J Med Syst (2016) 40: 117
DOI 10.1007/s10916-016-0474-9

MOBILE SYSTEMS

A Secure Cloud-Assisted Wireless Body Area Network in Mobile Emergency Medical Care System

Chun-Ta Li[1] · **Cheng-Chi Lee**[2,3] · **Chi-Yao Weng**[4]

Received: 4 November 2015 / Accepted: 8 March 2016 / Published online: 21 March 2016

Abstract Recent advances in medical treatment and emergency applications, the need of integrating wireless body area network (WBAN) with cloud computing can be motivated by providing useful and real time information about patients' health state to the doctors and emergency staffs. WBAN is a set of body sensors carried by the patient to collect and transmit numerous health items to medical clouds via wireless and public communication channels. Therefore, a cloud-assisted WBAN facilitates response in case of emergency which can save patients' lives. Since the patient's data is sensitive and private, it is important to provide strong security and protection on the patient's medical data over public and insecure communication channels. In this paper, we address the challenge of participant authentication in mobile emergency medical care systems for patients supervision and propose a secure cloud-assisted architecture for accessing and monitoring health items collected by WBAN. For ensuring a high level of security and providing a mutual authentication property, chaotic maps based authentication and key agreement mechanisms are designed according to the concept of Diffie-Hellman key exchange, which depends on the CMBDLP and CMBDHP problems. Security and performance analyses show how the proposed system guaranteed the patient privacy and the system confidentiality of sensitive medical data while preserving the low computation property in medical treatment and remote medical monitoring.

Keywords Authentication · Chaotic maps · Cloud computing · Emergency medical care system · Network security · Wireless body area network

This article is part of the Topical Collection on *Mobile Systems*

✉ Cheng-Chi Lee
cclee@mail.fju.edu.tw

Chun-Ta Li
th0040@mail.tut.edu.tw

Chi-Yao Weng
cyweng@mail.nptu.edu.tw

[1] Department of Information Management, Tainan University of Technology, No. 529, Zhongzheng Road, Tainan City 71002, Taiwan, People's Republic of China

[2] Department of Library and Information Science, Fu Jen Catholic University, No. 510, Jhongjheng Road, New Taipei City 24205, Taiwan, People's Republic of China

[3] Department of Photonics and Communication Engineering, Asia University, No. 500, Lioufeng Road, Taichung City 41354, Taiwan, People's Republic of China

[4] Department of Computer Science, National Pingtung University, No. 4-18, Min-Sheng Road, Pingtung City 90003, Taiwan, People's Republic of China

Introduction

Wireless body area networks (WBAN) allow the integration of intelligent and tiny body sensors in and/or around a human body to sense and collect personal health information (PHI) periodically. The PHI sensed by WBAN can be collected by user's personal mobile device, transmitted via wireless communication channels (WiFi, 3G/4G, or satellite) and processed by the authorized participants. WBAN are revolutionizing in a wide range of application domains [31], ranging from remote patient supervision, sport performance monitoring, and M-healthcare social networking. To fight against cardiovascular disease (CVD) and avoid critical emergencies, MyHeart project [9] was in progress and

supported by several partners from ten different countries. The MyHeart project used smart clothes in which sensors are powered from a centralized on-body power supply and embedded in the piece of clothing [32]. Thus it is capable of transmitting sense data to professional doctors or clinical staffs and this CVD system can monitor patient status in real time. In a common healthcare scenario, the sampling of body sensors is required to be scalably stored and must be accessible at anytime and from anywhere. Owing to the above-mentioned requirements, the cloud-assisted WBAN system can satisfy PHI saving, data analyzing and sharing of sensor data and provide anytime/anywhere access to medical monitoring applications. In this way, it allows monitored patients to leave the healthcare center, provides ubiquitous healthcare and improves their own health and quality of life. Moreover, the consideration of integrating WBAN with cloud-assisted system [7, 36, 39, 48] can be motivated by discussing the following issues:

Interfacing the cloud with WBAN: In order to manage sense data and maintain the quality of medical services, it is important to provide a well-designed interface between WBAN devices and the cloud-assisted platform.

Massive scale and real time processing: A cloud-assisted WBAN system requires ensuring scalability of processing power for different kinds of data analysis and accurately stores and processes the sense data in a cloud environment.

Medical application multiplicity: The development of cloud-assisted WBAN system is a complex task that needs to be tackled by exploiting software engineering methodologies and hardware smart sensors and seamlessly deployed onto the WBAN and cloud-assisted platform.

System efficiency and overhead: In order to develop a reliable and efficient architecture for a cloud-assisted WBAN system, the challenges of this issue include reducing computation complexity, energy consumption and storage/communication overheads.

Security and privacy: Considering ethical and legal aspects of medical systems, the PHI on cloud-assisted WBAN system may be exposed to various kinds of security attacks such as eavesdropping, modifying/forging messages to result in wrong medical diagnosis and masquerading medical participant to get all the private medical information. Therefore, it is important to guarantee both PHI privacy and system security in cloud-assisted WBAN system.

Because the sensitive PHI parameters transmitted over the air and stored in cloud-assisted WBAN system are the basis of medical diagnosis, any destruction of PHI parameters may bring fatal harm to patients and there is a need for introducing a cryptographic scheme to ensure secure communications [8, 34, 38, 42] in cloud-assisted WBAN system.

Related works

In recent years, secure authentication and pairwise key agreement schemes for cloud-assisted WBAN applications have been proposed [1, 17, 28, 47]. In [5, 6], Fortino et al. introduced SPINE2 for developing WBAN applications on heterogeneous sensor nodes and further proposed BodyCloud for integrating cloud computing into body sensor networks. In [37], Shen et al. proposed a hash chain and elliptic curve cryptosystem (ECC) based key management scheme to secure communication between the on-body devices. In [30], Muhammad et al. proposed BARI+, which is a key management scheme and the identities and authentication codes are pre-loaded among all the nodes. Their scheme achieves more efficiency and fulfills many security requirements for WBAN applications. In [29], Mana et al. proposed a trust key management scheme for WBANs and their scheme manages the generation and distribution of symmetric cryptographic keys to constituent body sensors and solves the problem of privacy in WBANs. In [46], Zhou et al. proposed an efficient and secure biometric based deterministic key agreement for WBANs by exploiting the overlap between the biometric characteristics collected by body sensors and the pairwise keys can be definitely negotiated by the interactions between body sensors embedded in the same human body for WBANs. In [33], Ren et al. introduced some approaches that can be used to monitor patients effectively and enhance the functionality of telemedicine systems. Moreover, they further discuss how current secure strategies can obstruct the security attacks faced by wireless communications in mobile healthcare systems. However, most of secure communication schemes are not suitable for WBAN applications due to unable to provide user anonymity [11, 13, 21, 22]. To protect user privacy in WBANs, Liu et al. [27] proposed two certificateless remote anonymous authentication schemes to enable remote WBAN users to anonymously enjoy healthcare service and their schemes ensure that application or service providers have no privilege to disclose the real identities of users. However, Zhao [45] pointed out that Liu et al.'s schemes cannot protect user anonymity and further proposed an identity and ECC based anonymous authentication scheme for WBANs. Zhao's scheme not only protects user anonymity but also improves system efficiency in the client side and the application provide side. Unfortunately, Wang and Zhang [40] pointed out that Zhao's scheme cannot ensure real anonymity because the users' pseudo identities are unchanging value and the attacker could track the

users. In [4], Chen et al. proposed a cloud-assisted medical data exchange scheme for WBAN healthcare service. They claimed that their scheme achieves better security as compared to those for other existing medical-oriented systems. However, in [25], Li et al. pointed out that Chen et al.'s scheme exposes the patient and the doctor to the flaw of private key reveal problem and is failing to provide real-time monitoring service and non-repudiation evidence in doctor diagnosis.

Our contributions

To solve the mentioned problems in previous schemes, we will proposed a new secure authentication system for cloud-assisted WBAN. The main contributions of this paper are described as follows.

- We propose a secure authentication and key agreement scheme for cloud-assisted WBAN system using extended chaotic maps [2, 18–20, 26, 43, 44]. Therefore, only authorized doctors and medical caregivers have ability to access patients' health information and the proposed system can ensure patient privacy and data integrity [12, 14, 23, 24].
- Our proposed system supports a real-time analytics with continuous remote monitoring on WBAN-oriented health items and monitored patients can get treated proactively before their condition worsen.
- Based on the attacker model description, we have analyzed and proved the proposed system is secure against many well-known attacks and provision of several functionality aspects.
- From the execution of the proposed procedures, our system allows system participants to reduce the burden on some computations and is suitable for implementation in the current mobile emergency medical care environment.

Paper organization

The organization of this paper is organized as follows. In "The architecture of cloud-assisted wireless body area network in mobile emergency medical care system", we first introduce the architecture of a cloud-based WBAN system and present a secure authentication scheme for mobile emergency medical care system in Section "The proposed mobile emergency medical care system". Section "Security analysis of our proposed system" gives the security analysis of the proposed system and evaluates the performance of the proposed system with other related E-health care schemes in "Performance and comparative analysis of our proposed system". Finally, we conclude the paper in "Conclusions".

