Chen *et al. Hum. Cent. Comput. Inf. Sci.* (2020) 10:21
https://doi.org/10.1186/s13673-020-00221-1

Human-centric Computing and Information Sciences

RESEARCH Open Access

A secure electronic medical record authorization system for smart device application in cloud computing environments

Chin-Ling Chen[1,2,3], Po-Tsun Huang[3], Yung-Yuan Deng[3*], Hsing-Chung Chen[4,5*] and Yun-Ciao Wang[6]

*Correspondence:
allen.nubi@gmail.com;
cdma2000@asia.edu.tw;
shin8409@ma6.hinet.net
[3] Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan
[4] Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan
Full list of author information is available at the end of the article

Abstract

As cloud computing technology matures, along with an increased application of distributed networks, increasingly larger amounts of data are being stored in the cloud, and are thus available for pervasive application. At the same time, current independent medical record systems tend to be inefficient, and most previous studies in this field fail to meet the security requirements of anonymity and unlinkability. Some proposed schemes are even vulnerable to malicious impersonation attacks. The scheme proposed in this study, therefore, combines public and private clouds in order to more efficiently and securely preserve and manage electronic medical records (EMR). In this paper, a new secure EMR authorization system is proposed, which uses elliptic curve encryption and public-key encryption, providing a health care system with both public and private cloud environments with a message authentication mechanism, allowing the secure sharing of medical resources. The analysis shows that the proposed scheme prevents known attacks, such as replay attacks, man-in-the-middle attacks and impersonation attacks, and provides user anonymity, unlinkability, integrity, non-repudiation, forward and backward security.

Keywords: Secure medical record system, Authorization, IoT, Cloud, Health care, Security

Introduction

Medical technology and health care have both improved significantly in recent years, as people have begun to eat more healthy and nutritious foods. According to the World Health Organization (WHO), the top two causes of death globally are ischemia heart disease and stroke [1]. Although knowledge and technology exist to treat and even cure many kinds of diseases, the time of diagnosis is also very important. Thus early access to comprehensive electronic medical record (EMR) data is crucial in combatting sudden onset diseases. To this end, this study proposes a unified database sharing data between multiple hospitals in order to increase access to such data, as well as the details available to health workers. Nowadays, the privacy of patients and the lack of security between one hospital and another are the top two issues in EMR sharing. In view of this, a positive step forward would be the development of a secure method for preserving and

sharing of EMR data [2, 3]. This necessary requires proper data management via a medical resources sharing system. The combination of public and private clouds is an efficient way to achieve this [4]: if patients' EMR data is stored in a private cloud, any doctor authorized to access that data can do so via authentication [5]. This method also ensures the consistency of health data [6].

The security of medical health care systems has been the topic of a number of recent studies. Chatterjee et al. [7] proposed a secure biometric-assisted access control protocol with an appropriate authentication structure that uses both a user password and biometric to provide better security as compared to other password-based authentication schemes. Amin et al. [8] suggested an anonymous user authentication framework to achieve patient unlinkability with anonymity preserving for electronic healthcare systems, and an anonymous user authentication scheme to monitor patient health using wireless medical sensor networks. Moreover, Islam et al. [9] presented a two-factor authentication protocol for an integrated patient data information system. Wazid et al. [10] suggested a three-factor authentication and key agreement framework with anonymity preservation for healthcare systems. Sutrala et al. [11] designed a secure RSA-assisted authentication protocol with patient anonymity. In 2014, Chen [12] proposed a cloud-based medical data exchange protocol that included privacy protection. However, Chen et al.'s scheme [12] did not offer a real-time-monitoring facility and non-disapproval conformation diagnosis. Chiou et al. [13] proposed an upgrade agreement to solve the shortcomings of Chen et al.'s scheme. Moreover, Mohit et al. [14] found in 2017 that Chiou et al.'s scheme [13] could not support patient anonymity, or ensure that even if a patient's mobile device was stolen, the device could not be used for a malicious attack. Kumar et al. [15] proposed an effective mutual authentication framework for cloud computing healthcare systems. Li et al. [16] showed that Mohit et al.'s scheme [14] fails to protect patient anonymity, fails to protect patient accessibility, and lacks medical records. Li et al. proposed cloud-based authentication and privacy protection schemes.

After analyzing the related works, this study identified some flaws to be addressed. For example, the schemes proposed by Chiou et al. [13], Mohit et al. and Li et al. [16] did not support patient anonymity and unlinkability, nor did they support smart and convenient authorization, and they were vulnerable to impersonation attacks.

According to the above analyses, how to use a smart device to achieve a secure electronic medical sharing [17–20] is a worthy research issue for health care systems [21–24]. This study proposes a secure electronic medical record (EMR) authorization system for smart device applications in cloud computing environments [25–28]. The security requirements met by the proposed model include mutual authentication, anonymity, unlinkability, data integrity, data non-repudiation, and forward and backward security [29, 30] while being secure against known attacks, such as replay attacks, man-in-the-middle attacks and impersonation attacks [31, 32].

The remainder of this paper is arranged as follows: In "Preliminary" section, we gives a brief description of the security requirements and the elliptic curve group. In "The proposed scheme" section, we also describes the proposed scheme. Next, in "Security analysis" section, the security analyses are conducted. In "Discussion" section, the detailed results of the security comparison and computation cost are discussed. Finally, conclusions are offered in "Conclusions" section.

Preliminary

Security requirements

In this paper, we assume the following assumptions based on the threat model mentioned in [33–36]. Therefore, the following list is the security requirements for a secure electronic medical record authorization system for smart device applications in cloud computing environments.

Mutual authentication

The message receiver should authenticate the legality of the message sender during the information transmission process. Therefore, in a secure electronic medical record authorization system for smart device applications in cloud computing environments, each party should authenticate the legality of the other party. If each other's legality of the two parties is confirmed, then it achieves mutual authentication.

User anonymity and unlinkability

Malicious attacks may also attempt to determine a person's physical location by tracing their personal mobile reader. Thus, a secure electronic medical record authorization system for smart device applications in cloud computing environments must prevent such positional tracking.

Integrity

When the message transferred through an insecure network environment, it is susceptible to the malicious attack that the attacker modifies the original message. Thus, the message received by the receiver may not the original message sent from the sender. It ensures the integrity of the transmitted data and also protects against tampering in transmission.

Non-repudiation

The message receiver must be able to verify the legality of the message sender during the information transmission process. Once the receiver confirms that the message was sent from the sender, the sender can't deny the message that he/she had sent. The sender uses his/her private key to sign the message, and the receiver can verify the digital signature from the sender.

Forward and backward security

The session key is established between the message sender and the message receiver. If it is compromised by an attacker at any point, he/she may use the session key for future communications, or use it to obtain previous messages.

Confidentiality

If the data is intercepted by a malicious attacker during transmission, the unencrypted data content will be exposed, which violates the principle of confidentiality

of information security. In order to prevent disclosure of data, sensitive data must be encrypted during transmission and storage.

Availability

A secure and reliable information system must use data encryption and identity verification technology, in order to ensure that data is not accessed by illegal users. Simultaneously, it must be ensured that legitimate users can correctly obtain the plain text of the transmitted message within an acceptable time, which meets the availability of the system.

Prevent replay attack

The attacker can intercept the messages transmitted between the sender and the receiver by malicious attacks. Then, the attacker impersonates a legitimate transmitter so as to send the same messages again to the intended receiver. The situation causes a serious security risk, and that must be prevented.

Prevent man-in-the-middle attack

This attack means the attacker intercepts the message during the communication phase and counterfeits the message. Then, the attacker sends this counterfeit message to other communication parties. The situation causes a serious security risk, and that must be prevented in a secure electronic medical record authorization system for smart device applications in cloud computing environments.

Prevent impersonation attack

This attack means an illegal user wants to disguise as the legal user to log into the server or to communicate with other legal users. The situation causes a serious security risk, thus a secure electronic medical record authorization system for smart device applications in cloud computing environments must prevent such attacks.

Elliptic curve group

E/F_q is an elliptic curve defined over a prime finite field F_q. P is a generator for a cyclic additive group of composite order q [37]. G is a cyclic additive group of the composite order q. A point on E/F_q together with an extra point Q is called the point at infinity from a group $G = \{(x, y) : x, y \in E/F_q\} \cup \{Q\}$. The scalar multiplication over E/F_q is calculated by the Eq. 1 as:

$$tP = P + P + \cdots + P, \ t \quad \text{times}. \tag{1}$$

Computational Diffie–Hellman (CDH) problem and Decisional Diffie–Hellman (DDH) problem exist for the elliptic curve group. The details are as follows:

Computational Diffie–Hellman (CDH) problem

$a, b \in R$, $Z \times q$ and P are the generators of G. Given aP and bP, the value abP can be computed.

Decisional Diffie–Hellman (DDH) problem

$a, b, c \in R$, $Z \times q$ and P are the generator of G. Given aP, bP, and cP, the value abP can be computed. Confirming that $cP = abP$ is equal to confirming that $c = ab \bmod q$.

The proposed scheme

System architecture

This study proposes a distributed EMR storage and sharing scheme. Figure 1 shows the proposed system architecture. There are four parties in the proposed system, including the patient, the doctor, the hospital's private cloud, and the public cloud. Each party is described in detail below.

1. Patient (P): The patient takes a smart device when they visit a doctor. They authenticate their identity with the smart device by entering their biometric password.
2. Doctor (D): The doctor verifies the EMR of the patient and the legality of the hospital's private cloud. In the EMR search phase, the doctor collects messages from both sides and then makes a professional diagnosis.
3. Hospital's private cloud (HPC): The hospital's private cloud is the cloud in which the patient's EMR is stored. It authenticates the legality of the doctor and then provides them with the correct EMR.
4. Public cloud (PC): A public cloud plays the role of generating secret keys. Every party gets a secret parameter from the public cloud during the registration phase. It stores the index of the patient's medical data during the EMR search phase. By checking the secret key given by the public cloud, the doctor can authenticate their patients. The public cloud and the private cloud form a medical union cloud. The medical union cloud achieves EMR sharing by authenticating each other.

The following is a description of the four steps process of a patient visiting a doctor:

Step 1: All parties are registered to the public cloud. The public cloud calculates secret keys by n elliptic curve. The cloud then issues the secret keys to parties.

