Sensors and Materials, Vol. 31, No. 3 (2019) 1037–1063
MYU Tokyo

S & M 1833

An Internet-of-Things-based Sensing Rural Medical Care System

Chin-Ling Chen,[1,2,3] Yong-Yuan Deng,[3*] Chin-Feng Lee,[4]
Shunzhi Zhu,[1**] Yi-Jui Chiu,[5] and Chih-Ming Wu[6]

[1]School of Computer and Information Engineering, Xiamen University of Technology,
No. 600 Ligong Road, Jimei District, Xiamen, Fujian Province 361024, China
[2]School of Information Engineering, Changchun Sci-Tech University,
Donghua Street No. 1699, Shuangyang District, Changchun City, Jilin Province 130600, China
[3]Department of Computer Science and Information Engineering, Chaoyang University of Technology,
168, Jifeng E. Rd., Wufeng District, Taichung 41349, Taiwan
[4]Department of Information Management, Chaoyang University of Technology,
168, Jifeng E. Rd., Wufeng District, Taichung 41349, Taiwan
[5]School of Mechanical and Automotive Engineering, Xiamen University of Technology,
No. 600 Ligong Road, Jimei District, Xiamen, Fujian Province 361024, China
[6]School of Civil Engineering and Architecture, Xiamen University of Technology,
No. 600 Ligong Road, Jimei District, Xiamen, Fujian Province 361024, China

(Received November 23, 2018; accepted January 30, 2019)

Keywords: sensing, Internet of Things, rural medical care, nonrepudiation, mutual authentication, privacy, untraceability

According to a recent World Health Organization report, people living in rural areas often lack access to medical resources and need to travel long distances to hospitals for medical treatment — a situation which, until recently, seemed to have no solution. As communication and hardware technologies have rapidly developed in recent years, however, many services and applications integrating these technologies into daily life have come to form an Internet of Things (IoT), and this makes it possible to address the problem of access to medical services in rural areas. In addition, governments formulate policies in order to respond to rural healthcare requirements and can provide patrolling medical vehicle services to take care of residents in these remote areas. On the other hand, owing to the rapid development of human physiological sensing devices, people with chronic diseases or those who require long-term monitoring of physiological conditions can wear these physiological sensing devices, and the sensing data can be provided to rural medical vehicles, so that doctors can diagnose symptoms. People with complicated or severe conditions can go to large hospitals in urban areas for further diagnosis and treatment. However, a great deal of the information transmitted during these processes is sensitive data, which must therefore be protected with security protocols. Therefore, in this study, we propose an IoT-based rural medical monitoring system. The proposed scheme provides mutual authentication and guarantees data integrity, user untraceability, nonrepudiation, and forward and backward secrecy, in addition to being resistant to replay attack.

[*]Corresponding author: e-mail: allen.nubi@gmail.com
[**]Corresponding author: e-mail: szzhu@xmut.edu.cn

https://doi.org/10.18494/SAM.2019.2227

1. Introduction

1.1 Background

Owing to the rapid development of network hardware technology, various services and applications that use wireless connections, such as 4G, 3G, Wi-Fi, Bluetooth, and ZigBee communication technologies, have become popular in daily life. One of the services is remote medical monitoring and care. At the same time, governments have formulated new policies in order to respond to the healthcare requirements of aging populations. Their aim is to build a comprehensive medical network using new wireless technologies, such as sensor networks and cloud computation,(1,2) to drive the medical industry, combined with the Internet of Things (IoT), to the next phase of application.

In current medical fields, information technology is already used for the secure management of drugs via a radio frequency identifier (RFID), patient information, and blood information, as well as the remote medical monitoring of newborns, and many other applications.(3,4) However, as populations continue to age, the need for expanded medical-care-related applications for elderly people has also grown. Examples of technologies in this field include smart wheelchairs, rural medical care, GPS location, and mobile health care, signifying very important development needs.(5,6) On the other hand, the rapid development of various physiological sensing devices has made them smaller in size and greater in energy efficiency, making them suitable for long-term wear by the elderly. These body sensor devices combined with a personal mobile reader compose a body area network (BAN). The personal mobile reader collects and integrates personal physiological data, and then transmits the data to the backend of the network for related diagnostics and application.(7–10)

This means that when people go to a hospital, the medical staff can obtain relevant medical data from their body sensor devices using a hospital medical reader. The body sensor devices will transmit the related sensing data to the personal mobile reader, which will transmit the data to the hospital medical reader.(11–14) The medical staff can then provide these data to a doctor for future reference or immediate medical diagnosis. These data can also be sent to the national medical server to be stored for related statistical big data analysis through cloud technology.(15,16)

In a recent study, Fortino *et al.*(17) proposed body cloud architecture for body sensor networks (BSNs). Their scheme defined a network communication protocol for the communication between the body sensors and the cloud server. Later, Fortino *et al.*(18) proposed another C-SPINE architecture for BSNs. Their scheme defined a network communication protocol for the communication between different body sensors. They also performed hardware implementation for C-SPINE architecture. Gravina *et al.*(19) proposed a survey for existing BSN environments, including body cloud and C-SPINE architecture.

However, many people still seek to violate the privacy of others or even harm others. For example, a malicious attacker could send incorrect sensing data to a hospital medical reader, causing an incorrect diagnosis. This could delay treatment or even result in the death of the patient.(20,21) In addition, attackers may seek to obtain the sensing data of public figures for blackmail or extortion. Therefore, there must be a complete set of encryption and authentication mechanisms that make it impossible for attackers to obtain and modify such sensitive information in order to protect people's safety and privacy.(22,23)

Although the development of medical services is widespread today, some residents in rural areas still find it very difficult to access medical care. According to a recent World Health Organization report, people living in rural areas that lack medical resources need to travel long distances to hospitals for medical treatment.(24) In recent years, the government has provided patrolling medical vehicle services to take care of residents in these remote areas. These patrolling medical vehicles go to remote areas and provide local residents with simple medical services. However, because medical vehicles are an interim type of medical service, there is a lack of long-term physiological data for the diagnosis of some long-term chronic diseases. In addition, medical vehicles may lack some high-level medical equipment. For residents with complicated or severe conditions, it is necessary to go to large hospitals in urban areas for further diagnosis and treatment.

Previously, while researchers proposed schemes based on the IoT environment, these schemes were either not for healthcare environments(2–4) or lacked the comprehensive security required for healthcare environments.(1–3) Junior *et al.*(2) proposed a scheme of session key establishment between an initiator and a responder for the IoT environment, but they did not mention how the initiator and responder would authenticate each other's legality. Ray *et al.*(4) proposed an RFID ownership transfer protocol based on the IoT environment with a comprehensive protocol related to the ownership transfer between two RFID tags; although their protocol achieved mutual authentication between an RFID tag and an RFID reader, the framework differs from the healthcare environment proposed in this study. Moosavi *et al.*(1) proposed a secure scheme for mobility healthcare based on the IoT environment, but actually, they only proposed a challenge-response concept for mobile sensors, smart gateway, and end-user; there is no detailed cryptography description in their article. Yang *et al.*(3) also proposed a framework for healthcare based on the IoT environment, but their protocol only focuses on the server and user; they did not make a comprehensive protocol for a body sensor device, a personal mobile reader, a rural medical vehicle, a hospital medical reader, and a medical cloud server.

Later, Rezaeibagha and Mu(25) proposed a practical and secure telemedicine system for user mobility, which provided a remote diagnosis architecture. However, their scheme is not complete; it lacks architecture to include body sensor devices and does not achieve nonrepudiation. Li *et al.*(26) proposed another cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems, which provided a generalized architecture. However, their scheme is also not complete, as it does not include a remote diagnosis authentication mechanism.

Therefore, in this study, we propose an IoT-based sensing rural medical care system. When a patient goes to a rural medical vehicle to seek medical services, doctors will obtain their physiological sensing data. This can increase the correctness and effectiveness of their diagnoses. After diagnosis, a doctor will inform the patient of the results. For further diagnosis or medical treatment, the patient can go to a large hospital to inform the doctors of the physiological sensing data and the diagnostic report of the rural medical vehicle. This can achieve a higher medical efficiency. The proposed IoT-based sensing rural medical care system achieves security, privacy, and efficiency.

1.2 Security requirements

The security requirements of an IoT-based sensing rural medical care system are listed as follows.(27–29)

1.2.1 Mutual authentication

In the information transmission process, the message receiver must be able to verify the identity legitimacy of the sender. Thus, each party must be able to verify the identity legitimacy of the other party in a BAN authentication environment. If the two parties can confirm each other's identities, then mutual authentication can be achieved.

1.2.2 Data integrity

Any information transferred in an unencrypted network environment is vulnerable to malicious attack in the form of modification, where the message delivered to the receiver is not the original message transmitted by the sender. The integrity of the transmitted data must therefore be ensured and protected against tampering in transit.

1.2.3 User untraceability

Malicious attacks may also attempt to determine a person's physical location by tracing their personal mobile reader. Thus, an IoT-based sensing rural medical care system must prevent such positional tracking.

1.2.4 Resisting replay attacks

Malicious attacks may also intercept the transmitted message between the personal mobile reader and the hospital medical reader, and then impersonate a legitimate transmitter in order to send the same message to the intended receiver. This constitutes a serious breach of personal data security and must be prevented by an IoT-based sensing rural medical care system.

1.2.5 Forward and backward secrecy

If the session key between the personal mobile reader and the hospital medical reader is compromised at any point by an attacker, the attacker may use the session key for future malicious communications or obtaining previous messages. An IoT-based sensing rural medical care system should thus achieve forward and backward secrecy.

1.2.6 Nonrepudiation

When the receiver receives the message sent by the sender, the sender may deny sending the message. Therefore, the message sent by the sender must be signed with the secret key of the sender. The receiver can verify the received message with the public key of the sender and the sender cannot deny sending the message. An IoT-based sensing rural medical care system should thus achieve nonrepudiation.

1.3 Preliminary introduction

Digital network systems are an indispensable technology in daily life, with massive numbers of documents and information being transmitted over networks every day; thus, measures guaranteeing the security of these messages are very important. Several digital encryption systems have therefore been proposed to ensure the security of important documents. In 1985, elliptic curve cryptography(30) was proposed, with a message length smaller than that of the RSA encryption system. The following is a brief introduction of the elliptic curve group and its corresponding mathematical hard problems.