The architecture of cloud-assisted wireless body area network in mobile emergency medical care system

For cloud-assisted wireless body area network in mobile emergency medical care system, five roles participate in this system: the patient (P), the healthcare center (HC), the medical caregiver (MC), the doctor (D) and a trusted medical cloud center (C). Before accessing the system, every participant must register with the medical cloud center C and C will issue one specific certificate based on Chebyshev chaotic maps. Figure 1 shows the entire architecture of cloud-assisted wireless body area network in mobile emergency medical care system. First the patient P can go to the healthcare center HC to take a health inspection and HC will upload P's personal health inspection reports to the medical cloud center C. Moreover, P can collect health personal items from WBAN and upload them to the medical cloud center C. Then the emergency monitoring applications which allow medical caregivers MC to access the uploaded data. Thus the monitored patient P can get treated proactively before his/her condition worsen.

On the other hand, once P goes to the hospital for medical treatment, the doctor C can download P's personal health inspection reports and collected personal health items of WBAN from medical cloud center C and diagnose the symptoms via P's authorization. As shown in [10], the format of patient's personal health inspection reports and collected personal health items of WBAN are shown in Tables 1 and 2, respectively.

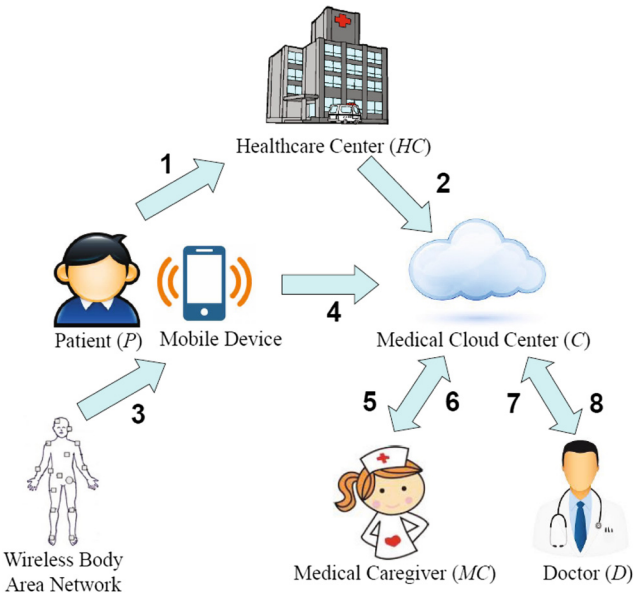

Fig. 1 The architecture of cloud-assisted wireless body area network in mobile emergency medical care system

Table 1 The patient's personal health inspection items

Item	Content
ID	The patient's identity
$Data_1$	General inspection
$Data_2$	Electrocardiography
$Data_3$	Blood test
$Data_4$	X-ray
$Data_5$	Scopy exam
$Data_6$	Preventive medicine series

Step 1. The patient P goes to the healthcare center HC to take a health inspection.
Step 2. The patient uploads his/her personal health inspection reports to the medical cloud center C and the designated doctor has ability to access P's health inspection reports via P's authorization.
Step 3. WBAN collect P's personal health items and send them to P's personal mobile device.
Step 4. The patient P uses personal mobile device to upload his/her personal health items to the medical cloud center C.
Step 5. In order to provide real time medical monitoring service, the patient P can authorize a medical caregiver MC to access P's collected health items of WBAN stored in medical cloud center.
Step 6. After verification, the medical caregiver MC can access P's personal health items of WBAN stored in medical cloud center. Thus the monitored patient P can get treated proactively before his/her condition worsen.
Step 7. In the doctor treatment time, the authorized doctor D can access and download P's personal health items of WBAN and health inspection reports stored in medical cloud center.
Step 8. The doctor D can diagnose the symptoms of P and upload P's treatment report to the medical cloud center as the non-repudiation evidence after treatment.

Table 2 The patient's collected health items of WBAN

Item	Content
ID	The patient's identity
BS_data_1	Electrocardiography
BS_data_2	Electromyography
BS_data_3	Electroencephalography
BS_data_4	Pulse oximetry
BS_data_5	Body pulse
BS_data_6	Heartbeat
BS_data_7	Blood pressure

The proposed mobile emergency medical care system

In this section, we will show how our proposed mobile emergency medical care system works step by step. There are four phases involve in the proposed system: participant registration phase, health examination phase, real time monitoring phase and doctor treatment phase. The notations used throughout this paper are summarized in Table 3.

Participant registration phase

For cloud-assisted WBAN in mobile emergency medical care system, the trusted medical cloud center C is a platform for patients, doctors and medical caregivers. In other words, anyone can register at C as a user, a doctor or a medical caregiver. Concerning the fact that the proposed system mainly relies on the design of Chebyshev chaotic maps, it is assumed that the system participants can register at C in some secure way or by secure channel. Moreover, all participants' certificates are issued by C and kept secret by them. The detailed steps are described as follows.

Step 1. When a patient wants to be a new legal patient, he/she chooses his/her identity ID_P and submits it to C via a secure channel. Upon receiving ID_P from P, C computes P's certificate $T_k(ID_P)$ mod p and P securely stores $(ID_P, T_k(ID_P) \text{ mod } p)$ in his/her mobile device via a secure channel, where k is the secret key of C.
Step 2. When a doctor wants to be a new legal doctor, he/she chooses his/her identity ID_D and submits it to C via a secure channel. Upon receiving ID_D from D, C computes D's certificate $T_k(ID_D)$ mod p and D stores $(ID_D, T_k(ID_D) \text{ mod } p)$ in a secure way via a secure channel.
Step 3. When a medical caregiver wants to be a new legal caregiver, he/she chooses his/her identity ID_{MC} and submits it to C via a secure channel. Upon receiving ID_{MC} from MC, C computes MC's certificate $T_k(ID_{MC})$ mod p and MC stores $(ID_{MC}, T_k(ID_{MC}) \text{ mod } p)$ in a secure way via a secure channel.

Health examination phase

In this phase, the patient P goes to the healthcare center HC to take a health inspection and P can upload his/her health inspection reports m_{HC} to the medical cloud center C, where $m_{HC} = (ID_P, data_1, data_2, ..., data_6, T_{HC})$ Moreover, if P wants to consult with some doctor D, C

Table 3 Notations used in the paper

Symbol	Description
ID_P	The identity of patient P.
ID_D	The identity of doctor D.
ID_{MC}	The identity of medical caregiver MC.
p	A large prime number.
k	C's secret key.
$(x, T_k(x) \bmod p)$	C's public key based on Chebyshev chaotic maps.
$T_k(ID_P) \bmod p$	P's certificate based on Chebyshev chaotic maps and issued by C.
$T_k(ID_D) \bmod p$	D's certificate based on Chebyshev chaotic maps and issued by C.
$T_k(ID_{MC}) \bmod p$	MC's certificate based on Chebyshev chaotic maps and issued by C.
T_{in}	The nth timestamp generated by entity i.
ΔT	The valid transmission time interval.
m_{HC}	P's health inspection reports generated by the healthcare center.
m_{BS}	P's health data items collected by WBAN.
m_{DG}	D's diagnose of P's symptom.
$E_K()/D_K()$	A pair of symmetric encryption/decryption functions with the key K
$Sig_i(M)$	The entity i uses his/her private key to sign the message M.
$H(\cdot)$	A secure one-way hash function, such as HMAC [35].
SK_{ij}	The session key, which is established between entity i and entity j
$\|\|$	Message concatenation

will help P to authenticate D and help P and D to establish the session key $SK_{PD} = SK_{DP}$ for protecting P's health inspection reports. Figure 2 shows the flowchart of the health examination phase and the detailed steps are described as follows.