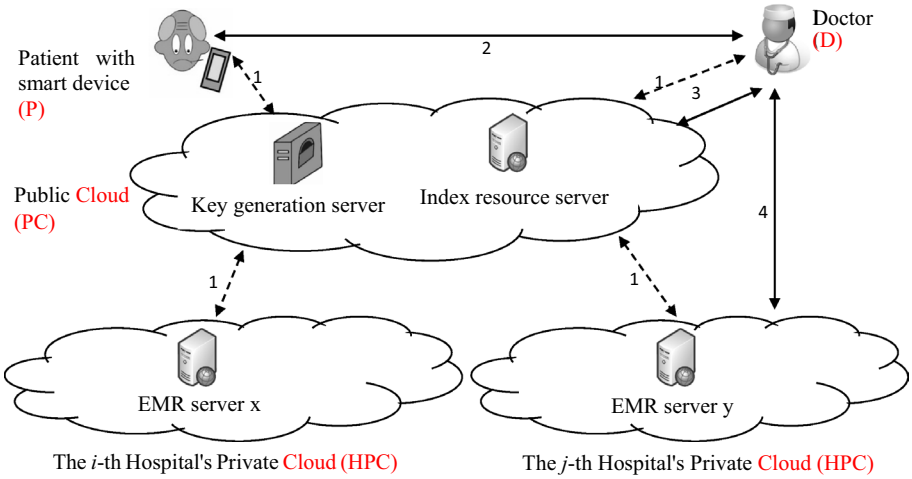

Fig. 1 The architecture of the proposed distributed EMR storage and sharing scheme

Step 2: The patient visits the doctor. The doctor authenticates the patient, and the patient sends their biomedical signal to the doctor.
Step 3: The doctor receives the index of the patient from the public cloud and then obtains the EMR from the hospital's private cloud.
Step 4: The doctor makes a diagnosis according to the EMR and the patient's current condition. Finally, the doctor sends the diagnosis messages to the public cloud.

Notation

The notations used in this paper are shown in Table 1.

Registration phase

All parties register in the cloud to get the secret key. The registration phase is divided into three parts which are the patient, the hospital's private cloud, and the doctor register with the public cloud.

The patient registers with the public cloud

This process consists of three steps, as shown in Fig. 2a.

Step 1: The patient selects an identity ID_P and a biometric password B_P. They then send both to the public cloud via a secure channel.
Step 2: When the public cloud receives the message, it selects a random number r_1, and uses it to multiply by the generator, the elliptic group, P to compute

Table 1 Notation

Notation	Meaning
P	A generator for the elliptic group
s	A secret key
PK	A public key, where $PK = sP$
$H(\cdot)$	Biometric hash function
$h(\cdot)$	One way hash function
ID_X	Identity of X
B_P	A biometric password
$Cert_D$	The doctor's certificate issued by a medical authority
T_{Xi}	The ith timestamp of sender X
T'_{Xi}	The ith received message timestamp from sender X
ΔT	A valid time interval
r_i	The ith random number
S_X	The secret key shared between the public cloud and X
SEK_i	The ith session key
M_{SD}	The biomedical signal sensed by a smart device
M_{EMR}	The electronic medical record
M_{DINF}	The diagnosis information on the smart device
$\|\|$	Concatenation function
$A \stackrel{?}{=} B$	Determines if A is equal to B
----->	Secure channel
——>	Insecure channel

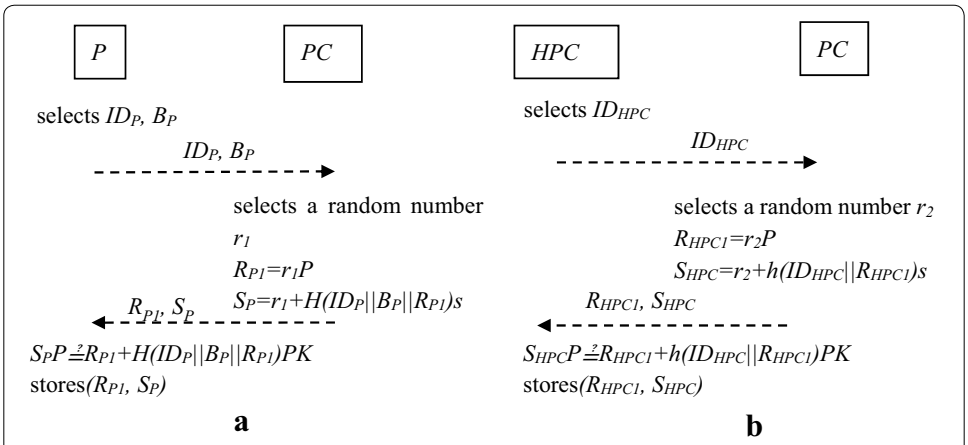

Fig. 2 **a** Flow chart of the patient registering with the public cloud, **b** flow chart of the hospital's private cloud registering with the public cloud

R_{P1} by using the Eq. 2, and then to compute S_P by using the Eq. 3, as follows:

$$R_{P1} = r_1 P, \tag{2}$$

$$S_P = r_1 + H(ID_P||B_P||R_{P1})s. \tag{3}$$

The public cloud then sends R_{P1} and S_P to the patient via a secure channel.

Step 3: Upon receiving the message from the public cloud, the patient verifies by using the Eq. 4 as follows:

$$S_P P \stackrel{?}{=} R_{P1} + H(ID_P||B_P||R_{P1})PK. \tag{4}$$

If it holds, then the patient stores (R_{P1}, S_P).

The hospital's private cloud registers with the public cloud

This process consists of three steps, as illustrated in Fig. 2b.

Step 1: The hospital's private cloud selects an identity ID_{HPC}, and then sends its identity ID_{HPC} to the public cloud via a secure channel.

Step 2: When the public cloud receives the message, it selects a random number r_2 and uses it with the generator for the elliptic group P to compute R_{HPC1} by using the Eq. 5. The public cloud computes S_{HPC} by using the Eq. 6. R_{HPC1} and S_{HPC} as follows:

$$R_{HPC1} = r_2 P. \tag{5}$$

$$S_{HPC} = r_2 + h(ID_{HPC}||R_{HPC1})s. \tag{6}$$

The public cloud sends R_{HPC1} and S_{HPC} to the hospital's private cloud via a secure channel.

Step 3: Upon receiving the message, the hospital's private cloud verifies by using the

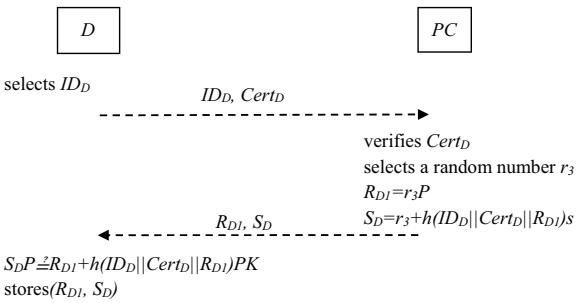

Fig. 3 The doctor registers with the public cloud

Eq. 7 as follows:

$$S_{HPC}P \stackrel{?}{=} R_{HPC1} + h(ID_{HPC}||R_{HPC1})PK. \tag{7}$$

If it holds, then the hospital's private cloud stores (R_{HPC1}, S_{HPC}).

The doctor registers with the public cloud

This process also consists of three steps, as shown in Fig. 3.

Step 1: The doctor selects an identity ID_D and their doctor's certificate $Cert_D$ and s both to the public cloud via a secure channel.

Step 2: When the public cloud receives the messages, it verifies whether $Cert_D$ is legal. If $Cert_D$ is illegal, the public cloud will terminate the registration phase. If it is legal, it selects a random number r_3 and uses it multiply by the generator for the elliptic group P to compute R_{D1} by using the Eq. 8, and to then compute S_D by using the Eq. 9 as follows:

$$R_{D1} = r_3P, \tag{8}$$

$$S_D = r_3 + H(ID_D||Cert_D||R_{D1})s. \tag{9}$$

The public cloud sends R_{D1} and S_D to the doctor via a secure channel.

Upon receiving the message from the public cloud, the doctor verifies by using the Eq. 10 as follows:

$$S_DP \stackrel{?}{=} R_{D1} + h(ID_D||Cert_D||R_{D1})PK. \tag{10}$$

If it holds, then the doctor stores (R_{D1}, S_D).

Patient visiting doctor (consultation) phase

In this phase, the patient goes to the doctor for a medical consultation. They bring their smart device with them in order to first authenticate the doctor. This section describes how the patient logs into the medical system, and how they achieve authentication with the doctor. This phase consists of four steps, as shown in Fig. 4.

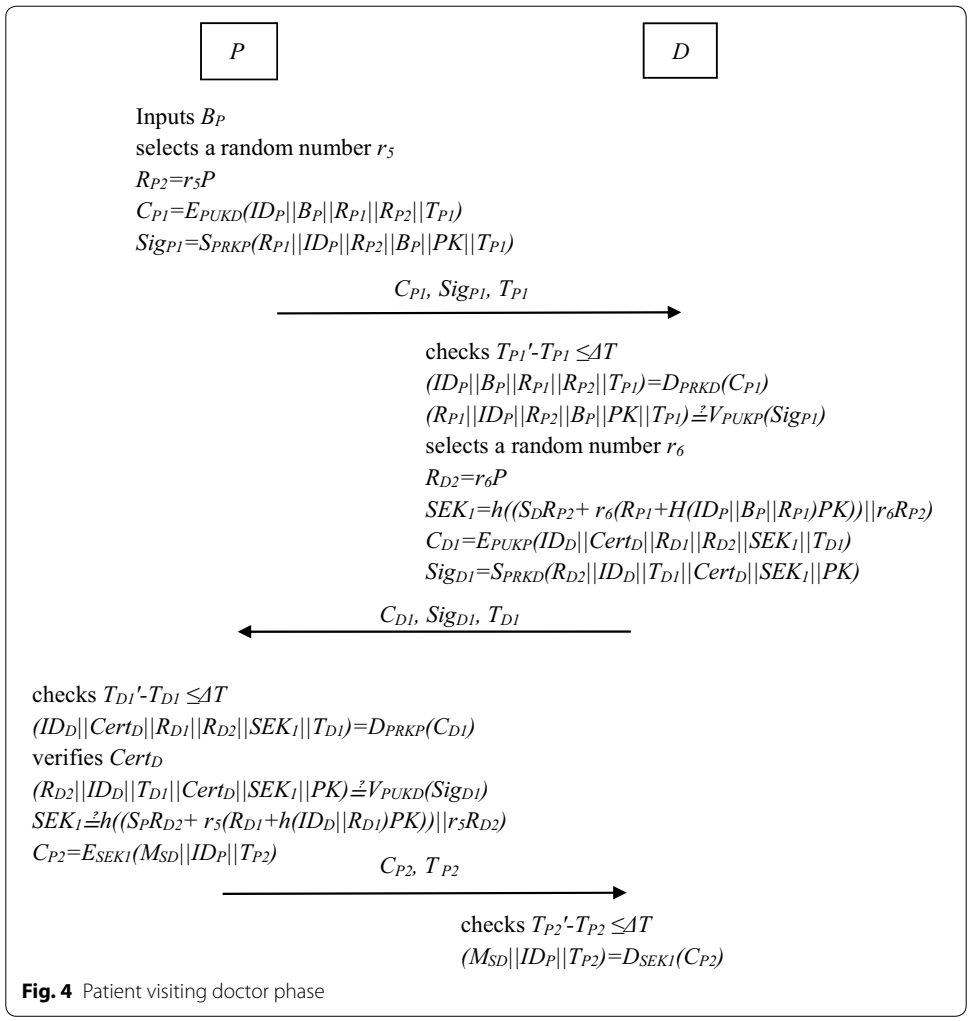

Fig. 4 Patient visiting doctor phase

The patient inputs their biometric password B_P and selects a random number r_5, and uses r_5 and P to compute R_{P2} by using the Eq. 11 as follows:

$$R_{P2} = r_5P. \tag{11}$$

He/She then uses the doctor's public key PUK_D to encrypt $(ID_P||B_P||R_{P1}||R_{P2}||T_{P1})$ into C_{P1} by using the Eq. 12 as follows.