Let F_q be a prime finite field, E/F_q an elliptic curve defined over F_q, and P a generator for a cyclic additive group of composite order q. The point on E/F_q and an extra point Θ, called the point at infinity, form a group $G = \{(x, y) : x, y \in F_q ; (x, y) \in E / F_q\} \bigcup \{\Theta\}$. G is a cyclic additive group of composite order q. Scalar multiplication over E/F_q can be computed as $tP = P + P + ... + P$ t times.

The following problems exist for the elliptic curve group:

Computational Diffie–Hellman (CDH) Problem: Given aP and bP, where $a, b \in R$, Z^*q, and P are the generator of G, compute abP.

Decisional Diffie–Hellman (DDH) Problem: Given aP, bP, and cP, where $a, b, c \in R$, Z^*q, and P are the generators of G, confirm whether or not $cP = abP$, which is equal to confirming whether or not $c = ab \bmod q$.

2. Proposed Scheme

2.1 System architecture

The framework of the rural medical care system proposed in this study is shown in Fig. 1. There are five parties in the scheme:

(1) Body Sensor Device: A small sensing device to measure various physiological data of a human body. Only a legal personal mobile reader can obtain the sensing data from the body sensor device.

(2) Personal Mobile Reader: A personal reading device carried by an individual. It can receive relevant data from a body sensor device and transmit the data to a rural medical vehicle or a hospital medical reader for analysis. It can also keep the inspection report from the rural medical vehicle and transmit the record to a hospital medical reader.

(3) Rural Medical Vehicle: A medical vehicle that visits rural areas. Patients go to the rural medical vehicle and transmit their body sensor device data from the personal mobile reader to the rural medical vehicle. The rural medical vehicle then makes a basic diagnosis of the patient.

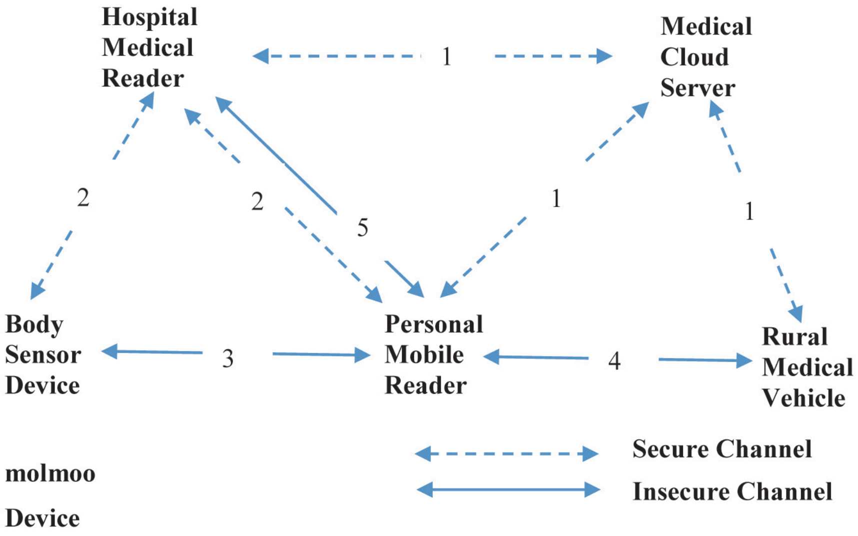

Fig. 1. System framework of the proposed scheme.

(4) Hospital Medical Reader: A device carried by medical staff in a medical facility or by caregivers in a care center. It can receive relevant data from a body sensor device or inspection report of the rural medical vehicle from a personal mobile reader for diagnosis by a medical doctor.

(5) Medical Cloud Server: A cloud server belonging to a national medical institution. It manages all personal mobile readers, rural medical vehicles, and hospital medical readers. All personal mobile readers, rural medical vehicles, and hospital medical readers must be registered on the medical cloud server.

1. All personal mobile readers, rural medical vehicles, and hospital medical readers must be registered with the medical cloud server through a secure channel. The personal mobile readers, rural medical vehicles, and hospital medical readers send their IDs [e.g., universally unique identifier (UUID)] to the medical cloud server. The medical cloud server returns information that includes parameters calculated by elliptic curve group technology.
2. All personal mobile readers and body sensor devices must register with hospital medical readers through a secure channel. The personal mobile reader and body sensor device send their IDs (e.g., UUID) to the hospital medical reader. The hospital medical reader returns information that includes parameters calculated by a lightweight polynomial function.
3. When a personal mobile reader needs to send related health data to a rural medical vehicle or hospital medical reader, it must first obtain the data from body sensor devices. After mutual authentication between the personal mobile reader and the body sensor device, the personal mobile reader receives the encrypted health data.
4. When patients take their personal mobile reader to the rural medical vehicle for health examination, the personal mobile reader and rural medical vehicle must authenticate the legality of each other. After mutual authentication between the personal mobile reader and the rural medical vehicle, the personal mobile reader transmits the body sensor device data

to the rural medical vehicle. After a basic diagnosis, the rural medical vehicle transmits the inspection report to the personal mobile reader.

5. The personal mobile reader sends its ID and parameters calculated by elliptic curve group technology to the hospital medical reader for authentication. After mutual authentication between the personal mobile reader and the hospital medical reader, the personal mobile reader sends the encrypted health sensing data and inspection report to the hospital medical reader. A medical doctor will get these data and report, and will make an advanced diagnosis.

2.2 Notations

q: k-bit prime
F_q: prime finite field
E/F_q: elliptic curve E over F_q
G: cyclic additive group of composite order q
P: generator for the group G
s: secret key of the system
PK: public key of the system, $PK = SP$
$H_i(\ )$: i^{th} one-way hash function
ID_x: x's identity, like a UUID code
r_x, a, b, c, d: random number of elliptic curve group
S_x: x's elliptic curve group signature
SEK_{xy}: session key established by x and y
$E_{\mathrm{x}}(m)$: Use a session key x to encrypt the message m
$D_{\mathrm{x}}(m)$: Use a session key x to decrypt the message m
CHK_x: x's verified message
$A = B$: determines if A is equal to B
data: body sensor's related sensing information
record: inspection report established by a doctor
c_i: session key encrypted sensitive information
$Cert_{doc}$: doctor's certificate, issued by government organizations
Sig: signature message signed by a doctor

2.3 System initialization phase

In the system initialization stage, the medical cloud server calculates some parameters and publishes the public parameters for personal mobile readers, rural medical vehicles, and hospital medical readers.

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

Step 2: The medical cloud server then chooses s as a secret key and computes

$$PK = sP$$

as a public system key.

Step 3: Finally, the medical cloud server chooses the hash function $(H_1(\cdot), H_2(\cdot), H_3(\cdot))$ and then publishes $(F_p, E/F_p, G, P, PK, H_1(\cdot), H_2(\cdot), H_3(\cdot))$ to all personal mobile readers, rural medical vehicles, and hospital medical readers.

2.4 Body sensor device registration phase

The body sensor device must register with the hospital medical reader. The body sensor device registration phase of the proposed scheme is shown in Fig. 2.

Step 1: The body sensor device chooses an identity ID_{BSD} (e.g., UUID) and sends it to the hospital medical reader.

Step 2: The hospital medical reader generates the polynomial $f(x, y)$, calculates

$$BP_{BSD} = f(ID_{BSD}, y),$$

$$e = h(SID),$$

and then sends (BP_{BSD}, SID) to the body sensor device.

Step 3: The body sensor device stores (BP_{BSD}, SID) in its memory.

2.5 Personal mobile reader registration phase

The personal mobile reader must register with the hospital medical reader and medical cloud server. The personal mobile reader registration phase of the proposed scheme is shown in Figs. 3 and 4.

Step 1: The personal mobile reader chooses an identity ID_{PMR} (e.g., UUID) and sends it to the hospital medical reader.

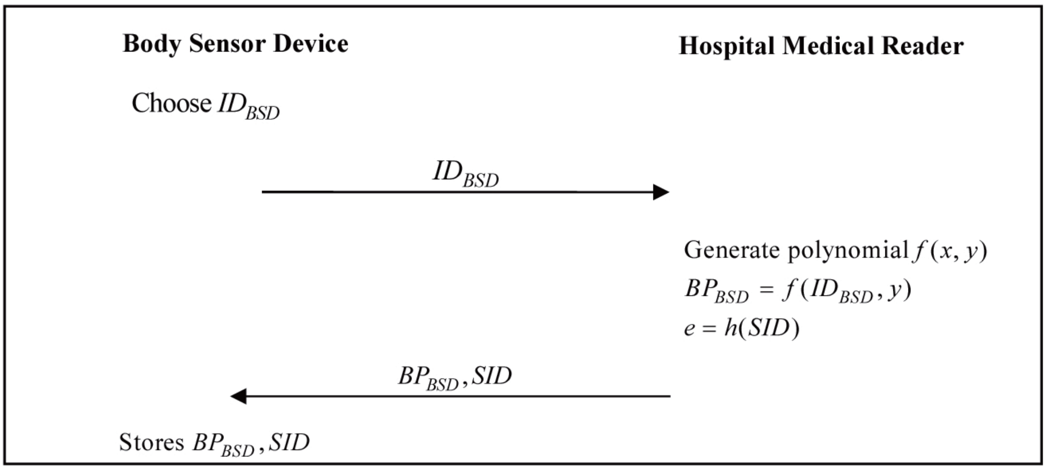

Fig. 2. Body sensor device registration phase of the proposed scheme.