Step 1. P chooses a random number a and computes $X_{P1} = T_a(x) \bmod p$ and $\theta_{P-C} = H(T_k(ID_P) \bmod p || X_{P1} || T_{P1})$, where T_{P1} is the current timestamp of P. Then P sends the request messages $M_1 = \{ID_P, ID_D, X_{P1}, T_{P1}\}$

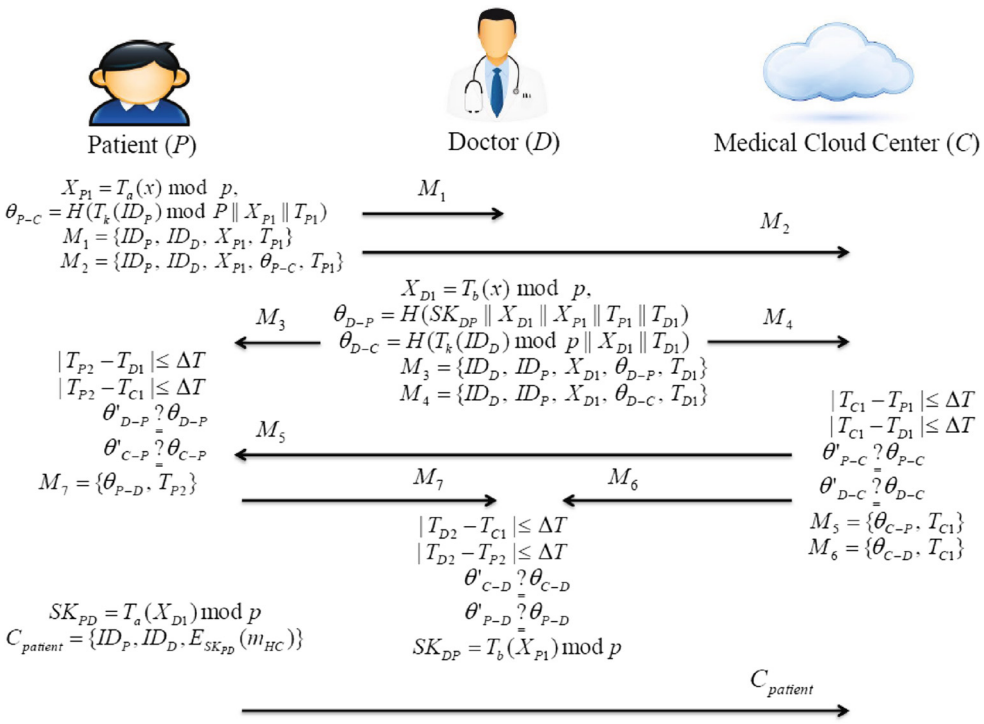

Fig. 2 The flowchart of the health examination phase

and $M_2 = \{ID_P, ID_D, X_{P1}, \theta_{P-C}, T_{P1}\}$ to D and C, respectively.

Step 2. After receiving P's request, D chooses a random number b and computes $X_{D1} = T_b(x) \bmod p$, $\theta_{D-P} = H(SK_{DP}||X_{D1}||X_{P1}||T_{P1}||T_{D1})$ and $\theta_{D-C} = H(T_k(ID_D) \bmod p||X_{D1}||T_{D1})$, where T_{D1} is the current timestamp of D and the session key $SK_{DP} = T_b(X_{P1}) \bmod p$. Then D sends $M_3 = \{ID_D, ID_P, X_{D1}, \theta_{D-P}, T_{D1}\}$ and $M_4 = \{ID_D, ID_P, X_{D1}, \theta_{D-C}, T_{D1}\}$ to P and C, respectively.

Step 3. After receiving M_2 and M_4 from P and D, C checks $|T_{C1} - T_{P1}| \leq \Delta T$ and $|T_{C1} - T_{D1}| \leq \Delta T$, where T_{C1} is the current timestamp of C. If it holds, C computes $\theta'_{P-C} = H(T_k(ID_P) \bmod p||X_{P1}||T_{P1})$ and checks if computed θ'_{P-C} equals received θ_{P-C}. If it holds, P is authenticated by C. Similarly, C computes $\theta'_{D-C} = H(T_k(ID_D) \bmod p||X_{D1}||T_{D1})$ and checks if computed θ'_{D-C} equals received θ_{D-C}. If it holds, D is also authenticated by C and it means D is the doctor that P wants to consult with. Next, C computes $\theta_{C-P} = H(ID_P||ID_D||T_k(ID_P) \bmod p||X_{P1}||X_{D1}||T_{C1})$ and $\theta_{C-D} = H(ID_P||ID_D||T_k(ID_D) \bmod p||X_{P1}||X_{D1}||T_{C1})$ and sends $M_5 = \{\theta_{C-P}, T_{C1}\}$ and $M_6 = \{\theta_{C-D}, T_{C1}\}$ to P and D, respectively. Note that the protocol will be terminated immediately if any authenticated process does not pass.

Step 4. After receiving M_3 and M_5 from D and C, P checks $|T_{P2} - T_{D1}| \leq \Delta T$ and $|T_{P2} - T_{C1}| \leq \Delta T$, where T_{P2} is the current timestamp of P. If it holds, P computes the session key $SK_{PD} = T_a(X_{D1}) \bmod p$ and $\theta'_{D-P} = H(SK_{PD}||X_{D1}||X_{P1}||T_{P1}||T_{D1})$ and checks if computed θ'_{D-P} equals received θ_{D-P}. If it holds, D is authenticated by P. Similarly, P computes $\theta'_{C-P} = H(ID_P||ID_D||T_k(ID_P) \bmod p||X_{P1}||X_{D1}||T_{C1})$ and checks if computed θ'_{C-P} equals received θ_{C-P}. If it holds, C is also authenticated by P. Then P generates another key confirmation message $\theta_{P-D} = H(SK_{PD}||X_{P1}||X_{D1}||T_{P2})$ for D and sends $M_7 = \{\theta_{P-D}, T_{P2}\}$ to D. Note that the protocol will be terminated immediately if any authenticated process does not pass.

Step 5. After receiving M_6 and M_7 from C and P, D checks $|T_{D2} - T_{C1}| \leq \Delta T$ and $|T_{D2} - T_{P2}| \leq \Delta T$, where T_{D2} is the current timestamp of D. If it holds, D computes $\theta'_{C-D} = H(ID_P||ID_D||T_k(ID_D) \bmod p||X_{P1}||X_{D1}||T_{C1})$ and checks if computed θ'_{C-D} equals received θ_{C-D}. If it holds, C is authenticated by D. Similarly, D computes $\theta'_{P-D} = H(SK_{DP}||X_{P1}||X_{D1}||T_{P2})$ and checks if computed θ'_{P-D} equals received θ_{P-D}. If it holds, P is also authenticated by D. As a result, both P and D treat $SK_{PD} = T_a(X_{D1}) \bmod p = T_{ab}(x) \bmod p = T_b(X_{P1}) \bmod p = SK_{DP}$ as the session key shared between them. Note that the protocol will be terminated immediately if any authenticated process does not pass.

Step 6. After that, P uses the session key SK_{PD} to encrypt the health inspection reports and uploads $C_{patient} = \{(ID_P, ID_D, E_{SK_{PD}}(m_{HC}))\}$ to the medical cloud center C. Finally, C stores $C_{patient}$ in its DB.

Remark 1 We can view D and C as an integrated system for P, so from the perspective of P, we adopt mutual authentication and key agreement that means only authorized D has ability to decrypt $C_{patient}$ and inspect P's health inspection reports in private way.

Real time monitoring phase

In this phase, body sensors of WBAN are embedded into the patient P's body and P uses his/her mobile device to collect the measured health items m_{BS}, where $m_{BS} = (ID_P, BS\_data_1, \ldots, BS\_data_6, T_{BS})$. Then P can use the mobile device to collect the measured health items m_{BS} and uploads them to C via a public channel. In order to protect patient privacy, m_{BS} must be encrypted before transmission. Moreover, in order to support real time analytics with continuous remote monitoring on stream-oriented health items, the monitored patient P can authorize a medical caregiver MC to access his/her collected health items of WBAN stored in C. Therefore, C will help P to authenticate MC and help P and MC to establish the session key $SK_{PMC} = SK_{MCP}$ for securing P's measured health items of WBAN. Finally, the health conditions of P can be monitored on a real time basis, avoiding unnecessary doctor visits. The advantage of this phase not only provides home care but also improves the quality of life. Figure 3 shows the flowchart of the real time monitoring phase and the detailed steps are described as follows.

Step 1. P chooses a random number c and computes $X_{P3} = T_c(x) \bmod p$ and $\beta_{P-C} = H(T_k(ID_P) \bmod p||X_{P3}||T_{P3})$, where T_{P3} is the current timestamp of P. Then P sends the request messages $N_1 = \{ID_P, ID_{MC}, X_{P3}, T_{P3}\}$ and $N_2 = \{ID_P, ID_{MC}, X_{P3}, \beta_{P-C}, T_{P3}\}$ to MC and C, respectively.

