An Enhanced Network Admission and Communication Scheme for Internet of Things Based Body Area Network Healthcare System

Chun-Ta Li, Dong-Her Shih, and Chun-Cheng Wang

***Abstract*—As an important part of Internet of Things (IoTs), body area networks (BAN) have been developed for providing medical diagnostics. A large number of wearable or embedded body sensors are used to sense and collect patient's personal physiological information and transmit it to the backend of the medical systems for healthcare monitoring. However, due to its openness, protecting sensitive data from unauthorized access is a vital issue in medical-related system. Recently, Deng *et al.* proposed a secure and lightweight network admission and communication scheme based on Internet of Things for body area network healthcare system. However, after a detailed inspection of their scheme, we found Deng *et al.*'s scheme is not secure enough as they claimed and then demonstrated that their scheme is vulnerable to various attacks, such as data replaying attack and user traceability attack. To eliminate the vulnerabilities of Deng *et al.*'s scheme, in this paper, we proposed an enhanced network admission and communication scheme for IoT-based body area network healthcare system while also providing mutual authentication, data confidentiality and data integrity.**

***Index Terms*—Body area network, cryptanalysis, mutual authentication, network admission, privacy, untraceability.**

I. Introduction

Over the years, Internet of Things based body area network system has gained a great deal of attention from researchers in medical fields [1]-[6]. With IoT-based BAN system, the body sensors are deployed on, in and/or around a designated patient and his/her personal health information (PHI) can be sensed and collected to the patient's mobile device [7]. Then the patient's PHI will be transmitted through the Internet and accessed by the remote caregivers in healthcare providers to implement real telemedicine. Owing to the PHI data is directly associated with a particular patient, it may lead to result in wrong medical diagnosis and treatment if it is short of appropriate security authentication and privacy preservation mechanisms. Therefore, the IoT-based BAN healthcare system must consider secure network admission to ensure the secure transmission. For the property of secure network admission, it can restrict network admission only to eligible medical participants. For the property of secure transmission, it can ensure confidential, authenticated and integrity transmission between each authorized medical participant.

The framework of IoT-based BAN healthcare system is shown in Fig. 1. There are four kinds of system participants in this system: the body sensor, the personal reader, the medical reader and the medical cloud server. The medical cloud server is a trusted medical institution and it manages all medical readers and personal readers. The body sensor is a small sensing device to collect patient's health data at regular intervals and forward it to the personal reader. The medical reader is a device carried by medical staff in a healthcare center and it is responsible for receiving patient's health data from a personal reader for diagnosis by a medical doctor. Before running the system, all personal readers and medical readers must register with the medical cloud server through a secure channel. Moreover, all body sensors and personal readers must register with the medical readers through a secure channel. In order to provide real time medical monitoring service, the personal reader must collect the health data from body sensors and transmit related health data to the remote medical reader through an insecure channel.

Recently, many researchers proposed the secure authentication schemes for healthcare systems [8]-[18], but their schemes focus on the authentication procedures between user and medical server without designing a comprehensive protocol for our healthcare scenario based on IoT environment. To cope with the security challenges associate with IoT-based BAN healthcare system, He *et al.* [2] introduced a secure and lightweight network admission and transmission protocol for body sensor networks that uses a polynomial-based authentication mechanism. However, Deng *et al.* [1] later showed that He *et al.*'s scheme fails to provide mutual authentication and suffers from illegal access, and proposed a more secure scheme to achieve mutual authentication between each system participant. However, we found that Deng *et al.*'s scheme fails to protect against data replaying and user traceability attacks and thus developed an improved network admission and transmission scheme for IoT-based BAN healthcare system based on Deng *et al.*'s scheme.

The remainder of the paper is organized as follows. A brief review of Deng *et al.*'s scheme is introduced in Section II. We demonstrate two security flaws of Deng *et al.*'s scheme in Section III and Section IV, respectively. The proposed scheme and the security analysis of our proposed scheme are presented in Section V and Section VI, respectively. Finally,

Manuscript received February 2, 2018; revised April 15, 2018. This work was supported in part by the Ministry of Science and Technology, Taiwan, R.O.C., under Grant MOST 106-3114-C-165-001-ES.

Chun-Ta Li is with the Department of Information Management, Tainan University of Technology, Tainan City 71002, Taiwan, R.O.C. (e-mail: th0040@mail.tut.edu.tw).

Dong-Her Shih and Chun-Cheng Wang are with the Department of Information Management, National Yunlin University of Science and Technology, Yunlin 64002, Taiwan, R.O.C. (e-mail: shihdh@yuntech.edu.tw, jim821112@gmail.com).

doi: 10.18178/jacn.2018.6.1.252

the conclusions are given in Section VII.

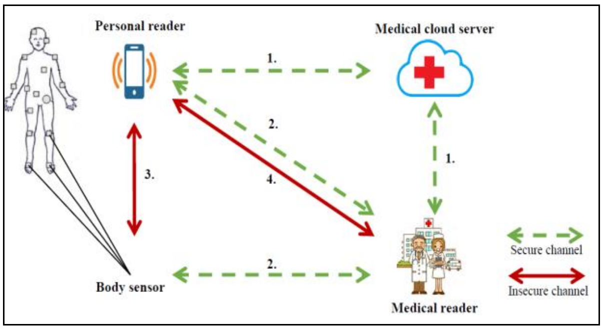

Fig. 1. The framework of IoT-based BAN healthcare system.

II. A Brief Review of Deng et al.'s Scheme

In this section, we review Deng *et al.*'s scheme [1] based on IoTs for BAN healthcare system. Deng *et al.*'s scheme consists of five phases: (i) system initialization phase, (ii) body-sensor registration phase, (iii) personal-reader registration phase, (iv) medical-reader registration phase, and (v) authentication and communication phase. For convenience of illustration, some notations used in this paper are listed in Table I the details of each phase are briefly illustrated in the following subsections.