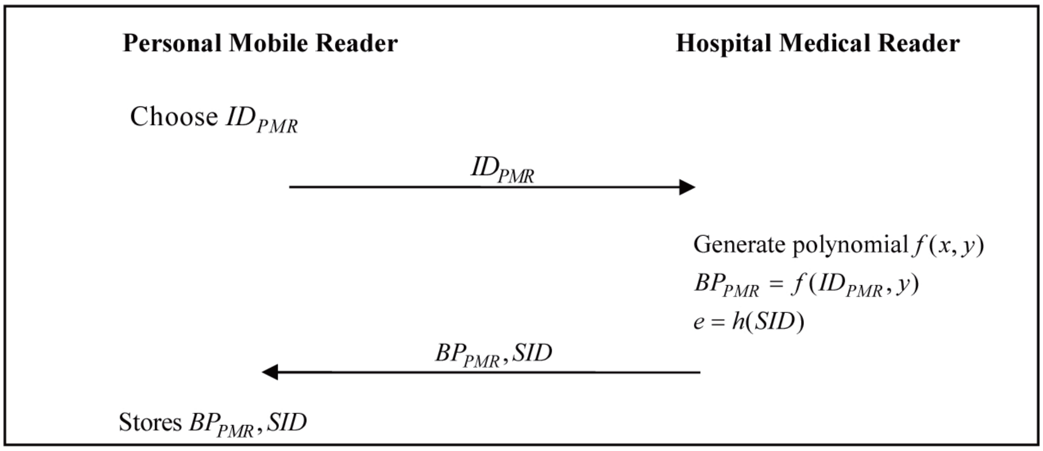
Personal Mobile Reader
Hospital Medical Reader
Choose ID_{PMR}
ID_{PMR}
Generate polynomial $f(x, y)$
$BP_{PMR} = f(ID_{PMR}, y)$
$e = h(SID)$
BP_{PMR}, SID
Stores BP_{PMR}, SID

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

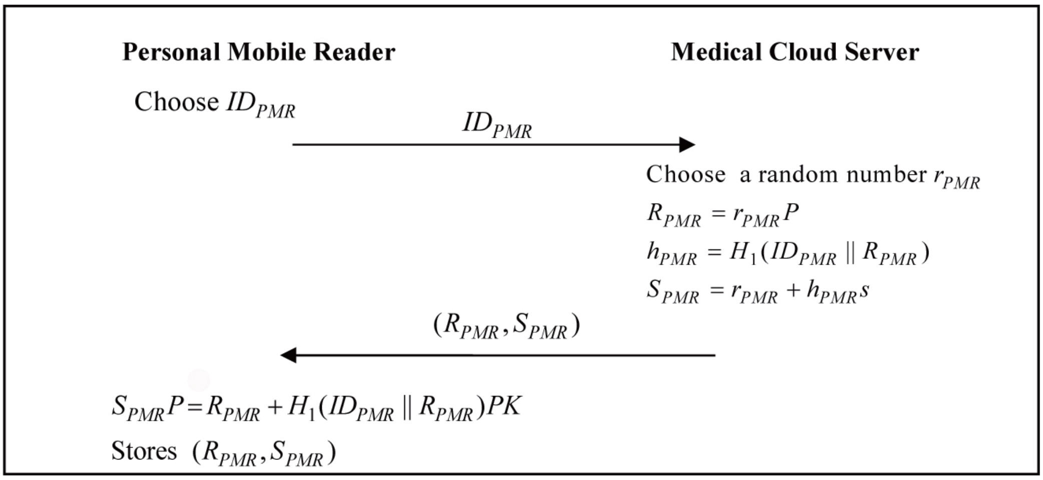
Personal Mobile Reader
Medical Cloud Server
Choose ID_{PMR}
ID_{PMR}
Choose a random number r_{PMR}
$R_{PMR} = r_{PMR}P$
$h_{PMR} = H_1(ID_{PMR} \| R_{PMR})$
$S_{PMR} = r_{PMR} + h_{PMR}s$
(R_{PMR}, S_{PMR})
$S_{PMR}P = R_{PMR} + H_1(ID_{PMR} \| R_{PMR})PK$
Stores (R_{PMR}, S_{PMR})

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

Step 2: The hospital medical reader generates the polynomial $f(x, y)$, calculates

$$BP_{PMR} = f(ID_{PMR}, y),$$

$$e = h(SID),$$

and then sends (BP_{PMR}, SID) to the personal mobile reader.

Step 3: The personal mobile reader stores (BP_{PMR}, SID) to its memory.

Step 4: The personal mobile reader chooses an identity ID_{PMR} (e.g., UUID) and sends it to the medical cloud server.

Step 5: The medical cloud server chooses a random number r_{PMR}, calculates

$$R_{PMR} = r_{PMR}P,$$

$$h_{PMR} = H_1(ID_{PMR}, R_{PMR}),$$

$$S_{PMR} = r_{PMR} + h_{PMR}s,$$

and then sends (R_{PMR}, S_{PMR}) to the personal mobile reader.

Step 6: The personal mobile reader verifies

$$S_{PMR}P = R_{PMR} + H_1(ID_{PMR}, R_{PMR})PK.$$

If it passes the verification, the personal mobile reader stores (R_{PMR}, S_{PMR}).

2.6 Rural medical vehicle registration phase

The rural medical vehicle must register with the medical cloud server. The rural medical vehicle registration phase of the proposed scheme is shown in Fig. 5.

Step 1: The rural medical vehicle chooses an identity ID_{RMV} (e.g., UUID) and sends it to the medical cloud server.

Step 2: The medical cloud server chooses a random number r_{RMV}, calculates

$$R_{RMV} = r_{RMV}P,$$
$$h_{RMV} = H_1(ID_{RMV}, R_{RMV}),$$
$$S_{RMV} = r_{RMV} + h_{RMV}s,$$

and then sends (R_{RMV}, S_{RMV}) to the rural medical vehicle.

Step 3: The rural medical vehicle verifies

$$S_{RMV}P = R_{RMV} + H_1(ID_{RMV}, R_{RMV})PK.$$

If it passes the verification, the rural medical vehicle stores (R_{RMV}, S_{RMV}).

2.7 Hospital medical reader registration phase

The hospital medical device must register with the medical cloud server. The hospital medical device registration phase of the proposed scheme is shown in Fig. 6.

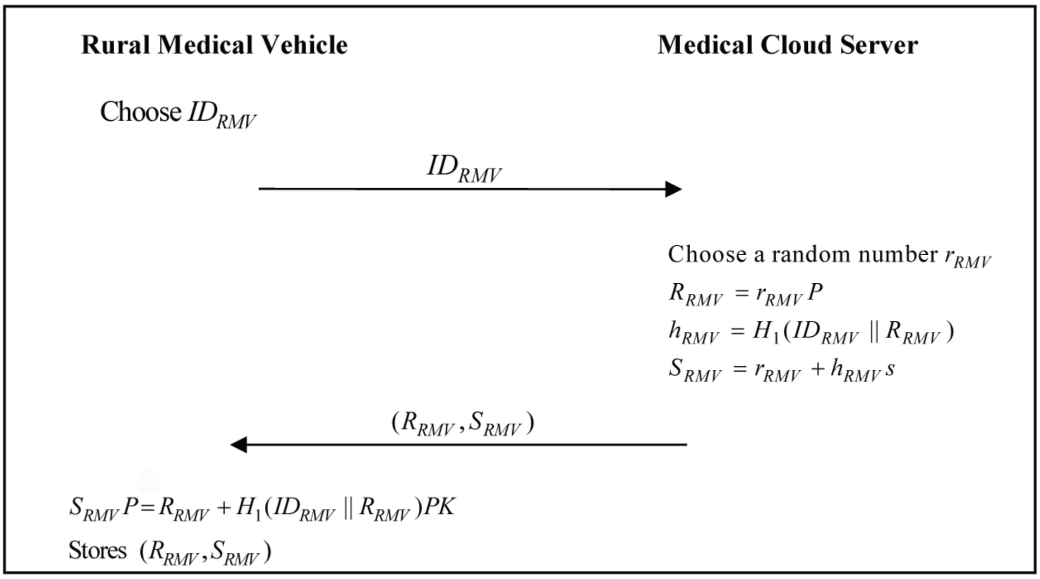
Rural Medical Vehicle
Medical Cloud Server
Choose ID_{RMV}
ID_{RMV}
Choose a random number r_{RMV}
$R_{RMV} = r_{RMV}P$
$h_{RMV} = H_1(ID_{RMV} \| R_{RMV})$
$S_{RMV} = r_{RMV} + h_{RMV}s$
(R_{RMV}, S_{RMV})
$S_{RMV}P = R_{RMV} + H_1(ID_{RMV} \| R_{RMV})PK$
Stores (R_{RMV}, S_{RMV})

Fig. 5. Rural medical vehicle registration phase of the proposed scheme with medical cloud server.

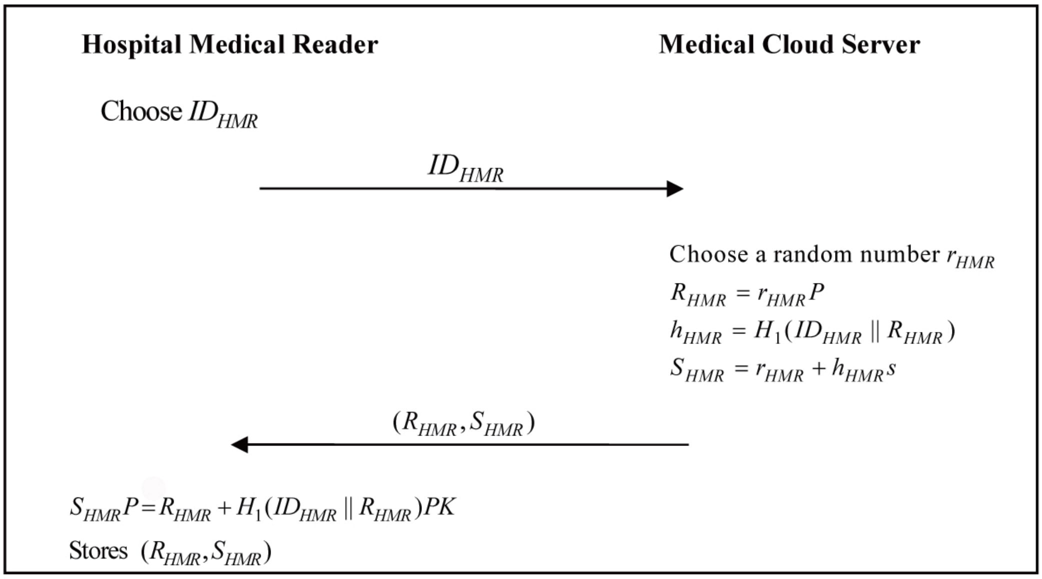
Hospital Medical Reader
Medical Cloud Server
Choose ID_{HMR}
ID_{HMR}
Choose a random number r_{HMR}
$R_{HMR} = r_{HMR}P$
$h_{HMR} = H_1(ID_{HMR} \| R_{HMR})$
$S_{HMR} = r_{HMR} + h_{HMR}s$
(R_{HMR}, S_{HMR})
$S_{HMR}P = R_{HMR} + H_1(ID_{HMR} \| R_{HMR})PK$
Stores (R_{HMR}, S_{HMR})

Fig. 6. Hospital medical reader registration phase of the proposed scheme.

Step 1: The hospital medical reader chooses an identity ID_{PMR} (e.g., UUID) and sends it to the medical cloud server.

Step 2: The medical cloud server chooses a random number r_{PMR}, calculates

$$R_{HMR} = r_{HMR}P,$$

$$h_{HMR} = H_1(ID_{HMR}, R_{HMR}),$$

$$S_{HMR} = r_{HMR} + h_{HMR}s,$$

and then sends (R_{HMR}, S_{HMR}) to the hospital medical reader.

