Computer Methods and Programs in Biomedicine 157 (2018) 191–203

Contents lists available at ScienceDirect

Computer Methods and Programs in Biomedicine

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

Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems

Chun-Ta Li[a,*], Dong-Her Shih[b], Chun-Cheng Wang[b]

[a] Department of Information Management, Tainan University of Technology, 529 Zhongzheng Road, Tainan City 71002, Taiwan, ROC
[b] Department of Information Management, National Yunlin University of Science and Technology, 123 University Road, Yunlin 64002, Taiwan, ROC

ARTICLE INFO

Article history:
Received 12 December 2017
Revised 25 January 2018
Accepted 2 February 2018

Keywords:
Authentication
Cloud computing
Cryptanalysis
Privacy preservation
Telecare medical information system

ABSTRACT

Background and Objective: With the rapid development of wireless communication technologies and the growing prevalence of smart devices, telecare medical information system (TMIS) allows patients to receive medical treatments from the doctors via Internet technology without visiting hospitals in person. By adopting mobile device, cloud-assisted platform and wireless body area network, the patients can collect their physiological conditions and upload them to medical cloud via their mobile devices, enabling caregivers or doctors to provide patients with appropriate treatments at anytime and anywhere. In order to protect the medical privacy of the patient and guarantee reliability of the system, before accessing the TMIS, all system participants must be authenticated.

Methods: Mohit et al. recently suggested a lightweight authentication protocol for cloud-based health care system. They claimed their protocol ensures resilience of all well-known security attacks and has several important features such as mutual authentication and patient anonymity. In this paper, we demonstrate that Mohit et al.'s authentication protocol has various security flaws and we further introduce an enhanced version of their protocol for cloud-assisted TMIS, which can ensure patient anonymity and patient unlinkability and prevent the security threats of report revelation and report forgery attacks.

Results: The security analysis proves that our enhanced protocol is secure against various known attacks as well as found in Mohit et al.'s protocol. Compared with existing related protocols, our enhanced protocol keeps the merits of all desirable security requirements and also maintains the efficiency in terms of computation costs for cloud-assisted TMIS.

Conclusions: We propose a more secure mutual authentication and privacy preservation protocol for cloud-assisted TMIS, which fixes the mentioned security weaknesses found in Mohit et al.'s protocol. According to our analysis, our authentication protocol satisfies most functionality features for privacy preservation and effectively cope with cloud-assisted TMIS with better efficiency.

1. Introduction

Regarding the use of information and communication technology for telecare medical information systems (TMIS) in hospitals and medical institutions, it enables medical personnel and patients to perform remote medical care services via Internet and reduces exorbitant medical expenditure and time to make hospital trips [2,3,5,11,13–15,18,19,21,23,24,31]. In case of patients were seeking medical treatments at different hospitals, the cloud-assisted platform enables the sharing of patient's electronic medical records (EMR) from one hospital to the next without reduplicated inspections. By integrating medical institutions and a cloud platform, patients and doctors can conveniently receive medical services for patients' health conditions at anywhere and check the medical measures according to the doctors' treatment reports to implement real telemedicine [20,22].

In cloud-assisted TMIS, four roles involve in this system: the patient, the trusted healthcare center, the doctor, and the cloud server. Before requesting for telemedicine, body sensors are embedded in the patient's body and collect the personal health information of the patient. The cloud-assisted TMIS features a healthcare center upload procedure (HUP), a patient data upload procedure (PUP), a treatment procedure (TP) and a check up procedure (CP). Fig. 2 illustrates the entire architecture of cloud-assisted TMIS and the detailed explanation is given below.

- HUP: The patient goes to the healthcare center for health inspection and performs registration with healthcare center. Once

[*] Corresponding author.
E-mail addresses: th0040@mail.tut.edu.tw (C.-T. Li), shihdh@yuntech.edu.tw (D.-H. Shih).

https://doi.org/10.1016/j.cmpb.2018.02.002
0169-2607/© 2018 Elsevier B.V. All rights reserved.