TABLE I: Notations Used in the Paper

Symbol	Description
q	A k-bit prime
F_q	A prime finite field
E/F_q	An elliptic curve E over F_q
G	A cyclic additive group of composite order q
P	A generator for the group G
(s, PK)	A private and public key of the system, where $PK=sP$
$f(x, y)$	A polynomial function that $f(x, y)$ equal to $f(y, x)$
$H_i()$	i^{th} one-way hash function
$h()$	A one-way hash function
ID_i	A universally unique identifier (UUID) code of party i
TID	A transaction number which changes every round
PEK	A session key established by personal reader and medical reader
$data$	Body sensor's sensing information
$E_k(m)$	Use a key k to encrypt the message m
$D_k(m)$	Use a key k to decrypt the message m
TS_i	A timestamp which is generated by party i
ΔT	A valid time interval for transmission delay
NID_i	A randomly unique identifier of party i
A ?= B	Determine if A is equal to B

A. System Initialization Phase

In this phase, the medical cloud server generates some parameter and publishes these parameters for all medical readers and personal readers.

Step 1. The medical cloud chooses a k-bit prime p and determines the tuple of elliptic curve group (F_q, E/F_q, G, P).

Step 2. The medical cloud computes a public system key $PK=sP$, where s is a private system key of medical cloud.

Step 3. Finally, the medical cloud chooses four hash functions (H_1(.), H_2(.), H_3(.), H_4(.)) and publishes the parameters (F_q, E/F_q, G, P, PK, H_1(.), H_2(.), H_3(.), H_4(.)) to all medical readers and personal readers.

B. Body-Sensor Registration Phase

In this phase, the body sensor must register with the medical reader through a secure channel by performing the following steps.

Step 1. The body sensor sends its identity ID_{HS} to the medical reader.

Step 2. The medical reader generates the polynomial $f(x, y)$ and computes $HP_{HS}= f(ID_{HS}, y)$ and $c=h(SID)$, where SID is an unique identifier shared between the body sensor and the personal reader. Then, the medical reader sends (HP_{HS}, SID) to the body sensor.

Step 3. The body sensor saves (HP_{HS}, SID) in its memory.

C. Personal-Reader Registration Phase

In this phase, the personal reader must register with the medical reader and the medical cloud server through a secure channel by performing the following steps.

Step 1. The personal reader selects a universally unique identifier ID_{PR} and sends it to the medical reader.

Step 2. The medical reader generates the polynomial $f(x, y)$ and computes $HP_{PR}= f(ID_{PR}, y)$ and $c=h(SID)$. Then, the medical reader sends (HP_{PR}, SID) to the personal reader.

Step 3. The personal reader saves (HP_{PR}, SID) in its memory.

Step 4. The personal reader sends its identity ID_{PR} to the medical cloud server.

Step 5. The medical cloud server generates a random number r and computes $R_{PR}= rP$, $h_{PR} = H_1(ID_{PR}||R_{PR})$ and $S_{PR} = r + h_{PR}s$. Then, the medical cloud server sends (R_{PR}, S_{PR}) to the personal reader.

Step 6. The personal reader verifies $S_{PR}P$?= $R_{PR} + H_1(ID_{PR}||R_{PR})PK$. If above holds, the personal reader stores (R_{PR}, S_{PR}) in its memory.

D. Medical Reader Registration Phase

In this phase, the medical reader must register with the medical cloud server through a secure channel by performing the following steps.

Step 1. The medical reader sends its identity ID_{MR} to the medical cloud server.

Step 2. The medical cloud server generates a random number r and computes $R_{PR}= rP$, $h_{MR} = H_1(ID_{MR}||R_{MR})$ and $S_{MR} = r + h_{MR}s$. Then, the medical cloud server sends (R_{MR}, S_{MR}) to the medical reader.

Step 3. The personal reader verifies $S_{MR}P$?= $R_{MR} + H_1(ID_{MR}||R_{MR})PK$. If above holds, the medical reader stores (R_{MR}, S_{MR}) in its memory.

E. Authentication and Communication Phase

When the personal reader needs to transmit the related health data to a medical reader, it must first receive *data* from body sensors. Therefore, two kinds of authentication models (1. Mutual authentication between the personal reader and the body sensor; 2. Mutual authentication between personal reader and the medical reader) will be demonstrated in the following steps.

Step 1. When the personal reader wants to receive the health data from the body sensor, it first computes $c=h(SID)$ and sends (ID_{PR}, c) to the body sensor through an insecure channel.

Step 2. The body sensor verifies the authenticity of the personal reader by checking c ?= $h(SID)$. If it holds, the body sensor computes $k_{HP} = f(ID_{HS}, ID_{PR})$, $d=Ek_{HP}(data)$ and $e=h(data||k_{HP})$ and sends (ID_{HS}, d, e) to the personal reader through an insecure channel.

Step 3. The personal reader computes $k_{HP} = f(ID_{PR}, ID_{HS})$ and $data = Dk_{HP}(d)$ and verifies e ?= $h(data||k_{HP})$. If above holds, the personal reader will transmit *data* to the medical reader in follow-up steps.

Step 4. The personal reader selects a random number a and computes $T_{PR}= aP$. Then the personal reader sends $(ID_{PR}, R_{PR}, T_{PR})$ to the medical reader through an insecure channel.

Step 5. The medical reader selects a random number b and computes $T_{MR}= bP$, $PK_{PR} = R_{PR} + H_1(ID_{PR}||R_{PR})PK$, $K_{MP1} = S_{MR}T_{PR} + bPK_{PR}$, $K_{MP2} = bT_{PR}$ and the session key $PEK = H_2(K_{MP1}||K_{MP2})$.

