Journal of Information Security and Applications 63 (2021) 102992

Contents lists available at ScienceDirect

Journal of Information Security and Applications

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

An efficient mutual authentication and privacy prevention scheme for e-healthcare monitoring

Prerna Mohit

Department of Computer Science and Engineering, Indian Institute of Information Technology Senapati, Manipur, India

ARTICLE INFO

Keywords:
Mutual authentication
Body sensor network
TMIS
BAN logic
ROR model

ABSTRACT

The progressive development in online healthcare monitoring may facilitate better service for recovered patients from some pandemic diseases like the novel Covid-19 and even in well-known diseases such as cancer, heart attack, and many more. This paper brings a mutual authentication protocol for the e-healthcare monitoring system using the telecare medical information system with body sensors. This scheme comes with a secure platform for communication by using three phases: patient data upload phase, treatment phase, and report delivery phase. The patient's medical information is susceptible and must be protected from any modification. The two security issues (secure communication and privacy of patient information) are essential for the transmission over the public channel. The proposed protocol uses mobile characteristics that allow the recovered patients to use medical facilities effectively. The well-known traditional informal security analysis like the Man-in-the-middle attack, patient anonymity, doctor anonymity, and many more are validated to judge the security aspect of the proposed protocol. In addition, the widely accepted formal security analysis (both Burrows–Abadi–Needham (BAN) logic and Real-or-Random Model (ROR)) are investigated for the session-key security. Finally, the proposed e-healthcare monitoring protocol provides an efficient characteristic in terms of communication, computation, and storage cost compared to existing literature.

1. Introduction

In this current digital world, health monitoring becomes a challenging task for some pandemic diseases such as current COVID-19, influenza, swine flu (H1N1 virus), Ebola, and many more in the last few decades. To ease the medical facilities through the telecare medical information system (TMIS) in remote areas with the help of the internet provides a sharp reduction in patient travel time and medical expenditure. With the advances in TMIS by employing various healthcare applications in the domain of Cloud Environment [1–4], Internet of Things platform [5–7], Wearable Devices [8,9], Wireless Body Area Network (WBAN) [10,11], Wireless Medical Sensor Network [12,13] are extensively focused in literature. Among the various applications, the cloud environment-based TMIS has received significant interest in the e-medical system. The proper communication (direct or indirect) between patient and doctor is made through cloud computing environment as a public cloud. It may have some security issues due to third party involvement [14,15]. To overcome this problem, we have designed an advance mutual authentication and privacy prevention technique using the private cloud for e-healthcare monitoring of recovered patients from any particular diseases. The proposed system has less complexity in addition to other ones and uses only three phases along with registration as patient data upload phase, treatment phase, report delivery phase. The operational functionality of the e-healthcare monitoring utilizes fundamental cryptography modules like concatenation, XOR operation, hash function, and symmetric encryption for the protection of message and session key. To provide confidentiality along with authentication, a digital signature mechanism is used before sending the encrypted message/report of the patient. Continuous observation of the patient's biological changes and corresponding physiological data are examined by the doctor/medical staff for a few and more years. Hence, recovered patients are properly monitored by the health professionals. The proposed scheme uses mobile device, body sensor, and healthcare private cloud through which patients and doctors can securely communicate with each other in real time intervals via the internet without the physical appearance of patient in hospital. Thus, the recovered patient may easily access the medical facility through TMIS. Moreover, security in message exchange and other entities is considered a critical concern in this proposed scheme. These issues for communications over a public channel can be smoothly handled by using secure mutual authentication and key agreement scheme for data integrity, confidentiality, and availability for the TMIS.

E-mail address: prernamohit@outlook.com.

https://doi.org/10.1016/j.jisa.2021.102992

Available online 13 October 2021

1.1. Motivation and contributions

Security and privacy are the two major issues in most applications such as Big data [16,17], healthcare [8,18], WSN [19,20], cloud [21,22] vehicular communication [23,24] and many more where information follows an unreliable channel. An authentication protocol plays an important role in these applications. Several user authentication schemes are enriched in the scientific literature with different environments and applications. Among them, healthcare application improvement becomes a trend to upgrade the current health care solution with a new authentication protocol for monitoring recovered patients after treatment from severe disease. To develop a new healthcare monitoring system, the author has proposed a scheme with the following contributions:

- *Mutual authentication* is achieved between patient and healthcare in which healthcare and doctor have to strengthen the security for transmitting or receiving information.
- *Patient anonymity* is also supported during data transmission by hiding the real identity of the patient.
- The protocol resists strong security attacks like security against patient *anonymity, non-repudiation,* and *confidentiality* of data.
- The authentication workability of the proposed scheme is validated with the help of BAN logic and ROR model that yields mutual authentication and session key agreement securely.
- A comparative analysis of our proposed protocol with other existing protocols is depicted with minimum *communication and computation overheads*.

1.2. Road map of the paper

The rest of this article is organized as follows: Section 2 reviews a complete survey of recent related work. In Section 3, the description of system models in terms of network, cryptographic models are outlined. Section 4 presents a detailed description of the proposed protocol. Both informal and formal security analysis are discussed in Section 5 and Section 6 respectively. Section 7 presents the performance analysis of the proposed scheme and its comparison with the existing protocols. Finally, this paper ends with concluding remarks in Section 8.

2. Related works

A wide array of research has been performed in the field of healthcare [25–33]. An interesting authentication scheme proposed by [25] facilitates medical service to the patient using smart card and password based authentication for TMIS. The pre-computing phase is used to avoid the time-consumption expenses with the rapid development of technologies. In 2012, [26] demonstrated an improvement over the scheme of [25] in terms of impersonation, insider, and stolen smart card attack. In the same year, [27] found that both [25,26] scheme failed against some common attacks and improved these schemes to a single protocol. However, [28] showed the pitfall of [27] protocol and resolved the technical flaws like online password guessing attack, the inefficacy of the password change phase, traceability of user's stolen smart card, and denial-of-service. [29] proposed an ECC-based user authentication and key agreement protocol using smart card for TMIS to fix the flip side of [30] in server impersonation attack, smart card theft attack and session key disclose attack. Then, [31] proposed improvement of the [29] in terms of privileged-insider, user impersonation, and strong reply attacks. In 2016, [34] proposed a lightweight authentication scheme for wearable devices to combine with sensor networks as a wireless body area network. [32] found that the scheme is vulnerable to impersonation attack, denial-of-service attack, and stolen-verifier attack and proposed a new scheme. However, [33] identified that [32] authentication scheme has some security weaknesses such as perfect forward secrecy, lack of no key control, and clock synchronization. In addition, [33] also suggested a new protocol to remove the drawbacks mentioned above [32].

Literature survey states numerous protocols with significant concern towards the security of user identity when it is openly transmitted over insecure channel [35–39]. Thus, it is very much essential in healthcare applications to preserve the anonymity of patients from attackers. Hence, [40] have reported an elliptic–curve-cryptosystem (ECC) based authentication scheme to ensure user anonymity. [41] also proposed a biometrics-based authentication scheme for a multi-server environment to provide user anonymity. [42] proposed a certificate less pairing-free authentication scheme for wireless body area network, which also supports patient anonymity. [33] presented an elliptic curve cryptography based authentication protocol to preserve user anonymity.