$$C_{P1} = E_{PUK_D}(ID_P||B_P||R_{P1}||R_{P2}||T_{P1}). \tag{12}$$

The patient then uses their private key PRK_P to generate their signature Sig_{P1} by using the Eq. 13 as follows:

$$Sig_{P1} = S_{PRK_P}(R_{P1}||ID_P||R_{P2}||B_P||PK||T_{P1}). \tag{13}$$

Finally, the patient sends $\left(C_{P1}, Sig_{P1}, T_{P1}\right)$ to the doctor, where T_{P1} is the timestamp.

Step 1: Upon receiving $(C_{P1}, Sig_{P1}, T_{P1})$, the doctor checks if $T'_{P1} - T_{P1} \leq \Delta T$. If ΔT is not valid, the doctor will terminate the communication. The doctor then decrypts C_{P1} and verifies Sig_{P1} by using the Eqs. 14 and 15 as follows:

$$(ID_P||B_P||R_{P1}||R_{P2}||T_{P1}) = D_{PRK_D}(C_{P1}), \tag{14}$$

$$\left(R_{P1}||ID_P||R_{P2}||B_P||PK||T_{P1}\right) \stackrel{?}{=} V_{PUK_P}(Sig_{P1}). \tag{15}$$

He/She then uses the random number r_6 with the generator for the elliptic group P to compute R_{D2}, and calculate a session key by using the Eqs. 16 and 17 as follows:

$$R_{D2} = r_6 P, \tag{16}$$

$$SEK_1 = h((S_D R_{P2} + r_6(R_{P1} + H(ID_P||B_P||R_{P1})PK))||r_6 R_{P2}). \tag{17}$$

The doctor uses patient's public key PUK_P to encrypt $(ID_D||Cert_D||R_{D1}||R_{D2}||SEK_1||T_{D1})$ into C_{D1} by using the Eq. 18 as follows:

$$C_{D1} = E_{PUK_P}(ID_D||Cert_D||R_{D1}||R_{D2}||SEK_1||T_{D1}), \tag{18}$$

then uses their private key PRK_D to generate their signature Sig_{D1} by using the Eq. 19 as follows:

$$Sig_{D1} = S_{PRK_D}(R_{D2}||ID_D||T_{D1}||Cert_D||SEK_1||PK). \tag{19}$$

Finally, the doctor sends $(C_{D1}, Sig_{D1}, T_{D1})$ to the patient. Where T_{D1} is the timestamp.

Step 2: Upon receiving $(C_{D1}, Sig_{D1}, T_{D1})$, the patient checks if $T'_{D1} - T_{D1} \leq \Delta T$. If ΔT is not valid, the communication is terminated. The patient decrypts C_{D1} by using the Eq. 20 as follows:

$$(ID_D||Cert_D||R_{D1}||R_{D2}||SEK_1||T_{D1}) = D_{PRK_P}(C_{D1}), \tag{20}$$

and verifies if $Cert_D$ is legal or not. And then the patient verifies Sig_{D1} by using the Eq. 21 as follows:

$$\left(R_{D2}||ID_D||T_{D1}||Cert_D||SEK_1||PK\right) \stackrel{?}{=} V_{PUK_P}(Sig_{D1}). \tag{21}$$

The patient then calculates a session key and verifies it by using the Eq. 22 as follows:

$$SEK_1 \stackrel{?}{=} h((S_P R_{D2} + r_5(R_{D1} + h(ID_D||R_{D1})PK))||r_5 R_{D2}) \tag{22}$$

and uses the session key SEK_1 to encrypt (M_{SD}, ID_P, T_{P2}) into C_{P2} by using the Eq. 23 as follows:

$$C_{P2} = E_{SEK_1}(M_{SD}, ID_P, T_{P2}). \tag{23}$$

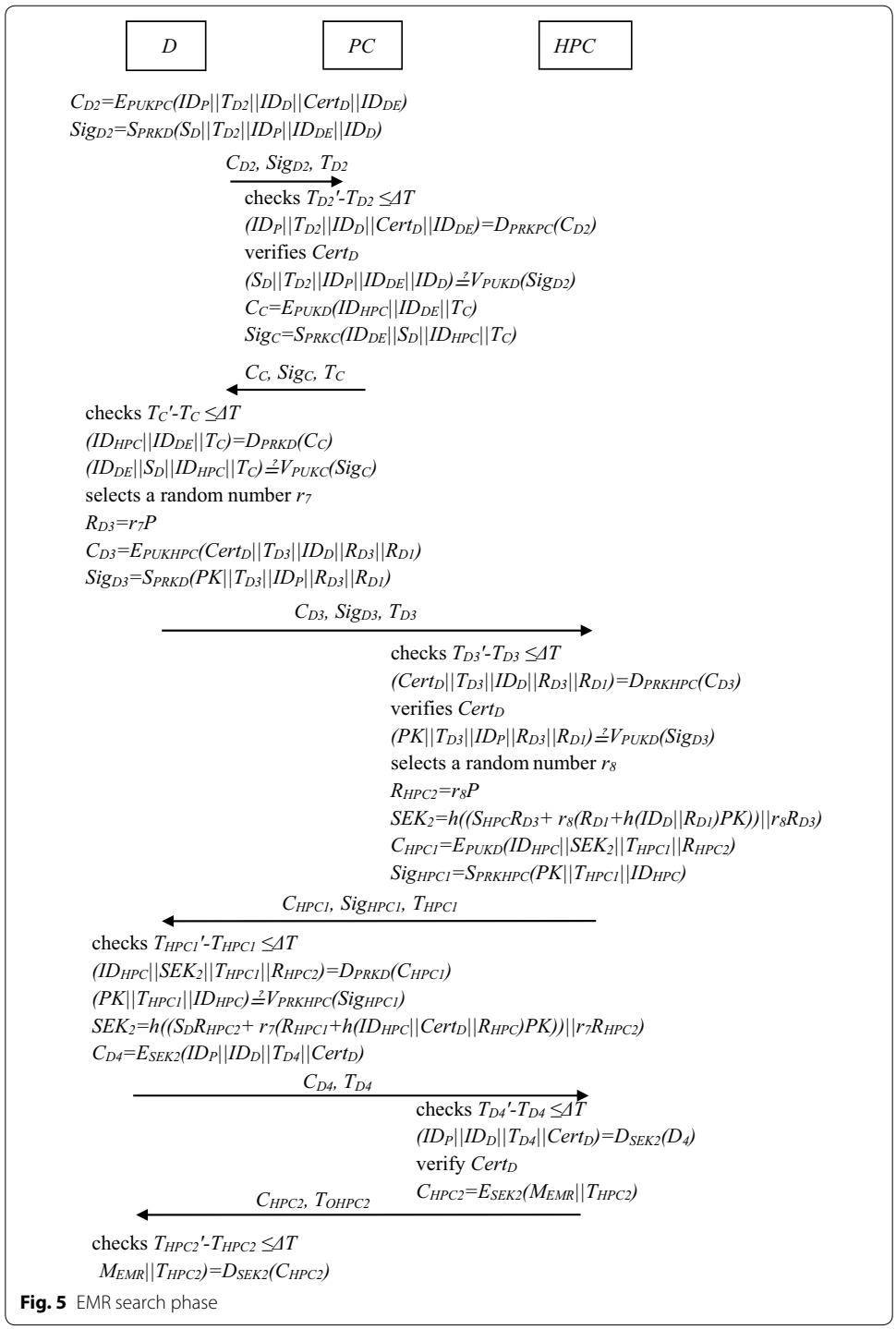

Fig. 5 EMR search phase

Finally, the patient sends C_{P2} and T_{P2} to the doctor.

Step 3: Upon receiving (C_{P2}, T_{P2}), the doctor checks if the timestamp $T'_{P2} - T_{P2} \leq \Delta T$, then decrypts C_{P2} via session key SEK_1 by using the Eq. 24 as follows:

$$\left(M_{SD}, ID_P, T_{P2}\right) = D_{SEK_1}\left(C_{P2}\right). \tag{24}$$

EMR search phase

The purpose of this phase is to search the EMR of the patient for information relevant to the current diagnosis process. The doctor contacts the hospital's private cloud to obtain the EMR of the patient, and thus needs to be authenticated with the private cloud. This phase consists of seven steps, as shown in Fig. 5.

Step 1: The doctor uses the public key of the public cloud PUK_{PC} to encrypt $(ID_P||T_{D2}||ID_D||Cert_D||ID_{DE})$ into C_{D2} by using the Eq. 25 as follows:

$$C_{D2} = E_{PUK_{PC}}(ID_P||T_{D2}||ID_D||Cert_D||ID_{DE}). \tag{25}$$

He/She then uses their private key to generate their signature Sig_{D2} by using the Eq. 26 as follows:

$$Sig_{D2} = S_{PRK_D}(S_D||T_{D2}||ID_P||ID_{DE}||ID_D). \tag{26}$$

Finally, the doctor sends $\left(C_{D2}, Sig_{D2}, T_{D2}\right)$ to the public cloud.