Step 6. The medical reader selects a transaction number *TID* and computes $g = E_{PEK}(TID)$ and $CHK_{PM} = H_3(PEK||T_{PR})$. Then the medical reader sends $(ID_{MR}, R_{MR}, T_{MR}, g, CHK_{PM})$ to the personal reader through an insecure channel.

Step 7. The personal reader computes $PK_{MR} = R_{MR} + H_1(ID_{MR}||R_{MR})PK$, $K_{PM1} = S_{PR}T_{MR} + aPK_{MR}$, $K_{PM2} = aT_{MR}$ and the session key $PEK = H_2(K_{PM1}||K_{PM2})$. Then the personal reader verifies the authenticity of the medical reader by checking CHK_{PM} ?= $H_3(PEK||T_{PR})$. If above holds, the personal reader computes $TID = D_{PEK}(g)$, $c_i = E_{(PEK||TID)}(data)$, $CHK_{MP} = H_3(PEK||T_{MR}||TID)$ and $TID_{new} = H_4(TID)$ and sends (ID_{PR}, CHK_{MP}, c_i) to the medical reader through an insecure channel.

Step 8. The medical reader verifies the authenticity of the personal reader by checking CHK_{MP} ?= $H_3(PEK||T_{MR}||TID)$. If above holds, the personal reader and the medical reader can communicate securely using *PEK*. Finally, the medical reader computes $data = D_{(PEK||TID)}(c_i)$ and $TID_{new} = H_4(TID)$ and replaces the original transmission number TID with new transmission number TID_{new} for future communication.

III. Data Replaying Attack on Deng et al.'s Scheme

In this section, we found Deng *et al.*'s scheme is insecure against data replaying attack in the authentication and communication phase and this design flaw can lead a malicious attacker U_A to impersonate as a body sensor to transmit duplicate physiological data to a personal reader. We further provide the detailed explanation of this attack through the following steps:

Step 1. A malicious attacker U_A eavesdrops the transmitted messages between the personal reader and the body sensor and collects the parameters $(ID_{PR}, c, ID_{HS}, d, e)$.

Step 2. When the personal reader sends the message (ID_{PR}, c) to its body sensor in Step 1 of authentication and communication phase of Deng *et al.*'s scheme, U_A intercepts this message to prevent it arrives body sensor.

Step 3. In Step 2 of authentication and communication phase of Deng *et al.*'s scheme, U_A transmits the eavesdropped message (ID_{HS}, d, e) to the personal reader.

Step 4. In Step 3 of authentication and communication phase of Deng *et al.*'s scheme, The personal reader then decrypts *data* using the key k_{HP} and verifies whether the computed $h(data||k_{HP})$ matches e. This condition holds, since all parameters were generated by a legitimate body sensor and the medical reader thus authenticates the body sensor successfully. Therefore, the medical reader will receive the previous health data in mistake and cannot distinguish whether the health data is sent by the legal body sensor or it is a replay health data. In other words, the medical reader cannot authenticate the legality of the body sensor in Deng *et al.*'s scheme.

IV. User Traceability Attack on Deng et al.'s Scheme

In authentication and communication phase of Deng *et al.*'s scheme, they claimed that the user untraceability of every session from the medical reader to body sensor is guaranteed in their scheme. However, we found that the property of user untraceability cannot be protected by launching message eavesdropping attack during the authentication and communication phase. In Step 1 of the authentication and communication phase of Deng *et al.*'s scheme, the message (ID_{PR}, c) transmitted from the medical reader to the body sensor is unchanging in every session. Hence, the user untraceability will not be protected because the medical reader's identity ID_{PR} is openly available on insecure channel.

At the same time, user traceability attack can be launched comfortably by an attacker between the personal reader and the medical reader. In Step 4 and Step 6 of the authentication and communication phase of Deng *et al.*'s scheme, an attacker U_A can easily eavesdrop the transmitted messages from the personal reader to the medical reader and obtain the identities ID_{PR} and ID_{MR}. As a result, U_A can know the relation of a connection between the personal reader and the medical reader as long as the communication messages transmitted on the insecure channel contains (ID_{PR}, ID_{MR}).

V. The Proposed Scheme

In order to remove the identified security flaws of Deng *et al.*'s scheme, we propose an improved scheme for BAN healthcare system in this section. Our proposed scheme can be described in the following phases.

A. System Initialization Phase

In this phase, the executed steps are the same as in Deng *et al.*'s scheme.

B. Body-Sensor Registration Phase

As shown in Fig. 2, the body sensor must register with the medical reader through a secure channel by performing the following steps.

Step 1. The body sensor generates a random and unique identifier NID_{HS} and sends it to the medical reader.

Step 2. The medical reader generates the polynomial $f(x, y)$ and NID_{PR} and computes $HP_{HS}= f(NID_{HS}, y)$. Then, the medical reader stores $(NID_{HS}, f(x, y), NID_{PR})$ in its memory and sends (HP_{HS}, NID_{PR}) to the body sensor, where NID_{PR} is a random identifier of the designated personal reader.

Step 3. The body sensor stores $(HP_{HS}, NID_{HS}, NID_{PR})$ in its memory.

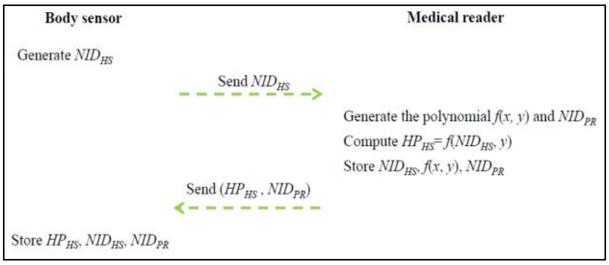
Body sensor
Medical reader
Generate NID_{HS}
Send NID_{HS}
Generate the polynomial $f(x, y)$ and NID_{PR}
Compute $HP_{HS}= f(NID_{HS}, y)$
Store $NID_{HS}, f(x, y), NID_{PR}$
Send (HP_{HS}, NID_{PR})
Store $HP_{HS}, NID_{HS}, NID_{PR}$

Fig. 2. Body-sensor registration phase of the proposed scheme.