Moreover, in recent years numerous medical-based authentication protocols are enriched in literature where the treatment of patients is done online through TMIS [1–4,43–47]. In 2014, [43] a medical data exchange protocol based on a cloud environment was proposed by incorporating the importance of confidentiality and authentication of patients. Initially, they suggested their scheme is free from traditional attacks and uses symmetric/asymmetric encryption, digital signature, and pairing-based technology. In the same year, [44] proposed an advance scheme over the first one with an emergency condition. In 2016, [45] pointed out that both the protocol of [43,44] have some flip side as common security problems like patient anonymity and identification of real telemedicine. To discard common security faults of [44,45] demonstrated an improvement in the [44] scheme and claim that the protocol does not provide anonymity, unlinkability, and message authentication. To overcome the issue of [45], a standard healthcare authentication protocol has been developed by [46] for the healthcare system. This scheme enables a design free from patient anonymity and mobile device verifier attacks. Furthermore, [1] developed an improved authentication protocol over [46]. Then, [2] proposed an authentication protocol for the same domain using ECC encryption for TMIS. To overcome the security weaknesses of [1] scheme such as patient anonymity attack, impersonation attack, message authentication, session key security, and patient unlinkability. In the same year, [3] have also proposed an authentication protocol for cloud-based e-healthcare monitoring of patients but the system is vulnerable to patient unlikability, impersonation attack, data non-repudiation. Then, [47] proposed an authentication protocol for smart devices using ECC by a combining public and private cloud for the healthcare application, unfortunately it does not resist clock synchronization problems. In the same year, [4] proposed a cloud-based secure framework for a smart medical system using ECC cryptography. [48] proposed an improved anonymous authentication protocol for wearable health monitoring systems, and [12] proposed a secure and lightweight healthcare authentication scheme for a patient using wireless body area networks. A brief comparative summary of the relevant healthcare-based protocol has been inserted in Table 1 with their description and drawback. As per the above intensive literature survey, most of the schemes proposed for healthcare uses the public cloud by employing a patient's mobile for communication of data to healthcare/cloud using body sensor. Some articles consist of various known attacks termed as patient/user anonymity, patient unlikability, and impersonation attacks. Hence, the author has proposed a private-cloud-based protocol for the monitoring of recovered patients. The heart of the proposed e-healthcare monitoring protocol is three phases with registration that makes the protocol light-weighted. The functional behavior along with the security analysis is well established and verified with formal and informal security.

3. System models

This section includes an overview of the network, attack, and cryptographic model for the proposed protocol. The useful symbol and notations are tabulated in Table 2.

Table 1
Brief summary of cloud related authentication scheme for e-healthcare.

Scheme	Description	Drawback
Chen et al. [43]	A secure medical data exchange protocol for electronic medical records based on cloud environment using Bilinear pairing.	Vulnerable to impersonation attack, patient anonymity, and known-key security attack.
Chen et al. [44]	A privacy authentication scheme based on cloud environment for the medical system with bilinear pairing, elliptic curve cryptography.	Design issues in message authentication and patient anonymity. Also limited to support real telemedicine and interactive medical facilities.
Chiou et al. [45]	Medical information sharing scheme implemented in the android system with one-way cryptographic hash function.	Failed to provide stolen mobile device attack, patient anonymity, patient unlinkability, and doctor unlinkability.
Mohit et al. [46]	A lightweight authentication protocol for TMIS in the cloud environment based on one-way cryptographic hash function.	It does not provide patient unlinkability, impersonation attack, and patient anonymity.
Li et al. [1]	A cloud-assisted authentication and privacy preservation scheme for TMIS with one-way cryptographic hash function.	Unable to provide impersonation attack, message authentication, patient anonymity, and session-key security.
Kumar et al. [2]	The protocol is an improvement of [1] protocol using elliptic curve cryptography.	Does not resist clock synchronization problem.
Chandrakar et al. [3]	E-healthcare monitoring system based on public cloud environment with seven phases, using one-way cryptographic hash function.	Vulnerable to patient unlikability, impersonation attack, data non-repudiation.
Chen et al. [47]	Secure electronic medical record(EMR) authentication protocol with elliptic curve cryptography.	Does not resist clock synchronization problem.
Kumari et al. [4]	ECC based smart medical system in cloud environment with six phases using elliptic curve cryptography.	Does not resist clock synchronization problem.
Proposed scheme	An efficient and lightweight e-healthcare monitoring system with three phases for the complete security of the patient. Using one-way cryptographic hash function.	Communication cost is slightly greater than [46].

Table 2
Frequently used symbol in protocol.

Symbol	*Description*
$E_x(m)$	Message m encrypted with secret key x
$D_x(m)$	Message m decrypted with secret key x
ID_i	Identity of entity i
NID	Pseudo-random Identity of Patient
PU_i	Public key of i
PR_i	Private key of i
SK_{xy}	Session key between x and y
$H(.)$	160-bits cryptographic hash function.
$X \parallel Y$	X concatenate with Y
$X \overset{?}{=} Y$	Whether X equal Y or not
$X \oplus Y$	Bitwise XOR operation
$S_k(m)$	Digital Signature on message m using key k
$V_k(m)$	Verification of m using key k
K_{xy}	Secret key between x and y
K_x	Secret key of x
K_H	Secret key of healthcare
MD_x	Message digest of x
PS	Secret key between patient and healthcare
Pw	Password of doctor
R_i	Random number generated by i
sn_i	sequence number of ith patient
Sig_i	Signature of i
$Report_i$	Report generated by sensors
$Data_i$	Medical data of patient given by i
$Gen(.)/Rep(.)$	Generate/Reproduce function of Fuzzy Extractor
$\mathcal{A}y$	An Adversary

Table 3
Patient's report.

Report	*Description*
$Report_1$	ECG (Electrocardiography)
$Report_2$	Blood pressure
$Report_3$	EMG (Electromyography)
$Report_4$	Body Temperature
$Report_5$	EEG (Electroencephalography)

3.1. Network model

The proposed architecture involves five entities for proper communication namely (1) Patient: A user/person that needs medical service, (2) Doctor: A person who provides medical consultation, (3) Healthcare: The organization/place where patient gets treatment, (4) Private cloud of healthcare: The place where healthcare stores the data of patient and (5) Body Sensor: A device that collects data from the body of patient. The complete architecture is shown in Fig. 1 with their phase execution. A brief explanation of the network model is described below as:

- The recovered patient goes out of healthcare after successful treatment by his/her medical staff such as doctors, nurses, etc. The patient has a file that contains description of the disease with a unique number that will be shared between healthcare and patient only (say PS_i). This file also carries the identity of healthcare and doctor (ID_H, ID_D) with whom treatment is going on. In addition, healthcare provides the patient's identity (ID_P) with the pseudo-random identity of patient (NID) to doctors, which also informs the doctor about the patient.
- There are two types of patients: one with embedded body sensors on the patient's body and another without any sensor. The patient without body sensors has to come to healthcare for regular check-ups.
- Patients with body sensors embedded in their body have to collect the health report of the patients and transfer it to a patient mobile device (securely) on regular basis. A medical report ($Report_i$) viz. ECG, Blood pressure, EMG, Body Temperature, EEG, and a few more can be generated for the patient using body sensors. The sample of the patient's report is shown in Table 3.
- After that, the recovered patient (with sensor) uploads a newly generated report by body sensor to the healthcare.
- Patients without body sensors have to physically appear to healthcare for routine check-ups. Hence, monitoring such patients might be performed in online mode. But, the patient has to provide the current report (maybe from some diagnostic center) to healthcare.
- Healthcare saves the information in its private cloud and sends the old and new report of the patient to the respective doctor to whom the patient wants to consult.
- The doctor prescribes treatment by looking into the report, uploading the new report with its digital signature, and sending it to the healthcare.
- Then, healthcare sends the final report to the patient, which contains the patient's treatment by the doctor and further saves the data in its private cloud for future use.

