Computers and Electrical Engineering 000 (2017) 1–12

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Certificateless searchable public key encryption scheme for mobile healthcare system☆

Mimi Ma[a], Debiao He[b,c,*], Muhammad Khurram Khan[d], Jianhua Chen[a]

[a] School of Mathematics and Statistics, Wuhan University, Wuhan, China
[b] State Key Lab of Software Engineering, Computer School, Wuhan University, Wuhan, China
[c] Co-Innovation Center for Information Supply and Assurance Technology, Anhui University, Hefei, China
[d] Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia

ARTICLE INFO

Article history:
Received 25 April 2017
Revised 10 May 2017
Accepted 12 May 2017
Available online xxx

Keywords:
Certificateless public key encryption
Keyword search
Semantically security
Mobile healthcare system

ABSTRACT

As mobile communication technology develops, mobile healthcare system (MHS) is becoming a hot topic in academia and healthcare industry. MHS refers to providing medical services through mobile communication equipments. However, it faces many challenges, such as the finite storage, computing power and communication capabilities of MHS devices. To address this problem, the concept of cloud-based MHS has been proposed recently. Meanwhile, healthcare data outsourcing to cloud raises privacy and confidentiality concerns. In order to protect data security, we present an efficient certificateless public key encryption with keyword search (CLPEKS). Security analysis indicates that our scheme is secure resist chosen keyword and keyword guessing attacks in random oracle model. The computation costs of KeyGen, CLPEKS, Trapdoor and Test phases decreased by 84.68%, 55.04%, 36.1% and 28.73%, respectively, compared with Peng *et al.'s* scheme.

1. Introduction

Mobile healthcare system (MHS) [1] is an important branch of electronic healthcare that provides medical services and informations by modern communication and sensor technologies. Its biggest feature is to provide healthcare services anytime anywhere or pervasively (Pervasive Healthcare). The application of MHS involves many aspects, mainly related to remote data acquisition, remote monitoring, tracking and diagnostic treatment and communication among medical workers. With the increasing popularity and coverage of mobile intelligent terminals and global mobile communication networks, mobile healthcare has also been made clear significant effect. MHS has a very broad application prospect as an effective service tool to achieve real-time delivery, access and storage of healthcare information. Although MHS is showing huge market potential and good application prospects, its development still faces enormous challenges, such as the limitations of computing capabilities and storage capabilities of mobile devices, data resources parallel operation problem and how to effectively realize the real-time sharing and management of medical information to meet the needs of different roles (e.g. patients, doctors and medical suppliers).

Advance in sensing technology and cloud computing [2,3], more and more individuals and organizations are opting for cloud services such as Microsoft Azure [4] and Amazon Simple Storage Service (Amazon S3) [5] to manage their data in

☆ Reviews processed and approved for publication by Editor-in-Chief.

* Corresponding author.
E-mail address: hedebiao@163.com (D. He).