C. Personal-Reader Registration Phase

As shown in Fig. 3 and Fig. 4, the personal reader must register with the medical reader and the medical cloud server through a secure channel by performing the following steps.

Step 1. The personal reader selects a universally unique identifier ID_{PR} and sends ID_{PR} to the medical reader.

Step 2. The medical reader uses the polynomial $f(x, y)$ and NID_{PR} to compute $HP_{PR}= f(NID_{PR}, y)$ and generates a random identifier NID_{MR}. Then, the medical reader stores (NID_{MR}, ID_{PR}) in its memory and sends $(HP_{PR}, NID_{PR}, NID_{MR}, NID_{HS})$ to the personal reader.

Step 3. The personal reader stores $(HP_{PR}, NID_{PR}, NID_{MR}, NID_{HS})$ in its memory.

Step 4. The personal reader sends its identity ID_{PR} to the medical cloud server.

Step 5. The medical cloud server generates a random number r and computes $R_{PR}= rP$, $h_{PR} = H_1(ID_{PR}||R_{PR})$ and $S_{PR} = r + h_{PR}s$. Then, the medical cloud server sends (R_{PR}, S_{PR}) to the personal reader.

Step 6. The personal reader verifies $S_{PR}P$?= $R_{PR} + H_1(ID_{PR}||R_{PR})PK$. If above holds, the personal reader stores (R_{PR}, S_{PR}) in its memory. Finally, the personal reader stores $(HP_{PR}, NID_{PR}, NID_{MR}, NID_{HS}, R_{PR}, S_{PR})$ in its memory.

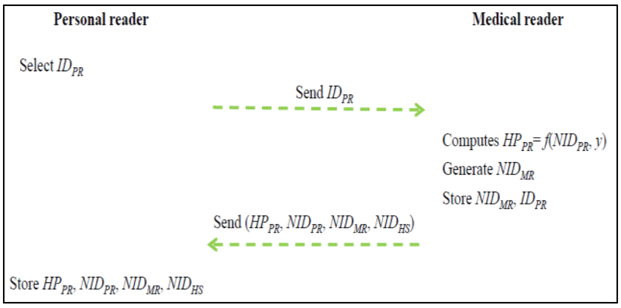
Personal reader
Medical reader
Select ID_{PR}
Send ID_{PR}
Computes $HP_{PR}= f(NID_{PR}, y)$
Generate NID_{MR}
Store NID_{MR}, ID_{PR}
Send $(HP_{PR}, NID_{PR}, NID_{MR}, NID_{HS})$
Store $HP_{PR}, NID_{PR}, NID_{MR}, NID_{HS}$

Fig. 3. Personal-reader registration phase of the proposed scheme with medical reader.

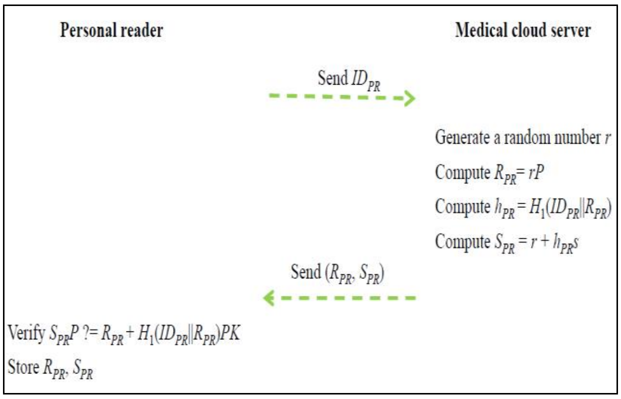
Personal reader
Medical cloud server
Send ID_{PR}
Generate a random number r
Compute $R_{PR}= rP$
Compute $h_{PR} = H_1(ID_{PR}||R_{PR})$
Compute $S_{PR} = r + h_{PR}s$
Send (R_{PR}, S_{PR})
Verify $S_{PR}P$?= $R_{PR} + H_1(ID_{PR}||R_{PR})PK$
Store R_{PR}, S_{PR}

Fig. 4. Personal-reader registration phase of the proposed scheme with medical cloud server.

D. Medical Reader Registration Phase

As shown in Fig. 5, the medical reader must register with the medical cloud server through a secure channel by performing the following steps.

Step 1. The medical reader sends its identity ID_{MR} to the medical cloud server.

Step 2. The medical cloud server generates a random number r and computes $R_{MR}= rP$, $h_{MR} = H_1(ID_{MR}||R_{MR})$ and $S_{MR} = r + h_{MR}s$. Then, the medical cloud server sends (R_{MR}, S_{MR}) to the medical reader.

Step 3. The personal reader verifies $S_{MR}P$?= $R_{MR} + H_1(ID_{MR}||R_{MR})PK$. If above holds, the medical reader stores (R_{MR}, S_{MR}) in its memory. Finally, the medical reader stores $(NID_{MR}, ID_{PR}, NID_{PR}, f(x, y), R_{MR}, S_{MR})$ in its memory.