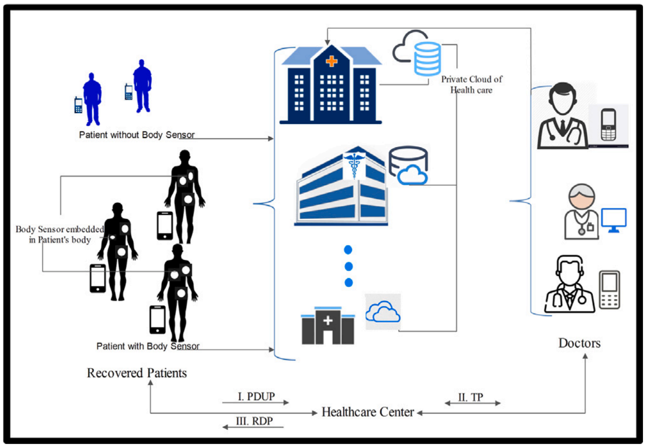

Private Cloud of Health care
Patient without Body Sensor
Body Sensor embedded in Patient's body
Patient with Body Sensor
Recovered Patients
Doctors
I. PDUP
II. TP
III. RDP
Healthcare Center

Fig. 1. Architecture of proposed protocol with different phases: I. PDUP → Patient Data Upload Phase, II.TP → Treatment Phase, III. RDP → Report Delivery Phase.

Note: The involvement of three-party (patient, doctor, and healthcare) makes a complete core of the proposed authentication scheme for e-healthcare monitoring. Healthcare plays a significant role in authenticating the patient with the concerned doctor. After successful authentication, the patient sends medical data to healthcare. Then, the healthcare sends the updated patient data to the concerned doctor, where the doctor verifies the authenticity of healthcare, and after successful verification, the doctor performs the treatment. Finally, the doctor sends the updated report of the patient to the healthcare, where healthcare again verifies the doctor. Hence, patients, healthcare, and doctors are the three main entities involved in the proposed (three-party) scheme.

3.2. Attack model

The attack model for the proposed system involves the widely-recognized Dolev and Yao threat model [49]. This model permits two end-users to communicate over an insecure channel, where the adversary $\mathcal{A}y$ can intercept the spoken message (Passive attack). In addition, the $\mathcal{A}y$ has access to manage the transmitted message. The accessibility of these messages during the communication by the $\mathcal{A}y$ may be in the form of reading, modify, delete, insert, and a few more (Active attack). Hence, both active and passive attacks among the communicating parties (example: Patient, healthcare, and doctor) in the proposed authentication protocol associate untrustworthy nodes.

3.3. Cryptographic models

A brief introduction of the cryptography models such as one-way hash function and encryption technology are described in this section.

3.3.1. One-way hash function

A hash function maps a string of arbitrary length to a fixed-length string called the *message digest*. It can be characterized as: $H : A \to B$, where $A = \{0,1\}^*$, and $B = \{0,1\}^n$. The (A, B) are binary strings of arbitrary length and fixed length (n) respectively. It is used in many cryptographic applications such as digital signature, random sequence generators in key agreement, and many more.

3.3.2. Encryption technique

Symmetric encryption technique uses one key for encryption/decryption operation where the asymmetric encryption involves a public key for encryption and a private key for decryption. These two keys are mathematically connected based on some challenging problems. The symmetric encryption is faster and less complex compared to the asymmetric technique [50]. Hence, the proposed design follows the symmetric encryption technique.

4. Proposed protocol

The proposed protocol brings a mutual authentication with session-key for e-healthcare monitoring employing TMIS, where the patient can get medical treatment online without the physical appearance in the healthcare. In this section, a complete description of associated phases has described the workability of the e-monitoring system. The careful treatment after the registration phase is monitored by the body sensor along with the following three phases as below:

- Patient Data Upload Phase (PDUP): Communication between patient and healthcare.
- Treatment Phase (TP): Communication between healthcare and doctor in both directions.
- Report Delivery Phase (RDP): Communication between healthcare and patient.

The involvement of Patient–Healthcare–Doctor makes the protocol a three-party scheme. Fig. 2 shows a brief description of message payloads in terms of patient data (m_B), healthcare data (m_H), and treatment data (m_D). The data collected by the mobile device is the updated report of the patient obtained by the body sensor. This data belongs to the sample of patient data. This $Data_i$ may be used to specify a particular disease from which the patient (P_i) is suffering. First, the body sensor forwards this data to healthcare as $Data_B$ with patient identity ID_P in PDUP. Then, healthcare sends the old patient data stored in private cloud $Data_H$ with received data $Data_B$ to the doctor as healthcare data (m_H). Here, the doctor performs treatment based on the $Data_H$, $Data_B$, and generates a new report as doctor's/treated data $Data_D$. Hence, treatment phase data contains $(ID_D, Data_H, Data_B, Data_D)$. After the treatment phase, this data needs to be sent back to the patient by healthcare.

4.1. Registration phase

The patient and doctor must have to register themselves with the healthcare before performing the e-healthcare monitoring process.

4.1.1. Patient registration

The recovered patients have to register themself with healthcare. The process of patient registration is shown in Fig. 3 and the following steps are involved:

Step 1. Patient inputs his/her identity (ID_P), pseudo-random identity (NID), imprints biometrics (BIO_P) such as fingerprint, iris, and calculates the one-way hash function using the secret key given by healthcare during the release of the patient as $p = H(PS)$. Then, it generate a function $Gen(.)$ called fuzzy extractor [51] as $Gen(BIO_P) = (\theta_i, U_i)$, $PB = H(ID_P \parallel \theta_i)$. Finally, the patient sends $\langle ID_P, p, PB \rangle$ to healthcare via a secure channel.

Step 2. The healthcare receives the patient message and computes $p' = H(PS)$. If healthcare finds $p' \overset{?}{=} p$; it stores the received values in its private cloud. After that, it chooses a random number q and computes $A = q \oplus PB$, $B = A \oplus H(K_H)$. Moreover, healthcare sends its identity with A, B to the patient via a secure channel.

Step 3. Then, the patient computes the value of $q = A \oplus PB$. Finally, the value of A, q, B are stored in the Patient's mobile device.

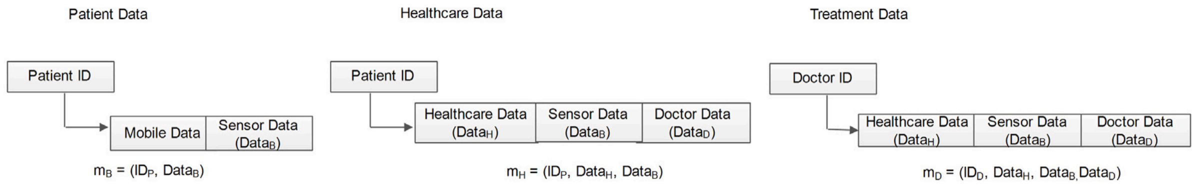


Fig. 2. Message payload of different data structure.