Step 3: The hospital medical reader verifies

$$S_{HMR}P = R_{HMR} + H_1(ID_{HMR}, R_{HMR})PK.$$

If it passes the verification, the rural medical vehicle stores (R_{HMR}, S_{HMR}).

2.8 Personal mobile reader authentication and communication phase

When the personal mobile reader requires related data from the body sensor device, the mobile reader and sensor device must authenticate each other. The personal mobile reader authentication and communication phase of the proposed scheme is shown in Fig. 7.

Step 1: When the personal mobile reader requires related health data from the body sensor device, it calculates

$$e = h(SID)$$

and sends (ID_{PMR}, e) to the body sensor device.

Step 2: The body sensor device verifies

$$e = h(SID)$$

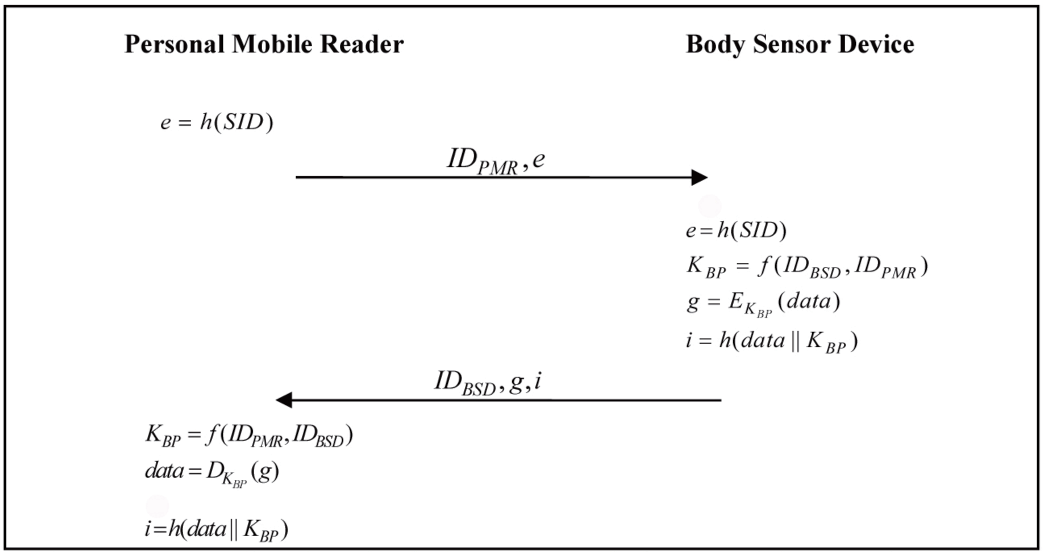

Fig. 7. Personal mobile reader authentication and communication phase of the proposed scheme.

to check the legality of the personal mobile reader. If it passes the verification, the body sensor device calculates

$$K_{BP} = f(ID_{BSD}, ID_{PMR}),$$
$$g = E_{K_{BP}}(data),$$
$$i = h(data \| K_{BP}),$$

and then sends (ID_{BSD}, g, i) to the personal mobile reader.

Step 3: The personal mobile reader calculates

$$K_{BP} = f(ID_{PMR}, ID_{BSD}),$$
$$data = D_{K_{BP}}(g),$$

and verifies

$$i = h(data \| K_{BP})$$

to check the legality of the body sensor device. If it passes the verification, the personal mobile reader receives the related health data from the body sensor device.

2.9 Rural medical vehicle authentication and communication phase

When patients take their personal mobile reader to the rural medical vehicle for medical services, the personal mobile reader and rural medical vehicle must authenticate each other. The personal mobile reader will then transmit the encrypted health sensing data to the rural medical vehicle and the rural medical vehicle will transmit the encrypted basic inspection report to the personal mobile reader. The rural medical vehicle authentication and communication phase of the proposed scheme is shown in Fig. 8.

Step 1: The personal mobile reader chooses a random number a, calculates

$$T_{PMR} = aP,$$

and then sends $(ID_{PMR}, R_{PMR}, T_{PMR})$ to the rural medical vehicle.

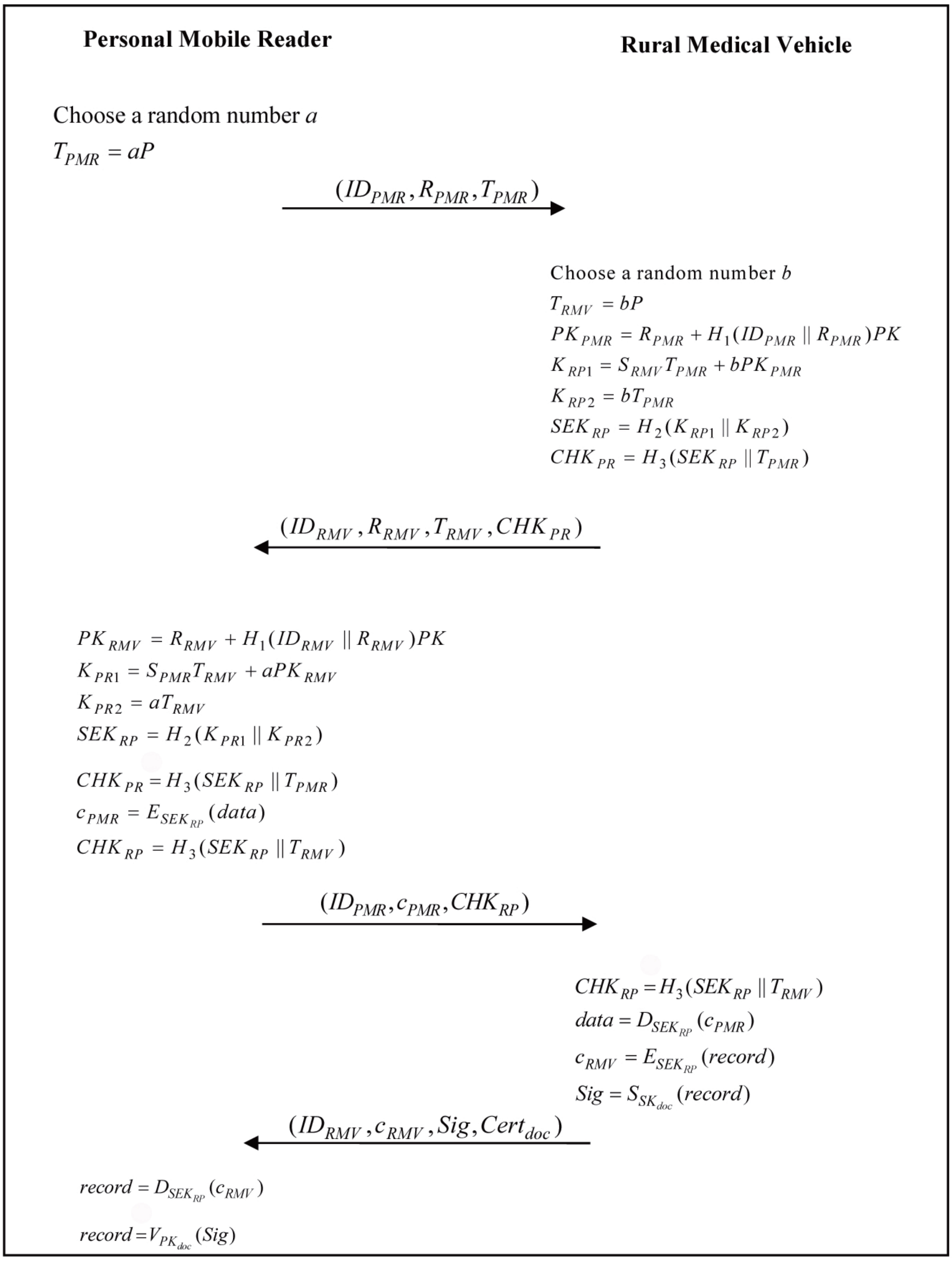
Personal Mobile Reader
Rural Medical Vehicle
Choose a random number a
$T_{PMR} = aP$
$(ID_{PMR}, R_{PMR}, T_{PMR})$
Choose a random number b
$T_{RMV} = bP$
$PK_{PMR} = R_{PMR} + H_1(ID_{PMR} \| R_{PMR})PK$
$K_{RP1} = S_{RMV}T_{PMR} + bPK_{PMR}$
$K_{RP2} = bT_{PMR}$
$SEK_{RP} = H_2(K_{RP1} \| K_{RP2})$
$CHK_{PR} = H_3(SEK_{RP} \| T_{PMR})$
$(ID_{RMV}, R_{RMV}, T_{RMV}, CHK_{PR})$
$PK_{RMV} = R_{RMV} + H_1(ID_{RMV} \| R_{RMV})PK$
$K_{PR1} = S_{PMR}T_{RMV} + aPK_{RMV}$
$K_{PR2} = aT_{RMV}$
$SEK_{RP} = H_2(K_{PR1} \| K_{PR2})$
$CHK_{PR} = H_3(SEK_{RP} \| T_{PMR})$
$c_{PMR} = E_{SEK_{RP}}(data)$
$CHK_{RP} = H_3(SEK_{RP} \| T_{RMV})$
$(ID_{PMR}, c_{PMR}, CHK_{RP})$
$CHK_{RP} = H_3(SEK_{RP} \| T_{RMV})$
$data = D_{SEK_{RP}}(c_{PMR})$
$c_{RMV} = E_{SEK_{RP}}(record)$
$Sig = S_{SK_{doc}}(record)$
$(ID_{RMV}, c_{RMV}, Sig, Cert_{doc})$
$record = D_{SEK_{RP}}(c_{RMV})$
$record = V_{PK_{doc}}(Sig)$

Fig. 8. Rural medical vehicle authentication and communication phase of the proposed scheme.

Step 2: The rural medical vehicle chooses a random number b, calculates

$$T_{RMV} = bP,$$

$$PK_{PMR} = R_{PMR} + H_1(ID_{PMR}, R_{PMR})PK,$$

$$K_{RP1} = S_{RMV}T_{PMR} + bPK_{PMR},$$

$$K_{RP2} = bT_{PMR} ,$$

and the session key

$$SEK_{RP} = H_2(K_{RP1}, K_{RP2}) .$$

The rural medical vehicle then calculates

$$CHK_{PR} = H_3(SEK_{RP}, T_{PMR})$$

and sends $(ID_{RMV}, R_{RMV}, T_{RMV}, CHK_{PR})$ to the personal mobile reader.