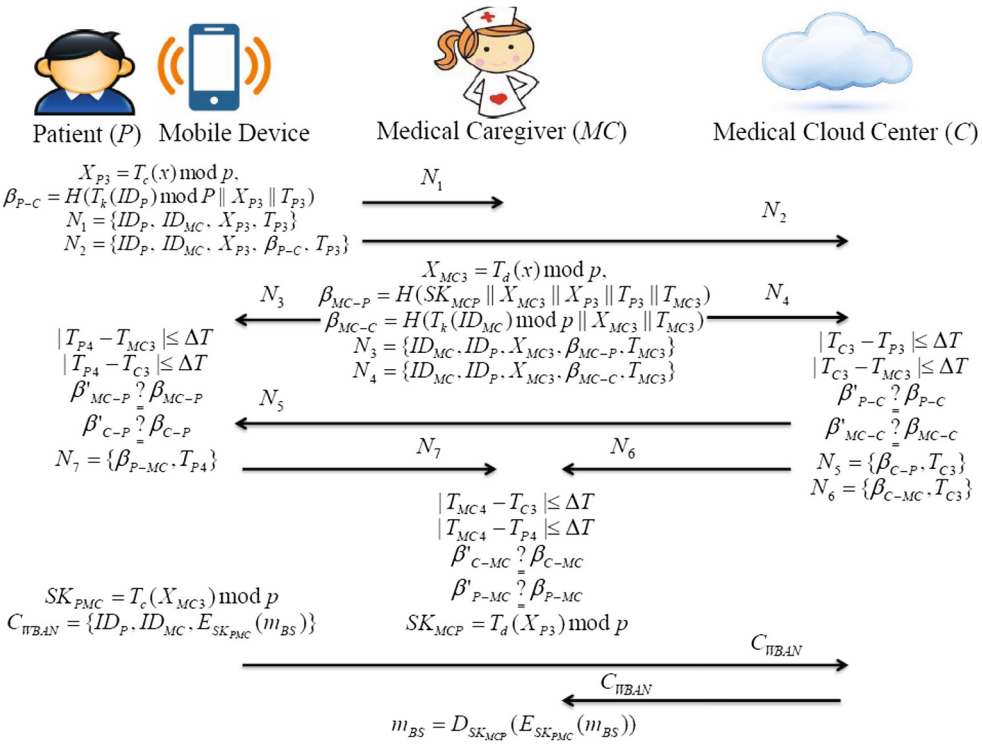

Fig. 3 The flowchart of the real time monitoring phase

Step 2. After receiving P's request, MC chooses a random number d and computes $X_{MC3} = T_d(x) \bmod p$, $\beta_{MC-P} = H(SK_{MCP}||X_{MC3}||X_{P3}||T_{P3}||T_{MC3})$ and $\beta_{MC-C} = H(T_k(ID_{MC}) \bmod p||X_{MC3}||T_{MC3})$, where T_{MC3} is the current timestamp of MC and the session key $SK_{MCP} = T_d(X_{P3}) \bmod p$. Then MC sends $N_3 = \{ID_{MC}, ID_P, X_{MC3}, \beta_{MC-P}, T_{MC3}\}$ and $N_4 = \{ID_{MC}, ID_P, X_{MC3}, \beta_{MC-C}, T_{MC3}\}$ to P and C, respectively.

Step 3. After receiving N_2 and N_4 from P and MC, C checks $|T_{C3} - T_{P3}| \leq \Delta T$ and $|T_{C3} - T_{MC3}| \leq \Delta T$, where T_{C3} is the current timestamp of C. If it holds, C computes $\beta'_{P-C} = H(T_k(ID_P) \bmod p||X_{P3}||T_{P3})$ and checks if computed β'_{P-C} equals received β_{P-C}. If it holds, P is authenticated by C. Similarly, C computes $\beta'_{MC-C} = H(T_k(ID_{MC}) \bmod p||X_{MC3}||T_{MC3})$ and checks if computed β'_{MC-C} equals received β_{MC-C}. If it holds, MC is also authenticated by C and it means MC is the designated medical caregiver that P wants to consult with. Next, C computes $\beta_{C-P} = H(ID_P||ID_{MC}||T_k(ID_P) \bmod p||X_{P3}||X_{MC3}||T_{C3})$ and $\beta_{C-MC} = H(ID_P||ID_{MC}||T_k(ID_{MC}) \bmod p||X_{P3}||X_{MC3}||T_{C3})$ and sends $N_5 = \{\beta_{C-P}, T_{C3}\}$ and $N_6 = \{\beta_{C-MC}, T_{C3}\}$ to P and MC, respectively. Note that the protocol will be terminated immediately if any authenticated process does not pass.

Step 4. After receiving N_3 and N_5 from MC and C, P checks $|T_{P4} - T_{MC3}| \leq \Delta T$ and $|T_{P4} - T_{C3}| \leq \Delta T$, where T_{P4} is the current timestamp of P. If it holds, P computes the session key $SK_{PMC} = T_c(X_{MC3}) \bmod p$ and $\beta'_{MC-P} = H(SK_{PMC}||X_{MC3}||X_{P3}||T_{P3}||T_{MC3})$ and checks if computed β'_{MC-P} equals received β_{MC-P}. If it holds, MC is authenticated by P. Similarly, P computes $\beta'_{C-P} = H(ID_P||ID_{MC}||T_k(ID_P) \bmod p||X_{P3}||X_{MC3}||T_{C3})$ and checks if computed β'_{C-P} equals received β_{C-P}. If it holds, C is also authenticated by P. Then P generates another key confirmation message $\beta_{P-MC} = H(SK_{PMC}||X_{P3}||X_{MC3}||T_{P4})$ for D and sends $N_7 = \{\beta_{P-MC}, T_{P4}\}$ to MC. Note that the protocol will be terminated immediately if any authenticated process does not pass.

Step 5. After receiving N_6 and N_7 from C and P, MC checks $|T_{MC4} - T_{C3}| \leq \Delta T$ and $|T_{MC4} - T_{P4}| \leq \Delta T$, where T_{MC4} is the current timestamp of MC. If it holds, MC computes $\beta'_{C-MC} = H(ID_P||ID_{MC}||T_k(ID_{MC}) \bmod p||X_{P3}||X_{MC3}||T_{C3})$ and checks if computed β'_{C-MC} equals received β_{C-MC}. If it holds, C is authenticated by MC. Similarly, MC computes $\beta'_{P-MC} = H(SK_{MCP}||X_{P3}||X_{MC3}||T_{P4})$ and checks if computed β'_{P-MC} equals received β_{P-MC}. If

it holds, P is also authenticated by MC. As a result, both P and MC treat $SK_{PMC} = T_c(X_{MC3}) \bmod p = T_{cd}(x) \bmod p = T_d(X_{P3}) \bmod p = SK_{MCP}$ as the session key shared between them. Note that the protocol will be terminated immediately if any authenticated process does not pass.

Step 6. After that, P uses the session key SK_{PMC} to encrypt the measured health items of WBAN and P's mobile device will periodically upload $C_{WBAN} = \{(ID_P, ID_{MC}, E_{SK_{PMC}}(m_{BS}))\}$ to the medical cloud center C. Thus MC can download C_{WBAN} from C and monitor P's measured health items of WBAN by computing $m_{BS} = D_{SK_{MCP}}(E_{SK_{PMC}}(m_{BS}))$. Finally, the proposed system can support real time analytics with continous remote monitoring on stream-oriented health items of WBAN and the monitored patient can get treated proactively before his/her condition worsen.

Step 7. Continued from previous phase, P can also use the session key SK_{PD} to encrypt the measured health items of WBAN and P's mobile device will periodically upload $C'_{WBAN} = \{(ID_P, ID_D, E_{SK_{PD}}(m_{BS}))\}$ to the medical cloud center C, where $SK_{PD} = SK_{DP}$ is a common session key shared between P and D. As a result, the authorized D can download C'_{WBAN} from C at any time and use the common session key SK_{DP} to inspect P's measured health items of WBAN by computing $m_{BS} = D_{SK_{DP}}(E_{SK_{PD}}(m_{BS}))$.

Remark 2 We can view MC and C as an integrated system for P, so from the perspective of P, we adopt mutual authentication and key agreement that means only designated MC has ability to decrypt C_{WBAN} and monitor P's measured health items of WBAN in real time.

Doctor treatment phase

In this phase, P goes to the hospital and tells the doctor D to download P's health inspection reports $C_{patient}$ and measured health items C'_{WBAN} from the medical cloud center C, where $C_{patient} = \{ID_P, ID_D, E_{SK_{PD}}(m_{HC})\}$ and $C'_{WBAN} = \{ID_P, ID_D, E_{SK_{PD}}(m_{BS})\}$. Then D can use the session key SK_{DP} which is established in health examination phase to reveal m_{HC} and m_{BS}. Finally, D uses these health information to diagnose P's symptom and uploads $Treatment_{P-D}$ to the medical cloud center as the non-repudiation evidence after the treatment. Figure 4 shows the flowchart of the doctor treatment phase and the detailed steps are described as follows.

