Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Verifiable searchable encryption with aggregate keys for data sharing system

Zheli Liu [a], Tong Li [a,*], Ping Li [b], Chunfu Jia [a], Jin Li [b]

[a] College of Computer and Control Engineering, Nankai University, Tianjin, China

[b] School of Computer Science, Guangzhou University, Guangzhou, China

HIGHLIGHTS

- We propose a basic scheme that enables each authorized user to retrieve encrypted documents and verify the results using a single aggregate key.
- In the data sharing system, most of users' computation and storage tasks are confidentially passed to the cloud server.
- Under multi-owner setting, an advance scheme is proposed to decrease users' storage overheads further.

ARTICLE INFO

Article history:
Received 6 June 2016
Received in revised form
9 February 2017
Accepted 12 February 2017
Available online xxxx

Keywords:
Cloud storage
Data sharing
Searchable encryption
Verifiable keyword search

ABSTRACT

In a secure data sharing system, the keyword search over encrypted files is a basic need of a user with appropriate privileges. Although the traditional searchable encryption technique can provide the privacy protection, two critical issues still should be considered. Firstly, a cloud server may be selfish in order to save its computing resources, and thus returns only a fragment of results to reply a search query. Moreover, since different keys are always used for different document sets, making a search query over massive sets and verifying the search results are both impractical for a user with massive keys. In this paper, we propose a scheme named "verifiable searchable encryption with aggregate keys". In the scheme, a data owner need only distribute a single aggregate key to other users to selectively share both search and verification privileges over his/her document sets. After obtaining such a key, a user can use it not only for generating a single trapdoor as a keyword search query, but for verifying whether the server just conducts a part of computing for the search request. Then, we give an advance scheme under the multi-owner setting. Finally, our analysis and performance evaluation demonstrate that the scheme are both practical and secure.

1. Introduction

With the proliferation of demands for personal data storage conveniently, the outsourced data storage technology becomes widely used in the wake of the arrival of the cloud computing paradigm [1–5]. In the fog networking, computing services are enabled to reside at the edge of the network rather than in a big data centre. Thus, besides the storage, today's commercial service-oriented storage systems, such as Dropbox and Sycany, are inclined to provide other services to satisfy clients' requirements that include sharing, retrieving, recovering, cooperative computing. [6–19].

Suppose that group of file owners want that their sensitive files could be securely shared with each other via a cloud server. In addition, an owner would like to authorize others several appreciate privileges like retrieving files over a subset of his/her. For the keyword search mentioned above, the searchable encryption (SE) technology [20,21] is proposed to ensure the privacy and confidentiality while the server performs search operations. Then, the public-key encryption with keyword search (PEKS) schemes [22–24] can be adapted to various scenarios on the cloud.

However, sometimes sharing the search privilege over massive document sets is not easy for their owner. In a traditional PEKS scheme, for confidentiality and efficiency considerations, different keys are always used for different document sets, so that the number of keys the users hold will scale with the number of document sets they can retrieve. Thus, the sharing will naturally involve

* Corresponding author.
E-mail addresses: liuzheli@nankai.edu.cn (Z. Liu), litongziyi@mail.nankai.edu.cn (T. Li), liping26@mail2.sysu.edu.cn (P. Li), cfjia@nankai.edu.cn (C. Jia), lijin@gzhu.edu.cn (J. Li).

http://dx.doi.org/10.1016/j.future.2017.02.024
0167-739X/© 2017 Published by Elsevier B.V.

Please cite this article in press as: Z. Liu, et al., Verifiable searchable encryption with aggregate keys for data sharing system, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.02.024

transmission and key management troubles which are difficult to process for mobile devices. Moreover, for some commercial reasons and hardware restrictions in the peak period, a public cloud server may tend to save its computation or bandwidth. That means, it executes only a fraction of search operations honestly instead of the whole, and then returns the corresponding results. Thus, users probably receive just a part of the search results. It is very essential to add the verification mechanism to PEKS schemes. To ensure the keyword privacy, only the users who hold appropriate verification tokens can verify the results over related document sets. What is worse, the number of tokens used for the verification is also considerable while the user finishes the search over massive document sets.

