Computers and Electrical Engineering 000 (2017) 1–12

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Verifiable keyword search over encrypted cloud data in smart city☆

Yinbin Miao[a,*], Jianfeng Ma[a], Qi Jiang[a,b], Xiong Li[c], Arun Kumar Sangaiah[d]

[a] School of Cyber Engineering, Xidian University, Xi'an 710071, China
[b] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China
[c] School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China
[d] School of Computer Science and Engineering, VIT University, Vellore, Tamil Nadu 632014, India

ARTICLE INFO

Article history:
Received 24 February 2017
Revised 16 June 2017
Accepted 22 June 2017
Available online xxx

Keywords:
Smart city
Cloud computing
Attribute-based keyword search
Access privilege control

ABSTRACT

In smart city, which integrates the Information and Communication Technologies (ICT) including cloud computing and internet of things, all kinds of data collected by smart devices help to make everything intelligent. Through outsourcing encrypted data to cloud server, data owners can reduce the high storage and computational burden on resources-constrained smart devices. To further avoid the semi-honest-but-curious cloud server returning a fraction of false search results, this paper proposes a verifiable attribute-based keyword search scheme, thereby allowing users to check the correctness of the search results and achieving the fine-grained access control. Besides, our scheme considers the access privileges of the same data according to attribute-based priority tree. The formal security analysis proves that our scheme is secure against the chosen-keyword attacks in the generic bilinear group model, and the experimental simulations using a real-world dataset demonstrate its efficiency and feasibility in practice.

1. Introduction

In smart city [1,2], which emerges for much more comfortable urban spaces and services by integrating multiple Information and Communication Technologies (ICT, for short), the cloud computing and Internet of Things (IOT, for short) are two popular ICT paradigms which have attracted much attention in both academic and industrial fields. In particular, the cloud computing helps to realize and promote the software and hardware resources. In this smart environment, a large amount of data (e.g., text, image and video) related to the urban living [3] are generated by the mobile devices and sensors in order to measure environmental conditions, supervise public safety, and so on. However, a new challenge about storage and sharing of the sensitive data in smart city needs to be solved. Due to the limited storage capacity and bandwidth resources of smart devices, the smart city has turned to cloud computing for data storage and sharing, whereas the weak security provisions in hostile environment remain the significant barriers to the adoption of cloud computing. Hence, the privacy-preserving content sharing has become an even important topic in smart city.

A promising method to enhance privacy [4,5] in smart city is to encrypt shared content before outsourcing it to the cloud servers, while it makes the traditional plaintext retrieval techniques unsuitable for encrypted content. To the best

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. S. Smys.

* Corresponding author.
E-mail address: ybmiao@xidian.edu.cn (Y. Miao).

http://dx.doi.org/10.1016/j.compeleceng.2017.06.021
0045-7906/

of our knowledge, the searchable encryption (SE) technology [6–9], which enables user to securely search over ciphertexts through keywords and selectively retrieve files of interest, is of prime importance in smart city. However, in practice, the cloud server is always treated as a semi-honest-but-curious [10] entity which may conduct a fraction of search operations and return a fraction of false search results to users. To this end, the results verification mechanism (or verifiable keyword search) [11,12] should be furnished in order to guarantee the accuracy of search results.

Besides, the access control is another security approach to facilitate content sharing in a controllable manner because it can empower owner to exert control over content access permissions. At present, the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) technique [13], which can gain one-to-many encryption rather than one-to-one, has turned to be a viable tool to tackle the problem of fine-grained access control. However, it is still a challenge to devise a suitable access control over the same content (e.g., records or documents) because each user has different access privilege [14]. For example, the enterprise manager can access the whole records, while the employees who have lower access privileges just can access the specific records. According to users' different attributes, the users should be assigned different access privileges over the encrypted content.

