a signature to each file stored in a cloud. We also observe that for verifiable keyword search schemes, there is a need to support multiple-keyword search in order to minimize bandwidth resources and improve user search experience (as a single keyword search returns many irrelevant search results [30, 21]).

To realize the above search functionalities simultaneously, we design a cryptographic primitive – hereafter referred to as **V**erifiable **M**ultiple **K**eywords **S**earch (VMKS). The latter allows one to perform a search over encrypted (cloud) data scheme by leveraging existing public auditing techniques, such

*Corresponding author
Email addresses: ybmiao@xidian.edu.cn (Yinbin Miao), cryptjweng@gmail.com (Jian Weng), xmliu@smu.edu.sg (Ximeng Liu), raymond.choo@fulbrightmail.org (Kim-Kwang Raymond Choo), zqliu@jnu.edu.cn (Zhiquan Liu), hongweili@uestc.edu.cn (Hongwei Li)