Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

Certificateless searchable public key encryption scheme secure against keyword guessing attacks for smart healthcare[☆]

Mimi Ma[a,b], Debiao He[c,*], Shuqin Fan[a], Dengguo Feng[a]

[a] State Key Laboratory of Cryptology, Beijing, China
[b] College of Information Science and Engineering, Henan University of Technology, Zhengzhou, China
[c] Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan, China

ARTICLE INFO

Article history:

Keywords:
Certificateless public key encryption
Searchable encryption
Privacy
Smart healthcare

ABSTRACT

The smart healthcare system (SHS) provides a new information service mode. It greatly improves the diagnostic efficiency by monitoring patients' signs information via various wearable devices. To ensure the confidentiality of sensitive information, the security and privacy issues have drawn wide attention. The searchable encryption technology is suitable for addressing these issues, because it supports search over encrypted data and provides data privacy protection. Recently, many searchable public-key encryption (SPE) schemes have been designed to balance security and efficiency. However, these SPE schemes face the challenge of certificate management or key escrow. This is because they are constructed based on public key infrastructure (PKI) or identity (ID) cryptosystem. Meanwhile, most of SPE schemes are subject to great security threats, such as keyword guessing attacks (KGA). To resolve the above problems, this paper designs a secure certificateless SPE scheme for SHS, and this scheme does not require the use of secure channels, i.e., a SCF-CLSPE scheme. We prove that this SCF-CLSPE scheme can resist KGA and chosen keyword attacks (CKA) under standard model. In addition, the results of performance analysis indicate that this SCF-CLSPE scheme can achieve better efficiency.

© 2019 Published by Elsevier Ltd.

1. Introduction

With Internet as core, the Internet of Things (IoT) embeds all objects in the network through various smart sensing devices, and provides an intelligent network integrating the technologies of intelligent identification, positioning, tracking and monitoring [1,2]. At present, the IoT technology has been gradually applied in many areas (e.g., intelligent logistics and smart healthcare), and has received widespread attention in academia and industry. In particular, the IoT has played a key role in healthcare industry, such as improving the quality of healthcare and realizing telemedicine, thus promoting the prosperous development of smart healthcare [3].

The SHS system relies on the advanced IoT technology to realize real-time interaction between patients, doctors and hospitals. It gradually becomes an information-based and intelligent medical service platform [4,5]. Compared to traditional healthcare system, SHS provides more flexible and convenient medical services for patients, and has significant advantages such as higher accuracy and lower cost. In SHS, some wearable smart devices (e.g., smart bracelet) are used to track and monitor patients' signs information (e.g., temperature and blood pressure) in real time, so that doctors can timely diagnose patients and effectively control the patients' conditions. In addition, it can improve the utilization rate of medical resources, so as to reduce the phenomenon such as difficulty in seeing a doctor, tension between doctors and patients, and frequent medical accidents.

However, as SHS matures, the amount of healthcare data it produces is also increasing rapidly [6]. How to deal with this big data becomes a challenge. What's remarkable is that the cloud computing can quickly process cumbersome data [7]. Therefore, cloud computing can not only greatly promote the healthy development of SHS, but also provide a broader prospects for SHS: 1) it improves the ability of data computing and storage; 2) it provides a platform for precise medical treatment to help doctors better conduct remote diagnosis for patients; 3) the healthcare data can be collected more comprehensively, and doctors can share the latest data in real time. Fig. 1 is the architecture diagram of a cloud-based SHS. In cloud-based SHS system, the healthcare data is first collected through various smart sensing devices, and then

[☆] The work was supported by the National Natural Science Foundation of China (Nos. 61902111, 61932016, 61972294) and the High-level talent Fund Project of Henan University of Technology (No. 31401164).

[*] Corresponding author.

E-mail addresses: mamimi421@126.com (M. Ma), hedebiao@163.com (D. He), fansq@sklc.org (S. Fan), fengdg@263.net (D. Feng).

https://doi.org/10.1016/j.jisa.2019.102429
2214-2126/© 2019 Published by Elsevier Ltd.

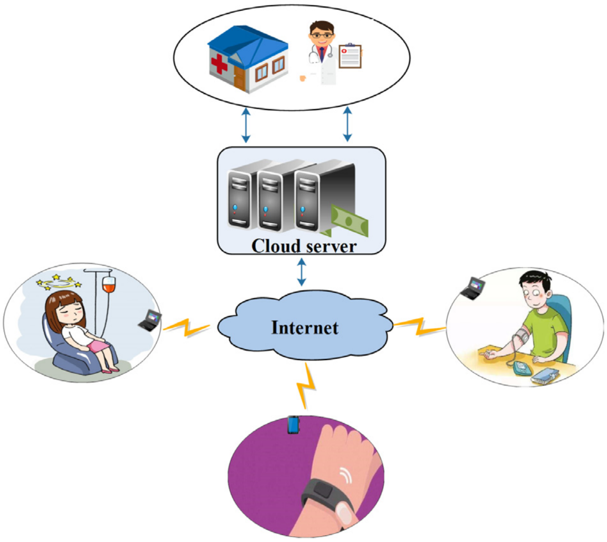

Fig. 1. The architecture of cloud-based SHS.

uploaded to the cloud, which can not only reduce overhead for hospitals, but also improve work efficiency. However, if this data is to be shared, the patients' rights and privacy will be involved.