In this paper, the semi-honest-but-curious server [25], who may execute only a fraction of honest search operations, is set as a computationally bounded adversary. And we propose a verifiable scheme called verifiable searchable encryption with aggregate keys (VSEAK) for data sharing systems to fight against it. In the scheme, the search keys and verification tokens, which is used over a subset of a owner's document sets, are aggregated to one single key. Therefore, in our proposed scheme, to selectively sharing the search privileges of documents, the owner can only send them a single aggregate key instead of massive keys for both the search and verification. Thus, each user only needs to generate a single aggregate trapdoor of a keyword by such a key to perform the keyword search, and then execute the verification by the same key. Somewhat similar to the most existing searchable encryption schemes for the group sharing [26–28], the proposed scheme also set several auxiliary values as public for reducing the repeated calculations and pass some tasks to the server securely. Furthermore, in the multi-owner setting, a user could have several aggregate keys received from different document owners. In order to reduce storage and computation burdens of a user further, we propose an advance scheme. In such a scheme, the user only need store a single user key for operations above, and generate a single trapdoor for searching over multiple users' document sets. The contribution summarized as follows:

1. We propose a basic scheme that enables each authorized user to confidentially retrieve encrypted documents selectively shared by a document provider using a single aggregate key, and to verify the results using the same key.
2. We give a concrete construction which can meet the requirements. In the construction, we design an algorithm to generate a single aggregate key for both search and verification.
3. Under multi-owner setting, we propose an advance scheme which can make the data sharing system more practical.
4. We also conduct related performance evaluation of the basic scheme. The evaluation confirms that the scheme is practical for applications.

The rest of the work is organized as follows: Section 2 is a brief literature review. In Section 3, we state some preliminaries. Section 4 describes the problem statement, the framework of our basic VSEAK scheme, the definition of requirements, and the concrete construction. In Section 5, we give an advance scheme for the multi-owner scenario. In Section 6, we make the security analysis of the basic VSEAK scheme. And Section 7 reports the performance evaluation. Finally, Section 8 concludes the work with a discussion.

2. Related work

Multi-user Search Encryption for Data Sharing. There have been many literatures that measure the cloud security using forensic methods [29–33]. Boneh et al. [22] introduced the public key searchable encryption based on the identity-based encryption, and there is a rich literature on both symmetric searchable encryption (SSE) schemes [20,21] and PEKS schemes [34,23,24]. Under the multi-user setting [35,28,36,37], data owners always want to share their documents with a group of authorized users, and each user who has the search privilege can provide trapdoors of a keyword to perform the search over the shared documents.

For confidentiality considerations, different keys are always used for different documents in data sharing systems during both searching and decrypting. Thus, in most cases of the access control [38], the main problem is how to control which users can access which documents, whereas how to reduce the number of shared keys and trapdoors is not considered. Zheng et al. [39,40] proposed the attribute-based keyword search scheme, which allows a data owner to control the search privilege according to some access control key- or ciphertext-policy.

Verifiable Searchable Encryption. Verifiable computing methods [41,42] have been widely used in the secure outsourced computation. A threat model was considered by Chai et al. [25], in which there is a computationally bounded adversary called semi-honest-but-curious server. Such an adversary satisfies: (1) the server is a storage provider who neither modifies nor destroys the stored documents; (2) the server tries to learn the underlying plaintext or sensitive information from stored documents; (3) the server may forge a fraction of the search outcome as it may execute only a fraction of search operations honestly.

Some approaches about the verifiable keyword search over plaintext have been conducted in [43,44], which is not suitable for the threat model. In the PEKS setting, the keyword search has some requirements like other verifiable computations [45]. Note that, to ensure the keyword privacy, the access control of the verification [46,47] should be achieved. The Bloom filter is used by Zheng et al. [39] to verify whether a keyword really exists in a document set.

Key-aggregate Method. To reduce the number of distributed data encryption keys in a data sharing system, Chu et al. [26] proposed the key-aggregate encryption (KAE) scheme that allows a set of documents encrypted by different keys to be decrypted with a single aggregate key. In addition, such a method of the aggregation can be also applied in the group keyword search [27]. Aiming at the challenge of reducing keys, a PEKS scheme for sharing privileges conveniently is proposed to generate an aggregate key, by which the user can perform the keyword search over each encrypted document set in the key's scope. Therefore, the key-aggregate method allows the efficiently delegating of both decryption and search privileges in a group. This is the main inspiration of our study that the verification privileges of several document sets can also be aggregated.

3. Preliminary

In this section, we review some basic assumptions and cryptology concepts which will be needed later in this paper.

3.1. Complexity assumption

Bilinear Map. A bilinear map is a map $e : \mathcal{G} \times \mathcal{G} \rightarrow \mathcal{G}_1$ with the following properties:

1. Bilinearity: for all $u, v \in \mathcal{G}$ and $a, b \in \mathcal{Z}_p^*$, we have $e(u^a, v^b) = e(u, v)^{ab}$.
2. Non-degeneracy: $e(g, g) \neq 1$.
3. Computability: there is an efficient algorithm to compute $e(u, v)$ for any $u, v \in \mathcal{G}$.