Upon receiving $\left(C_{D2}, Sig_{D2}, T_{D2}\right)$, the public cloud checks if $T'_{D2} - T_{D2} \leq \Delta T$, then the public cloud decrypts C_{D2} and verifies whether $Cert_D$ is legal by using the Eq. 27 :

$$\left(ID_P||T_{D2}||ID_D||Cert_D||ID_{DE}\right) = D_{PRK_{PC}}\left(C_{D2}\right). \tag{27}$$

The public cloud also uses the doctor's public key to verify the signature Sig_{D2} by using the Eq. 28 as follows:

$$\left(S_D||T_{D2}||ID_P||ID_{DE}||ID_D\right) \stackrel{?}{=} V_{PUK_D}\left(Sig_{D2}\right). \tag{28}$$

It also verifies whether $Cert_D$ is legal. Then the public cloud searches the patient's index record in its database according to ID_P and ID_{DE}. After this, it uses the doctor's public key PUK_D to encrypt $(ID_{HPC}||ID_{DE}||T_C)$ into C_C by using the Eq. 29 as follows, where ID_{DE} is the hospital department's identity.

$$C_C = E_{PUK_D}(ID_{HPC}||ID_{DE}||T_C). \tag{29}$$

The public cloud then uses its private key PRK_C to generate the public cloud signature Sig_C by using the Eq. 30 as follows:

$$Sig_C = S_{PRK_C}(ID_{DE}||S_{SD}||ID_{HPC}||T_C). \tag{30}$$

After this, the public cloud stores $(h(ID_P||ID_{DE}), (ID_{CHPC}||ID_D) \oplus h(s))$.

Finally, the public cloud sends (C_C, Sig_C, T_C) to the doctor.

Step 2: Upon receiving (C_C, Sig_C, T_C), the doctor checks if $T'_C - T_C \leq \Delta T$. The doctor then decrypts C_C and verifies Sig_C by using the Eqs. 31 and 32 as follows:

$$(ID_{HPC}||ID_{DE}||T_C) = D_{PRK_D}(C_C), \tag{31}$$

$$(ID_{DE}||S_{SD}||ID_{HPC}||T_C) \stackrel{?}{=} V_{PUK_C}(Sig_C). \tag{32}$$

Then the doctor uses the random number r_7 with the generator for the elliptic group P to compute R_{D3} by using the Eq. 33. They then use the public key of the hospital's private cloud PUK_{HPC} to encrypt $(Cert_D||T_{D3}||ID_D||R_{D3}||R_{D1})$ into C_{D3} by using the Eq. 34 as follows:

$$R_{D3} = r_7 P, \tag{33}$$

$$C_{D3} = E_{PUK_{HPC}}(Cert_D||T_{D3}||ID_D||R_{D3}||R_{D1}). \tag{34}$$

The doctor then uses their private key to generate their signature Sig_{D3} by using the Eq. 35 as follows:

$$Sig_{D3} = S_{PRK_D}(PK||T_{D3}||ID_P||R_{D3}||R_{D1}). \tag{35}$$

Finally, the doctor sends $(C_{D3}, Sig_{D3}, T_{D3})$ to the hospital's private cloud.

Step 3: Upon receiving $(C_{D3}, Sig_{D3}, T_{D3})$, the hospital's private cloud checks if $T'_{D3} - T_{D3} \leq \Delta T$. It then decrypts C_{D3} by using the Eq. 36 as follows:

$$(Cert_D||T_{D3}||ID_D||R_{D3}||R_{D1}) = D_{PRK_{HPC}}(C_{D3}), \tag{36}$$

and verifies whether $Cert_D$ is legal. It then verifies Sig_{D3} by using the Eq. 37 as follows:

$$(PK||T_{D3}||ID_P||R_{D3}||R_{D1}) \stackrel{?}{=} V_{PUK_D}(Sig_{D3}). \tag{37}$$

The private cloud then uses the random number r_8 with the generator for the elliptic group P to compute R_{HPC2}, and calculates a session key by using the Eqs. 38 and 39 as follows:

$$R_{HPC2} = r_8 P, \tag{38}$$

$$SEK_2 = h((S_{HPC}R_{D3} + r_8(R_{D1} + h(ID_D||Cert_D||R_{D1})PK))||r_8 R_{D3}). \tag{39}$$

It then uses the doctor's public key PUK_D to encrypt $(ID_{HPC}||SEK_2||T_{HPC1}||R_{HPC2})$ into C_{HPC1} by using the Eq. 40 as follows:

$$C_{HPC1} = E_{PUK_D}(ID_{HPC}||SEK_2||T_{HPC1}||R_{HPC2}). \tag{40}$$

It uses the private cloud's own private key to generate its signature Sig_{HPC1} by using the Eq. 41 as follows:

$$Sig_{HPC1} = S_{PRK_{HPC}}(PK||T_{HPC1}||ID_{HPC}). \tag{41}$$

Finally, the private cloud sends $(C_{HPC1}, Sig_{HPC1}, T_{HPC1})$ to the doctor.

Step 4: Upon receiving $(C_{HPC1}, Sig_{HPC1}, T_{HPC1})$, the doctor checks if $T'_{HPC1} - T_{HPC1} \leq \Delta T$, decrypts C_{HPC1}, and verifies Sig_{HPC1} by using the

Eqs. 42 and 43 as follows:

$$(ID_{HPC}||SEK_2||T_{HPC1}||R_{HPC2}) = D_{PRK_D}(C_{HPC1}), \tag{42}$$

$$(PK||T_{HPC1}||ID_{HPC}) \stackrel{?}{=} S_{PRK_{HPC}}(Sig_{HPC1}). \tag{43}$$

He/She verifies the session key by using the Eq. 44 as follows:

$$SEK_2 \stackrel{?}{=} h((S_D R_{HPC2} + r_7(R_{HPC1} + h(ID_{HPC}||R_{HPC1})PK))||r_7 R_{HPC2}), \tag{44}$$

and then use the session key SEK_2 to encrypt $(ID_P||ID_D||T_{D4}||Cert_D)$ into C_{D4} by using the Eq. 45 as follows:

$$C_{D4} = E_{SEK_2}(ID_P||ID_D||T_{D4}||Cert_D). \tag{45}$$

Finally, the doctor sends (C_{D4}, T_{D4}) to the private cloud.

Step 5: Upon receiving C_{D4}, the private cloud checks the timestamps to determine if $T'_{D4} - T_{D4} \leq \Delta T$, and then decrypts C_{D4} by using the Eq. 46 as follows:

$$(ID_P||ID_D||T_{D4}||Cert_D) = D_{SEK_2}(C_{D4}). \tag{46}$$

It verifies whether $Cert_D$ is legal, and then uses the session key SEK_2 to encrypt $(M_{EMR}||T_{HPC2})$ into C_{HPC2} by using the Eq. 47 as follows:

$$C_{HPC2} = E_{SEK_2}(M_{EMR}||T_{HPC2}). \tag{47}$$

Finally, the hospital's private cloud sends (C_{HPC2}, T_{HPC2}) to the doctor.

Step 6: When the doctor receives C_{HPC2}, they check the timestamp to determine if $T'_{HPC2} - T_{HPC2} \leq \Delta T$, and then decrypt C_{HPC2} by using the Eq. 48 as follows:

$$(M_{EMR}||T_{HPC2}) = D_{SEK_2}(C_{HPC2}). \tag{48}$$

Diagnosis phase

Once the doctor receives the patient's EMR and the sensing message M_{SD} from the patient's smart device, the doctor uses the patient's EMR from the hospital's private cloud and the M_{SD} to make a professional medical diagnosis. After this, they inform the patient of the diagnosis result. Figure 6 is the diagnosis phase of the proposed scheme.

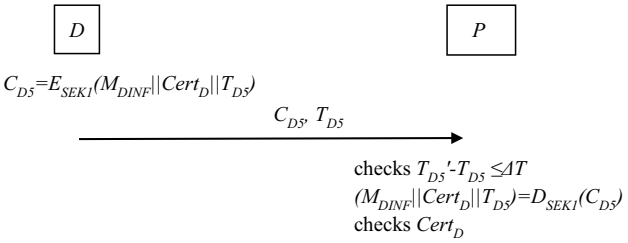

Fig. 6 Diagnosis phase

First, the doctor uses the session key SEK_1 to encrypt $(M_{DINF}||Cert_D||T_{D5})$ into C_{D5} by using the Eq. 49 as follows:

$$C_{D5} = E_{SEK_1}(M_{DINF}||Cert_D||T_{D5}). \tag{49}$$

Then the doctor sends (C_{D5}, T_{D5}) to the patient.

Step 1: When the patient receives (C_{D5}, T_{D5}), the patient checks the timestamps to determine if $T'_{D5} - T_{D5} \leq \Delta T$, then decrypts C_{D5} by using the Eq. 50 as follows:

$$(M_{DINF}||Cert_D||T_{D5}) = D_{SEK_1}(C_{D5}). \tag{50}$$

The patient then verifies that $Cert_D$ is legal.

Security analysis

This section analyzes the security issues of mutual authentication, anonymity, unlinkability, data integrity, data non-repudiation, and forward and backward security in the proposed scheme. It also analyzes the proposed scheme's security against replay attacks, man-in-the-middle attacks, and impersonation attacks.

Mutual authentication

There are four parties in the proposed scheme, namely the patient, the hospital's private cloud, the public cloud, and the doctor. This paper uses BAN logic [38] to prove that the proposed scheme achieves mutual authentication.

Goals

The following goals must be derived step by step so that all parties are able to authenticate each other. Goals are listed as G1 to G16 as follows:

G1	$D\| \equiv D \overset{SEK_1}{\leftrightarrow} P$
G2	$D\| \equiv P\| \equiv D \overset{SEK_1}{\leftrightarrow} P$
G3	$P\| \equiv D \overset{SEK_1}{\leftrightarrow} P$
G4	$P\| \equiv D\| \equiv D \overset{SEK_1}{\leftrightarrow} P$
G5	$HPC\| \equiv HPC \overset{SEK_2}{\leftrightarrow} D$
G6	$HPC\| \equiv D\| \equiv HPC \overset{SEK_2}{\leftrightarrow} D$
G7	$D\| \equiv HPC \overset{SEK_2}{\leftrightarrow} D$
G8	$D\| \equiv HPC\| \equiv HPC \overset{SEK_2}{\leftrightarrow} D$
G9	$D\| \equiv ID_P$
G10	$D\| \equiv P\| \equiv ID_P$
G11	$P\| \equiv ID_D$
G12	$P\| \equiv D\| \equiv ID_D$
G13	$HPC\| \equiv ID_D$
G14	$HPC\| \equiv D\| \equiv ID_D$
G15	$D\| \equiv ID_{HPC}$
G16	$D\| \equiv HPC\| \equiv ID_{HPC}$

Messages delivered between parties

The messages are numbered for the purposes of proving the proposed scheme, as follows:

M1	$(\{R_{P1}\|\|ID_P\|\|R_{P2}\|\|B_P\|\|PK\|\|T_{P1}\}_{PRK_P}, \{M_{SD}\|\|ID_P\|\|T_{P2}\}_{SEK_1})$
M2	$(\{R_{D2}\|\|ID_D\|\|T_{D1}\|\|Cert_D\|\|SEK_1\|\|PK\}_{PRK_D}, \{M_{DINF}\|\|Cert_D\|\|T_{D5}\}_{SEK_1})$
M3	$(\{PK\|\|T_{D3}\|\|ID_P\|\|R_{D3}\|\|R_{D1}\}_{PRK_D}, \{ID_P\|\|ID_D\|\|T_{D4}\|\|Cert_D\}_{SEK_2})$
M4	$(\{PK\|\|T_{HPC1}\|\|ID_{HPC}\}_{PRK_{HPC}}, \{M_{EMR}\|\|T_{HPC2}\}_{SEK_2})$

Assumptions

The following assumptions are made to help achieve the goals:

A1	$D\| \equiv \#(T_{P1})$
A2	$P\| \equiv \#(T_{P1})$
A3	$D\| \equiv \#(T_{D1})$
A4	$P\| \equiv \#(T_{D1})$
A5	$HPC\| \equiv \#(T_{D3})$
A6	$D\| \equiv \#(T_{D3})$
A7	$HPC\| \equiv \#(T_{HPC1})$
A8	$D\| \equiv \#(T_{HPC1})$
A9	$D\| \equiv \#SEK_1$
A10	$P\| \equiv \#SEK_1$
A11	$HPC\| \equiv \#SEK_2$
A12	$D\| \equiv \#SEK_2$
A13	$P\| \equiv \|\overset{PUK_P}{\rightarrow} D$
A14	$D\| \equiv \|\overset{PUK_P}{\rightarrow} D$
A15	$P\| \equiv \|\overset{PUK_D}{\rightarrow} P$
A16	$D\| \equiv \|\overset{PUK_D}{\rightarrow} P$
A17	$D\| \equiv \|\overset{PUK_{QHPC}}{\rightarrow} D$
A18	$HPC\| \equiv \|\overset{PUK_{QHPC}}{\rightarrow} D$
A19	$D\| \equiv \|\overset{PUK_D}{\rightarrow} HPC$
A20	$HPC\| \equiv \|\overset{PUK_D}{\rightarrow} HPC$
A21	$D\| \equiv P\| \Rightarrow D \overset{SEK_1}{\leftrightarrow} P$
A22	$P\| \equiv D\| \Rightarrow D \overset{SEK_1}{\leftrightarrow} P$
A23	$HPC\| \equiv D\| \Rightarrow HPC \overset{SEK_2}{\leftrightarrow} D$
A24	$D\| \equiv HPC\| \Rightarrow HPC \overset{SEK_2}{\leftrightarrow} D$
A25	$D\| \equiv P\| \Rightarrow ID_P$
A26	$P\| \equiv D\| \Rightarrow ID_D$
A27	$HPC\| \equiv D\| \Rightarrow ID_D$
A28	$D\| \equiv HPC\| \Rightarrow ID_{HPC}$

The doctor authenticates the patient

The doctor's authentication of the patient can be proved by the assumptions and BAN logic, as follows:

By *M1* and the seeing rule, the following Statement 1 can be derived:

(Statement 1) $D \triangleleft (\{R_{P1}||ID_P||R_{P2}||B_P||PK||T_{P1}\}_{PRK_P}, \{M_{SD}||ID_P||T_{P2}\}_{SEK_1})$.

By *A1*, *A2* and the freshness rule, the following Statement 2 can be derived:

(Statement 2) $D| \equiv \#(\{R_{P1}||ID_P||R_{P2}||B_P||PK||T_{P1}\}_{PRK_P}, \{M_{SD}||ID_P||T_{P2}\}_{SEK_1})$.

By Statement 1, *A9*, *A13*, *A14* and the message meaning rule, the following Statement 3 can be derived:

(Statement 3) $D| \equiv P| \sim \#(\{R_{P1}||ID_P||R_{P2}||B_P||PK||T_{P1}\}_{PRK_P}, \{M_{SD}||ID_P||T_{P2}\}_{SEK_1})$.

By Statement 2, Statement 3 and the verification rule, the following Statement 4 can be derived:

(Statement 4) $D| \equiv P| \equiv (\{R_{P1}||ID_P||R_{P2}||B_P||PK||T_{P1}\}_{PRK_P}, \{M_{SD}||ID_P||T_{P2}\}_{SEK_1})$.

By Statement 4 and the belief rule, the following Statement 5 can be derived:

(Statement 5) $D| \equiv P| \equiv D \overset{SEK_1}{\leftrightarrow} P$.

By Statement 4, *A21* and the jurisdiction rule, the following Statement 6 can be derived:

(Statement 6) $D| \equiv D \overset{SEK_1}{\leftrightarrow} P$.

By Statement 6 and the belief rule, the following Statement 7 can be derived:

(Statement 7) $D| \equiv P| \equiv ID_P$.

By Statement 6, *A25* and the belief rule, the following Statement 8 can be derived:

(Statement 8) $D| \equiv ID_P$.

According to Statement 6 and Statement 8, we prove that the doctor can surely authenticate the patient by using the Eq. 15 as follows:

$$(R_{P1}||ID_P||R_{P2}||B_P||PK||T_{P1}) \overset{?}{=} V_{PUK_P}(Sig_{P1}). \tag{15}$$

The patient authenticates the doctor

The patient's authentication of the doctor can be shown by the assumptions and BAN logic, as follows:

By *M2* and the seeing rule, the following Statement 9 can be derived:

(Statement 9) $P \triangleleft (\{R_{D2}||ID_D||T_{D1}||Cert_D||SEK_1||PK\}_{PRK_D}, \{M_{DINF}||Cert_D||T_{D5}\}_{SEK_1})$.

By *A3, A4* and the freshness rule, the following Statement 10 can be derived:

(Statement 10) $P| \equiv \#(\{R_{D2}||ID_D||T_{D1}||Cert_D||SEK_1||PK\}_{PRK_D}, \{M_{DINF}||Cert_D||T_{D5}\}_{SEK_1})$.

By Statement 9, *A10, A15, A16* and the message meaning rule, the following Statement 11 can be derived:

(Statement 11) $P| \equiv D| \sim \#(\{R_{D2}||ID_D||T_{D1}||Cert_D||SEK_1||PK\}_{PRK_D}, \{M_{DINF}||Cert_D||T_{D5}\}_{SEK_1})$.

By Statement 10, Statement 11 and the verification rule, the following Statement 12 can be derived:

(Statement 12) $P| \equiv D| \equiv (\{R_{D2}||ID_D||T_{D1}||Cert_D||SEK_1||PK\}_{PRK_D}, \{M_{DINF}||Cert_D||T_{D5}\}_{SEK_1})$.

By Statement 12 and the belief rule, the following Statement 13 can be derived:

(Statement 13) $P| \equiv D| \equiv D \overset{SEK_1}{\leftrightarrow} P$.

By Statement 13, *A22* and the jurisdiction rule, the following Statement 14 can be derived:

(Statement 14) $P| \equiv D \overset{SEK_1}{\leftrightarrow} P$.

By Statement 14 and the belief rule, the following Statement 15 can be derived:

(Statement 15) $P| \equiv D| \equiv ID_D$.

By Statement 15, *A26* and the belief rule, the following Statement 16 can be derived:

(Statement 16) $P| \equiv ID_D$.

According to Statements 14 and 16, the patient's authentication of the doctor can be proved by using the Eq. 21 as follows:

$$(R_{D2}||ID_D||T_{D1}||Cert_D||SEK_1||PK) \stackrel{?}{=} V_{PUK_P}(Sig_{D1}). \tag{21}$$

The hospital's private cloud authenticates the doctor

The private cloud's authentication of the doctor can be shown by the assumptions and BAN logic as follows:

By *M3* and the seeing rule, the following Statement 17 can be derived:

(Statement 17) $HPC \triangleleft (\{PK||T_{D3}||ID_P||R_{D3}||R_{D1}\}_{PRK_D}, \{ID_P||ID_D||T_{D4}||Cert_D\}_{SEK_2})$.

By *A5*, *A6* and the freshness rule, the following Statement 18 can be derived:

(Statement 18) $HPC| \equiv \#(\{PK||T_{D3}||ID_P||R_{D3}||R_{D1}\}_{PRK_D}, \{ID_P||ID_D||T_{D4}||Cert_D\}_{SEK_2})$.

By Statement 17, *A11, A17, A18* and the message meaning rule, the following Statement 19 can be derived:

(Statement 19) $HPC| \equiv D| \sim \#(\{PK||T_{D3}||ID_P||R_{D3}||R_{D1}\}_{PRK_D}, \{ID_P||ID_D||T_{D4}||Cert_D\}_{SEK_2})$.

By Statements 18 and 19, and the verification rule, the following Statement 20 can be derived:

(Statement 20) $HPC| \equiv D| \equiv (\{PK||T_{D3}||ID_P||R_{D3}||R_{D1}\}_{PRK_D}, \{ID_P||ID_D||T_{D4}||Cert_D\}_{SEK_2})$.

By Statement 20 and the belief rule, the following Statement 21 can be derived:

(Statement 21) $HPC| \equiv D| \equiv HPC \overset{SEK_2}{\leftrightarrow} D$.

By Statement 21, *A23* and the jurisdiction rule, the following Statement 22 can be derived:

(Statement 22) $HPC| \equiv HPC \overset{SEK_2}{\leftrightarrow} D$.

By Statement 22 and the belief rule, the following Statement 23 can be derived:

(Statement 23) $HPC| \equiv D| \equiv ID_D$.

By Statement 23, *A27* and the belief rule, the following Statement 24 can be derived:

(Statement 24) $HPC| \equiv ID_D$.

According to Statements 22 and 24, the doctor's authentication of the patient can be proved by using the Eq. 37 as follows:

$$(PK||T_{D3}||ID_P||R_{D3}||R_{D1}) \overset{?}{=} V_{PUK_D}(Sig_{D3}). \tag{37}$$

The doctor authenticates the hospital's private cloud

The doctor's authentication of the private cloud can be shown by the assumptions and BAN logic as follows:

By *M4* and the seeing rule, the following Statement 25 can be derived:

(Statement 25) $D \triangleleft (\{PK||T_{HPC1}||ID_{HPC}\}_{PRK_{HPC}}, \{M_{EMR}||T_{HPC2}\}_{SEK_2})$.

By *A7*, *A8* and the freshness rule, the following Statement 26 can be derived:

(Statement 26) $D| \equiv \#(\{PK||T_{HPC1}||ID_{HPC}\}_{PRK_{HPC}}, \{M_{EMR}||T_{HPC2}\}_{SEK_2})$.