Step 1. D chooses a random number e and computes $X_{D5} = T_e(x) \bmod p$ and $\delta_{D-C} = H(T_k(ID_D) \bmod p || X_{D5} || T_{D5})$, where T_{D5} is the current timestamp of D. Then D makes a download request message $O_1 =$

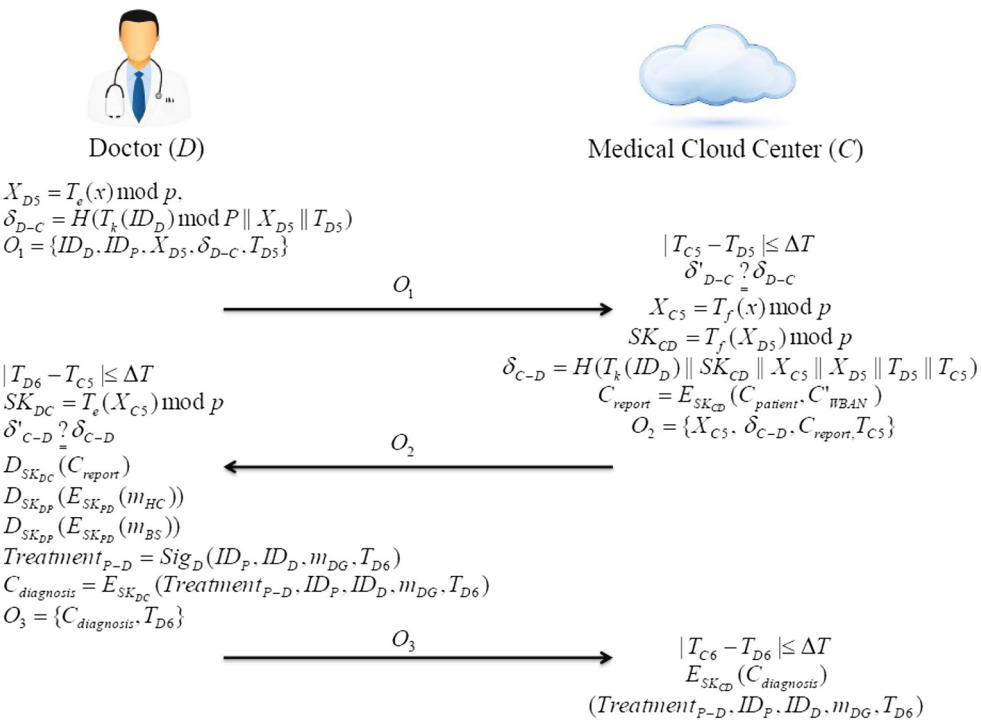

Fig. 4 The flowchart of the doctor treatment phase

$\{ID_D, ID_P, X_{D5}, \delta_{D-C}, T_{D5}\}$ and sends it to the medical cloud center C via a public channel.

Step 2. After receiving the download request O_1 from D, C checks $|T_{C5} - T_{D5}| \leq \Delta T$, where T_{C5} is the current timestamp of C. If it holds, C computes $\delta'_{D-C} = H(T_k(ID_D) \bmod p||X_{D5}||T_{D5})$ and checks if computed δ'_{D-C} equals received δ_{D-C}. If it holds, D is authenticated by C. Next, C chooses a random number f and computes $X_{C5} = T_f(x) \bmod p$, the session key $SK_{CD} = T_f(X_{D5}) \bmod p$, $\delta_{C-D} = H(T_k(ID_D) \bmod p||SK_{CD}||X_{C5}||X_{D5}||T_{D5}||T_{C5})$ and $C_{report} = E_{SK_{CD}}(C_{patient}, C'_{WBAN})$. Then C sends the download response message $O_2 = \{X_{C5}, \delta_{C-D}, C_{report}, T_{C5}\}$ to D. Note that the protocol will be terminated immediately if any authenticated process does not pass.

Step 3. After receiving the download response O_2 from C, D checks $|T_{D6} - T_{C5}| \leq \Delta T$, where T_{D6} is the current timestamp of D. If it holds, D computes $SK_{DC} = T_e(X_{C5}) \bmod p$ and $\delta'_{C-D} = H(SK_{DC}||X_{C5}||X_{D5}||T_{D5}||T_{C5})$ and checks if computed δ'_{C-D} equals received δ_{C-D}. If it holds, C is authenticated by D. Then D uses SK_{DC} to reveal $C_{patient}$ and C'_{WBAN} by computing $D_{SK_{DC}}(C_{report})$. Finally, D uses the session key SK_{DP} which is established in health examination phase to reveal health inspection reports m_{HC} and measured health items of WBAN m_{BS} by computing $D_{SK_{DP}}(E_{SK_{PD}}(m_{HC}))$ and $D_{SK_{DP}}(E_{SK_{PD}}(m_{BS}))$, respectively.

Step 4. After the treatment, in order to provide non-repudiation evidence in doctor diagnosis, D uses his/her private key to sign the medical diagnoses of P's symptom by computing $Treatment_{P-D} = Sig_D(ID_P, ID_D, m_{DG}, T_{D6})$, where m_{DG} means D's medical diagnosis of P's symptom. Finally, D computes $C_{diagnosis} = E_{SK_{DC}}(Treatment_{P-D}, ID_P, ID_D, m_{DG}, T_{D6})$ and uploads $O_3 = \{C_{diagnosis}, T_{D6}\}$ to C.

Step 5. After receiving O_3 from D, C checks $|T_{C6} - T_{D6}| \leq \Delta T$, where T_{C6} is the current timestamp of C. If it holds, C reveals $(Treatment_{P-D}, ID_P, ID_D, m_{DG}, T_{D6})$ by computing $E_{SK_{CD}}(C_{diagnosis})$ and stores them in its DB as the non-repudiation evidence.

Security analysis of our proposed system

Before analysing the security of our proposed system, we will present an attacker model which discusses several valid assumptions including capabilities of the attacker. In the following subsections, we have analyzed and proved the security of the proposed system based on the attacker model description.

Attack model

Due to the authentication systems are executed over insecure channels, the malicious attackers may have several capabilities to damage the security of the proposed system and we listed some widely accepted valid assumptions in the following.

- An attacker may eavesdrop all the communications between participants involved of the system over the public channels. Then the attacker can modify, delete, resend and reroute the eavesdropping messages. Note that an attacker cannot intercept the message during participant registration phase.
- An attacker may guess low entropy password easily, but guessing secret parameters (e.g. certificate, random number) is computationally infeasible in polynomial time.
- An attacker may try to impersonate as a medical worker (e.g. doctor, medical caregiver) and reply malicious responses during execution of the proposed system.
- An attacker may try to impersonate as a patient to the medical worker after intercepting the request message during execution of the proposed system.

Security proof of the proposed system

In the following, we informally analyzed the security of the proposed system and proved that the system provides many security criteria and it is secure against several well-known attacks.

Theorem 1 *The proposed authentication scheme for mobile emergency medical care system is able to provide mutual authentication property.*

Proof In the health examination phase of the proposed system, C has common secret certificates $T_k(ID_P) \bmod p$ and $T_k(ID_D) \bmod p$ shared with P and D and can authenticate P and D by verifying θ_{P-C} and θ_{D-C}. In addition, after receiving M_3 and M_5 from D and C, P has a secret certificate $T_k(ID_P) \bmod p$ shared with C and can authenticate C and D by verifying θ_{C-P} and θ_{D-P}. Moreover, after receiving M_6 and M_7 from C and P, D has a secret certificate $T_k(ID_D) \bmod p$ shared with C and can authenticate C and P by verifying δ_{D-C}.

On the other hand, in the real time monitoring phase of the proposed system, C has common secret certificates $T_k(ID_{MC}) \bmod p$ and $T_k(ID_P) \bmod p$ shared with MC

and P and can authenticate MC and P by verifying β_{MC-C} and β_{P-C}. Next, after receiving N_3 and N_5 from MC and C, P has a secret certificate $T_k(ID_P)$ mod p shared with C and can authenticate MC and C by verifying β_{MC-P} and β_{C-P}. Furthermore, after receiving N_6 and N_7 from C and P, MC has a secret certificate $T_k(ID_{MC})$ mod p shared with C and can authenticate C and P by verifying β_{C-MC} and β_{P-MC}.

Besides, in the doctor treatment phase of the proposed system, C has a common secret certificate $T_k(ID_D)$ mod p shared with D and can authenticate D by verifying δ_{D-C}. Finally, after receiving the download response O_2 from C, D can authenticate C by verifying SK_{DC} and δ_{C-D}. Therefore, the malicious attacker cannot generate fake request and response messages which not only avoids congestion in the network system but also achieves mutual authentication property. □

Theorem 2 *The proposed authentication scheme for mobile emergency medical care system is able to provide the property of session key security.*

Proof During the authentication phases of our proposed system, a common session key should be established after the successful authentication steps. In the health examination phase, both patient P and doctor D will exchange secret parameters $T_a(x)$ mod p and $T_a(x)$ mod p and they will use them to generate a common session key $SK_{DP} = SK_{PD}$ for protecting P's health inspection reports m_{HC} and establishing a secure channel. An extended chaotic map is used to ensure the correctness of the scheme and is given below.

$$\begin{aligned} SK_{PD} &\equiv T_a(X_{D1}) \bmod p \\ &\equiv T_b(T_a(x)) \bmod p \\ &\equiv T_{ab}(x) \bmod p \\ &\equiv T_b(X_{P1}) \bmod p \equiv SK_{DP} \end{aligned}$$