Patient (P)		**Healthcare** (HC)
Input ID_P, BIO_P, NID		
$p = H(PS)$		
$Gen(BIO_P) = (\theta_i, U_i)$		
$PB = H(ID_P \parallel \theta_i)$	$\xrightarrow[\text{(secure channel)}]{< ID_P, NID, p, PB >}$	
		$p' = H(PS)$
		$p' \overset{?}{=} p$
		select a random numbers q
		$A = q \oplus PB$
		$B = A \oplus H(K_H)$
	$\xleftarrow[\text{(secure channel)}]{< ID_H, A, B >}$	
$q = A \oplus PB$		

Fig. 3. Patient Registration..

Doctor (D)		**Healthcare** (HC)
Input ID_D, b		
$RPw = H(ID_D \parallel b)$		
	$\xrightarrow[\text{(secure channel)}]{< ID_D, RPw >}$	
		Input ID_H, a
		$HH = H(ID_D \parallel ID_H)$
		$HA = HH \oplus a$
	$\xleftarrow[\text{(secure channel)}]{< ID_H, HA >}$	
$HH = H(ID_D \parallel ID_H)$		
$a = HH \oplus HA$		

Fig. 4. Doctor Registration.

4.1.2. Doctor registration

The doctor has to register himself with the healthcare to perform the online treatment of the patient. The process of doctor registration is shown in Fig. 4, which involves two steps:

Step 1. Doctor inputs its identity ID_D, computes $RPw = H(ID_D \parallel b)$, where b is a random number, and sends $\langle ID_D, RPw \rangle$ to the healthcare via a secure channel.

Step 2. After receiving $\langle ID_D, RPw \rangle$ the healthcare inputs its identity ID_H and computes $HH = H(ID_D \parallel ID_H)$, $HA = HH \oplus a$, where a is a random number and sends $\langle ID_H, HA \rangle$ to doctor via a secure channel.

Step 3. On receiving the message $\langle ID_H, HA \rangle$, the doctor computes values of HH as $H(ID_D \parallel ID_H)$ and $a = HH \oplus HA$.

4.2. Patient Data Upload Phase (PDUP)

In PDUP, the body sensor embedded in the patient's body has to collect the data and sends it to the patient mobile device. The process of PDUP is described in Fig. 5 and follows the following steps:

Step 1. The healthcare initializes the process by asking the patient to send the updated patient report (m_B).

Step 2. The patient gets health information $(Data_B)$ from the body sensor via mobile phone. So, the patient inputs his/her identity (ID_P), imprints biometrics (BIO_P) into the terminal and calculates $Rep(BIO_P, U_i) = \theta_i$, $PB = H(ID_P \parallel \theta_i)$, $q' = A \oplus PB$ and check whether $q' \overset{?}{=} q$. Then, the patient generates a random number R_P, calculates $F_1 = B \oplus PB$, $F_2 = NID \oplus R_P$, $S_0 = H(ID_P \parallel R_P \parallel q')$, encrypts $C_0 = E_p[S_0, F_1, F_2]$, and sends message $M_1 = \langle C_0 \rangle$ to healthcare via an insecure channel.

Step 3. After receiving M_1, healthcare decrypts $D'_p[C_0] = \{S_0, F_1, F_2\}$ using the key p, computes $q = F_1 \oplus H(K_H)$, $R_P = NID \oplus F_2$, $G = H(ID_P \parallel R_P)$, $S'_0 = H(ID_P \parallel R_P \parallel q)$, and checks whether $S'_0 \overset{?}{=} S_0$, if

Patient (P)		**Healthcare** (HC)
	$\xleftarrow{\text{Ask to send } m_B}$ (insecure channel)	
$m_B = (ID_P, Data_B)$ Input ID_P, BIO_P $Rep(BIO_P, U_i) = \theta_i$ $PB = H(ID_P \| \theta_i)$ $q' = A \oplus PB$ $q' \overset{?}{=} q$ Generate a random number R_P $F_1 = B \oplus PB$ $F_2 = NID \oplus R_P$ $S_0 = H(ID_P \| R_P \| q)$ $C_0 = E_p[S_0, F_1, F_2]$		
	$\xrightarrow{M_1 =< C_0 >}$ (insecure channel)	
		$D_p[C_0] = S_0, F_1, F_2$ $q = F_1 \oplus H(K_H)$ $R_P = NID \oplus F_2$ $S'_0 = H(ID_P \| R_P \| q)$ $S'_0 \overset{?}{=} S_0$ $G = H(ID_P \| R_P)$ Generate a random number R_H $S_1 = H(ID_H \| R_H \| q)$ $I = sn \oplus q$ $F_3 = R_P \oplus R_H$ $C_1 = E_G[S_1, I, F_3]$
	$\xleftarrow{M_2 =< C_1 >}$ (insecure channel)	
$G' = H(ID_P \| R_P)$ $D_{G'}[C_1] = S_1, I, F_3$ $R_H = R_P \oplus F_3$ $S'_1 = H(ID_H \| R_H \| q)$ $S'_1 \overset{?}{=} S_1$ $sn' = q' \oplus I$ $SK_{PH} = H(ID_P \| ID_H \| R_P \| R_H \| S'_1)$ $K_{PD} = H(ID_P \| ID_D \| sn')$ $C_P = E_{K_{PD}}(Data_B)$ $Sig_P = S_{PR_P}(MD_B)$ $K_1 = H(ID_H \| q') \oplus sn$ $S_2 = H(SK_{PH} \| C_P \| Sig_P \| S'_1 \| R_P)$ $C_2 = E_{K_1}(C_P, S_2, Sig_P)$		
	$\xrightarrow{M_3 =< S_2, C_2 >}$ (insecure channel)	
		$SK'_{PH} = H(ID_P \| ID_H \| R_P \| R_H \| S_1)$ $K'_1 = H(ID_H \| q) \oplus sn$ $D_{K'_1}[C_2] = C_P, S_2, Sig_P$ $S'_2 = H(SK'_{PH} \| C_P \| Sig_P \| S_1 \| R_P)$ $S'_2 \overset{?}{=} S_2$

Fig. 5. Patient Data upload phase (PDUP).

it does not hold: terminate session otherwise healthcare authorize the patient. Then, healthcare generate a random number R_H and computes $S_1 = H(ID_H \| R_H \| q)$, $I = sn \oplus q$, $R_P \oplus R_H = F_3$, encrypts $C_1 = E_G[S_1, I, F_3]$ and sends $M_2 = \langle C_1 \rangle$ to patient.

