Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Secure-channel free keyword search with authorization in manager-centric databases

Peng Jiang [a,*], *Yi Mu* [b,*], *Fuchun Guo* [b], *Qiaoyan Wen* [a]

[a] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*
[b] *Centre for Computer and Information Security Research, School of Computing and Information Technology, University of Wollongong, Wollongong, Australia*

ARTICLE INFO

Article history:
Available online

Keywords:
Searchable encryption
Secure keyword search
Authorization
Provable security
Database system management

ABSTRACT

Public key encryption with keyword search (PEKS) provides the functionality of encrypted data retrieval with keyword privacy in database systems. PEKS allows a user to specify a keyword and search the encrypted data associated with this keyword that is uploaded by others. In this paper, we investigate the retrieval privilege management in the manager-centric model, where each user has a different search right over the unique keyword set. Unfortunately, employing the prior PEKS and other related cryptographic techniques might suffer from the problems of key abuse and bandwidth consumption. To address these issues, we introduce a new cryptographic primitive called public key encryption with authorized keyword search (PEAKS). In PEAKS, the search right is assigned by the authority over a distinct keyword set and the user with an authorized search right can only search data associated with these keywords. We propose two constructions with formal security proof, namely the basic PEAKS scheme and the secure channel-free PEAKS (SCF-PEAKS) scheme. Both schemes feature with the constant-size authorized token, while the SCF-PEAKS scheme is also resistant against the outsider keyword guessing attacks. The performance evaluation shows that the proposed schemes consume less bandwidth for frequent token update.

1. Introduction

Cyber development, computer advancement and big data emergement benefit much to our real life while kinds of cyber threats over data processing bring about unprecedent challenges to the data security. Security data science (SDS) (Security Data Science) plays a critical role to tackle these threats in the cyber threat management framework (IOCTM) and it has been believed to be the next evolution in the information security and fraud industry. In order to meet the challenges for big data and information explosion, security data scientist put emphasis on new analytic techniques for general/special network environments or systems. Given the volume of data that will be collected, the big data management is necessary and should remain effective in both risk mitigation and practicality.

Cloud database systems have become attractive to enterprises to moderate local burden of maintaining big data in recent years. In reality, data storage in an encrypted format is preferred to protect data privacy while compromising the data utilization. Searchable encryption is a fundamental operation in the database systems and allows searching encrypted

* *Corresponding authors.*
E-mail addresses: pennyjiang0301@gmail.com (P. Jiang), ymu@uow.edu.au (Y. Mu).

http://dx.doi.org/10.1016/j.cose.2016.11.015
0167-4048/© 2016 Elsevier Ltd. All rights reserved.

data that contain the user-specified keyword without decryption. Searchable encryption can be realized in either symmetric setting or asymmetric setting. Although the symmetric searchable encryption (SSE), introduced by Song et al. (2000), enjoys high efficiency (Cash et al., 2013; Curtmola et al., 2006; Kamara et al., 2012), it suffers from complicated secret key distribution/management when users want to share their data. To resolve this problem, Boneh et al. proposed an elegant cryptographic method, namely public key encryption with keyword search (PEKS) (Boneh et al., 2004), which applies the asymmetric encryption setting to enable users to search encrypted data.

Despite advantages in shared data search, the traditional PEKS provides no control about the search privileges over the class of keywords. We consider a scenario that an enterprise outsources business data to a remote server for sharing (Centric Consulting ; CyberArk). For the consideration of sensitiveness, data is encrypted for sharing before outsourcing. To facilitate management, the enterprise applies a manager-centric model and assigns a global manager to manage the access privileges of all employees. In particular, the manager assigns each employee with a class of keywords, with which the employee can retrieve and access a corresponding collection of data (e.g., the data is associated with corresponding keywords). By this, each employee has a different search right, controlled by the manager. Despite enthusiasm around the idea of the manager-centric model, its fulfillment needs secure and effective data utilization.