Step 3: The personal mobile reader calculates

$$PK_{RMV} = R_{RMV} + H_1(ID_{RMV}, R_{RMV})PK,$$

$$K_{PR1} = S_{PMR}T_{RMV} + aPK_{RMV},$$

$$K_{PR2} = aT_{RMV},$$

and the session key

$$SEK_{RP} = H_2(K_{PR1}, K_{PR2}).$$

The personal mobile reader verifies

$$CHK_{PR} = H_3(SEK_{RP}, T_{PMR})$$

to check the legality of the rural medical vehicle. If it passes the verification, the personal mobile reader calculates

$$c_{PMR} = E_{SEK_{RP}}(data),$$

$$CHK_{RP} = H_3(SEK_{RP}, T_{RMV}),$$

and sends $(ID_{PMR}, c_{PMR}, CHK_{RP})$ to the rural medical vehicle.

Step 4: The rural medical vehicle verifies

$$CHK_{RP} = H_3(SEK_{RP}, T_{RMV})$$

to check the legality of the personal mobile reader. If it passes the verification, the session key SEK_{RP} between the personal mobile reader and the rural medical vehicle is established successfully. The rural medical vehicle calculates

$$data = D_{SEK_{RP}}(c_{PMR})$$

to obtain the health sensing information of the patient. After the patient's diagnosis, the rural medical vehicle generates the encrypted basic inspection report

$$c_{RMV} = E_{SEK_{RP}}(record),$$

$$Sig = S_{SK_{doc}}(record),$$

and sends $(ID_{RMV}, c_{RMV}, Sig, Cert_{doc})$ to the personal mobile reader.

Step 5: The personal mobile reader decrypts the received message

$$record = D_{SEK_{RP}}(c_{RMV}),$$

obtains the doctor's public key PK_{dx} through $Cert_{doc}$, verifies the signature

$$record = V_{PK_{doc}}(Sig),$$

and obtains the encrypted basic inspection report from the rural medical vehicle.

2.10 Hospital medical reader authentication and communication phase

After the patients receive the basic inspection report from the rural medical vehicle, they may go to the hospital for an advanced diagnosis. When the patients take their personal mobile reader to the hospital for medical services, the personal mobile and hospital medical readers must authenticate each other. The personal mobile reader then transmits the encrypted health sensing data and basic inspection report to the hospital medical reader, and the medical doctor at the hospital makes an advanced diagnosis. The hospital medical reader authentication and communication phase of the proposed scheme is shown in Fig. 9.

Step 1: The personal mobile reader chooses a random number *c*, calculates

$$T_{PMR2} = cP,$$

and then sends $(ID_{PMR}, R_{PMR}, T_{PMR2})$ to the hospital medical reader.

Step 2: The hospital medical reader chooses a random number *d*, calculates

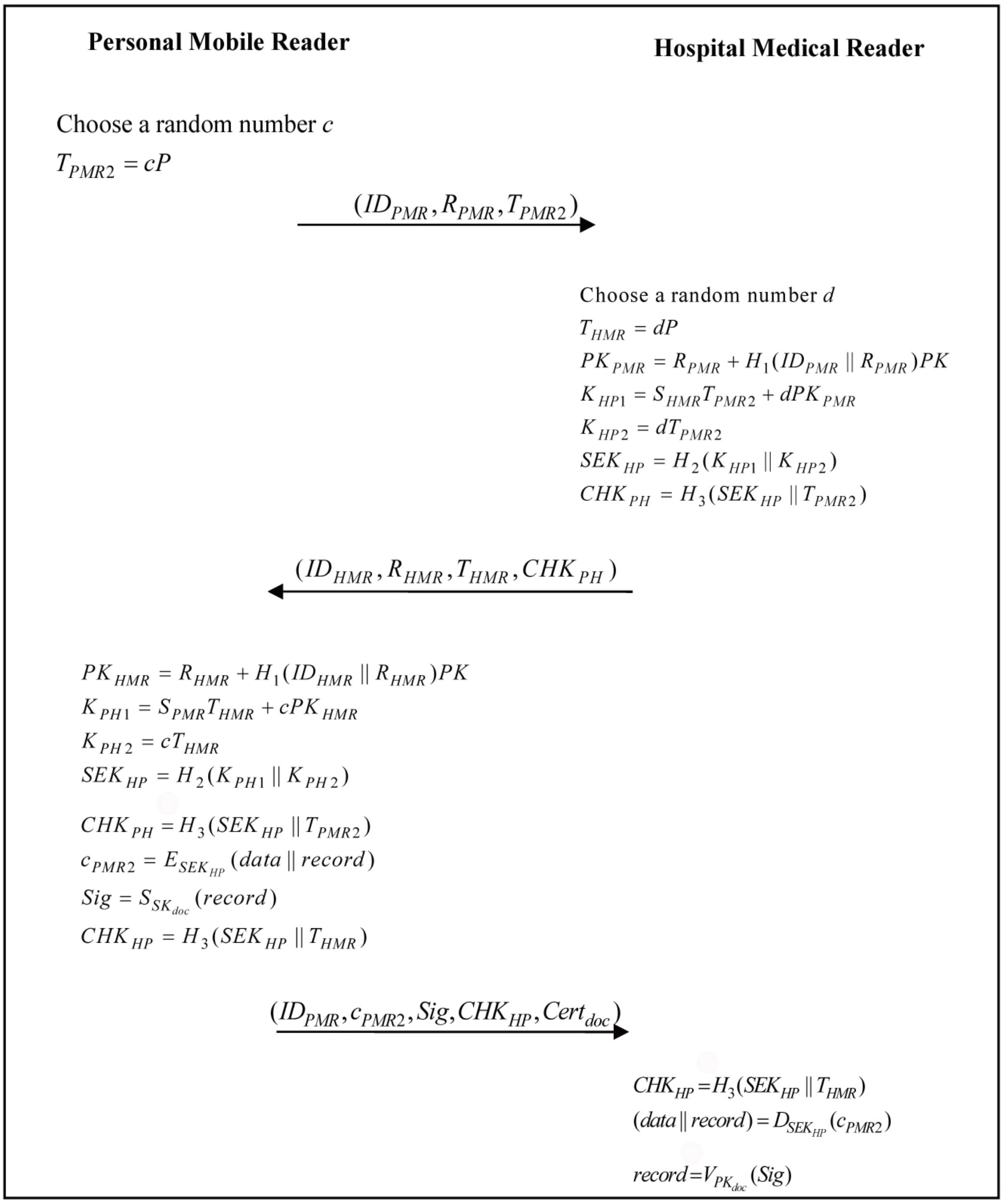
Personal Mobile Reader
Hospital Medical Reader
Choose a random number c
$T_{PMR2} = cP$
$(ID_{PMR}, R_{PMR}, T_{PMR2})$
Choose a random number d
$T_{HMR} = dP$
$PK_{PMR} = R_{PMR} + H_1(ID_{PMR} \| R_{PMR})PK$
$K_{HP1} = S_{HMR}T_{PMR2} + dPK_{PMR}$
$K_{HP2} = dT_{PMR2}$
$SEK_{HP} = H_2(K_{HP1} \| K_{HP2})$
$CHK_{PH} = H_3(SEK_{HP} \| T_{PMR2})$
$(ID_{HMR}, R_{HMR}, T_{HMR}, CHK_{PH})$
$PK_{HMR} = R_{HMR} + H_1(ID_{HMR} \| R_{HMR})PK$
$K_{PH1} = S_{PMR}T_{HMR} + cPK_{HMR}$
$K_{PH2} = cT_{HMR}$
$SEK_{HP} = H_2(K_{PH1} \| K_{PH2})$
$CHK_{PH} = H_3(SEK_{HP} \| T_{PMR2})$
$c_{PMR2} = E_{SEK_{HP}}(data \| record)$
$Sig = S_{SK_{doc}}(record)$
$CHK_{HP} = H_3(SEK_{HP} \| T_{HMR})$
$(ID_{PMR}, c_{PMR2}, Sig, CHK_{HP}, Cert_{doc})$
$CHK_{HP} = H_3(SEK_{HP} \| T_{HMR})$
$(data \| record) = D_{SEK_{HP}}(c_{PMR2})$
$record = V_{PK_{doc}}(Sig)$

Fig. 9. Hospital medical reader authentication and communication phase of the proposed scheme.

$$T_{HMR} = dP,$$
$$PK_{PMR} = R_{PMR} + H_1(ID_{PMR}, R_{PMR})PK,$$
$$K_{HP1} = S_{HMR}T_{PMR2} + dPK_{PMR},$$
$$K_{HP2} = dT_{PMR2},$$

and the session key

$$SEK_{HP} = H_2(K_{HP1}, K_{HP2}).$$

The hospital medical reader then calculates

$$CHK_{PH} = H_3(SEK_{HP}, T_{PMR2})$$

and sends $(ID_{HMR}, R_{HMR}, T_{HMR}, CHK_{PH})$ to the personal mobile reader.

Step 3: The personal mobile reader calculates

$$PK_{HMR} = R_{HMR} + H_1(ID_{HMR}, R_{HMR})PK,$$
$$K_{PH1} = S_{PMR}T_{HMR} + cPK_{HMR},$$
$$K_{PH2} = cT_{HMR},$$

and the session key

$$SEK_{HP} = H_2(K_{PH1}, K_{PH2}).$$

The personal mobile reader verifies

$$CHK_{PH} = H_3(SEK_{HP}, T_{PMR2})$$

to check the legality of the hospital medical reader. If it passes the verification, the personal mobile reader calculates

$$c_{PMR2} = E_{SEK_{HP}}(data \,\|\, record),$$
$$Sig = S_{SK_{doc}}(record),$$
$$CHK_{HP} = H_3(SEK_{HP}, T_{HMR}),$$

and sends $(ID_{PMR}, c_{PMR2}, Sig, CHK_{HP}, Cert_{doc})$ to the hospital medical reader.

Step 5: The hospital medical reader verifies

$$CHK_{HP} = H_3(SEK_{HP}, T_{HMR})$$

to check the legality of the personal mobile reader. If it passes the verification, the session key SEK_{HP} between the personal mobile reader and the hospital medical reader is established successfully. The hospital medical reader decrypts the received message

$$(data \,\|\, record) = D_{SEK_{HP}}(c_{PMR2}),$$

obtains the doctor's public key through $Cert_{doc}$, verifies the signature

$$record = V_{PK_{doc}}(Sig),$$

and obtains the encrypted health sensing information and basic inspection report from the personal mobile reader. The medical doctor at the hospital then makes an advanced diagnosis for the patient.