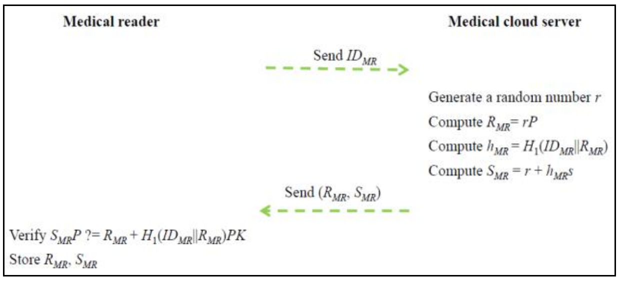
Medical reader
Medical cloud server
Send ID_{MR}
Generate a random number r
Compute $R_{MR}= rP$
Compute $h_{MR} = H_1(ID_{MR}||R_{MR})$
Compute $S_{MR} = r + h_{MR}s$
Send (R_{MR}, S_{MR})
Verify $S_{MR}P$?= $R_{MR} + H_1(ID_{MR}||R_{MR})PK$
Store R_{MR}, S_{MR}

Fig. 5. Medical-reader registration phase of the proposed scheme.

E. Authentication and Communication Phase

As shown in Fig. 6 and Fig. 7, when the personal reader needs to transmit the related health data to a medical reader, it must first receive *data* from body sensors. Therefore, two kinds of authentication models (1. Mutual authentication between the personal reader and the body sensor; 2. Mutual authentication between personal reader and the medical reader) will be demonstrated in the following steps.

Step 1. When the personal reader wants to receive the health data from the body sensor, it first generates a timestamp TS_{PR} and computes $k_{PH} = f(NID_{PR}, NID_{HS})$ and $c=h(k_{PH}, TS_{PR})$. Then the personal reader sends (NID_{PR}, TS_{PR}, c) to the body sensor.

Step 2. Upon receiving the message from the personal reader, the body sensor first checks the validity of NID_{PR} and $(TS_{HS} - TS_{PR}) \leq \Delta T$ are valid or not, where TS_{HS} denotes receiving timestamp of personal reader's message and ΔT denotes the expected valid time interval for transmission delay. If above are not valid, the body sensor rejects the personal reader's request. If above are valid, the body sensor generates a new random identifier NID_{HS_new} and computes $k_{HP} = f(NID_{HS}, NID_{PR})$. Then the body sensor verifies c ?= $h(k_{PH}, TS_{PR})$. If it holds, the personal reader is authenticated by the body sensor. Next, the body sensor computes $d=Ek_{HP}(data, NID_{PR}, NID_{HS\_new})$ and $e=h(data|| NID_{HS\_new}||TS_{HS})$ and sends $(NID_{HS}, TS_{HS}, d, e)$ to the personal reader.

Step 3. Upon receiving the message from the body sensor, the personal reader first checks the validity of NID_{HS} and $(TS_{PR}{}' – TS_{HS}) \leq \Delta T$ are valid or not, where $TS_{PR}{}'$ denotes receiving timestamp of body sensor's message and ΔT denotes the expected valid time interval for transmission delay. If above are not valid, the personal reader terminates this session. If above are valid, the personal reader computes

$Dk_{PH}(d)$ = ($data$, NID_{PR}, NID_{HS_new}) and verifies $h(data\|NID_{HS\_new}\|TS_{MR})$?= e. If it holds, the personal reader generates a new random identifier NID_{PR_new} and computes $g{=}Ek_{HP}(TS_{PR}{}', NID_{PR\_new}, NID_{HS\_new})$. Then the personal reader sends (g, $TS_{PR}{}'$) to the body sensor and replaces NID_{PR} with NID_{PR_new}. Moreover, the personal reader stores NID_{HS_new} in its memory. Finally, the format of its memory is (HP_{PR}, NID_{PR_new}, NID_{MR}, NID_{HS}, R_{PR}, S_{PR}, NID_{HS_new}).

Step 4. Upon receiving the message from the personal reader, the body sensor first checks if $(TS_{HS}{}' - TS_{PR}{}') \leq \Delta T$, where $TS_{HS}{}'$ denotes receiving timestamp of personal reader's message and ΔT denotes the expected valid time interval for transmission delay. If above is not valid, the body sensor terminates this session. If above is valid, the body sensor computes $Dk_{HP}(g) = (TS_{PR}{}', NID_{PR\_new}, NID_{HS\_new})$ and verifies $TS_{PR}{}'$ and NID_{HS_new}. If above are valid, the body sensor replaces NID_{HS} with NID_{HS_new} and stores NID_{PR_new} in its memory. Finally, the format of its memory is (HP_{HS}, NID_{HS_new}, NID_{PR}, NID_{PR_new}).

Step 5. The personal reader selects a random number a and computes $T_{PR}= aP$, $k_{PM} = f(NID_{PR}, NID_{MR})$ and $i{=}Ek_{PM}(ID_{PR}, R_{PR}, T_{PR}, TS_{PR}{}'')$. Then the personal reader sends (NID_{MR}, i, $TS_{PR}{}''$) to the medical reader, where $TS_{PR}{}''$ is the current timestamp of the personal reader.

Step 6. Upon receiving the message from the personal reader, the medical reader first checks the validity of NID_{MR} and $(TS_{MR} - TS_{PR}{}'') \leq \Delta T$ are valid or not, where TS_{MR} denotes receiving timestamp of personal reader's message and ΔT denotes the expected valid time interval for transmission delay. The medical reader computes $k_{MP} = f(NID_{MR}, NID_{PR})$ and $Dk_{MP}(i) = (ID_{PR}, R_{PR}, T_{PR}, TS_{PR}{}'')$. Then the medical reader selects a random number b and computes $T_{MR}= bP$, $PK_{PR} = R_{PR} + H_1(ID_{PR}\|R_{PR})PK$, $K_{MP1} = S_{MR}T_{PR} + bPK_{PR}$, $K_{MP2} = bT_{PR}$, the session key $PEK = H_2(K_{MP1}\|K_{MP2})$.

Step 7. The medical reader selects a new random identifier NID_{MR_new} and computes $j = Ek_{MP}(NID_{MR\_new}, R_{MR}, T_{MR}, TS_{MR})$ and $CHK_{PM} = H_3(PEK\|NID_{MR\_new})$. Then the medical reader sends (j, CHK_{PM}, TS_{MR}) to the personal reader.