Step 4. Upon receiving the message $M_2 = \langle C_1 \rangle$, patient computes $G' = H(ID_P \| R_P)$, decrypts $D_{G'}[C_1]$ to get $\{S_1, I, F_3\}$ and computes $R_H = R_P \oplus F_3$, $S'_1 = H(ID_H \| R_H \| q)$. Then, the patient checks whether $S'_1 \overset{?}{=} S_1$, if it does not hold: terminate the session otherwise patient authorizes the healthcare. Moreover, the patient computes $sn' = q' \oplus I$, session key between patient and healthcare $SK_{PH} = H(ID_P \| ID_H \| R_P \| R_H \| S_1)$, the secret key of patient and doctor as $K_{PD} = H(ID_P \| ID_D \| sn')$, encrypts the report send by body sensor $Data_B$ using the key K_{PD} as $C_P = E_{K_{PD}}(Data_B)$ and the patient performs digital signature using its private key on message digest $MD_B = H(Data_B)$

Healthcare (HC)		**Doctor** (D)
$m_H = (ID_P, Data_H, Data_B)$ Input ID_H, a Generate a random number R_{H1} $HR = a \oplus R_{H1}$ $J = sn \oplus R_{H1}$ $K_2 = H(ID_H \parallel ID_D \parallel a)$ $C_H = E_{K_2}(Data_H)$ $Sig_H = S_{PR_H}(MD_H)$ $S_3 = H(C_H \parallel Sig_H \parallel R_{H1} \parallel NID)$ $C_3 = E_{RPw}(C_H, Sig_H, C_P, Sig_P, S_3, NID, J, HR)$		
	$\xrightarrow[\text{(insecure channel)}]{M_4 =< S_3, C_3 >}$	
		$D_{RPw}[C_3] = (C_H, Sig_H, C_P,$ $Sig_P, S_3, NID, J, HR)$ $R_{H1} = HR \oplus a$ $S_3' = H(C_H \parallel Sig_H \parallel R_{H1} \parallel NID)$ $S_3' \overset{?}{=} S_3$ $sn'' = J \oplus R_{H1}$ $K_{PD}' = H(ID_P \parallel ID_D \parallel sn'')$ $D_{K_{PD}'}[C_P] = Data_B$ $V_{PU_P}[Sig_P] \overset{?}{=} H(Data_B)$ $K_2' = H(ID_H \parallel ID_D \parallel a)$ $D_{K_2'}[C_H] = Data_H$ $V_{PU_H}[Sig_H] \overset{?}{=} H(Data_H)$ $C_D = E_{K_{PD}'}(Data_H, Data_B, Data_D)$ $Sig_D = S_{PR_D}[H(Data_D)]$ Generate a randome number R_D $SK_{DH} = H(ID_D \parallel ID_H \parallel R_{H1} \parallel R_D)$ $K_3 = H(ID_D \parallel HR)$ $S_4 = H(SK_{DH} \parallel C_D \parallel Sig_D \parallel R_D)$ $C_4 = E_{K_3}[C_D, Sig_D, S_4, R_D]$
	$\xleftarrow[\text{(insecure channel)}]{M_5 =< C_4, S_4 >}$	
$K_3 = H(ID_D \parallel HR)$ $D_{K_3}[C_4] = C_D, Sig_D, S_4, R_D$ $SK_{DH}' = H(ID_D \parallel ID_H \parallel R_{H1} \parallel R_D)$ $S_4' = H(SK_{DH} \parallel C_D \parallel Sig_D \parallel R_D)$ $S_4' \overset{?}{=} S_4$		

Fig. 6. Treatment phase (TP).

as $Sig_P = S_{PR_P}(MD_B)$. Again, it computes $K_1 = H(ID_H \parallel q') \oplus sn$, $S_2 = H(SK_{PH} \parallel C_P \parallel Sig_P \parallel S_1' \parallel R_P)$, $C_2 = E_{K_1}(C_P, S_2, Sig_P)$ and sends $M_3 = \langle S_2, C_2 \rangle$ to healthcare via public channel.

Step 5. On receiving messages M_3, healthcare computes $SK_{PH}' = H(ID_P \parallel ID_H \parallel R_P \parallel R_H \parallel S_1)$, $K_1' = H(ID_H \parallel q) \oplus sn$ and decrypts C_2 as $D_{K_1'}[C_2]$ to get $\{C_P, S_2, Sig_P\}$. Then, the patient computes $S_2' = H(SK_{PH}' \parallel C_P \parallel Sig_P \parallel S_1 \parallel R_P)$ and verifies whether equation $S_2' \overset{?}{=} S_2$ holds or not. If it holds: healthcare stores C_P and Sig_P otherwise, it terminates the session.

4.3. Treatment Phase (TP)

The healthcare initiates the process by sending data to the doctor of the respective patient. A complete TP analysis is shown in Fig. 6 and the execution steps are as followed:

Step 1. Healthcare inputs its identity ID_H, a, and generates a random number R_{H1}. Then, healthcare computes $HR = a \oplus R_{H1}$, $J = sn \oplus R_{H1}$, $K_2 = H(ID_H \parallel ID_D \parallel a)$, encrypts the report of patient $C_H = E_{K_2}(Data_H)$, and generates the signature corresponding to $Data_H$ using the private key as $Sig_H = S_{PR_H}(MD_H)$, where $MD_H = H(Data_H)$, $S_3 = H(C_H \parallel Sig_H \parallel R_{H1} \parallel NID)$, encrypts $C_3 = E_{RPw}(C_H, Sig_H, C_P, Sig_P, S_3, NID, J, HR)$ and sends $M_4 = \langle S_3, C_3 \rangle$ to doctor via a public channel.

Step 2. Upon receiving these messages, the doctor decrypts the received ciphertext as $D_{RPw}[C_3] = \{C_H, Sig_H, C_P, Sig_P, S_3, NID, J, HR\}$, Where NID is a pseudo-random identity of the patient. The doctor tracks the identity of patient (ID_P) using NID. Then, computes $R_{H1} = HR \oplus a$, $S_3' = H(C_H \parallel Sig_H \parallel R_{H1} \parallel NID)$ and finally checks whether $S_3' \overset{?}{=} S_3$ holds or not. If it does, the doctor authenticates the healthcare and computes $sn'' = J \oplus R_{H1}$, otherwise terminated by the session.

Step 3. After that, the doctor computes the key of patient and doctor as $K_{PD}' = H(ID_P \parallel ID_D \parallel sn'')$, decrypts the report of the patient as $D_{K_{PD}'}[C_P] = Data_B$, and verifies the patient's signature using the public key of the patient as $V_{PU_P}[Sig_P] \overset{?}{=} H(Data_B)$. If it does, the doctor computes $K_2' = H(ID_H \parallel ID_D \parallel a)$, decrypts the report of healthcare

Table 4
Security analysis.

Schemes ↓ Phases →	MIMTA	PA	DA	PU	IA	KKS	SKS	FS	MA	DC	DNR	PCAR
Chen et al. [43]	√	χ	√	√	χ	χ	√	χ	√	√	√	√
Chen et al. [44]	√	χ	√	χ	√	√	√	√	χ	√	√	√
Chiou et al. [45]	√	χ	√	χ	χ	χ	√	χ	√	√	√	χ
Mohit et al. [46]	√	χ	√	χ	χ	√	√	√	√	√	√	χ
Li et al. [1]	√	χ	√	χ	χ	√	χ	√	χ	√	√	χ
Kumar et al. [2]	√	√	√	√	√	√	√	√	√	√	√	χ
Chandrakar et al. [3]	√	√	√	χ	χ	√	√	√	√	√	χ	χ
Chen et al. [47]	√	√	√	√	√	√	√	√	√	√	√	√
Kumari et al. [4]	√	√	√	√	√	√	√	√	√	√	√	χ
Proposed	√	√	√	√	√	√	√	√	√	√	√	√

MITMA: Man-in-the-middle attack, PA: Patient Anonymity, DA: Doctor Anonymity, PU: Patient Unlikability, IA: Impersonation Attack, KKS: Known-key Security, SKS: Session-key Security, FA: Forward Secrecy, MA: Message authentication, DC: Data Confidentiality, DNR: Data non-repudiation, PCAR: public cloud attack resistance.

as $D_{K_2'}[C_H] = Data_H$, and verifies the healthcare signature using the public key of healthcare as $V_{PU_H}[Sig_H] \overset{?}{=} MD_H$.