3. Security Analysis

3.1 Mutual authentication

In this study, we use BAN logic to prove that the proposed scheme achieves mutual authentication between different parties in each phase.

In the rural medical vehicle authentication and communication phase of the proposed scheme, the main goal of the scheme is to authenticate the session key establishment between the personal mobile reader *P* and the rural medical vehicle *R*.

G1: $P \mid\equiv P \overset{SEK_{RP}}{\leftrightarrow} R$

G2: $P \mid\equiv R \mid\equiv P \overset{SEK_{RP}}{\leftrightarrow} R$

G3: $R \mid\equiv P \overset{SEK_{RP}}{\leftrightarrow} R$

G4: $R \mid\equiv P \mid\equiv P \overset{SEK_{RP}}{\leftrightarrow} R$

G5: $P \mid\equiv ID_{RMV}$
G6: $P \mid\equiv R \mid\equiv ID_{RMV}$
G7: $R \mid\equiv ID_{PMR}$
G8: $R \mid\equiv P \mid\equiv ID_{PMR}$

According to the rural medical vehicle authentication and communication phase, BAN logic is used to produce an idealized form as follows:
M1: $(< ID_{PMR}, R_{PMR}, T_{PMR} >_{PK_{RMV}}, < H(SEK_{RP}, T_{RMV}) >_{CHK_{RP}})$,
M2: $(< ID_{RMV}, R_{RMV}, T_{RMV} >_{PK_{PMR}}, < H(SEK_{RP}, T_{PMR}) >_{CHK_{PR}})$.
To analyze the proposed scheme, the following assumptions are made:
A1: $P \mid\equiv \#(T_{PMR})$,
A2: $R \mid\equiv \#(T_{PMR})$,
A3: $P \mid\equiv \#(T_{RMV})$,
A4: $R \mid\equiv \#(T_{RMV})$,
A5: $P \mid\equiv R \mid\Rightarrow P \overset{SEK_{RP}}{\leftrightarrow} R$,

A6: $R \mid\equiv P \mid\Rightarrow P \overset{SEK_{RP}}{\leftrightarrow} R$,

A7: $P \mid\equiv R \mid\Rightarrow ID_{RMV}$,
A8: $R \mid\equiv P \mid\Rightarrow ID_{PMR}$.

According to these assumptions and rules of BAN logic, the main proof of the rural medical vehicle authentication and communication phase is as follows:

a. The rural medical vehicle *R* authenticates the personal mobile reader *P*.

By M1 and the seeing rule, derive

$$R \lhd (< ID_{PMR}, R_{PMR}, T_{PMR} >_{PK_{RMV}}, < H(SEK_{RP}, T_{RMV}) >_{CHK_{RP}}). \quad \text{(Statement 1)}$$

By A2 and the freshness rule, derive

$$R \mid\equiv \#(< ID_{PMR}, R_{PMR}, T_{PMR} >_{PK_{RMV}}, < H(SEK_{RP}, T_{RMV}) >_{CHK_{RP}}). \quad \text{(Statement 2)}$$

By Statement 1, A4, and the message meaning rule, derive

$$R \mid\equiv P \mid\sim (< ID_{PMR}, R_{PMR}, T_{PMR} >_{PK_{RMV}}, < H(SEK_{RP}, T_{RMV}) >_{CHK_{RP}}).\text{(Statement 3)}$$

By Statements 2 and 3, and the nonce verification rule, derive

$$R \mid\equiv P \mid\equiv (< ID_{PMR}, R_{PMR}, T_{PMR} >_{PK_{RMV}}, < H(SEK_{RP}, T_{RMV}) >_{CHK_{RP}}).\text{(Statement 4)}$$

By Statement 4 and the belief rule, derive

$$R \mid\equiv P \mid\equiv P \overset{SEK_{RP}}{\leftrightarrow} R\,. \qquad \text{(Statement 5)}$$

By Statement 5, A6, and the jurisdiction rule, derive

$$R \mid\equiv P \overset{SEK_{RP}}{\leftrightarrow} R\,. \qquad \text{(Statement 6)}$$

By Statement 6 and the belief rule, derive

$$R \mid\equiv P \mid\equiv ID_{PMR}\,. \qquad \text{(Statement 7)}$$

By Statement 7, A8, and the jurisdiction rule, derive

$$R \mid\equiv ID_{PMR}\,. \qquad \text{(Statement 8)}$$

b. The personal mobile reader *P* authenticates the rural medical vehicle *R*.

By M2 and the seeing rule, derive

$$P \triangleleft (< ID_{RMV}, R_{RMV}, T_{RMV} >_{PK_{PMR}}, < H(SEK_{RP}, T_{PMR}) >_{CHK_{PR}})\,. \qquad \text{(Statement 9)}$$

By A1 and the freshness rule, derive

$$P \mid\equiv \#(< ID_{RMV}, R_{RMV}, T_{RMV} >_{PK_{PMR}}, < H(SEK_{RP}, T_{PMR}) >_{CHK_{PR}})\,. \qquad \text{(Statement 10)}$$

By Statement 9, A3, and the message meaning rule, derive

$$P \mid\equiv R \mid\sim (< ID_{RMV}, R_{RMV}, T_{RMV} >_{PK_{PMR}}, < H(SEK_{RP}, T_{PMR}) >_{CHK_{PR}})\,. \qquad \text{(Statement 11)}$$

By Statements 10 and 11, and the nonce verification rule, derive

$$P \mid\equiv R \mid\equiv (< ID_{RMV}, R_{RMV}, T_{RMV} >_{PK_{PMR}}, < H(SEK_{RP}, T_{PMR}) >_{CHK_{PR}})\,. \qquad \text{(Statement 12)}$$

By Statement 12 and the belief rule, derive

$$P \mid\equiv R \mid\equiv P \overset{SEK_{RP}}{\leftrightarrow} R\,. \qquad \text{(Statement 13)}$$

By Statement 13, A5, and the jurisdiction rule, derive

$$P \mid\equiv P \overset{SEK_{RP}}{\leftrightarrow} R\,. \qquad \text{(Statement 14)}$$

By Statement 14 and the belief rule, derive

$$P \mid\equiv R \mid\equiv ID_{RMV}\,. \qquad \text{(Statement 15)}$$

By Statement 15, A7, and the jurisdiction rule, derive

$$P \mid\equiv ID_{RMV}\,. \qquad \text{(Statement 16)}$$

By Statements 6, 8, 14, and 16, it can be proved that, in the proposed scheme, the personal mobile reader *P* and rural medical vehicle *R* authenticate each other. Moreover, it can also be proved that the proposed scheme can establish a session key between the personal mobile reader *P* and the rural medical vehicle *R*.

In the proposed scheme, the rural medical vehicle authenticates the personal mobile reader by

$$CHK_{RP} = H_3(SEK_{RP}, T_{RMV})\,.$$

If it passes the verification, the rural medical vehicle authenticates the legality of the personal mobile reader. The personal mobile reader authenticates the rural medical vehicle by

$$CHK_{PR} = H_3(SEK_{RP}, T_{PMR}).$$

If it passes the verification, the personal mobile reader authenticates the legality of the rural medical vehicle. The rural medical vehicle authentication and communication phase of the proposed scheme thus guarantees mutual authentication between the rural medical vehicle and the personal mobile reader.

In the hospital medical reader authentication and communication phase of the proposed scheme, the main goal of the scheme is to authenticate the session key establishment between the personal mobile reader *P* and the hospital medical reader *H*.

G9: $P \mid\equiv P \overset{SEK_{HP}}{\leftrightarrow} H$

G10: $P \mid\equiv H \mid\equiv P \overset{SEK_{HP}}{\leftrightarrow} H$

G11: $H \mid\equiv P \overset{SEK_{HP}}{\leftrightarrow} H$

G12: $H \mid\equiv P \mid\equiv P \overset{SEK_{HP}}{\leftrightarrow} H$

G13: $P \mid\equiv ID_{HMR}$
G14: $P \mid\equiv H \mid\equiv ID_{HMR}$
G15: $H \mid\equiv ID_{PMR}$
G16: $H \mid\equiv P \mid\equiv ID_{PMR}$

According to the hospital medical reader authentication and communication phase, BAN logic is used to produce an idealized form as follows:

M3: $(< ID_{PMR}, R_{PMR}, T_{PMR2} >_{PK_{HMR}}, < H(SEK_{HP}, T_{HMR}) >_{CHK_{HP}})$,

M4: $(< ID_{HMR}, R_{HMR}, T_{HMR} >_{PK_{HMR}}, < H(SEK_{HP}, T_{PMR2}) >_{CHK_{PH}})$.

To analyze the proposed scheme, the following assumptions are made:

A9: $P \mid\equiv \#(T_{PMR2})$,

A10: $H \mid\equiv \#(T_{PMR2})$,

A11: $P \mid\equiv \#(T_{HMR})$,

A12: $H \mid\equiv \#(T_{HMR})$,

A13: $P \mid\equiv H \mid\Rightarrow P \overset{SEK_{HP}}{\leftrightarrow} H$,

A14: $H \mid\equiv P \mid\Rightarrow P \overset{SEK_{HP}}{\leftrightarrow} H$,

A15: $P \mid\equiv H \mid\Rightarrow ID_{HMR}$,

A16: $H \mid\equiv P \mid\Rightarrow ID_{PMR}$.

According to these assumptions and the rules of BAN logic, the hospital medical reader authentication and communication phase is as follows:

a. The hospital medical reader *H* authenticates the personal mobile reader *P*.

By M3 and the seeing rule, derive

$$H \lhd (< ID_{PMR}, R_{PMR}, T_{PMR2} >_{PK_{HMR}}, < H(SEK_{HP}, T_{HMR}) >_{CHK_{HP}}). \text{ (Statement 17)}$$

By A10 and the freshness rule, derive

$$H |\equiv \#(<ID_{PMR}, R_{PMR}, T_{PMR2}>_{PK_{HMR}}, <H(SEK_{HP}, T_{HMR})>_{CHK_{HP}}) . \qquad \text{(Statement 18)}$$

By Statement 17, A12, and the message meaning rule, derive

$$H |\equiv P |\sim (<ID_{PMR}, R_{PMR}, T_{PMR2}>_{PK_{HMR}}, <H(SEK_{HP}, T_{HMR})>_{CHK_{HP}}) . \qquad \text{(Statement 19)}$$

By Statements 18, 19, and the nonce verification rule, derive

$$H |\equiv P |\equiv (<ID_{PMR}, R_{PMR}, T_{PMR2}>_{PK_{HMR}}, <H(SEK_{HP}, T_{HMR})>_{CHK_{HP}}) . \text{(Statement 20)}$$

By Statement 20 and the belief rule, derive

$$H |\equiv P |\equiv P \overset{SEK_{HP}}{\leftrightarrow} H . \qquad \text{(Statement 21)}$$

By Statement 21, A14, and the jurisdiction rule, derive

$$H |\equiv P \overset{SEK_{HP}}{\leftrightarrow} H . \qquad \text{(Statement 22)}$$

By Statement 22 and the belief rule, derive

$$H |\equiv P |\equiv ID_{PMR} . \qquad \text{(Statement 23)}$$

By Statement 23, A16, and the jurisdiction rule, derive

$$H |\equiv ID_{PMR} . \qquad \text{(Statement 24)}$$

b. The personal mobile reader *P* authenticates the hospital medical reader H.

