Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Cost-effective secure E-health cloud system using identity based cryptographic techniques

Xu An Wang[a,c,*], Jianfeng Ma[b], Fatos Xhafa[d], Mingwu Zhang[e], Xiaoshuang Luo[c]

[a] School of Telecommunications Engineering, Xidian University, PR China
[b] School of Cyber Engineering, Xidian University, PR China
[c] Engineering University of Chinese Armed Police Force, PR China
[d] Department of Computer Science, Technical University of Catalonia, Spain
[e] Hubei University of Technology, PR China

HIGHLIGHTS

- We show how to securely integrate the IBE and IBPRE into an E-health cloud system.
- We also propose a novel IBE scheme and prove its security.
- Furthermore, we propose a novel IBPRE scheme. It does not follow Green's paradigm.
- We propose an E-health cloud system framework based on our IBE and IBPRE.
- Our IBPRE scheme can be highly cost-effective for E-health cloud system users.

ARTICLE INFO

Article history:
Received 16 January 2016
Received in revised form
15 July 2016
Accepted 16 August 2016
Available online xxxx

Keywords:
Secure e-health cloud system
Identity based encryption
Identity based proxy re-encryption
Cost-effective

ABSTRACT

Nowadays E-health cloud systems are more and more widely employed. However the security of these systems needs more consideration for the sensitive health information of patients. Some protocols on how to secure the e-health cloud system have been proposed, but many of them use the traditional PKI infrastructure to implement cryptographic mechanisms, which is cumbersome for they require every user having and remembering its own public/private keys. Identity based encryption (IBE) is a cryptographic primitive which uses the identity information of the user (e.g., email address) as the public key. Hence the public key is implicitly authenticated and the certificate management is simplified. Proxy re-encryption is another cryptographic primitive which aims at transforming a ciphertext under the delegator *A* into another ciphertext which can be decrypted by the delegatee *B*. In this paper, we describe several identity related cryptographic techniques for securing E-health system, which include new IBE schemes, new identity based proxy re-encryption (IBPRE) schemes. We also prove these schemes' security and give the performance analysis, the results show our IBPRE scheme is especially highly efficient for re-encryption, which can be used to achieve cost-effective cloud usage.

1. Introduction

E-health system. E-health systems nowadays are becoming more and more popular for its smoothly integrating information technology and traditional medical diagnosis process [1]. Traditionally when we have some troubles with ourselves like headaches, we go to hospital to see a doctor. The doctor needs carefully check our body's state to decide what kind of disease we have. In this process, he needs to handle many images, referrals, medical records, etc., and these are tedious tasks. E-health systems can handle all these work automatically, the purpose of them is to develop and manage the information system of health care. In China, as one typical application of the promising *Internet*+ technology, we hope in the near future it will be one of the most practical public administration services. Electronic Health Records (EHR) play a central role in the E-health system, they can be recorded by doctors and nursers, collected by sensors in wireless body sensor network, etc. By using E-health system, medical doctors can freely exchange health records, patient can easily access his or her health records through

[*] Corresponding author at: School of Telecommunications Engineering, Xidian University, PR China.
E-mail address: wangxazjd@163.com (X.A. Wang).

http://dx.doi.org/10.1016/j.future.2016.08.008
0167-739X/© 2016 Elsevier B.V. All rights reserved.

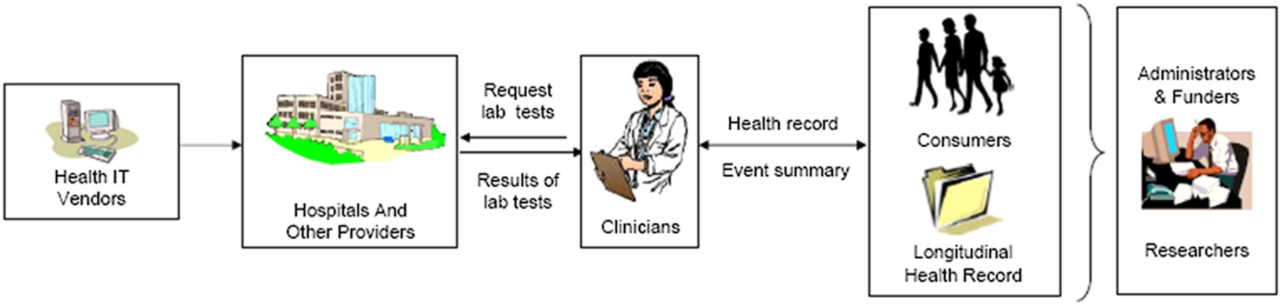

Fig. 1. Overview on E-health system.

a designated patients portal, and the health care providers can enquire patients time-critical and general data smoothly. The system stores the patients medical history and is a vital information source for physicians. We can see an overview on E-health system in Fig. 1. Clinicians record EHRs and related event summary from E-health system consumers and longitudinal health records. These EHRs can be further supplied to hospitals and other medical providers for deep analysis like lab tests. Health IT vendors can also better support these hospitals from these health records by dynamically adjusting their policy. Administers, funders or researchers can also benefit from this process. Security and privacy are one of the main issues to hesitate to widely adapt E-health systems, for electronic health records are sensitive information. Malicious attackers can use them to cause troubles, for example, they can stop running the patient's heart pacemaker and thus endanger the patient's life. Although there are proposals on how to secure the E-health system, many of them use traditional PKI infrastructure to implement cryptographic mechanisms and this is not convenient for many users. In this paper, we show how to secure E-health systems, mainly on fuzzy biometric E-health system using the identity based cryptographic techniques, which no more need the certificates.