Step 8. Upon receiving the message from the medical reader, the personal reader first checks if $(TS_{PR}{}^{*} - TS_{MR}) \leq \Delta T$ is valid or not, where $TS_{PR}{}^{*}$ denotes receiving timestamp of medical reader's message and ΔT denotes the expected valid time interval for transmission delay. If it is valid, the personal reader computes $Dk_{PM}(j) = (NID_{MR\_new}, R_{MR}, T_{MR}, TS_{MR})$, $PK_{MR} = R_{MR} + H_1(ID_{MR}\|R_{MR})PK$, $K_{PM1} = S_{PR}T_{MR} + aPK_{MR}$, $K_{PM2} = aT_{MR}$ and the session key $PEK = H_2(K_{PM1}\|K_{PM2})$. Then the personal reader verifies the authenticity of the medical reader by checking CHK_{PM} ?= $H_3(PEK\|NID_{MR\_new})$. If above holds, the personal reader computes $m = E_{PEK}(data)$ and $CHK_{MP} = H_3(PEK\|NID_{MR\_new}\|TS_{PR}{}^{*})$ and sends (m, CHK_{MP}, $TS_{PR}{}^{*}$) to the medical reader. Finally, the personal reader replaces NID_{MR} with NID_{MR_new} and the format of its memory is (HP_{PR}, NID_{PR_new}, NID_{MR_new}, NID_{HS}, R_{PR}, S_{PR}, NID_{HS_new}).

Step 9. Upon receiving the message from the personal reader, the medical reader first checks if $(TS_{MR}{}' - TS_{PR}{}^{*}) \leq \Delta T$ is valid or not, where $TS_{MR}{}'$ denotes receiving timestamp of personal reader's message and ΔT denotes the expected valid time interval for transmission delay. The medical reader verifies the authenticity of the personal reader by checking CHK_{MP} ?= $H_3(PEK\|NID_{MR\_new}\|TS_{PR}{}^{*})$. If above holds, the personal reader and the medical reader can communicate securely using PEK. Then the medical reader computes $data = D_{PEK}(m)$ and replaces NID_{MR} with NID_{MR_new}. Finally, the format of its memory is (NID_{MR_new}, ID_{PR}, NID_{PR}, $f(x, y)$, R_{MR}, S_{MR}).

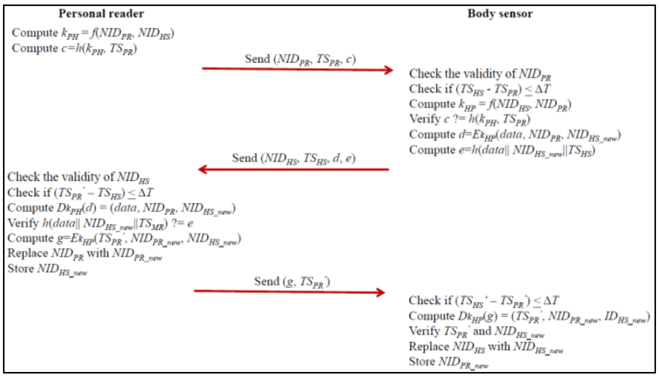
Personal reader
Body sensor
Compute $k_{PH} = f(NID_{PR}, NID_{HS})$
Compute $c{=}h(k_{PH}, TS_{PR})$
Send (NID_{PR}, TS_{PR}, c)
Check the validity of NID_{PR}
Check if $(TS_{HS} - TS_{PR}) \leq \Delta T$
Compute $k_{HP} = f(NID_{HS}, NID_{PR})$
Verify c ?= $h(k_{PH}, TS_{PR})$
Compute $d{=}Ek_{HP}(data, NID_{PR}, NID_{HS\_new})$
Compute $e{=}h(data\| NID_{HS\_new}\|TS_{HS})$
Send (NID_{HS}, TS_{HS}, d, e)
Check the validity of NID_{HS}
Check if $(TS_{PR}{}' - TS_{HS}) \leq \Delta T$
Compute $Dk_{PH}(d) = (data, NID_{PR}, NID_{HS\_new})$
Verify $h(data\| NID_{HS\_new}\|TS_{MR})$?= e
Compute $g{=}Ek_{HP}(TS_{PR}{}', NID_{PR\_new}, NID_{HS\_new})$
Replace NID_{PR} with NID_{PR_new}
Store NID_{HS_new}
Send (g, $TS_{PR}{}'$)
Check if $(TS_{HS}{}' - TS_{PR}{}') \leq \Delta T$
Compute $Dk_{HP}(g) = (TS_{PR}{}', NID_{PR\_new}, ID_{HS\_new})$
Verify $TS_{PR}{}'$ and NID_{HS_new}
Replace NID_{HS} with NID_{HS_new}
Store NID_{PR_new}

Fig. 6. Authentication and communication phase of the proposed scheme for a personal reader and the body sensor.