Step 4. After successful verification of healthcare signature, the doctor makes a medical diagnosis based on the reports with m_H, m_B that generates medical records $m_D = (ID_P, Data_D)$ and encrypts (m_H, m_B, m_D) using the key K'_{PD} as $C_D = E_{K'_{PD}}(Data_H, Data_B, Data_D)$. Then the doctor performs signature $Sig_D = S_{PR_D}[H(Data_D)]$ and generates a random number R_D, followed by computation of session key between doctor and healthcare $SK_{DH} = H(ID_D \parallel ID_H \parallel R_{H1} \parallel R_D)$, $K_3 = H(ID_H \parallel HR)$, $S_4 = H(SK_{DH} \parallel C_D \parallel Sig_D \parallel R_D)$, encrypts $C_4 = E_{K_3}[C_D, Sig_D, S_4, R_D]$. Finally, it sends $M_5 = \langle C_4, S_4 \rangle$ to healthcare via a public channel.

Step 5. Upon receiving message M_5, healthcare compute $K_3 = H(ID_D \parallel HR)$, decrypts the ciphertext C_4 as $D_{K_3}[C_4] = \{C_D, Sig_D, S_4, R_D\}$, computes $S'_4 = H(SK_{DH} \parallel C_D \parallel Sig_D \parallel R_D)$ and verifies whether $S'_4 \overset{?}{=} S_4$ holds or not. If it does, the healthcare stores C_D, Sig_D otherwise terminate the session.

4.4. Report Delivery Phase (RDP)

After successful treatment by the doctor, healthcare delivers the updated report to the patient. The execution of RDP phase is visualized by Fig. 7, and details of the steps are as below:

Step 1. The healthcare computes $S_5 = H(SK'_{PH} \parallel C_D \parallel Sig_D)$, encrypts the final report of the patient with the session key of patient and healthcare as $C_5 = E_{SK'_{PH}}[C_D, Sig_D, S_5]$ and sends message $M_6 = \langle C_5, S_5 \rangle$ to patient via public channel.

Step 2. On receiving message M_6, the patient decrypts the ciphertext C_5 as $D_{SK_{PH}}[C_5] = \{C_D, Sig_D, S_5\}$, computes $S'_5 = H(SK_{PH} \parallel C_D \parallel Sig_D)$ and verifies whether $S'_5 \overset{?}{=} S_5$ holds or not. If it does, the patient decrypts the ciphertext using K_{PD} as $D_{K_{PD}}[C_D]$ to get $(Data_H, Data_B, Data_D)$ and verifies the signature as $V_{PU_D}[Sig_D] \overset{?}{=} H(Data_D)$. Then, patient encrypts the report $C_6 = E_{K_P}[Data_B, Data_D]$ using its own key $K_P = H(ID_P \parallel p)$, where p is a random number. Patient further computes $S_6 = H(SK_{PH} \parallel C_6)$, $C_7 = E_{SK_{PH}}[S_6, C_6]$ and sends $M_7 = \langle S_6, C_7 \rangle$ to the healthcare via public channel.

Step 3. Finally, after receiving message M_7, the healthcare first decrypts the ciphertext C_7 as $D_{SK_{PH}}[C_7] = \{S_6, C_6\}$, computes $S'_6 = H(SK_{PH} \parallel C_6)$ and verifies whether $S'_6 \overset{?}{=} S_6$ holds or not. If it does, the healthcare stores C_6 otherwise terminate.

5. Informal security analysis

This section describes the security issues and their implementation aspects in our proposed protocol. We have considered that an adversary $(\mathcal{A}y)$ with the capacity to modify and eavesdrop on the communicating message over the public channel. A brief overview of various security protection against some common threats via. Man-in-the-middle attack, anonymity, unlikability, impersonation attack, session-key security, known-key security are well compared in Table 4. The sign (√) represents the presence of a particular feature, and (χ) designates the absence of the features.

5.1. Man-in-the-middle attack (MITMA)

In MITMA, the attacker $\mathcal{A}y$ intercepts transmitted messages and tries to collect information from the public channel. This attempt will be unsuccessful due to the protection of public messages by symmetric-key encryption or a one-way hash function. The received message are also validated using other communicating parties. For instance, during PDUP attacker interrupts message $M_3 = \langle S_2, C_2 \rangle$ he/she will not be able to compute the values of C_2/S_2 as C_2 encrypted by the key only known to patient and healthcare as well as S_2 due to the use of an irreversible one-way hash function.

5.2. Patient Anonymity (PA)

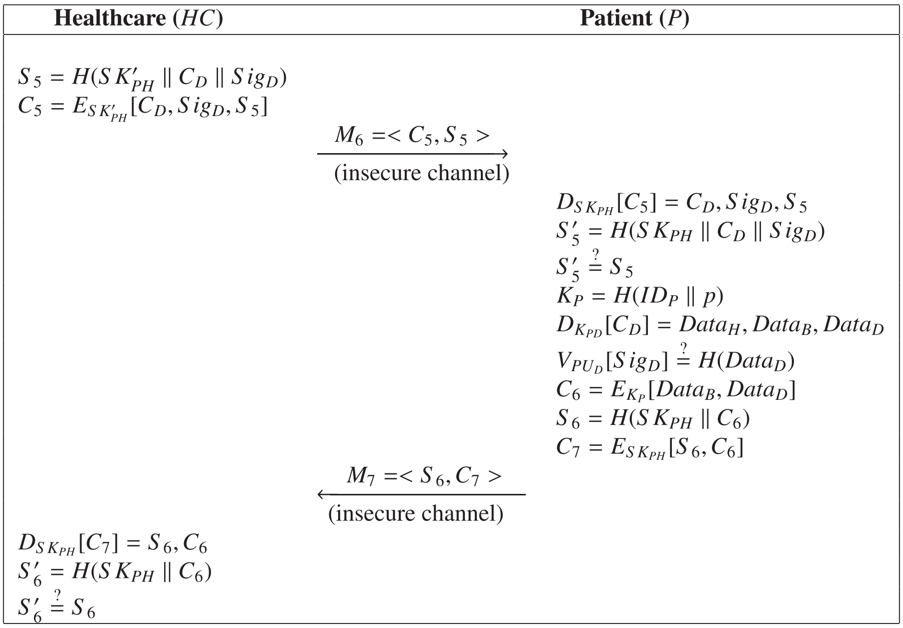
For healthcare applications, it is very much essential to protect the real identity of the patient. During the PDUP, the identity of a patient ID_P is hidden in the session key between patient and healthcare (SK_{PH}). However, the session key is hashed with other parameters to compute and send S_2 over a public channel. If an adversary $\mathcal{A}y$ interrupts the message S_2. He/she will be unable to identify the patient. Hence, PA is not possible in this scheme.