IBE. In 1984, Shamir [2] introduced the concept of identity-based cryptography to ease the certificate management in traditional public key system. A user's public key in an IBE scheme which the identity information of the user (e.g., email address). Hence the public key is implicitly authenticated and the certificate management is simplified. However, the first practical IBE scheme [3] was only proposed 17 years after its concept was proposed. Since then, many practical IBE schemes with different properties have been proposed [4–7].

Until now, there are many interesting applications of IBE, but nearly no work on how to apply them to the E-health system. Although we can see some work on using attribute based encryption (ABE) in the E-health system, but no work concentrates on how to handle identities directly in these systems. If we can directly use some string such as the email address as the identity public key, then the workload of patient users can be decreased much. We can see an overview on IBE in Fig. 2. In Fig. 2, Alice encrypted her health information using identity "bob@medical.com " to doctor Bob, while doctor Bob requests his private key from the CA/PKG.

IBPRE. The concept of proxy re-encryption (PRE) was proposed by Blaze et al. [8] in 1998, which allows a semi-trusted proxy, with some information (a.k.a., the re-encryption key), to translate a ciphertext under the delegator's public key into another ciphertext that can be decrypted by the delegatee's secret key. However, the proxy cannot access the plaintext. According to the direction of transformation, PRE schemes can be classified into bidirectional schemes and unidirectional schemes. Also according to the times the transformation can apply on the ciphertext, PRE schemes can be classified into single-hop schemes and multi-hop schemes. At NDSS'05, Ateniese et al. [9] proposed a few unidirectional PRE schemes and discussed its several potential applications such as distributed secure file systems. Later, many unidirectional PRE schemes with different properties have been proposed [10–15]. Due to the simpler certificate management in IBE, Green and Ateniese [16] extended PRE to the IBE setting, i.e. identity based proxy re-encryption (IBPRE). They also discussed its several interesting applications such as bridging IBE and PKE. Since then, several IBPRE schemes have been proposed [17,18,12,19,14,20], but none of them except [13,14] can achieve master secret security: the corrupted proxy and delegatee cannot derive the delegator's private key. However, IBPRE schemes in [13] are generic constructions relying on CCA-secure 2-level hierarchical ID-based (2,2) threshold cryptosystem, they are inefficient. IBPRE schemes in [14] rely on conditional proxy broadcast re-encryption, they are also inefficient and can only achieve security against replayable chosen ciphertext attacks (RCCA). We can see an overview on IBPRE in Fig. 3. In Fig. 3, patient encrypts her health information using doctor's identity "Doctor@medical.com ", and outsources the ciphertexts to the cloud. In the setup phase, doctor has sent the re-encryption key to the proxy, and thus the proxy can re-encrypt the ciphertexts to be the ciphertexts under the assistant doctor's identity "AssistantDoctor@medical.com ". By using IBPRE, the assistant doctor shares the patient's health information without the cloud knowing any sensitive information.

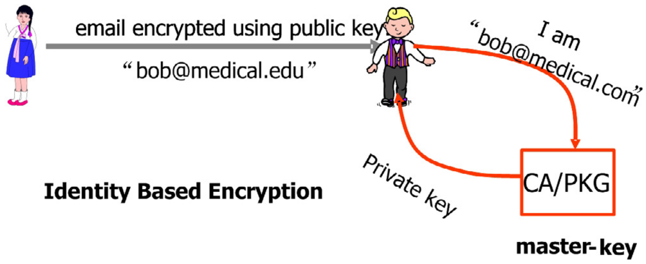

Fig. 2. Overview on IBE.

1.1. Our contribution

We show how to securely integrate the IBE and IBPRE into an E-health cloud system, and thus explore on how to use identity related cryptographic techniques for securing the E-health cloud system, especially on the confidential property. We also propose novel IBE and IBPRE schemes and prove their security. Although there exist many IBE schemes with different properties, however one part of the private key in all these IBE schemes is of the form: $y = f(msk)$ where msk is the master key and y is an element in the underlying bilinear group $\mathbb{G}$. We construct a new identity based encryption scheme. The main novelty of our IBE is that: one part of the private key is $y = f(msk)$, where msk is the master key and y is an element in $\mathbb{Z}_p^*$. Here p is the underlying bilinear group's prime order. To resist the adversary to extract useful information on the master key from this part of the private key, we introduce