In this paper, we first try to explore the verifiable keyword search through a third-party audit server [15,16], then make a further step toward specifying access privileges for the encrypted documents in smart city, whereas the most of existing schemes have not considered the two practical issues simultaneously. To address these problems, we present a verifiable keyword search over encrypted cloud data in smart city (VKSE for short) scheme by using the verifiable attribute-based keyword search (VABKS for short) [17] scheme. Similar to the previously proposed CP-VABKS scheme [17], our scheme can achieve selective secure against the chosen-keyword attacks and collusion attacks. Besides, our scheme can accurately verify the correctness of search results and achieve access privilege control over the same data when compared with CP-VABKS scheme. As a further contribution, performance evaluation using a real-world dataset demonstrates that our scheme is efficient and feasible in practice. Specifically, the main contributions of our scheme can be shown as follows:

- *Secure content storage*. To cater for storage-limited entities (e.g., sensor nodes and mobile terminals), our scheme delivers the high content storage burden to a cloud server without leaking the content privacy.
- *Verifiable keyword search*. On the one hand, our scheme enables user to quickly locate the content of interest according to his specified keyword. On the other hand, it can check the correctness of the search results.
- *Access privilege control*. To enhance the access control over the encrypted content, the users are assigned different access privileges according to their attribute sets.

The reminder of this paper is organized as follows. Section 2 provides an overview of the related work. Section 3 gives some preliminary cryptographic backgrounds associated with our work. The problem formulations are described in Section 4, followed by Section 5 which shows the concrete construction of our scheme. Section 6 presents the security and performance analysis. Section 7 draws the concluding remark of this whole paper.

2. Related work

With the emergence of cloud computing, a mass of individuals and enterprises tend to outsource their shared data to the cloud servers for the sake of reducing the local data maintenance and management. Although the encryption mechanism can protect data confidentiality to some extent, it will make the retrieval over encrypted data extremely difficult. Thus, Song et al. [18] gave the first symmetric notion of SE scheme, in which the full text search was allowed. After that, Boneh et al. [6] presented the public key encryption with keyword search scheme. However, these schemes just support single keyword search, which will yield many irrelevant search results and definitely bring down user search experience. To compensate for this, abundant multi-keyword search schemes [19–23] enriched with different features have been proposed.

However, most of the SE schemes suffer from the rigid and inflexible definition of fine-grained access control. A way to solve this problem is to utilize the CP-ABE [13] technique which is suitable for granting the access permissions according to users' attributes rather than user-list. In the CP-ABE scheme, the ciphertexts are described by an access policy, while the user's secret key is associated with an attribute set. Thus, the user can decrypt the ciphertexts if and only if there is a match between attribute set and access policy. To enable keyword search in the context of CP-ABE, Zheng et al. [17] put forward the first ciphertext-policy attribute-based keyword search (CP-ABKS) scheme, whereas this scheme is susceptible to the off-line keyword guessing attacks. For this reason, Qiu et al. [24] gave a hidden policy CP-ABKS scheme with leaking nothing to unauthorized users.

Besides, in real-world applications, the cloud server is always assumed to be semi-honest-but-curious. That is to say, aiming to save computing resources and hide data loss accidents, the cloud server may selfishly execute a fraction of search operations and return a fraction of false search results. Hence, it is critical important to provide a results verification mechanism to guarantee the correctness of search results. Although the CP-VABKS scheme [17] can check the accuracy of returned results, it will incur high communication costs due to the high false positive rate caused by Bloom Filter. Inspired by the VABKS scheme, Sun et al. [11] provided an authenticity check over the search results as well as a fine-grained authorization, whereas this scheme leaded to high computational burden increasing with the number of attributes in system.

The previous schemes can achieve the verifiable keyword search over the encrypted content to some extent by employing Bloom Filter, while these schemes cannot accurately verify the authenticity of the search results due to the high false positive rate caused by the inherent defect of Bloom Filter. In addition, theses schemes cannot be applied to a broad

Please cite this article as: Y. Miao et al., Verifiable keyword search over encrypted cloud data in smart city, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.06.021