By M4 and the seeing rule, derive

$$P \triangleleft (<ID_{HMR}, R_{HMR}, T_{HMR}>_{PK_{HMR}}, <H(SEK_{HP}, T_{PMR2})>_{CHK_{PH}}) . \text{(Statement 25)}$$

By A9 and the freshness rule, derive

$$P |\equiv \#(<ID_{HMR}, R_{HMR}, T_{HMR}>_{PK_{HMR}}, <H(SEK_{HP}, T_{PMR2})>_{CHK_{PH}}) . \qquad \text{(Statement 26)}$$

By Statement 25, A11, and the message meaning rule, derive

$$P |\equiv H |\sim (<ID_{HMR}, R_{HMR}, T_{HMR}>_{PK_{HMR}}, <H(SEK_{HP}, T_{PMR2})>_{CHK_{PH}}) . \text{(Statement 27)}$$

By Statements 26 and 27, and the nonce verification rule, derive

$$P |\equiv H |\equiv (<ID_{HMR}, R_{HMR}, T_{HMR}>_{PK_{HMR}}, <H(SEK_{HP}, T_{PMR2})>_{CHK_{PH}}) . \text{(Statement 28)}$$

By Statement 28 and the belief rule, derive

$$P |\equiv H |\equiv P \overset{SEK_{HP}}{\leftrightarrow} H . \qquad \text{(Statement 29)}$$

By Statement 29, A13, and the jurisdiction rule, derive

$$P |\equiv P \overset{SEK_{HP}}{\leftrightarrow} H . \qquad \text{(Statement 30)}$$

By Statement 30 and the belief rule, derive

$$P |\equiv H |\equiv ID_{HMR} . \qquad \text{(Statement 31)}$$

By Statement 31, A15, and the jurisdiction rule, derive

$$P |\equiv ID_{HMR} . \qquad \text{(Statement 32)}$$

By Statements 22, 24, 30, and 32, it can be proved that, in the proposed scheme, the personal mobile reader *P* and the hospital medical reader *H* authenticate each other. Moreover, it can also be proved that the proposed scheme can establish a session key between the personal mobile reader *P* and the hospital medical reader *H*.

In the proposed scheme, the hospital medical reader authenticates the personal mobile reader by

$$CHK_{HP} = H_3(SEK_{HP}, T_{HMR}).$$

If it passes the verification, the hospital medical reader authenticates the legality of the personal mobile reader. The personal mobile reader authenticates the hospital medical reader by

$$CHK_{PH} = H_3(SEK_{HP}, T_{PMR2}).$$

If it passes the verification, the personal mobile reader authenticates the legality of the hospital medical reader. The hospital medical reader authentication and communication phase of the proposed scheme thus guarantees mutual authentication between the hospital medical reader and the personal mobile reader.

Scenario: A malicious attacker uses an illegal hospital medical reader to obtain a patient's health data from a legal personal mobile reader.
Analysis: The attacker will not succeed because the illegal hospital medical reader has not been registered to the medical cloud server and thus cannot calculate the correct session key SEK_{HP}. Thus, the attack will fail when the legal personal mobile reader attempts to authenticate the illegal hospital medical reader. In the proposed scheme, the attacker cannot achieve their purpose using an illegal hospital medical reader. In the same scenario, the proposed scheme can also defend against a malicious attack using an illegal personal mobile reader to send fake health data to a legal hospital medical reader, because the illegal personal mobile reader has not been registered to the medical cloud server and thus cannot calculate the correct session key SEK_{HP}. Thus, the attack will fail when the legal hospital medical reader attempts to authenticate the illegal personal mobile reader.

3.2 Data integrity

To ensure the integrity of the transaction data, in this study, we use elliptic curve cryptography to calculate the session keys SEK_{RP} and SEK_{HP}, and also to protect the data integrity. The malicious attacker cannot use the signatures (K_{RP1}, K_{RP2}), (K_{PR1}, K_{PR2}), (K_{HP1}, K_{HP2}), and (K_{PH1}, K_{PH2}) to calculate the correct session keys SEK_{RP} and SEK_{HP}.

Only a legal personal mobile reader or rural medical vehicle can calculate the correct session key SEK_{RP}. The legal rural medical vehicle calculates the session key

$$SEK_{RP} = H_2(K_{RP1}, K_{RP2})$$

and the legal personal mobile reader calculates the session key

$$SEK_{RP} = H_2(K_{PR1}, K_{PR2}).$$

$$\begin{aligned} K_{PR1} &= S_{PMR}T_{RMV} + aPK_{RMV} \\ &= S_{PMR}bP + aS_{RMV}P \\ &= bS_{PMR}P + S_{RMV}aP \\ &= bPK_{PMR} + S_{RMV}T_{PMR} = K_{RP1} \\ K_{PR2} &= aT_{RMV} = abP = baP = bT_{PMR} = K_{RP2} \end{aligned}$$

Only a legal personal mobile or hospital medical reader can calculate the correct session key SEK_{HP}. The legal hospital medical reader calculates the session key

$$SEK_{HP} = H_2(K_{HP1}, K_{HP2})$$

and the legal personal mobile reader calculates the session key

$$SEK_{HP} = H_2(K_{PH1}, K_{PH2})\ .$$

$$\begin{aligned} K_{PH1} &= S_{PMR}T_{HMR} + cPK_{HMR} \\ &= S_{PMR}dP + cS_{HMR}P \\ &= dS_{PMR}P + S_{HMR}cP \\ &= dPK_{PMR} + S_{HMR}T_{PMR2} = K_{HP1} \\ K_{PH2} &= cT_{HMR} = cdP = dcP = dT_{PMR2} = K_{HP2} \end{aligned}$$

Only the correct session key will allow successful communication. Thus, attackers cannot modify the transmitted message. Therefore, the proposed scheme achieves data integrity.

Scenario: A malicious attacker intercepts the transmitted message from the hospital medical reader to the personal mobile reader and sends a modified message to the personal mobile reader.

Analysis: The attacker will not succeed because the legal personal mobile reader will use

$$CHK_{PH} = H_3(SEK_{HP} \,\|\, T_{PMR2})$$

to check the data integrity. The attacker cannot calculate the correct session key SEK_{HP}. Thus, the attack will fail when the legal personal mobile reader authenticates the received message. In the proposed scheme, the attacker cannot achieve his/her purpose by sending a modified message to the personal mobile reader. For the same reason, the attack will fail when the legal hospital medical reader uses

$$CHK_{HP} = H_3(SEK_{HP} \,\|\, T_{HMR})$$

to check data integrity. Therefore, attackers cannot achieve their purpose by sending a modified message to the hospital medical reader.

3.3 User untraceability

Another form of privacy attack involves attempting to obtain a person's physical location by tracing any personal device (in this case, the personal mobile reader). If the personal mobile reader sends the same message continuously, an attacker can trace its location. In the proposed architecture, the session keys SEK_{RP} and SEK_{HP} are changed for every communication round in order to avoid location tracing. Thus, location privacy is protected and user untraceability is achieved.

3.4 Resisting replay attack

An attacker may also intercept the message transmitted between the sender and the receiver. They impersonate a legal sender and then send the same message again to the intended receiver. However, this attack will fail in the proposed scheme, as all messages between the sender and the receiver are protected with the session keys SEK_{RP} and SEK_{HP}, and the attacker cannot calculate the correct session key. Because the transmitted messages are changed every round, the same message cannot be sent twice. Thus, the replay attack cannot succeed.

3.5 Forward and backward secrecy

Even if the session keys SEK_{RP} and SEK_{HP} between the sender and the receiver are compromised at any point by an attacker, the system still satisfies forward and backward secrecy. The attacker may use the session keys SEK_{RP} and SEK_{HP} for future communication or to obtain previous messages. However, in the proposed scheme, the session keys SEK_{RP} and SEK_{HP} are randomly chosen by the sender and receiver, and may only be used in the current round. The attacker cannot use the same session keys SEK_{RP} and SEK_{HP} for future communication or to obtain previous messages. Thus, the proposed scheme achieves forward and backward secrecy.

3.6 Nonrepudiation

In the proposed scheme, a digital signature is used to achieve nonrepudiation for the inspection report compiled by a doctor. In the rural medical vehicle authentication and communication phase, the doctor uses his/her private key to sign the patient's inspection report $Sig = S_{SK_{doc}}(record)$ and then the signed message is transmitted to the patient. The patient obtains the doctor's public key through the doctor's certificate $Cert_{doc}$ and then uses the doctor's public key to verify the signed message $record = V_{PK_{doc}}(Sig)$. In the hospital medical reader authentication and communication phase, the patient sends the original signed message and doctor's certificate $Cert_{doc}$ to the hospital medical reader. Another doctor obtains the original doctor's public key through the doctor's certificate $Cert_{doc}$ and then uses the doctor's public key to verify the received message $record = V_{PK_{doc}}(Sig)$. Thus, the proposed scheme achieves nonrepudiation for the inspection report established by a doctor.

3.7 Computation cost

From Table 1, the proposed scheme's computation costs for the medical cloud server, hospital medical reader, rural medical vehicle, personal mobile reader, and body sensor device in each phase are analyzed. For the highest computation cost in the rural medical vehicle authentication and communication phase, a rural medical vehicle needs five multiplication operations, four hash function operations, one comparison operation, two symmetric encryption operations, and one signature operation. A personal mobile reader needs five multiplication operations, four hash function operations, two comparison operations, two symmetric encryption operations, and one signature operation. The computation cost and complexity are thus acceptable.

Table 1
Computation cost of the proposed scheme.