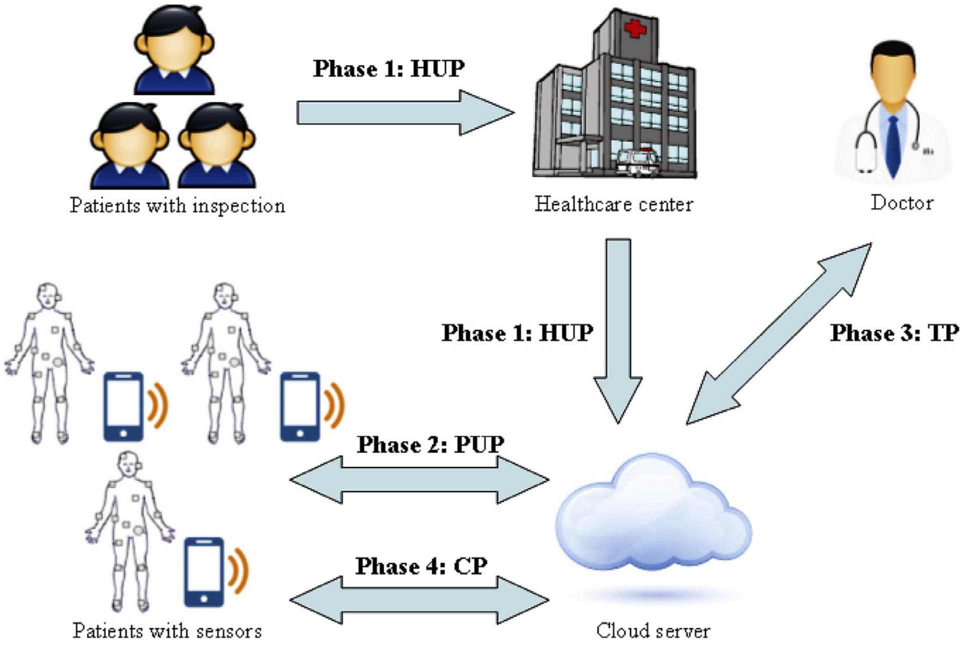

Fig. 1. Cloud-assisted TMIS.

Healthcare center (H)		Cloud (C)
Input ID_H, random number R		
	$\xrightarrow[\text{(secure channel)}]{< ID_H, R >}$	
		$A = h(ID_H\|\|R\|\|x)$ $S_1 = h(A)$ $B = ID_H \oplus x$
	$\xleftarrow[\text{(public channel)}]{< B, S_1 >}$	
$x' = B \oplus ID_H$ $A' = h(ID_H\|\|x'\|\|R)$ $S_1 \overset{?}{=} h(A')$ $SK_{HC} = h(ID_H\|\|A'\|\|B)$ $key_1 = h(ID_P\|\|OTP)$ $C_H = E_{key_1}(m_H)$ $Sig_H = S_{PR_H}(MD_H)$ $C_1 = E_{SK_{HC}}(ID_P, C_H, Sig_H, NID)$ $S_2 = h(SK_{HC}\|\|C_1)$		
	$\xrightarrow[\text{(public channel)}]{< S_2, C_1 >}$	
		$SK'_{HC} = h(ID_H\|\|A\|\|B)$ $S_2 \overset{?}{=} h(SK'_{HC}\|\|C_1)$ $D_{SK'_{HC}}(C_1)$ Store ID_P, C_H, Sig_H, NID

Fig. 2. Overview of the healthcare center upload phase of Mohit et al.'s protocol.

the patient's inspection report is released, the healthcare center uploads it to the cloud server.

- PUP: After finishing the healthcare center upload procedure, the patient can download his/her health inspection report from the cloud. Then the patient uses personal mobile device to upload the new report by integrating the health inspection report with the sensing report collected from body sensors to the cloud server.
- TP: After finishing the patient upload data procedure, the doctor can download the new report of the patient from the cloud server and perform treatment by looking into the report. Then the doctor generates the medical diagnosis of the patient's symptom and uploads it to the cloud server.
- CP: After finishing the treatment procedure, in order to provide telemedicine service, the patient can download the medical diagnosis from the cloud and view the medical measures according to the doctor's treatment report.