To strengthen data management and enhance data security, users usually tend to encrypt data and then outsource ciphertext to the cloud. However, once the data is encrypted, its original structure will change, and the search algorithm designed for original plaintext will not work. To address this issue, the technology of searchable encryption (SE) is introduced [8]. SE allows encrypted data to be searched by keywords, and does not expose any information about original data. According to the different ways of secret key selection, SE can be divided into two forms, one is searchable public key encryption (SPE), and the other is searchable symmetric encryption (SSE) [9]. SSE schemes have high efficiency, but it cannot be well applied to the multi-user data sharing scenario due to the symmetry of its key [10]. In this paper, we focus on the SPE schemes. Recently, several SPE schemes have been constructed for protecting data privacy [11–17]. The previously proposed SPE schemes provide different search functions and security guarantees for data privacy, however, these schemes cannot avoid the inherent burden of certificate management and key escrow. That is because they are constructed based on public key infrastructure (PKI) cryptosystem or identity (ID) cryptosystem. To address these issues that exist in PKI-based or ID-based schemes, a new definition of certificateless public key cryptography (CLPKC) is given by Al-Riyam et al. [18]. Recently, Peng et al. [19] proposed a certificateless searchable public key encryption (CLSPE) scheme. He et al. [20] proposed an authenticated CLSPE scheme. However, all of the existing CLSPE schemes are only proven secure under random oracle model, which only provides a heuristic argument. We therefore argue that it's meaningful to design a CLSPE scheme without random oracle model, and we present a new system/security model for CLSPE scheme on the basis of scheme [17] in this paper.

1.1. Our contributions

We construct a secure-channel free certificateless searchable public key encryption (SCF-CLSPE) scheme without random oracle model for SHS. Specifically, the main contributions are described as below:

- Firstly, we design a new SCF-CLSPE scheme for SHS, and the proposed scheme avoids the use of secure channels by involving the server's public/private key pair.
- Secondly, we analyze the security of SCF-CLSPE, and the security analysis indicates that SCF-CLSPE could resist KGA and CKA attacks.
- Finally, we test the efficiency of SCF-CLSPE from the aspects of computation cost and communication cost, and the test results demonstrate that SCF-CLSPE has lower computation/communication costs.

1.2. Organization of the rest paper

Below is the framework for the remainder of this paper. Section 2 summarizes some related work. Section 3 presents some preliminary knowledge including complexity assumptions and the system model for SCF-CLSPE. Section 4 gives a concrete instance of SCF-CLSPE. Section 5 defines the security model for SCF-CLSPE and presents the security analysis. The performance of SCF-CLSPE is analyzed in Section 6. Finally, Section 7 makes a summary for this paper.

2. Related literature

Song et al. [8] gave the first SE scheme on the basis of symmetric cryptosystem, i.e., a SSE scheme, which only allows users with the secret key to search for encrypted data. However, their scheme cannot resist statistical attack. And in Song et al.'s scheme, the search complexity grows linearly with files' size due to their construction is based on the idea of linear scanning. Later on, many SSE schemes have been designed to balance security and efficiency [21–24]. SSE is of high speed and easy to implement. However, it faces threats in secret-key distribution and management.

To resolve above issues, a new cryptographic primitive called SPE was proposed by Boneh et al. [10]. They considered the email system and gave a concrete scheme of SPE. The SPE scheme contains three participants, namely a mail server, a data owner and a data receiver. The search process is performed as the following steps: 1) some keywords are extracted from each document; 2) the data owner uses receiver's public-key to encrypt the extracted keywords, and then uploads all encrypted data to the mail server; 3) the receiver generates a trapdoor of the keywords to be retrieved using his/her own private-key, and transmits the generated trapdoor to the server; 4) the server tests the match between ciphertext and trapdoor, and feeds the test result back to the receiver.

Abdalla et al. [25] analyzed that scheme [10] is computationally consistent, and then they designed a statistically consistent scheme. Baek et al. [26] found that the scheme [10] is inefficient and impractical because it cannot transmit the trapdoor between server and receiver via public channel. To resolve this issue, they constructed a SPE scheme with no secure channels, i.e., a SCF-SPE, which involved the server's public/private keys. The test algorithm in SCF-SPE can only be executed by the designated server. Later, the security model of scheme [26] is improved by Rhee et al. [27]. And in [27], they constructed a new SCF-SPE instance under the improved security model. Byun et al. [28] observed that many SPE schemes [10,29] are vulnerable to KGA attack due to the following reasons: 1) the space that keywords chosen from is usually smaller; 2) users tend to search using some commonly keywords.

Fang et al. [30] presented an efficient SCF-SPE scheme under the standard model, and stated that their scheme is secure against KGA attack. However, Shao et al. [31] analyzed that the scheme [30] cannot resist KGA attack if the attacker is the server. To enhance the security, they improved the security model of SCF-SPE, and constructed a modified SCF-SPE scheme. Recently, Lu et al. [17] analyzed schemes [30,31], and proved that neither

Download English Version:

https://daneshyari.com/en/article/13432355

Download Persian Version:

https://daneshyari.com/article/13432355

Daneshyari.com