By Statement 25, *A12*, *A19*, *A20* and the message meaning rule, the following Statement 27 can be derived:

(Statement 27) $D| \equiv HPC| \sim \#(\{PK||T_{HPC1}||ID_{HPC}\}_{PRK_{HPC}}, \{M_{EMR}||T_{HPC2}\}_{SEK_2})$.

By Statements 26 and 27, and the verification rule, the following Statement 28 can be derived:

(Statement 28) $D| \equiv HPC| \equiv (\{PK||T_{HPC1}||ID_{HPC}\}_{PRK_{HPC}}, \{M_{EMR}||T_{HPC2}\}_{SEK_2})$.

By Statement 28 and the belief rule, the following Statement 29 can be derived:

(Statement 29) $D| \equiv HPC| \equiv HPC \overset{SEK_2}{\leftrightarrow} D$.

By Statement 29, *A24* and the jurisdiction rule, the following Statement 30 can be derived:

(Statement 30) $D| \equiv HPC \overset{SEK_2}{\leftrightarrow} D$.

By Statement 30 and the belief rule, the following Statement 31 can be derived:

(Statement 31) $D| \equiv HPC| \equiv ID_{HPC}$.

By Statement 31, *A28* and the belief rule, the following Statement 32 can be derived:

(Statement 32) $D| \equiv ID_{HPC}$.

According to Statements 30 and 32, the doctor's authentication of the patient can be proved by using the Eq. 43 as follows:

$$(PK||T_{HPC1}||ID_{HPC}) \overset{?}{=} S_{PRK_{HPC}}(Sig_{HPC1}). \tag{43}$$

User anonymity and unlinkability

During the patient visiting doctor (consultation) phase, the EMR search phase, and the diagnosis phase, information is transmitted via a public channel, and it is crucial that a patient's identity is secured against malicious attack. The proposed scheme encrypts these messages using public key operations by using the following Eqs. 12, 18, 25, 29, 34 and 40 as follows:

$$C_{P1} = E_{PUK_D}(ID_P||B_P||R_{P1}||R_{P2}||T_{P1}), \tag{12}$$

$$C_{D1} = E_{PUK_P}(ID_D||Cert_D||R_{D1}||R_{D2}||SEK_1||T_{D1}), \tag{18}$$

$$C_{D2} = E_{PUK_{PC}}(ID_P||T_{D2}||ID_D||Cert_D||ID_{DE}), \tag{25}$$

$$C_C = E_{PUK_D}(ID_{HPC}||ID_{DE}||T_C), \tag{29}$$

$$C_{D3} = E_{PUK_{HPC}}(Cert_D||T_{D3}||ID_D||R_{D3}||R_{D1}), \tag{34}$$

$$C_{HPC1} = E_{PUK_D}(ID_{HPC}||SEK_2||T_{HPC1}||R_{HPC2}), \tag{40}$$

and encrypts the transmitted messages by session keys by using the following Eqs. 23 and 45 as follows:

$$C_{P2} = E_{SEK_1}(M_{SD}, ID_P, T_{P2}), \tag{23}$$

$$C_{D4} = E_{SEK_2}(ID_P||ID_D||T_{D4}||Cert_D). \tag{45}$$

Because the messages are encrypted by public keys or session keys, attackers cannot obtain a patient's identity by intercepting the messages transmitted via a public channel. In addition, all messages have timestamps that change every session, thus encrypted messages with different timestamps can be identified, ensuring that malicious attackers cannot trace users. The proposed scheme, therefore, offers user anonymity and unlinkability.

Integrity

The patient visiting doctor (consultation) phase

The patient's signature Sig_{P1} can be verified by its public key by using the following Eqs. 13 and 15 as follows:

$$Sig_{P1} = S_{PRK_P}(R_{P1}||ID_P||R_{P2}||B_P||PK||T_{P1}), \tag{13}$$

$$(R_{P1}||ID_P||R_{P2}||B_P||PK||T_{P1}) \stackrel{?}{=} V_{PUK_P}(Sig_{P1}). \tag{15}$$

Thus, the doctor can ensure the integrity of the messages.

Meanwhile, the doctor's signature Sig_{D1} can be verified by its public key by using the following Eqs. 19 and 21 as follows:

Table 2 Proof of the non-repudiation offered by the proposed scheme

Evidence	Evidence issuer	Evidence holder	Verification equation
$Sig_{P1} = S_{PRK_P}(R_{P1}\|\|ID_P\|\|R_{P2}\|\|B_P\|\|PK\|\|T_{P1})$	Patient	Doctor	$(R_{P1}\|\|ID_P\|\|R_{P2}\|\|B_P\|\|PK\|\|T_{P1}) \stackrel{?}{=} V_{PUK_P}(Sig_{P1})$
$Sig_{D1} = S_{PRK_D}(R_{D2}\|\|ID_D\|\|T_{D1}\|\|Cert_D\|\|SEK_1\|\|PK)$	Doctor	Patient	$(R_{D2}\|\|ID_D\|\|T_{D1}\|\|Cert_D\|\|SEK_1\|\|PK) \stackrel{?}{=} V_{PUK_P}(Sig_{D1})$
$Sig_{D2} = S_{PRK_D}(S_D\|\|T_{D2}\|\|ID_P\|\|ID_{DE}\|\|ID_D)$	Doctor	Public cloud	$(S_D\|\|T_{D2}\|\|ID_P\|\|ID_{DE}\|\|ID_D) \stackrel{?}{=} V_{PUK_D}(Sig_{D2})$
$Sig_C = S_{PRK_C}(ID_{DE}\|\|S_{SD}\|\|ID_{HPC}\|\|T_C)$	Public cloud	Doctor	$(ID_{DE}\|\|S_{SD}\|\|ID_{HPC}\|\|T_C) \stackrel{?}{=} V_{PUK_C}(Sig_C)$
$Sig_{D3} = S_{PRK_D}(PK\|\|T_{D3}\|\|ID_P\|\|R_{D3}\|\|R_{D1})$	Doctor	Hospital's private cloud	$(PK\|\|T_{D3}\|\|ID_P\|\|R_{D3}\|\|R_{D1}) \stackrel{?}{=} V_{PUK_D}(Sig_{D3})$
$Sig_{HPC1} = S_{PRK_{HPC}}(PK\|\|T_{HPC1}\|\|ID_{HPC})$	Hospital's private cloud	Doctor	$(PK\|\|T_{HPC1}\|\|ID_{HPC}) \stackrel{?}{=} S_{PRK_{HPC}}(Sig_{HPC1})$

$$Sig_{D1} = S_{PRK_D}(R_{D2}||ID_D||T_{D1}||Cert_D||SEK_1||PK), \tag{19}$$

$$(R_{D2}||ID_D||T_{D1}||Cert_D||SEK_1||PK) \stackrel{?}{=} V_{PUK_P}(Sig_{D1}). \tag{21}$$

Thus, the patient can ensure the integrity of the messages.

The EMR search phase

The doctor's signature Sig_{D2} can be verified by its public key by using the following Eqs. 26 and 28 as follows:

$$Sig_{D2} = S_{PRK_D}(S_D||T_{D2}||ID_P||ID_{DE}||ID_D), \tag{26}$$

$$(S_D||T_{D2}||ID_P||ID_{DE}||ID_D) \stackrel{?}{=} V_{PUK_D}(Sig_{D2}). \tag{28}$$

Thus, the public cloud can ensure the integrity of the messages.

At the same time, public cloud's signature Sig_C can be verified by its public key by using the following Eqs. 30 and 32 as follows:

$$Sig_C = S_{PRK_C}(ID_{DE}||S_{SD}||ID_{HPC}||T_C), \tag{30}$$

$$(ID_{DE}||S_{SD}||ID_{HPC}||T_C) \stackrel{?}{=} V_{PUK_C}(Sig_C). \tag{32}$$

Therefore, the doctor can ensure the integrity of the messages, while the doctor's signature Sig_{D3} can be verified by its public key by using the following Eqs. 35 and 37 as follows:

$$Sig_{D3} = S_{PRK_D}(PK||T_{D3}||ID_P||R_{D3}||R_{D1}), \tag{35}$$

$$(PK||T_{D3}||ID_P||R_{D3}||R_{D1}) \stackrel{?}{=} V_{PUK_D}(Sig_{D3}). \tag{37}$$

Thus, the hospital's private cloud can ensure the integrity of the messages.

The private cloud's signature Sig_{HPC1} can be verified by its public key by using the following Eqs. 41 and 43 as follows:

$$Sig_{HPC1} = S_{PRK_{HPC}}(PK||T_{HPC1}||ID_{HPC}), \tag{41}$$

$$(PK||T_{HPC1}||ID_{HPC}) \stackrel{?}{=} S_{PRK_{HPC}}(Sig_{HPC1}). \tag{43}$$

Thus, the doctor can ensure the integrity of the messages. In the proposed scheme, all parties create a signature, and their authenticity is ensured by these signatures. Therefore, the proposed scheme meets the integrity requirement.

Non-repudiation

While all parties send messages, it is also important that no party can deny sending a message that they have sent. The proof of the non-repudiation offered by the proposed scheme is given in Table 2.

Forward and backward security

New random numbers are selected for session keys in every session, thus changing the session key by using the following Eqs. 17 and 39 for every session on the proposed scheme, as follows:

$$SEK_1 = h((S_D R_{P2} + r_6(R_{P1} + H(ID_P||B_P||R_{P1})PK))||r_6 R_{P2}), \tag{17}$$

$$SEK_2 = h((S_{HPC} R_{D3} + r_8(R_{D1} + h(ID_D||Cert_D||R_{D1})PK))||r_8 R_{D3}). \tag{39}$$

The encryptions in the proposed scheme are changed every session because it contains time stamps which change every session. The encrypted messages, which are caculated by using the following Eqs. 12, 18, 23, 29, 34, 40, 45 and 47 are as follows:

$$C_{P1} = E_{PUK_D}(ID_P||B_P||R_{P1}||R_{P2}||T_{P1}), \tag{12}$$

$$C_{D1} = E_{PUK_P}(ID_D||Cert_D||R_{D1}||R_{D2}||SEK_1||T_{D1}), \tag{18}$$

$$C_{P2} = E_{SEK_1}(M_{SD}, ID_P, T_{P2}), \tag{23}$$

$$C_{D2} = E_{PUK_{PC}}(ID_P||T_{D2}||ID_D||Cert_D||ID_{DE}), \tag{25}$$

$$C_C = E_{PUK_D}(ID_{HPC}||ID_{DE}||T_C), \tag{29}$$

$$C_{D3} = E_{PUK_{HPC}}(Cert_D||T_{D3}||ID_D||R_{D3}||R_{D1}), \tag{34}$$

$$C_{HPC1} = E_{PUK_D}(ID_{HPC}||SEK_2||T_{HPC1}||R_{HPC2}), \tag{40}$$

$$C_{D4} = E_{SEK_2}(ID_P||ID_D||T_{D4}||Cert_D), \tag{45}$$

$$C_{HPC2} = E_{SEK_2}(M_{EMR}||T_{HPC2}). \tag{47}$$

The timestamps in the encrypted messages and the random numbers in the session keys ensure that attackers cannot decrypt messages sent in the current session, and they cannot use messages from previous sessions as duplicate or replacement messages. For the same reason, if attackers obtain current messages, they cannot decrypt old messages. Therefore, the proposed scheme offers both forward and backward security.