5.3. Doctor Anonymity (DA)

The doctor's identity plays a vital role in this protocol. During the treatment phase, the doctors' identity is kept hidden by using the session key between doctor and healthcare (SK_{DH}). To preserve DA, the communicating entities doctor and healthcare share S_4 over a public channel, where S_4 is the hash of SK_{DH} with other parameters. If $\mathcal{A}y$ attacks on the message S_4, he/she will not obtain the doctor's identity. Therefore, the protocol is protected by DA.

5.4. Patient Unlikability (PU)

During PDUP, the data transferred between patient and healthcare over an insecure channel (M_1, M_2, M_3) are truly random in nature and session-dependent. Every field in $M_1 = \langle C_0 \rangle = \{E_P[S_0, F_1, F_2]\}$, $M_2 = \langle C_1 \rangle = \{E_G[S_1, I, F_3]\}$, and $M_3 = \langle S_2, C_2 \rangle = \{H(SK_{PH} \parallel C_P \parallel Sig_P \parallel S_1 \parallel R_P), E_{K1}[C_P, S_2, Sig_P]\}$ are different in each session. The transmitted messages are different in all sessions due to the involvement of random numbers (R_P, R_H) in the computation of M_i. Based on dynamic values, $\mathcal{A}y$ cannot identify the status of patients involved in the different sessions and unable to determine the relationship between messages from several sessions. Hence, tracking the patient is not possible. Thus, the proposed scheme provides unlikability, and the $\mathcal{A}y$ cannot trace patients by intercepting messages.



Healthcare (HC) **Patient** (P)

$S_5 = H(SK'_{PH} \parallel C_D \parallel Sig_D)$

$C_5 = E_{SK'_{PH}}[C_D, Sig_D, S_5]$

$\xrightarrow[\text{(insecure channel)}]{M_6 =< C_5, S_5 >}$

$D_{SK_{PH}}[C_5] = C_D, Sig_D, S_5$

$S'_5 = H(SK_{PH} \parallel C_D \parallel Sig_D)$

$S'_5 \overset{?}{=} S_5$

$K_P = H(ID_P \parallel p)$

$D_{K_{PD}}[C_D] = Data_H, Data_B, Data_D$

$V_{PU_D}[Sig_D] \overset{?}{=} H(Data_D)$

$C_6 = E_{K_P}[Data_B, Data_D]$

$S_6 = H(SK_{PH} \parallel C_6)$

$C_7 = E_{SK_{PH}}[S_6, C_6]$

$\xleftarrow[\text{(insecure channel)}]{M_7 =< S_6, C_7 >}$

$D_{SK_{PH}}[C_7] = S_6, C_6$

$S'_6 = H(SK_{PH} \parallel C_6)$

$S'_6 \overset{?}{=} S_6$

Fig. 7. Report Delivery Phase (RDP).

5.5. Impersonation Attack (IA)

One of the potential attacks is IA, in which an adversary $\mathcal{A}y$ interrupts in between the communicating entity. Ay can trap the transmitting messages via the public channel. After getting the transmitted message, $\mathcal{A}y$ can alter the message and retransmit the modified message. Moreover, the modified message must have to pass the verification process performed by the other party, which is impossible in the proposed protocol. A brief detail is described in terms of PDUP and follows the same concept for different phases as:

- An adversary $\mathcal{A}y$ tries to impersonate as legal healthcare and eavesdrops on the transmitted message $M_2 = \langle C_1 \rangle$ and tries to computes $G = H(ID_P \parallel R_P)$. $\mathcal{A}y$ cannot be able to calculate G, which is the hash of parameters ID_P, R_P. ID_P is the unique identity of the patient, and R_P is random numbers generated by the patient. Further, $\mathcal{A}y$ cannot compute $p' = H(PS)$ because healthcare and patient share PS in the offline phase. Thus, any adversary cannot impersonate valid healthcare.
- If $\mathcal{A}y$ tries to impersonate as a legal patient by using a different identity or guessing the ID_A. It results in computing the value of $M_1 = \langle C_0 \rangle$ and tries to computes p, $S_0 = H(ID_P \parallel R_P \parallel q)$. $\mathcal{A}y$ cannot compute S_0, which is hash of parameters ID_P, R_P, q. The ID_P is the unique identity of the patient R_P, q is random numbers generated by the patient.
- If $\mathcal{A}y$ tries to impersonate as a patient by computing the message M_3 as $\langle S_2, C_2 \rangle$. The computation of S_2 involves the five other parameters: (1) Session key between P and HC: SK_{PH}, (2) Ciphertext of the patient: C_P, (3) Signature of the patient: Sig_P, (4) S_1 hash of ID_H with random number R_H, q, and (5) Random number generated by patient R_P. Note: The high entropy property may cause an unsuccessful prediction of the above set of parameters at a particular time. Hence, the incorrect value of any parameter leads to an false value of S_2. Thus, the adversary cannot impersonate a legal patient.

5.6. Known-key Security (KKS)

A unique session key is generated in each session. But the disclosure of any session-key should not be compromised by the other session-key. The patient, healthcare, and doctor must have random numbers to generate their session key. The session key of patient and healthcare is $SK_{PH} = H(ID_P \parallel ID_H \parallel R_P \parallel R_H \parallel S_1)$. To computes SK_{PH} two random numbers R_P, R_H are used. Similarly, the session key of healthcare and doctor ($SK_{DH} = (ID_D \parallel ID_H \parallel R_{H1} \parallel R_D)$) uses random number R_{H1}, R_D. So, if $\mathcal{A}y$ has the previous session key: he/she cannot generate the session key for the current session. Thus, our protocol is protected against KKS.

5.7. Session-key Security (SKS)

The SKS is one of the fundamental security aspects. The availability of session-key is limited to legitimate parties. In this protocol, two session keys are computed between (1) the Patient and Healthcare and (2) the Doctor and Healthcare. All of these session keys are well secured by using the following steps:

- The session key between Patient and Healthcare $SK_{PH} = H(ID_P \parallel ID_H \parallel R_P \parallel R_H \parallel S_1)$ brings hashing of $ID_P, ID_H, R_P, R_H, S_1$. These values need to be determined by the attacker $\mathcal{A}y$ for generating an exact session key. The adversary $\mathcal{A}y$ cannot extract the parameter S_1 because it uses a one-way hash function. The identity of the patient ID_P, healthcare ID_H are not directly involved in the transmission of messages. R_P, R_H are random value generated in each session by patient, healthcare. Thus, $\mathcal{A}y$ fails to compute session key (SK_{PH}) due to the unavailability of parameters $ID_P, ID_H, R_P, R_H, S_1$.
- The session key between healthcare and doctor $SK_{DH} = (ID_D \parallel ID_H \parallel R_{H1} \parallel R_D)$ must have to hash of ID_D, ID_H, R_{H1}, and R_D that need to be determined by $\mathcal{A}y$ for the exact session key. The identity of healthcare ID_H and doctor ID_D are not involved in the transmission of messages. R_{H1}, R_D are the random value generated in each session by healthcare, doctor. Hence, $\mathcal{A}y$ cannot access the session key without knowing the parameters ID_D, ID_H, R_D, R_{H1}. It ensures that an $\mathcal{A}y$ cannot compute the session key SK_{DH}.