http://dx.doi.org/10.1016/j.compeleceng.2017.05.014
0045-7906/

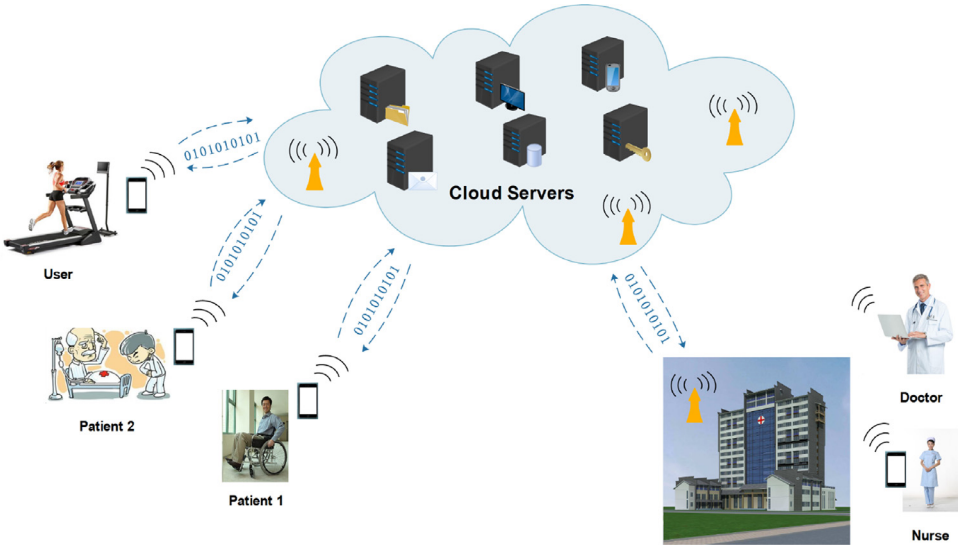

Fig. 1. A typical mobile healthcare system architecture.

order to avoid troublesome data management at local machines and enjoy convenient service. Recently, the concept of cloud computing has been introduced to MHS [6].

Cloud computing can be an effective solution to massive data analysis and processing problem, and provides reliable, scalable data-processing storage center, in reducing the terminal equipment required while improving the processing of data to meet needs of storage and management user's data in MHS. By outsourcing data to cloud server, MHS can provide more richer services. Fig. 1 shows a typical architecture of mobile healthcare system based on cloud platform. Meanwhile, data outsourcing raises confidentiality and privacy concerns, since the cloud server may be corrupted or may be malicious.

In order to ensure that security and confidentiality of sensitive data, data owner can encrypt his data prior to uploading it into cloud server. But it produces another problem, that is how to search the encrypted data. A simple solution is that the user could download all the encrypted data, then decrypt the ciphertext before retrieve. This is undoubtedly, it requires a great number of calculation overhead and needs plenty of device's space. Therefore, it is inefficient for large databases. Searchable encryption technology came into being, it not only accomplishes the ciphertext search, but also ensures the confidentiality of the data [7,8].

Searchable encryption techniques can be classify into symmetric and asymmetric searchable encryption. Song *et al.* [9] first put forward symmetric searchable encryption on the basis of stream cipher. But a big disadvantage of searchable encryption scheme based on symmetric key is key distribution difficulties, and application scenarios are very limited. To solve this problem, public-key encryption with keyword search, or PEKS for short, is designed by Boneh *et al.* [10]. In PEKS, suppose Alice wants to send medical records M with some keywords $W = \{w_1, w_2, \cdots, w_n\}$ to Bob through an untrusted cloud server. Alice uses Bob's public key to generate encrypted data $Enc(M)$ and the encrypted keyword index $ind\{W\}$. Then, Alice sends both $Enc(M)$ and $ind\{W\}$ to cloud. If Bob wants to search the medical records comprising keyword w, he first uses his own private key to generate the trapdoor T_w of keyword w, and sends it to server. Once receiving T_w, server will start to test keyword index $ind\{w\}$ matching the trapdoor T_w, and returns the corresponding encrypted records $Enc(M)$ to Bob.

Public-key infrastructure (PKI for short) is a significant platform that could provide public key encryption and digital signature services. Certificate Authority (CA) is the kernel part of PKI system, which is responsible for issuing and managing all users' digital certificates. However, certificate management becomes an intractable problem as the increase of the number of users. To reduce the need for certificate management, identity-based public key cryptography (ID-PKC) was presented by Shamir [11], where user's public key could be directly obtained from his identification (e.g. telephone number, e-mail address or user's name). A trusted key generation center (KGC) will be an indispensable part in ID-PKC to generate user's private key. In these circumstances, KGC could decrypt any ciphertext and forge any message's signature. Therefore, ID-PKC system faces the challenge of key escrow problem. Certificateless public key cryptography (CLPKC) is showed by Al-Riyami and Paterson [12], which gets rid of key escrow problem. In CLPKC system, on the one hand, KGC generates a partial private key, on the other hand, the user chooses a random number as its secret value. The user's private key generated by the above two parts and can't be obtained by KGC. Later on, many of public-key encryption models and signature schemes in certificateless system have been presented [13–15]. But little scheme has been satisfied both PEKS system and certificateless features.

Please cite this article as: M. Ma et al., Certificateless searchable public key encryption scheme for mobile healthcare system, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.05.014