Known attacks

Replay attack

The proposed scheme uses two forms of encryption, namely the public key operation, and the session key operation. Both are secure against replay attacks. In the public-key operation, all messages include a timestamp. The timestamps prevent replay attacks because the timestamp is different at any time, which means that encrypted messages are different for every session. The details of the public key operations which are computed by using the following Eqs. 12, 18, 25, 29, 34 and 40 are as follows:

$$C_{P1} = E_{PUK_D}(ID_P||B_P||R_{P1}||R_{P2}||T_{P1}), \tag{12}$$

$$C_{D1} = E_{PUK_P}(ID_D||Cert_D||R_{D1}||R_{D2}||SEK_1||T_{D1}), \tag{18}$$

$$C_{D2} = E_{PUK_{PC}}(ID_P||T_{D2}||ID_D||Cert_D||ID_{DE}), \tag{25}$$

$$C_C = E_{PUK_D}(ID_{HPC}||ID_{DE}||T_C), \tag{29}$$

$$C_{D3} = E_{PUK_{HPC}}(Cert_D||T_{D3}||ID_D||R_{D3}||R_{D1}), \tag{34}$$

$$C_{HPC1} = E_{PUK_D}(ID_{HPC}||SEK_2||T_{HPC1}||R_{HPC2}). \tag{40}$$

The session keys are also changed every session by the random number chosen. The session keys which are calculated by using the following Eqs. 17 and 39 are as follows:

$$SEK_1 = h((S_D R_{P2} + r_6(R_{P1} + H(ID_P||B_P||R_{P1})PK))||r_6 R_{P2}), \tag{17}$$

$$SEK_2 = h((S_{HPC} R_{D3} + r_8(R_{D1} + h(ID_D||Cert_D||R_{D1})PK))||r_8 R_{D3}). \tag{39}$$

The transmitted messages also contain timestamps. So, even if an attacker intercepts previous messages and sends them back to the current session, they will fail the verification, and communication will be terminated.

Man-in-the-middle attack

For an attacker to conduct a man-in-the-middle attack, they need to intercept transmitted messages. Then they will modify the intercepted message, and send the modified message to the destination party. However, all signatures in the proposed scheme involve a timestamp, the scheme uses public-key cryptography, and public and private keys. Therefore, the public key is used to encrypt the message, and the private key is used to sign the message. An attacker cannot modify a signature while it involves a private key, and cannot modify the timestamp. Therefore, they cannot conduct a man-in-the-middle attack, as it is not possible to successfully modify a message. The signatures which are computed by using the following Eqs. 13, 19, 26, 30, 35 and 41 are listed as follows:

$$Sig_{P1} = S_{PRK_P}(R_{P1}||ID_P||R_{P2}||B_P||PK||T_{P1}), \tag{13}$$

$$Sig_{D1} = S_{PRK_D}(R_{D2}||ID_D||T_{D1}||Cert_D||SEK_1||PK), \tag{19}$$

$$Sig_{D2} = S_{PRK_D}(S_D||T_{D2}||ID_P||ID_{DE}||ID_D), \tag{26}$$

$$Sig_C = S_{PRK_C}(ID_{DE}||S_{SD}||ID_{HPC}||T_C), \tag{30}$$

$$Sig_{D3} = S_{PRK_D}(PK||T_{D3}||ID_P||R_{D3}||R_{D1}), \tag{35}$$

Table 3 Comparison of the security attributes of the proposed scheme with those of other schemes

Security attack	Chiou et al. [13]	Mohit et al. [14]	Kumar et al. [15]	Li et al. [16]	The proposed scheme
Patient anonymity	No	No	Yes	No	Yes
Patient unlinkability	No	No	Yes	No	Yes
Doctor unlinkability	No	No	No	No	Yes
Mutual authentication	Yes	Yes	Yes	Yes	Yes
Data integrity	Yes	Yes	Yes	Yes	Yes
Data non-repudiation	Yes	Yes	Yes	Yes	Yes
Confidentiality	Yes	Yes	Yes	Yes	Yes
Availability	Yes	Yes	Yes	Yes	Yes
Replay attack	Yes	Yes	Yes	Yes	Yes
Man-in-the-middle attack	Yes	Yes	Yes	Yes	Yes
Impersonation attack	No	No	Yes	No	Yes

Table 4 Comparison of computation costs

Protocol	Chiou et al. [13]	Mohit et al. [14]	Kumar et al. [15]	Li et al. [16]	The proposed scheme
Patient visiting doctor phase	$1T_{Sign}+3T_P+2T_S+7T_H$	$1T_{Sign}+3T_S+11T_H$	$1T_{Sign}+3T_S+10T_H$	$1T_{Sign}+3T_S+11T_H$	$4T_{Sign}+4T_A+2T_S+2T_H$
Electrical medical record search phase	$3T_{Sign}+4T_M+8T_P+6T_S+18T_H$	$4T_{Sign}+4T_S+19T_H$	$4T_{Sign}+12T_S+20T_H$	$5T_{Sign}+10T_S+20T_H$	$8T_{Sign}+8T_A+4T_S+2T_H$
Diagnosis phase	$1T_{Sign}+2T_S+8T_H+2T_P$	$1T_{Sign}+2T_S+5T_H$	$1T_{Sign}+5T_S+10T_H$	$1T_{Sign}+2T_S+8T_H$	$2T_A$
Total cost	$5T_{Sign}+4T_M+13T_P$	$6T_{Sign}+9T_S+35T_H$	$6T_{Sign}+20T_S+40T_H$	$7T_{Sign}+15T_S+36T_H$	$12T_{Sign}+14T_A+6T_S+4T_H$

T_{Sign}: The time is taken to execute/verify a signature. T_A: The time is taken to calculate an asymmetric encryption/decryption operation. T_M: The time is taken to calculate a multiplication operation. T_P: The time is taken to calculate a bilinear pairing operation. T_S: The time taken to calculate a symmetric encryption/decryption operation. T_H: The time is taken to calculate a one-way hash function

$$Sig_{HPC1} = S_{PRK_{HPC}}(PK||T_{HPC1}||ID_{HPC}). \tag{41}$$

Impersonation attack

An impersonation attack occurs when an attacker poses as a legitimate party in order to access sensitive information.

(1) Impersonation of the patient

If an attacker can impersonate a legitimate user, then they can forge a Sig_{P1} message to appear as if it was sent by the patient. Sig_{P1} is computed by using the following Eq. 13 as follows:

Table 5 Communication cost comparison

Protocol	Chiou et al. [13]	Mohit et al. [14]	Kumar et al. [15]	Li et al. [16]	Our scheme
Patient visiting doctor phase	704 bits	592 bits	624 bits	592 bits	1456 bits
Electrical medical record search phase	3712 bits	3526 bits	1088 bits	1952 bits	3008 bits
Diagnosis phase	2122 bits	1184 bits	1300 bits	1232 bits	176 bits
Total cost	6528 bits	5312 bits	2912 bits	3776 bits	4640 bits
4G (100 Mbps)	6528/102,400 = 0.064 ms	5312/102,400 = 0.052 ms	2912/102,400 = 0.028 ms	3776/102,400 = 0.037 ms	4640/102,400 = 0.045 ms
5G (20 Gbps)	6528/20,480,000 = 0.319 us	5312/20,480,000 = 0.260 us	2912/20,480,000 = 0.142 us	3776/20,480,000 = 0.184 us	4640/20,480,000 = 0.227 us

$$Sig_{P1} = S_{PRK_P}(R_{P1}||ID_P||R_{P2}||B_P||PK||T_{P1}). \tag{13}$$

Even if the attacker knows the patient's public key, they still cannot forge Sig_{P1} since it is signed with the patient's private key.

(2) Impersonation of the hospital's private cloud

If an attacker can impersonate the hospital's private cloud, they can forge a Sig_{HPC1} message by receiving the C_{D3} and Sig_{D3} messages. Sig_{HPC1} is computed by using the following Eq. 41 as follows:

$$Sig_{HPC1} = S_{PRK_{HPC}}(PK||T_{HPC1}||ID_{HPC}). \tag{41}$$

However, even if the attacker obtains the private cloud's public key, they still cannot forge Sig_{HPC1} because it is signed with the original private cloud private key.

(3) Impersonation of the doctor

If an attacker can impersonate the doctor, then they can forge a Sig_{D1} message using the C_{P1} and Sig_{P1} messages. Sig_{D1} is computed by using the following Eq. 19 as follows:

$$Sig_{D1} = S_{PRK_D}(R_{D2}||ID_D||T_{D1}||Cert_D||SEK_1||PK). \tag{19}$$

However, even if the attacker knows the doctor's public key, they will still not be able to forge Sig_{D1} since it is signed with the doctor's private key. For the same reason, during the EMR search phase, the attacker may wish to forge the C_{D2}, Sig_{D2} and Sig_{D3} messages. Sig_{D2} and Sig_{D3} are computed by using the following Eqs. 26 and 35 as follows:

$$Sig_{D2} = S_{PRK_D}(S_D||T_{D2}||ID_P||ID_{DE}||ID_D), \tag{26}$$

$$Sig_{D3} = S_{PRK_D}(PK||T_{D3}||ID_P||R_{D3}||R_{D1}). \tag{35}$$

Thus, even if the attacker knows the doctor's public key, the attacker still cannot forge Sig_{D2} and Sig_{D3} since they are signed with the doctor's private key.

(4) Impersonation of the public cloud

If an attacker is able to impersonate the public cloud, then they can forge a Sig_C message according to the received C_{D2} and Sig_{D2} messages. Sig_C is computed by using the following Eq. 30 as follows:

$$Sig_C = S_{PRK_C}(ID_{DE}||S_{SD}||ID_{HPC}||T_C). \tag{30}$$

Even if the attacker can obtain the public cloud's public key, they will still be unable to forge Sig_C because it is signed with the public cloud's original private key.

It is therefore impossible for malicious attackers to successfully impersonate any party in the proposed scheme.

Discussion

Security comparison

Table 3 gives a comparison of the security attributes of the proposed scheme with those of other schemes.