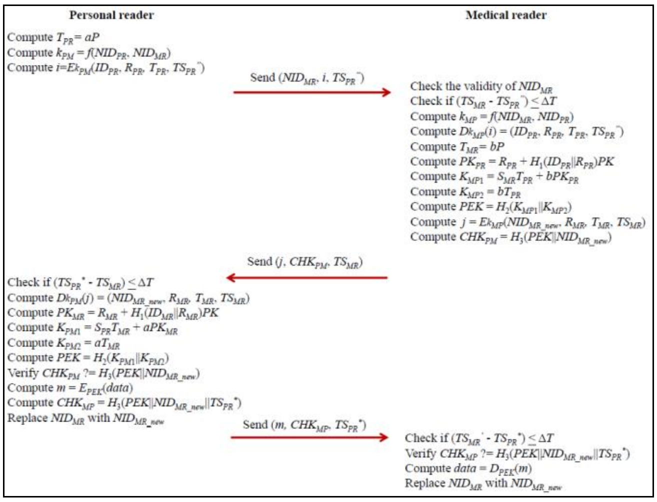
Personal reader
Medical reader
Compute $T_{PR}= aP$
Compute $k_{PM} = f(NID_{PR}, NID_{MR})$
Compute $i{=}Ek_{PM}(ID_{PR}, R_{PR}, T_{PR}, TS_{PR}{}'')$
Send (NID_{MR}, i, $TS_{PR}{}''$)
Check the validity of NID_{MR}
Check if $(TS_{MR} - TS_{PR}{}'') \leq \Delta T$
Compute $k_{MP} = f(NID_{MR}, NID_{PR})$
Compute $Dk_{MP}(i) = (ID_{PR}, R_{PR}, T_{PR}, TS_{PR}{}'')$
Compute $T_{MR}= bP$
Compute $PK_{PR} = R_{PR} + H_1(ID_{PR}\|R_{PR})PK$
Compute $K_{MP1} = S_{MR}T_{PR} + bPK_{PR}$
Compute $K_{MP2} = bT_{PR}$
Compute $PEK = H_2(K_{MP1}\|K_{MP2})$
Compute $j = Ek_{MP}(NID_{MR\_new}, R_{MR}, T_{MR}, TS_{MR})$
Compute $CHK_{PM} = H_3(PEK\|NID_{MR\_new})$
Send (j, CHK_{PM}, TS_{MR})
Check if $(TS_{PR}{}^{*} - TS_{MR}) \leq \Delta T$
Compute $Dk_{PM}(j) = (NID_{MR\_new}, R_{MR}, T_{MR}, TS_{MR})$
Compute $PK_{MR} = R_{MR} + H_1(ID_{MR}\|R_{MR})PK$
Compute $K_{PM1} = S_{PR}T_{MR} + aPK_{MR}$
Compute $K_{PM2} = aT_{MR}$
Compute $PEK = H_2(K_{PM1}\|K_{PM2})$
Verify CHK_{PM} ?= $H_3(PEK\|NID_{MR\_new})$
Compute $m = E_{PEK}(data)$
Compute $CHK_{MP} = H_3(PEK\|NID_{MR\_new}\|TS_{PR}{}^{*})$
Replace NID_{MR} with NID_{MR_new}
Send (m, CHK_{MP}, $TS_{PR}{}^{*}$)
Check if $(TS_{MR}{}' - TS_{PR}{}^{*}) \leq \Delta T$
Verify CHK_{MP} ?= $H_3(PEK\|NID_{MR\_new}\|TS_{PR}{}^{*})$
Compute $data = D_{PEK}(m)$
Replace NID_{MR} with NID_{MR_new}

Fig. 7. Authentication and communication phase of the proposed scheme for a personal reader and the medical reader.

VI. Security Analysis of the Proposed Scheme

In this section, we provide analysis of our proposed scheme with respect to security. In order to emphasis on describing the security of our proposed scheme, we assume that all participants' secret polynomial function $f(x, y)$ has been well-protected by themselves.

Property 1. The data replaying attack does not work in our proposed scheme.

Proof. Based on the design of our proposed scheme, the data replaying attack cannot be launched in the authentication and communication phase. We assume that a malicious attacker U_A intends to collect the transmitted messages (NID_{PR}, TS_{PR}, c, NID_{HS}, TS_{HS}, d, e) between the personal reader and the body sensor and transmits duplicate physiological data to a personal reader. However, these duplicated parameters must fail since the personal reader can confirm whether the timestamp is fresh or not. As a result, the proposed scheme is secure against data replaying attack because all the transmitted messages are valid only for a short time and the replaying of previous messages will not be successfully launched by the verification of the timestamps.

Property 2. The user traceability attack does not work in our proposed scheme.

Proof. In Deng *et al*.'s scheme without user untraceability, some fixed parameters are contained in transmitted messages and these fixed parameters can be used to track the medical relationship between the personal reader and the medical reader. The proposed scheme can protect user untraceability by masking original identities (ID_{PR}, ID_{MR}, ID_{HS}) behind pseudonyms (NID_{PR}, NID_{MR}, NID_{HS}). In Step 1 of the authentication and communication phase, the personal reader sends NID_{PR} instead of ID_{PR} every time it initiates a session. In addition, in Step 2 of the authentication and communication phase, the body sensor sends NID_{HS} instead of ID_{HS}. In this manner the personal reader and the body sensor cannot be traced since both them send random (NID_{PR}, NID_{HS}) for every session. Similarly, in Step 5 and Step 7 of the authentication and communication phase, the personal reader and the medical reader cannot be traced since them send random (NID_{MR}, NID_{MR_new}) for every session. Therefore, the proposed scheme provides the property of user untraceability.

Property 3. The proposed scheme ensures the properties of data confidentiality and data integrity.

Proof. The property of data confidentiality is to achieve protection on transmitting of medical data from the attacker. In addition, the property of data integrity is to prevent an attacker to modify or inject forged messages during communication. In Step 2 of the authentication and communication phase, the body sensor's sensing information *data* is encrypted with k_{HP} and U_A gets encrypted $d=Ek_{HP}(data, NID_{PR}, NID_{HS\_new})$ which cannot be decrypted and forged without having key $k_{HP} = f(NID_{HS}, NID_{PR})$. In the same way, in Step 8 of the authentication and communication phase, the proposed scheme uses the session key PEK to generate the encrypted message $m = E_{PEK}(data)$. Thus the malicious attacker cannot reveal and modify the sensing information *data*. Therefore, the properties of data confidentiality and the data integrity can be guaranteed in our proposed scheme.