Phase	Party				
	Medical cloud server	Hospital medical reader	Rural medical vehicle	Personal mobile reader	Body sensor device
Body sensor device registration phase	N/A	$1T_P + 1T_H$	N/A	N/A	N/A
Personal mobile reader registration phase	$2T_{Mul} + 1T_H$	$1T_P + 1T_H$	N/A	$2T_{Mul} + 1T_H$ $+1T_{Cmp}$	N/A
Rural medical vehicle registration phase	$2T_{Mul} + 1T_H$	N/A	$2T_{Mul} + 1T_H$ $+1T_{Cmp}$	N/A	N/A
Hospital medical reader registration phase	$2T_{Mul} + 1T_H$	$2T_{Mul} + 1T_H$ $+1T_{Cmp}$	N/A	N/A	N/A
Personal mobile reader authentication and communication phase	N/A	N/A	N/A	$1T_P + 2T_H$ $+1T_{Cmp} + 1T_{Enc}$	$1T_P + 2T_H$ $+1T_{Cmp} + 1T_{Enc}$
Rural medical vehicle authentication and communication phase	N/A	N/A	$5T_{Mul} + 4T_H$ $+1T_{Cmp} + 2T_{Enc}$ $+1T_{Sig}$	$5T_{Mul} + 4T_H$ $+2T_{Cmp} + 2T_{Enc}$ $+1T_{Sig}$	N/A
Hospital medical reader authentication and communication phase	N/A	$5T_{Mul} + 4T_H$ $+2T_{Cmp} + 1T_{Enc}$ $+1T_{Sig}$	N/A	$5T_{Mul} + 4T_H$ $+1T_{Cmp} + 1T_{Enc}$ $+1T_{Sig}$	N/A

T_P: Polynomial function operation
T_{Mul}: Multiplication operation
T_H: Hash function operation
T_{Cmp}: Comparison operation
T_{Enc}: Symmetric encryption operation
T_{Sig}: Signature operation

3.8 Communication performance

The communication cost of the proposed scheme is shown in Table 2. The communication efficiency of the proposed scheme during the transaction process of each phase was also analyzed. It was assumed that a polynomial function operation required 160 bits, an elliptic curve modular operation required 160 bits, a hash operation required 160 bits, an AES operation required 256 bits, a signature operation required 1024 bits, and a doctor's certificate required 512 bits, while other messages, such as *id*, *pid*, and *random number*, required 80 bits. For example, the rural medical vehicle authentication and communication phase of the proposed scheme requires four elliptic curve modular messages, two hash messages, two AES messages, one signature operation message, one doctor's certificate message, and four other messages. It thus requires 160*4 + 160*2 + 256*2 + 1024*1 + 512*1 + 80*4 = 3328 bits. In a 3.5 G environment, the maximum transmission speed is 14 Mbps. In this study, we also considered

Table 2
Communication cost of the proposed scheme.

Phase	Item			
	Message length	Round	3.5G (14 Mbps)	4G (100 Mbps)
Body sensor device registration phase	400 bits	2	0.029 ms	0.004 ms
Personal mobile reader registration phase	880 bits	4	0.063 ms	0.009 ms
Rural medical vehicle registration phase	480 bits	2	0.034 ms	0.005 ms
Hospital medical reader registration phase	480 bits	2	0.034 ms	0.005 ms
Personal mobile reader authentication and communication phase	736 bits	2	0.053 ms	0.007 ms
Rural medical vehicle authentication and communication phase	3328 bits	4	0.238 ms	0.033 ms
Hospital medical reader authentication and communication phase	2992 bits	3	0.214 ms	0.030 ms

Table 3
Functionality comparison of previous schemes and the proposed scheme.

Functionality	Scheme		
	Rezaeibagha *et al.* (2018)$^{(25)}$	Li *et al.* (2018)$^{(26)}$	Our Scheme
Mutual authentication	Yes	Yes	Yes
Data integrity	Yes	Yes	Yes
User untraceability	Yes	Yes	Yes
Resisting replay attack	Yes	Yes	Yes
Forward and backward secrecy	Yes	Yes	Yes
Nonrepudiation	No	Yes	Yes
BAN logic proof	No	No	Yes
Offline authentication	No	No	Yes

the rural medical vehicle authentication and communication phase of the proposed scheme, which only takes 0.238 ms to transfer all messages. In a 4 G environment, the maximum transmission speed is 100 Mbps and the transmission time is reduced to 0.033 ms (ITU 2016).

3.9 Functionality comparison

The functionality comparison of previous schemes and the proposed scheme is shown in Table 3.

4. Conclusions

Recent developments in sensor network and cloud computation technology have given rise to what is known as the IoT. Many services can be provided through network cloud environments, including rural medical care services. The government provides rural medical vehicles to visit rural areas for medical services. Residents with chronic diseases or those who need long-term monitoring of physiological conditions can wear physiological sensing devices, and these sensing data can be provided to rural medical vehicles, so that doctors can diagnose symptoms. For patients with complicated or severe conditions, it is necessary to go to large hospitals in urban areas for further diagnosis and treatment. To improve the medical efficiency, the patient can inform the doctors of the physiological sensing data and the diagnostic report of the rural medical vehicle. In addition, aging populations mean an increased need for expanded healthcare, which has resulted in a new technology development trend. Elderly people can now wear body sensor devices and personal mobile readers to establish a BAN, which can provide medical care workers and doctors with necessary patient data for diagnoses. However, malicious attackers may seek to obtain sensitive personal data for various reasons. Thus, an IoT-based sensing rural medical care system that can provide security, privacy, and efficiency is necessary.

Previously proposed architectures for a healthcare environment lack comprehensive consideration. Therefore, in this study, we propose an IoT-based sensing rural medical care system, which consists of a secure and lightweight BSN based on the IoT for rural medical care environments. We use sensor and network technology to propose an intelligent rural medical healthcare environment. The sensors can monitor physiological condition and transfer the sensing data to a cloud server. To sum up, in this work, we mainly achieved the following three contributions. First, a comprehensive framework for an IoT-based sensing rural medical care system was proposed, including body sensor devices, personal mobile readers, rural medical vehicles, hospital medical readers, and a medical cloud server. Second, a secure communication architecture for all roles was designed, unlike previous studies that have only mentioned the concept. Third, the proposed authentication mechanism ensures mutual authentication, data integrity, user untraceability, nonrepudiation, forward and backward secrecy, and security against replay attacks.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (No. 61672442) and the Science and Technology Planning Project of Fujian Province (No. 2016Y0079).

Author Contributions

Chin-Ling Chen and Yong-Yuan Deng designed the protocol and analyzed the security property. Chin-Feng Lee and Shunzhi Zhu proposed the original idea and design protocol. Yi-Jui Chiu and Chih-Ming Wu surveyed the related works.

Conflicts of Interest

The authors declare no conflict of interest.

References

1 S. R. Moosavi, T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho: Future Gener. Comput. Syst. **64** (2016) 108.

2 M. A. S. Junior, M. V. M. Silva, R. C. A. Alves, and T. K. C. Shibata: Comput. Commun. **98** (2017) 43.

3 Y. Yang, X. Zheng, and C. Tang: J. Netw. Comput. Appl. **89** (2017) 26.

4 B. R. Ray, J. Abawajy, M. Chowdhury, and A. Alelaiwi: Future Gener. Comput. Syst. **78** (2018) 838.

5 M. Simplicio, B. Oliveira, P. Barreto, C. Margi, T. Carvalho, and M. Naslund: Proc. 36th IEEE Conf. Local Computer Networks (LCN) (2011) 454.

6 I. Chiuchisan and M. Dimian: IEEE Int. Workshop on Computational Intelligence for Multimedia Understanding (IWCIM) (2015) 1.

7 H. Khemissa and D. Tandjaoui: Int. Conf. Next Generation Mobile Applications, Services and Technologies (2015) 90.

8 Y. Yang and M. Ma: IEEE Trans. Inf. Forensics Secur. **11** (2016) 746.

9 J. Lee, K. Kapitanova, and S. Son: Int. J. Comput. Telecommun. Netw. **54** (2010) 2967.

10 A. Abbas and S. Khan: IEEE J. Biomed. Health Inf. **18** (2014) 1431.

11 K. Liang and W. Susilo: IEEE Trans. Inf. Forensics Secur. **10** (2015) 1981.

12 J. Yang, J. Li, and Y. Niu: Future Gener. Comput. Syst. **43–44** (2015) 74.

13 D. He, C. Chen, S. Chan, and J. Bu: IEEE Trans. Ind. Electron. **59** (2012) 4155.

14 J. Han, W. Susilo, and Y. Mu: IEEE Trans. Inf. Forensics Secur. **10** (2015) 665.

15 S. Zhao, A. Aggarwal, R. Frost, and X. Bai: IEEE Commun. Surv. Tutorials **14** (2012) 380.

16 A. Whitmore, A. Agarwal, and L. Da Xu: Inf. Syst. Front. **17** (2015) 261.

17 G. Fortino, D. Parisi, V. Pirrone, and G. D. Fatta: Future Gener. Comput. Syst. **35** (2014) 62.

18 G. Fortino, S. Galzarano, R. Gravina, and W. Li: Inf. Fusion **22** (2015) 50.

19 R. Gravina, P. Alinia, H. Ghasemzadeh, and G. Fortino: Inf. Fusion **35** (2017) 68.

20 Z. Zhou, D. Huang, and Z. Wang: IEEE Trans. Comput. **64** (2015) 126.

21 A. Ali, S. Irum, F. Kausar, and F. Khan: Multimedia Tools Appl. **66** (2013) 201.

22 S. Mollera, T. Newe, and S. Lochmann: Sens. Actuators, A **173** (2012) 55.

23 H. Kim, C. H. Kim, and J. M. Chung: Wireless Commun. Mobile Comput. **12** (2012) 145.

24 A. Papali: Bull. World Health Organ. **94** (2016) 73.

25 F. Rezaeibagha and Y. Mu: IEEE Trans. Inf. Technol. Biomed. **78** (2018) 24.

26 C. T. Li, D. H. Shih, and C. C. Wang: Comput. Methods Programs Biomed. **157** (2018) 191.

27 X. Yao, Z. Chen, and Y. Tian: Future Gener. Comput. Syst. **49** (2015) 104.

28 D. He, C. Chen, S. Chan, J. Bu, and A. Vasilakos: IEEE Trans. Inf. Technol. Biomed. **16** (2012) 1164.

29 D. He, C. Chen, S. Chan, J. Bu, and A. Vasilakos: IEEE Trans. Inf. Technol. Biomed. **16** (2012) 623.

30 W. Han and Z. Zhu: Int. J. Commun. Syst. **27** (2014) 1173.