This study found that the schemes proposed by Chiou et al. [13], Mohit et al. [14] and Li et al. [16] do not support patient anonymity and patient unlinkability, are not secure against impersonation attacks and do not support doctor unlinkability, while the proposed scheme can achieve all of these. We applied encryption and signature mechanism to protect transmitted messages, which guarantees confidentiality and integrity. Our proposed architecture is indeed applicable in real environments, which also fully ensures availability.

Computation cost

The computation cost of the proposed scheme is $12T_{Sign} + 14T_A + 6T_S + 4T_H$, which is higher than those of other schemes because it uses both asymmetric and symmetric encryption for improved security. Although other schemes require less execution time, they do have some related flaws, as there are some security requirements that they do not meet, such as patient anonymity, patient unlinkability, and doctor unlinkability. To sum up, the proposed scheme is more secure than others. Table 4 shows the computation cost comparison.

Communication cost

The communication cost comparison is shown in Table 5. This study adopts the approach described for the Mohit et al. scheme [14] to compute the communication cost. The proposed scheme incurs a communication cost lower than those of the schemes proposed by Chiou et al. and Mohit et al. [13], and higher than those of the schemes proposed by Kumar et al. and Li et al., because the proposed scheme uses signatures in every session, which incur a greater communication cost, but enables non-repudiation. The cost of communication at each stage was analyzed in a 4G environment, with a maximum transmission speed of 100 Mbps, and in a 5G environment, with a maximum transmission speed of 20 Gbps [39].

Conclusion

EMR security is a significant issue in current distributed EMR storage and sharing schemes, as it is crucial that any system be secure against malicious attacks. The scheme proposed in this study offers secure and efficient distributed sharing of EMR data between four parties using cloud computing technology and encryption, such as public-key operation, session key operation, and elliptic curve cryptography. The proposed scheme offers patient privacy during the consultation phase, ensures message integrity and non-repudiation, achieves mutual authentication between parties, offers authentication of medical resource sharing via cloud technology, and is secure against known attacks, thus providing a convenient and secure way to store, use and share medical information resources between hospitals, ensuring more efficient use of

medical information resources, and offering patients better and more timely diagnosis and treatment.

Acknowledgements
This work was supported by Asia University, Taiwan, and China Medical University Hospital, China Medical University, Taiwan, under Grant ASIA-108-CMUH-05 and ASIA-107-CMUH-05. This work was also supported by Asia University, Taiwan, UMY, Indonesian, under Grant 107-ASIA-UMY-02. This study is also supported by the Ministry of Science and Technology (MOST), Taiwan, Republic of China, under the Grants of MOST 108-2221-E-324-013 and MOST 107-2221-E-468-015.

Authors' contributions
C-LC and Y-YD have made substantial contributions to conception and design, involved in drafting the manuscript. P-TH and Y-CW have made the acquisition of data and analysis and interpretation of data. The critically important intellectual contents of this manuscript have been revised by H-CC. The corresponding authors are H-C Chen and Y-Y Deng. All authors read and approved the final manuscript.

Funding
This work was supported by the National Natural Science Foundation of China under Grants 61801413, by the Natural Science Foundation of Fujian Province of China under Grant 2017J05110, and by Education and Scientific Research Project for Young and Middle-aged Teachers in Fujian Province under Grant JAT160345.

Availability of data and materials
Not applicable.

Competing interests
The authors declare that they have no competing interests.

Author details
[1] School of Computer and Information Engineering, Xiamen University of Technology, Xiamen 361005, China. [2] School of Information Engineering, Changchun Sci-Tech University, Changchun 130600, China. [3] Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung 41349, Taiwan. [4] Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan. [5] Department of Medical Research, China Medical University Hospital, China Medical University, Taichung 40402, Taiwan. [6] National Museum of Marine Biology & Aquarium, Pingtung 94450, Taiwan.

Received: 7 May 2019 Accepted: 4 April 2020
Published online: 07 May 2020

References

1. World Health Organization. The top 10 causes of death. https://www.who.int/news-room/fact-sheets/detail/the-top-10-causes-of-death. Accessed 27 Dec 2018
2. Qi M, Chen J, Chen Y (2018) A secure biometrics-based authentication key exchange protocol for multi-server TMIS using ECC. Comput Methods Progr Biomed 164:101–109
3. Masdari M, Ahmadzadeh S (2017) A survey and taxonomy of the authentication schemes in Telecare Medicine Information Systems. J Netw Comput Appl 87:1–19
4. Puthal D, Ranjan R, Nanda A, Nanda P, Jayaraman PP, Zomaya AY (2019) Secure authentication and load balancing of distributed edge datacenters. J Parallel Distrib Comput 124:60–69
5. Iribarren SJ, Brown W III, Giguere R, Stone P, Schnall R, Staggers N, Carballo-Diéguez A (2017) Scoping review and evaluation of SMS/text messaging platforms for mHealth projects or clinical interventions. Int J Med Inform 101:28–40
6. Song R (2010) Advanced smart card based password authentication protocol. Comput Stand Interfaces 32(5–6):321–325
7. Chatterjee S, Roy S, Das AK, Chattopadhyay S, Kumar N, Reddy AG, Park Y (2017) On the design of fine grained access control with user authentication scheme for telecare medicine information systems. IEEE Access 5:7012–7030
8. Amin R, Islam SH, Biswas GP, Khan MK, Kumar N (2018) A robust and anonymous patient monitoring system using wireless medical sensor networks. Future Gener Comput Syst 80:483–495
9. Mohit P, Amin R, Biswas GP (2017) Design of authentication protocol for wireless sensor network-based smart vehicular system. Veh Commun 9:64–71
10. Wazid M, Das AK, Kumari S, Li X, Wu F (2016) Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS. Secur Commun Netw 9(13):1983–2001
11. Sutrala AK, Das V, Odelu M, Wazid M, Kumari S (2016) Secure anonymity-preserving password-based user authentication and session key agreement scheme for telecare medicine information systems. Comput Methods Progr Biomed 135:167–185
12. Chen CL, Yang TT, Shih TF (2014) A secure medical data exchange protocol based on cloud environment. J Med Syst 38(9):112
13. Chiou SY, Ying Z, Liu J (2016) Improvement of a privacy authentication scheme based on cloud for medical environment. J Med Syst 40(4):101
14. Mohit P, Amin R, Karati A, Biswas GP, Khan MK (2017) A standard mutual authentication protocol for cloud computing based health care system. J Med Syst 41(4):50

15. Kumar V, Jangirala S, Ahmad M (2018) An efficient mutual authentication framework for healthcare system in cloud computing. J Med Syst 42(8):142
16. Li CT, Shih DH, Wang CC (2018) Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. Comput Methods Progr Biomed 157:191–203
17. Moon AH, Iqbal U, Bhat GM (2016) Implementation of node authentication for WSN using hash chains. Procedia Comput Sci 89:90–98
18. Chaturvedi A, Mishra D, Mukhopadhyay S (2017) An enhanced dynamic ID-based authentication scheme for telecare medical information systems. J King Saud Univ-Comput Inf Sci 29(1):54–62
19. Amin R, Islam SH, Gope P, Choo KKR, Tapas N (2018) Anonymity preserving and lightweight multimedical server authentication protocol for telecare medical information system. IEEE J Biomed Health Inform 23(4):1749–1759
20. Chen L, Lee WK, Chang CC, Choo KKR, Zhang N (2019) Blockchain based searchable encryption for electronic health record sharing. Future Gener Comput Syst 95:420–429
21. Sureshkumar V, Amin R, Vijaykumar VR, Sekar SR (2019) Robust secure communication protocol for smart healthcare system with FPGA implementation. Future Gener Comput Syst 100:938–951
22. Soni P, Pal AK, Islam SH (2019) An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system. Comput Methods Progr Biomed 182:105054
23. Azeez NA, Vyver CVD (2019) Security and privacy issues in e-health cloud-based system: a comprehensive content analysis. Egypt Inform J 20(2):97–108
24. Tanwar S, Parekh K, Evans R (2020) Blockchain-based electronic healthcare record system for healthcare 4.0 applications. J Inf Secur Appl 50:102407
25. Lin B, Guo W, Xiong N, Chen G, Vasilakos AV, Zhang H (2016) A pretreatment workflow scheduling approach for big data applications in multicloud environments. IEEE Trans Netw Serv Manage 13(3):581–594
26. Yang Y, Zheng X, Chang V, Ye S, Tang C (2018) Lattice assumption based fuzzy information retrieval scheme support multi-user for secure multimedia cloud. Multimed Tools Appl 77(8):9927–9941
27. Yang Y, Ma M (2016) Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for E-Health clouds. IEEE Trans Inf Forensics Secur 11(4):746–759
28. Guo L, Shen H (2017) Efficient approximation algorithms for the bounded flexible scheduling problem in clouds. IEEE Trans Parallel Distrib Syst 28(12):3511–3520
29. Liao YP, Hsiao CM (2014) A secure ECC-based RFID authentication scheme integrated with ID-verifier transfer protocol. Ad Hoc Netw 18:133–146
30. Odelu V, Das AK, Goswami A (2015) An efficient ECC-based privacy-preserving client authentication protocol with key agreement using smart card. J Inf Secur Appl 21:1–19
31. Yeh HL, Chen TH, Shih WK (2014) Robust smart card secured authentication scheme on SIP using elliptic curve cryptography. Comput Standards Interfaces 36(2):397–402
32. Shankar SK, Tomar AS, Tak GK (2015) Secure medical data transmission by using ECC with mutual authentication in WSNs. Procedia Comput Sci 70:455–461
33. Roy S, Das AK, Chatterjee S, Kumar N, Chattopadhyay S, Rodrigues JJ (2018) Provably secure fine-grained data access control over multiple cloud servers in mobile cloud computing based healthcare applications. IEEE Trans Ind Inf 15(1):457–468
34. Gope P, Das AK (2017) Robust anonymous mutual authentication scheme for n-times ubiquitous mobile cloud computing services. IEEE Internet Things J 4(5):1764–1772
35. Odelu V, Das AK, Kumari S, Huang X, Wazid M (2017) Provably secure authenticated key agreement scheme for distributed mobile cloud computing services. Future Gener Comput Syst 68:74–88
36. Wazid M, Das AK, Kumari S, Li X, Wu F (2016) Provably secure biometric-based user authentication and key agreement scheme in cloud computing. Secur Commun Netw 9(17):4103–4119
37. Chandrakar P, Om H (2017) A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC. Comput Commun 110:26–34
38. Van OP (1993) Extending cryptographic logics of belief to key agreement protocols. In: Proceedings of the 1st ACM conference on computer and communications security, ACM, pp 232–243
39. Marcus MJ (2015) 5G and IMT for 2020 and beyond. IEEE Wirel Commun 22(4):2–3

Publisher's Note