Moreover, in the real time monitoring phase, both patient P and medical caregiver MC will exchange secret parameters $T_c(x)$ mod p and $T_d(x)$ mod p and they will use them to generate a common session key $SK_{PMC} = SK_{MCP}$ for protecting P's measured health items of WBAN m_{BS} and establishing a secure channel. An extended chaotic map is used to ensure the correctness of the scheme and is given below.

$$\begin{aligned} SK_{PMC} &\equiv T_c(X_{MC3}) \bmod p \\ &\equiv T_c(T_d(x)) \bmod p \\ &\equiv T_{cd}(x) \bmod p \\ &\equiv T_d(X_{P3}) \bmod p \equiv SK_{MCP} \end{aligned}$$

Finally, in the doctor treatment phase, both doctor D and medical cloud center C will exchange secret parameters $T_e(x)$ mod p and $T_f(x)$ mod p and they will use them to generate a common session key $SK_{DC} = SK_{CD}$ for protecting P's $C_{patient}$ and C'_{WBAN} and establishing a secure channel. An extended chaotic map is used to ensure the correctness of the scheme and is given below.

$$\begin{aligned} SK_{DC} &\equiv T_e(X_{C5}) \bmod p \\ &\equiv T_e(T_f(x)) \bmod p \\ &\equiv T_{ef}(x) \bmod p \\ &\equiv T_f(X_{D5}) \bmod p \equiv SK_{CD} \end{aligned}$$

□

Theorem 3 *The proposed authentication scheme for mobile emergency medical care system is able to provide the property of perfect forward secrecy.*

Proof In the health examination phase of the proposed system, the session key $SK_{PD} = T_a(X_{D1})$ mod $p = T_b(X_{P1})$ mod $p = SK_{DP}$ is related to random numbers a and b, which were randomly chosen by P and D, respectively. So any session key has not related to C's secret key. Since the random numbers are different in every request session, it is computationally infeasible for an attacker to derive the previously established session keys due to it is as difficult as solving the Diffie-Hellman problem.

Similarly, in the real time monitoring phase, the session key $SK_{PMC} = T_c(X_{MC3})$ mod $p = T_d(X_{P3})$ mod $p = SK_{MCP}$ is related to random numbers c and d, which were randomly chosen by P and MC, respectively. Since the random numbers are different in every request session, an attacker cannot compute the previously established session keys because of the intractability of the Diffie-Hellman problem.

Finally, in the doctor treatment phase, the session key $SK_{DC} = T_e(X_{C5})$ mod $p = T_f(X_{D5})$ mod $p = SK_{CD}$ is related to random numbers e and f, which were randomly chosen by D and C, respectively. Since the random numbers are different in every request session, an attacker cannot compute the previously established session keys because of the intractability of the CMBDLP and CMBDHP problems [3]. Therefore, the proposed system achieves perfect forward secrecy. □

Theorem 4 *The proposed authentication scheme for mobile emergency medical care system is able to provide the properties of patient privacy and data integrity.*

Proof In our proposed system, in order to ensure the patients' privacy and protect the data integrity, we use the session key to encrypt the private information of patients and the medical cloud center has inability to know patients' health inspection reports m_{HC} and health data items collected by WBAN m_{BS}. In Step 6 of the health examination phase, the patient uses the session key SK_{PD} to protect his/her health inspection reports and only authorized doctor has ability to reveal patient's health inspection reports in private way. Moreover, In Step 6 and Step 7 of the real time monitoring phase, the patient also uses the session keys SK_{PMC} and SK_{PD} to protect his/her health data items collected by WBAN and only authorized medical caregiver and authorized doctor have ability to monitor and inspect patient's measured health items of WBAN in real time way. Finally, according to the proof of Theorem 2, we prove that the proposed system could provide the property of session key security and no outsiders can reveal patients' health inspection reports m_{HC} and health data items collected by WBAN m_{BS}. Therefore, the proposed system could ensure patient privacy and data integrity. □

Theorem 5 *The proposed authentication scheme for mobile emergency medical care system is able to provide the property of non-repudiation in doctor diagnosis.*

Proof In Step 4 of the doctor treatment phase, we suggest doctor's diagnose of P's symptom m_{DG} should be involved in $Treatment_{P-D} = Sig_D(ID_P, ID_D, m_{DG}, T_{D6})$, where Sig_D is doctor's private key and it is used to sign the messages $(ID_P, ID_D, m_{DG}, T_{D6})$. Finally, in Step 5 of this phase, the doctor uploads the current timestamp T_{D6} and $C_{diagnosis} = E_{SK_{DC}}(Treatment_{P-D}, ID_P, ID_D, m_{DG}, T_{D6})$ to the medical cloud center as the non-repudiation evidence. Therefore, the proposed system achieves non-repudiation in doctor diagnosis. □

Theorem 6 *The proposed authentication scheme for mobile emergency medical care system is secure against the replay attacks.*

Proof In this attack, an attacker may eavesdrop request messages during execution of the protocol and transmit the same messages to system participants. In order to avoid the replay attacks, we have adopted the random numbers and timestamps in the proposed system. As discussed in Step 1 and Step 2 of the health examination phase, our proposed system ingeniously uses the random numbers a and b and timestamps T_{P1} and T_{D1} to avoid the immediate replay attacks within the valid time interval. Similarly, as discussed in Step 1 and Step 2 of the real time monitoring phase, our proposed system successfully uses the random numbers c and d and timestamps T_{P3} and T_{MC3} to avoid the strong replay attacks within the valid time interval. Furthermore, as discussed in Step 1 and Step 2 of the doctor treatment phase, our proposed system smartly uses the random numbers e and f and timestamps T_{D5} and T_{C5} to avoid the malicious replay attacks within the valid time interval. As a result, our proposed system provides the message freshness property and the system participants could avoid the replay attacks by checking the freshness of random numbers and timestamps. □

Theorem 7 *The proposed authentication scheme for mobile emergency medical care system is secure against the man-in-the-middle attacks.*

Proof In this attack, we suppose an attacker intercepts the request messages during execution of the protocol and transmits the modified messages to system participants. As discussed in Step 1 of the health examination phase, an attacker intercepts the messages $M_1 = \{ID_P, ID_D, X_{P1}, T_{P1}\}$ and $M_2 = \{ID_P, ID_D, X_{P1}, \theta_{P-C}, T_{P1}\}$ and computes $X_{A1} = T_{a'}(x) \bmod p$, where a' is a random number chosen by the attacker. Then the attacker changes M_1 to $M_1' = \{ID_P, ID_D, X_{A1}, T_{A1}\}$, where T_{A1} is the current timestamp of the attacker. However, the attacker cannot modify M_2 because it involves computation of $H(T_k(ID_P) \bmod p||X_{A1}||T_{A1})$, which needs the secret certificate $T_k(ID_P) \bmod p$ of the patient. Since $T_k(ID_P) \bmod p$ is protected by a secure one-way cryptographic hash function $H(\cdot)$, it is computationally infeasible for the attacker to modify M_2. Therefore, the attacker does not have any ability to modify patient's request messages and sends them to the doctor and the medical cloud center. In a similar manner, the attacker also has inability to modify other request messages (N_1, N_2) and O_1 during the real time monitoring phase and the doctor treatment phase. Hence, our proposed system is secure against the man-in-the-middle attacks. □

Theorem 8 *The proposed authentication scheme for mobile emergency medical care system is secure against the participant impersonation attacks.*

Proof For participant impersonation attacks, two kinds of cases are taken into consideration. Case 1: an attacker may attempt to impersonate as a system participant (i.e. patient, doctor and medical caregiver) to transmit fake requests to

the medical cloud center. Case 2: an attacker may attempt to impersonate as a medical cloud center to cheat the system participant.

– Case 1: During the health examination phase of this case, the attacker has to generate some correct request messages $M_1 = \{ID_P, ID_D, X_{A1}, T_{A1}\}$ and $M_2 = \{ID_P, ID_D, X_{A1}, \theta_{A-C}, T_{A1}\}$ to impersonate as a legal patient, where a' is a random number chosen by the attacker, $X_{A1} = T_{a'}(x) \bmod p$, $\theta_{A-C} = H(T_k(ID_P) \bmod p || X_{A1} || T_{A1})$ and T_{A1} is current timestamp of the attacker. The attacker could generate $X_{A1} = T_{a'}(x) \bmod p$ and T_{A1} easily. However, the attacker cannot generate a valid θ_{A-C} without knowing the patient's certificate $T_k(ID_P) \bmod p$. On the other hand, in Step 2 of the real time monitoring phase, the attacker may generate some fake response messages $N_3 = \{ID_{MC}, ID_P, X_{A3}, \beta_{A-P}, T_{A3}\}$ and $N_4 = \{ID_{MC}, ID_P, X_{A3}, \beta_{A-C}, T_{A3}\}$ to impersonate as a legal medical caregiver, where a' is a random number chosen by the attacker, $X_{A3} = T_{a'}(x) \bmod p$, $\beta_{A-C} = H(T_k(ID_{MC}) \bmod p || X_{A3} || T_{A3})$ and T_{A3} is current timestamp of the attacker. Also, the attacker could generate $X_{A3} = T_{a'}(x) \bmod p$ and T_{A3} easily. However, the attacker cannot generate a valid β_{A-C} without knowing the medical caregiver's certificate $T_k(ID_{MC}) \bmod p$. Finally, in Step 1 of the doctor treatment phase, the attacker may generate a malicious request message $O_1 = \{ID_D, ID_P, X_{A5}, \delta_{A-C}, T_{A5}\}$ to impersonate as a valid doctor, where a' is a random number chosen by the attacker, $X_{A5} = T_{a'}(x) \bmod p$, $\delta_{A-C} = H(T_k(ID_D) \bmod p || X_{A5} || T_{A5})$ and T_{A5} is current timestamp of the attacker. Thus the attacker could generate $X_{A5} = T_{a'}(x) \bmod p$ and T_{A5} easily. However, the attacker cannot generate a valid δ_{A-C} without knowing the doctor's certificate $T_k(ID_D) \bmod p$ and participant impersonate attacks of Case 1 can be prevented by the proposed system.