Inspired by the above scenario, the encrypted data retrieval with different search rights is desirable without comprising privacy or efficiency. We find that it seems to be implausible to apply PEKS in such a manager-centric model. In PEKS, a sender uploads the encrypted data accompanied with a searchable ciphertext to a remote server. The receiver can generate a trapdoor for some keyword, which allows the server to return the data associated with specified keyword without fully decrypting the data. One limitation of PEKS is that the searchable ciphertext is generated from a specific receiver's public key, and only the receiver with corresponding secret key can search. We argue that this limitation makes PEKS incompatible with our scenario, where employees are required to hold search privileges in the setting of the public key corresponding to the enterprise. By using PEKS, each employee has to be given the enterprise's secret key to generate trapdoors for search. This approach suffers from the underlying risk of key abuse, as the enterprise's secret key will be leaked if any user was compromised. In addition, it has restrictions on the manager' control of the searchability to different employees.

With concern of sensitive data, the manager-centric database system has useful applications in the group-based organizations, such as company with business file (Centric Consulting) and DNA institute with DNA information (DNA Group). These information is sensitive and not fully public to anyone. A manager is necessary here to maintain the whole database operation while other members can only have a certain access right to the sensitive data based on their classes, which benefits data management from two main aspects. On one hand, it greatly releases the local storage space and makes data available from anywhere; on the other hand, it enables the manager to control all members in a centralized profile while facilitates members to individually utilize the database.

In this paper, we generalize a new authorized keyword search architecture in which an authority (i.e., manager) keeps the enterprise's secret key and authorizes the search rights to users (i.e., employees). The authority can assign an authorized keyword set to each user, where any keyword in this set can be searched. For keyword search, a straightforward approach is that the authority generates a token for each authorized keyword seperately and provides all tokens corresponding to the authorized keyword set to users. It brings about a drawback that significant bandwidth is due to the authorized tokens consumed from authority to user. To minimize bandwidth, we borrow the property of the aggregation algorithm in token generation for the authorized keyword set. The generated search token for any authorized keyword set is merely one group element, independent of the keyword set size. We insert a timestamp into the authorization. The token can be used to generate the trapdoor for any keyword as long as it belongs the authorized keyword set. It guarantees that only a trapdoor created with a fresh search token is available in passing server's verification and retrieving data. In the meanwhile, we define the security of PEAKS from terms of semantic security against chosen keyword attacks (SS-CKA), indistinguishability against outsider keyword guessing attacks (IND-O-KGA) and trapdoor existential unforgeability (T-EUF). We construct a basic PEAKS scheme to instantiate the new notion. We notice that this basic scheme needs a secure channel between the user and the server like (Boneh et al., 2004), which is usually costly for deployment. For the security, the adversary can launch the keyword guessing attacks to the basic scheme. To remove the secure channel and resist keyword guessing attacks, we design a secure-channel free PEAKS (SCF-PEAKS) scheme by designating a server.

Our contributions can be summarized in threefold.

- We propose a new notion of public key encryption with authorized keyword search (PEAKS). In PEAKS, the authority issues the search ability over a negotiated keyword set to each user with an authorized token. This authorized token needs to be re-issued with time update. Compatible with the notion, we build security models capturing SS-CKA, IND-O-KGA and T-EUF.
- We present two constructions, namely, the basic PEAKS scheme and the SCF-PEAKS scheme. Both schemes achieve the constant-size authorized token and the security of SS-CKA and T-EUF, while the SCF-PEAKS scheme additionally features with IND-O-KGA against the outsider attackers.
- We conduct security analysis and experiment evaluation on the proposed PEAKS and SCF-PEAKS schemes. Both are provable secure and with less bandwidth consumption, particularly efficient in the sensitive database with necessity of frequent token update.

1.1. *Differences between this work and its preliminary version (Jiang et al., 2016)*

Portions of the work presented in this paper have previously appeared as an extended abstract (Jiang et al., 2016). Compared to Jiang et al. (2016), we have enriched and revised the work substantially in the following aspects.

Please cite this article in press as: Peng Jiang, Yi Mu, Fuchun Guo, Qiaoyan Wen, Secure-channel free keyword search with authorization in manager-centric databases, computers & security (2016), doi: 10.1016/j.cose.2016.11.015