VII. Conclusions

In this paper, we first reviewed Deng *et al.*'s authentication scheme for cloud healthcare environments and demonstrated that their scheme has two security weaknesses of data replaying attack and user traceability attack in the authentication and communication phase with the threat of eavesdropping. In this paper, we attempted to repair the above-mentioned problems by adopting timestamps and pseudonyms during message transmissions through the insecure channel. The proposed network admission and communication scheme not only preserves healthcare system from potential attacks but also ensures the excellent properties of mutual authentication, user untraceability, data confidentiality and data integrity in Internet of things based body area network healthcare system.

References

[1] Y. Y. Deng, C. L. Chen, W. J. Tsaur, Y. W. Tang, and J. H. Chen, "Internet of things (IoT) based design a secure and lightweight body area network (BAN) healthcare system," *Sensors*, vol. 17, no. 2, pp. 1-18, 2017.

[2] D. He, C. Chen, S. Chan, J. Bu, and P. Zhang, "Secure and lightweight network admission and transmission protocol for body sensor networks," *IEEE Journal of Biomedical and Health Informatics*, vol. 17, no. 3, pp. 664-674, 2013.

[3] D. He, S. Zeadally, N. Kumar, and J. H. Lee, "Anonymous authentication for wireless body area networks with provable security," *IEEE Systems Journal*, vol. 11, no. 4, pp. 2590-2601, 2017.

[4] C. T. Li, T. Y. Wu, C. L. Chen, C. C. Lee, and C. M. Chen, "An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system," *Sensors*, vol. 17, no. 7, pp. 1-18, 2017.

[5] C. T. Li, C. C. Lee, C. Y. Weng, and C. M. Chen, "Towards secure authenticating of cache in the reader for RFID-based IoT systems," *Peer-to-Peer Networking and Applications*, vol. 11, no. 1, pp. 198-208, 2018.

[6] Q. Q. Xie, S. R. Jiang, L. M. Wang, and C. C. Chang, "Composable secure roaming authentication protocol for cloud-assisted body sensor networks," *International Journal of Network Security*, vol. 18, no. 5, pp. 816-831, 2016.

[7] Y. Tian, Y. Peng, G. Gao, and X. Peng, "Role-based access control for body area networks using attribute-based encryption in cloud storage," *International Journal of Network Security*, vol. 19, no. 5, pp. 720-726, 2017.

[8] A. K. Das, "A secure smartcard-based anonymous user authentication scheme for healthcare applications using wireless medical sensor network," *Wireless Personal Communications*, vol. 94, no. 3, pp. 1899-1933, 2017.

[9] R. Guo and H. Shi, "Confidentiality-preserving personal health records in tele-healthcare system using authenticated certificateless encryption," *International Journal of Network Security*, vol. 19, no. 6, pp. 995-1004, 2017.

[10] Q. Jiang, M. K. Khan, X. Lu, J. Ma, and D. He, "A privacy preserving three-factor authentication protocol for e-health clouds," *The Journal of Supercomputing*, vol. 72, no. 10, pp. 3826-3849, 2016.

[11] T. F. Lee, "An efficient chaotic map-based authentication and key agreement scheme using smartcards for telecare medicine information systems," *Journal of Medical Systems*, vol. 37, no. 6, pp. 9985, 2013.

[12] C. T. Li, C. C. Lee, and C. Y. Weng, "A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems," *Journal of Medical Systems*, vol. 38, no. 9, pp. 1-11, 2014.

[13] C. T. Li, C. C. Lee, and C. Y. Weng, "A secure cloud-assisted wireless body area network in mobile emergency medical care system," *Journal of Medical Systems*, vol. 40, no. 5, pp. 1-15, 2016.

[14] C. T. Li, C. C. Lee, C. Y. Weng, and S. J. Chen, "A secure dynamic identity and chaotic maps based user authentication and key agreement scheme for e-healthcare systems," *Journal of Medical Systems*, vol. 40, no. 11, pp. 1-10, 2016.

[15] C. T. Li, D. H. Shih, and C. C. Wang, "On the security of a privacy authentication scheme based on cloud for medical environment," in *Prof. 8th iCatse Conference on Information Science and Applications – ICISA 2017, Lecture Notes in Electrical Engineering*, vol. 424, pp. 241-248, 2017.

[16] C. T. Li, D. H. Shih, and C. C. Wang, "Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems," *Computers Methods and Programs in Biomedicine*, vol. 157, pp. 191-203, 2018.

[17] H. X. Shi and R. Guo, "Provably-secure certificateless key encapsulation mechanism for e-healthcare system," *International Journal of Network Security*, vol. 17, no. 5, pp. 548-557, 2015.

[18] A. K. Sutrala, A. K. Das, V. Odelu, M. Wazid, and S. Kumari, "Secure anonymity-preserving password-based user authentication and session key agreement scheme for telecare medicine information systems," *Computer Methods and Programs in Biomedicine*, vol. 135, pp. 167-185, 2016.

Chun-Ta Li received the Ph.D degree in computer science and engineering from National Chung Hsing University, Taiwan, in 2008. He is currently an associate professor with the Department of Information Management at Tainan University of Technology, Taiwan. His research interests include information and network security, wireless sensor networks, mobile computing, and security protocols for RFID, IoTs and cloud computing.

Dong-Her Shih received the Ph.D degree in electrical engineering from the National Cheng Kung University, Tainan, Taiwan, in 1986. He is currently a senior professor in the Department of Information Management, National Yunlin University of Science and Technology, Taiwan. His current research interests include intrusion prevention system (IPS), machine learning, datamining, security, ontology and wireless network.

Chun-Cheng Wang is currently a graduate student with the Department of Information Management at National Yunlin University of Science and Technology, Taiwan. His research interests include network security and security protocols for telemedicine information system.