– Case 2: In this case, we suppose the attacker wants to impersonate as a medical cloud center to cheat the system participants when he/she intercepts the request messages (M_1, M_2), (N_3, N_4) and (O_1) sent by the patient, medical caregiver and doctor, respectively. The attacker must reply correct responses $(M_5 = \{\theta_{A-P}, T_{A1}\}, M_6 = \{\theta_{A-D}, T_{A1}\})$, $(N_5 = \{\beta_{A-P}, T_{A1}\}, N_6 = \{\beta_{A-MC}\})$ and (O_2) and send them to the patient, medical caregiver and doctor, respectively. However, the attacker cannot generate correct response $(\theta_{A-P}, \theta_{A-D})$, $(\beta_{A-P}, \beta_{A-MC})$ and δ_{A-D} and send them to P, MC and D without knowing patient's certificate $T_k(ID_P) \bmod p$, medical caregiver's certificate $T_k(ID_{MC}) \bmod p$ and doctor's certificate $T_k(ID_D) \bmod p$, respectively. Therefore, we claim that the proposed system resists medical cloud center impersonation attack.

□

Theorem 9 *The proposed authentication scheme for mobile emergency medical care system is secure against the known-key attacks.*

Proof During the health examination phase of the proposed system, we know a common session key $SK_{PD} = T_a(X_{D1}) \bmod p = T_{ab}(x) \bmod p = T_b(X_{P1}) \bmod p = SK_{DP}$ is only shared between the patient and the doctor. Thus the compromise of a session key in previous session does not influence the security of session keys in other sessions because the patient and the doctor will generate new random numbers (a, b) and it is protected by CMBDLP and CMBDHP problems [3]. In a similar manner, the attacker also has inability to derive other session keys $SK_{PMC} = T_c(X_{MC3}) \bmod p = T_{cd}(x) \bmod p = T_d(X_{P3}) \bmod p = SK_{MCP}$ and $SK_{DC} = T_e(X_{D5}) \bmod p = T_{ef}(x) \bmod p = T_f(X_{C5}) \bmod p = SK_{CD}$ during the real time monitoring phase and the doctor treatment phase. Therefore, the attacker cannot extract random numbers from any session key and our proposed system resists the known-key attacks. □

Theorem 10 *The proposed authentication scheme for mobile emergency medical care system is secure against the stolen-verifier attacks.*

Proof For a secure authentication scheme, there must be a password/verifier table stored in server side to verify the validity of system participants. However, in our scheme, the medical cloud center uses Chebyshev chaotic maps to generate system participants' certificates and the medical cloud center does not maintain any password/verifier tables in its DB. Therefore, an attacker has no ability to get the secret information of the system participants and our system can avoid the stolen-verifier attack. □

Performance and comparative analysis of our proposed system

In the following, we define some cryptographic notations and evaluate the computation cost of our proposed system in Table 4. We have followed the experimental results performed in [15] with specifications as CPU: 2.4 GHz Intel core i5, RAM: 4.0 GB, using a GNU with multiple precision

Table 4 The computation cost of our proposed system

Phase → Entity ↓	Health examination	Real time monitoring	Doctor treatment
Patient	4 T_{Hash}+1 T_{Sym}+2 T_{Che}	4 T_{Hash}+1 T_{Sym}+2 T_{Che}	N/A
Doctor	4 T_{Hash}+2 T_{Che}	N/A	2 T_{Hash}+1 T_{Sig}+3 T_{Sym}+2 T_{Che}
Medical caregiver	N/A	4 T_{Hash}+1 T_{Sym}+2 T_{Che}	N/A
Medical cloud server	4 T_{Hash}	4 T_{Hash}	2 T_{Hash}+2 T_{Sym}+2 T_{Che}
Total computations	12 T_{Hash}+1 T_{Sym}+4 T_{Che}	12 T_{Hash}+2 T_{Sym}+4 T_{Che}	4 T_{Hash}+1 T_{Sig}+5 T_{Sym}+4 T_{Che}
Total execution time	131.882 ms	131.924 ms	132.77 ms
Communication rounds	4	5	3

library and OpenSSL library. The average time of executing one T_{Hash}, one T_{Che} and one T_{Sym} are 0.02 ms, 32.9 ms and 0.042 ms, respectively. As seen in Table 4, our proposed system allows participants to reduce the burden on some computations, and thus is more suitable for practical usages including mobile emergency medical care systems.

- T_{Hash}: The time for executing a one-way hash function.
- T_{Sig}: The time for executing a signature computation.
- T_{Sym}: The time for executing a symmetric en/decryption computation.
- T_{Che}: The time for executing a Chebyshev polynomial computation.

In Table 5, we compared the proposed system with existing related schemes in terms of different functional requirements and security attacks. It is visible from Table 5 that the schemes in [4, 16, 41] cannot provide real time monitoring and non-repudiation properties in E-health care systems. In contrast, our proposed system not only achieves several functionality aspects but also provides strong security protection on the relevant security attacks.

Table 5 Comparisons of our proposed system with related E-health care schemes

Scheme → Functionality ↓	Wu et al.'s [41] (2012)	Jiang et al.'s [16] (2013)	Chen et al.'s [4] (2014)	Our proposed system
F1	Yes	Yes	Yes	Yes
F2	Yes	Yes	Yes	Yes
F3	Yes	No	Yes	Yes
F4	Yes	Yes	Yes	Yes
F5	No	No	No	Yes
F6	No	No	No	Yes
F7	Yes	No	Yes	Yes
F8	No	Yes	Yes	Yes
F9	No	No	Yes	Yes
F10	No	Yes	Yes	Yes
F11	Yes	Yes	Yes	Yes

F1: Provision of patient privacy and data integrity
F2: Provision of session key agreement
F3: Provision of perfect forward secrecy
F4: Provision of mutual authentication between participants
F5: Provision of real time monitoring
F6: Provision of non-repudiation in doctor diagnosis
F7: Prevention of impersonation attack
F8: Prevention of message replay attack
F9: Prevention of stolen-verifier attack
F10: Prevention of man-in-the-middle attack
F11: Prevention of known-key attack

Conclusions

With the medical application of cloud-assisted WBAN in our daily life, it is urgent to design a remote medical care system for cloud-assisted WBAN to allow medical staffs to monitor patients' health in real time. Thus the monitored patient can get treated proactively before his/her health condition worsen. In order to get rid of the various security threats, this paper designed a secure emergency medical care system using medical cloud, WBAN, symmetric encryption/decryption algorithm, hash function and chaotic maps. The major advantage of the proposed system is providing continuous remote patient supervision both in and out of hospital conditions and this way improves the quality of life of monitored patients as well as the treatment efficiency. The security and performance analysis shows that the proposed system not only protects patient privacy and data integrity but also reduces the burden of system overhead. Additionally, our proposed system achieves desirable security functionalities such as mutual authentication, session key agreement, perfect forward secrecy and non-repudiation in doctor diagnosis. Finally, the above-mentioned properties and advantages demonstrate that the proposed cloud-assisted WBAN scheme is worth implementing in mobile emergency medical care system.

Acknowledgments The authors would like to thank the anonymous reviewers for their valuable suggestions and comments. This research was partially supported by the National Science Council, Taiwan, R.O.C.

References

1. Ali, A., and Khan, F.A., Key agreement schemes in wireless body area networks: taxonomy and state-of-the-art. *J. Med. Syst.* 39:115, 2015.
2. Bergamo, P., Arco, P., Santis, A., and Kocarev, L., Security of public-key cryptosystems based on Chebyshev polynomials. *IEEE Transactions on Circuits and Systems I* 52(7):1382–1393, 2005.
3. Canetti, R., and Krawczyk, H., Analysis of key-exchange protocols and their use for building secure channels. *Lect. Notes Comput. Sci.* 2045:453–474, 2001.
4. Chen, C.L., Yang, T.T., and Shih, T.F., A secure medical data exchange protocol based on cloud environments. *J. Med. Syst.* 38:112, 2014.
5. Fortino, G., Guerrieri, A., Giannantonio, R., and Bellifemine, F., SPINE2: developing BSN applications on heterogeneous sensor nodes. In: Proceedings of IEEE Symposium on Industrial Embedded Systems (SIES 2009), pp. 8–10. Lausanne: Special Session on Wireless Health, 2009.
6. Fortino, G., Pathan, M., and DiFatta, G., BodyCloud: integration of cloud computing and body sensor networks. In: Proceedings of IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom 2012), pp. 3–6. Taipei, 2012.
7. Fortino, G., and Pathan, M., Integration of Cloud computing and body sensor networks. *Futur. Gener. Comput. Syst.* 35:57–61, 2014.
8. Guo, P., Wang, J., Li, B., and Lee, S., A variable threshold-value authentication architecture for wireless mesh networks. *J. Internet Technol.* 15(6):929–936, 2014.
9. Habetha, J., The myheart project - fighting cardiovascular diseases by prevention and early diagnosis. In: Proceedings of 28th IEEE Annual International Conference on Engineering in Medicine and Biology Society (EMBS 2006), pp. 6746–6749. New York, 2006.
10. HAVO: http://www.hvc.com.tw/lang/HAVO-E/Home%20HAVO.html, Available access: 2015/04/18.
11. He, D., Kumar, N., and Chilamkurti, N., A secure temporal-credential-based mutual authentication and key agreement scheme with pseudo identity for wireless sensor networks. *Inf. Sci.* 321:263–277, 2015.
12. He, D., and Zeadally, S., Authentication protocol for ambient assisted living system. *IEEE Commun. Mag.* 35(1):71–77, 2015.
13. He, D., Kumar, N., and Chen, J., Robust anonymous authentication protocol for healthcare applications using wireless medical sensor networks. *Multimedia Systems* 21(1):49–60, 2015.
14. He, D., and Wang, D., Robust biometrics-based authentication scheme for multi-server environment. *IEEE Syst. J.* 9(3):816–823, 2015.
15. Jabbari, A., and Bagherzadeh, J., A revised key agreement protocol based on chaotic maps. *Nonlinear Dyn.* 78(1):669–680, 2014.
16. Jiang, Q., Ma, J., Ma, Z., and Li, G., A privacy enhanced authentication scheme for telecare medical information systems. *J. Med. Syst.* 37:9897, 2013.
17. Khan, F.A., Ali, A., Abbas, H., and Haldar, N.A.H., A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks. *Procedia Comput. Sci.* 34:511–517, 2014.
18. Li, C.T., Lee, C.C., and Weng, C.Y., An extended chaotic maps based user authentication and privacy preserving scheme against DoS attacks in pervasive and ubiquitous computing environments. *Nonlinear Dyn.* 74(4):1133–1143, 2013.
19. Li, C.T., Lee, C.C., and Weng, C.Y., A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems. *J. Med. Syst.* 38(9):1–11, 2014.
20. Li, C.T., Lee, C.W., and Shen, J.J., An extended chaotic maps based keyword search scheme over encrypted data resist outside and inside keyword guessing attacks in cloud storage services. *Nonlinear Dyn.* 80(3):1601–1611, 2015.
21. Li, C.T., Lee, C.C., and Weng, C.Y., A dynamic identity-based user authentication scheme for remote login systems. *Security and Communication Networks* 8(18):3372–3382, 2015.
22. Li, C.T., Lee, C.C., Weng, C.Y., and Fan, C.I., A secure dynamic identity based authentication protocol with smart cards for multi-server architecture. *J. Inf. Sci. Eng.* 31(6):1975–1992, 2015.
23. Li, C.T., Weng, C.Y., and Lee, C.C., A secure RFID tag authentication protocol with privacy preserving in telecare medicine information systems. *J. Med. Syst.* 39(8):1–8, 2015.
24. Li, C.T., Weng, C.Y., Lee, C.C., and Wang, C.C., A hash based remote user authentication and authenticated key agreement scheme for the integrated EPR information system. *J. Med. Syst.* 39(11):1–11, 2015.
25. Li, C.T., Lee, C.C., Wang, C.C., Yang, T.H., and Chen, S.J., Design flaws in a secure medical data exchange protocol based on cloud environments. *Lect. Notes Comput. Sci.* 9532, 2015.
26. Li, C.T., Lee, C.C., and Weng, C.Y., A chaotic maps based key agreement and user anonymity protocol without using smart cards

and symmetric key en/decryptions. *J. Internet Technol.*, 2015. article in press.
27. Liu, J., Zhang, Z., Chen, X., and Kwak, K., Certificateless remote anonymous authentication schemes for wireless body sensor networks. *IEEE Transactions on Parallel and Distributed Systems* 25(2):332–342, 2014.
28. Lounis, A., Hadjidj, A., Bouabdallah, A., and Challal, Y., Healing on the cloud: Secure cloud architecture for medical wireless sensor networks. *Futur. Gener. Comput. Syst.*, 2015. article in press.
29. Mana, M., Feham, M., and Bensaber, B.A., Trust key management scheme for wireless body area networks. *Int. J. Netw. Security* 12(2):75–83, 2011.
30. Muhammad, K.R.R.S., Lee, H., Lee, S., and Lee, Y.K., BARI+: a biometric based distributed key management approach for wireless body area networks. *Sensors* 10(4):3911–3933, 2010.
31. Nadeem, A., Hussain, M.A., Owais, O., Salam, A., Iqbal, S., and Ahsan, K., Application specific study, analysis and classification of body area wireless sensor network applications. *Comput. Netw.* 83:363–380, 2015.
32. Pacelli, M., Loriga, G., Taccini, N., and Paradiso, R., Sensing fabrics for monitoring physiological and biomechanical variables: E-textile solutions. In: 3rd IEEE/EMBS International Summer School on Medical Devices and Biosensors, pp. 1–4. Cambridge, 2006.
33. Ren, Y., Pazzi, R.W.N., and Boukerche, A., Monitoring patients via a secure and mobile healthcare system. *IEEE Wirel. Commun.* 17(1):59–65, 2010.
34. Ren, Y., Shen, J., Wang, J., Han, J., and Lee, S., Mutual verifiable provable data auditing in public cloud storage. *J. Internet Technol.* 16(2):317–324, 2015.
35. RFC 2104 - HMAC: Keyed-hashing for message authentication. <http://www.ietf.org/rfc/rfc2104.txt>.
36. Saleem, S., Ullah, S., and Kwak, K.S., A study of IEEE 802.15.4 security framework for wireless body area networks. *Sensors* 11(2):1383–1395, 2011.
37. Shen, J., Moh, S., and Chung, I., A novel key management protocol in body area networks. In: Proceedings of the Seventh International Conference on Networking and Services (ICNS 2011), pp. 246–251. Venice, 2011.
38. Shen, J., Tan, H., Wang, J., and Lee, S., A novel routing protocol providing good transmission reliability in underwater sensor networks. *J. Internet Technol.* 16(1):171–178, 2015.
39. Subashini, S., and Kavitha, V., A survey on security issues in service delivery models of cloud computing. *J. Netw. Comput. Appl.* 34(1):1–11, 2011.
40. Wang, C., and Zhang, Y., New authentication scheme for wireless body area networks using the bilinear pairing. *J. Med. Syst.* 39:136, 2015.
41. Wu, Z.Y., Lee, Y.C., Lai, F., Lee, H.C., and Chung, Y., A secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1529–1535, 2012.
42. Xia, Z., Wang, X., Sun, X., and Wang, Q., A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data. *IEEE Transactions on Parallel and Distributed Systems* 27(2):340–352, 2016.
43. Xie, Q., Zhao, J., and Yu, X., Chaotic maps-based three-party password-authenticated key agreement scheme. *Nonlinear Dyn.* 74(4):1021–1027, 2013.
44. Zhang, L., Cryptanalysis of the public key encryption based on multiple chaotic systems. *Chaos, Solitons & Fractals* 37(3):669–674, 2008.
45. Zhao, Z., An efficient anonymous authentication scheme for wireless body area networks using elliptic curve cryptosystem. *J. Med. Syst.* 38(2):1–7, 2014.
46. Zhou, J., Cao, Z., and Dong, X., BDK: secure and efficient biometric based deterministic key agreement in wireless body area networks. In: Proceedings of 8th International Conference on Body Area Networks (BodyNets 2013). Boston, 2013.
47. Zhou, J., Cao, Z., Dong, X., Xiong, N., and Vasilakos, A.V., 4S: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. *Inf. Sci.* 314:255–276, 2015.
48. Zissis, D., and Lekkas, D., Addressing cloud computing security issues. *Futur. Gener. Comput. Syst.* 28(3):583–592, 2012.