Hence, the session key can only be generated by a legitimate party.

5.8. Forward Secrecy (FS)

The forward secrecy enables potent security for session keys if the long-term key gets compromised in the proposed scheme and an attacker captures the message $M_1 = \langle C_0 \rangle$, $M_2 = \langle C_2 \rangle$, $M_3 = \langle S_2, C_2 \rangle$ during PDUP. Then, $\mathcal{A}y$ can get the values as S_0, F_1, F_2, S_1, I, F_3, S_2, C_P, Sig_P but from all these values attacker cannot find the value of R_P, R_H, ID_P and ID_H, which is essential for the calculation of session key $SK_{PH} = H(ID_P \parallel ID_H \parallel R_P \parallel R_H \parallel S_1)$. In the present protocol, two session keys (SK_{PH}, SK_{DH}) are computed, (1) $SK_{PH} = H(ID_P \parallel ID_H \parallel R_P \parallel R_H \parallel S_1)$ and (2) $SK_{DH} = H(ID_D \parallel ID_H \parallel R_{H1} \parallel R_D)$. A similar proceeding as that of the first session key is also applicable in the calculation of SK_{DH}. For example, if $\mathcal{A}y$ has long-term key and message M_4, M_5, he/she can obtain $S_3, C_H, Sig_H, C_P, Sig_P, S_3, NID, J, HR, C_D, Sig_D, S_4, R_D$. So, the attacker will be unable to find the value of ID_D, ID_H, and R_{H1}. The necessary parameters for the calculation of session key between healthcare and doctor. Hence, the proposed protocol comes with forward secrecy.

5.9. Message authentication (MA)

Message authentication is a mechanism used to verify the integrity of the message. Here, we have described the MA in each phase as:

- During PDUP, the Patient authenticates healthcare if $S_1' \overset{?}{=} H(ID_H \parallel R_H \parallel q)$ holds, which involves random numbers R_H. Therefore, to recover random values, $\mathcal{A}y$ predicts the random numbers generated by patients. On the other side, healthcare authenticates patient if $S_2' \overset{?}{=} H(SK_{PH} \parallel C_P \parallel Sig_P \parallel S_1 \parallel R_P)$ holds. In this case, only the legal patient can successfully authenticate because Sig_P needs the value of the patient private key. The value of SK_{PH} can also be retrieved by healthcare. Hence, the patient and healthcare mutually authenticate each other.
- In TP, the doctor verifies message $M_4 = \langle S_3, C_3 \rangle$ by checking whether $S_3' \overset{?}{=} H(C_H \parallel Sig_H \parallel R_{H1} \parallel NID)$ holds. Then, the healthcare authenticates the received message $M_5 = \langle C_4, S_4 \rangle$ as $S_4' \overset{?}{=} H(SK_{DH} \parallel C_4 \parallel Sig_D \parallel R_D)$ hold. If any of the verification fails, the messages will not be accepted.
- In RDP, the patient verifies message $M_6 = \langle C_5, S_5 \rangle$ as $S_5' \overset{?}{=} H(SK_{PH} \parallel C_D \parallel Sig_D)$ and healthcare verifies the message $M_7 = \langle S_6, C_7 \rangle$ as $S_6' \overset{?}{=} H(SK_{PH} \parallel C_6)$.

Hence, our scheme protects MA in each phase.

5.10. Data Confidentiality (DC)

Confidentiality offers protection of transmitted data from the adversary during transmission. A clear description for the above claim can be explained as below:

- During PDUP, the patient's report $m_B = (Data_B)$ will be encrypted with K_{PD} to obtains $C_P = E_{K_{PD}}(Data_B)$, Afterward, C_P is encrypted using key K_1 to get C_1 and C_1 is sent to the healthcare server.
- In TP, the healthcare report m_H as encrypted data with K_2 to obtains $C_H = E_{K_2}(Data_H)$. However, C_H is further encrypted using key RPw to evaluate C_3 and finally sent to the doctor.
- In TP, the doctor report m_D is encrypted data with K_{PD} to obtains $C_D = E_{K_{PD}}(Data_B, Data_D)$. Again C_D is further encrypted using key K_3 to get C_4 for healthcare.
- In RDP, the K_P is used to encrypt $C_6 = E_{K_P}(m_B, m_D)$.

Hence, if $\mathcal{A}y$ tries to accumulate information during communication, he/she gets encrypted data. But one cannot decrypt the message without the key. Thus, our scheme supports confidentiality.

5.11. Data non-repudiation (DNR)

"Non-repudiation" refers to the ability of the sender/receiver to ensure that a communicating party cannot deny the authenticity of their signature on a document.

- During PDUP, the patient makes digital signature on a message $Sig_P = S_{PR_P}(MD_B)$.
- During TP, healthcare performs digital signature $Sig_H = S_{PR_H}(MD_H)$. The Doctor must has to verify healthcare and patient's digital signature by using $V_{PU_H}[Sig_H] \overset{?}{=} H(Data_H)$, $V_{PU_P}[Sig_P] \overset{?}{=} H(Data_B)$ and makes digital signature as $Sig_D = S_{PR_D}(Data_D)$.
- During RDP, the patient verifies the doctor's digital signature as $V_{PU_D}[Sig_D] \overset{?}{=} H(Data_D)$.

Therefore, our protocol protects DNR.

Note: The number of stages in the proposed protocol is only three, which is less than the existing protocols. Besides, public cloud attack resistance (PCAR) is also available in our protocol.

6. Formal security analysis

To judge the security of the session key formal security analysis in terms of BAN logic and ROR model are presented in the proposed scheme. The detail of BAN logic and ROR model are described in Section 6.1, and 6.2 respectively.

6.1. Authentication proof based on BAN logic

The first section of the formal security analysis describes the well known Burrows–Abadi–Needham (BAN) logic [52]. BAN logic investigation enables us to validate the proposed authentication protocol that establishes secure communication between the (1) patient and healthcare, (2) healthcare and doctor. For simple observation, the symbols (R,S) designate principals, and the symbols (E and Key) nominate the statements. The fundamental postulates (P_i) for BAN logic investigation are given below:

Message-meaning (P_{MM}):	$\frac{R \mid\equiv R \overset{Key}{\longleftrightarrow} S,\ R \triangleleft <E>_{Key}}{R \mid\equiv S \mid\sim E}$.
Freshness-conjuncatenation (P_{FC}):	$\frac{R \mid\equiv \sharp(E)}{R \mid\equiv \sharp(E, Key)}$.
Nonce-verification (P_{NV}):	$\frac{R \mid\equiv \sharp(E),\ R \mid\equiv S \mid\sim E}{R \mid\equiv S \mid\equiv E}$.
Jurisdiction (P_{JD}):	$\frac{R \mid\equiv S \Rightarrow E,\ R \mid\equiv S \mid\equiv E}{R \mid\equiv E}$.
Session keys (P_{SK}):	$\frac{R \mid\equiv \sharp(E), R \mid\equiv S \mid\equiv E}{R \mid\equiv R \overset{Key}{\longleftrightarrow} S}$.

To verify the proposed protocol, the following eight goals (GL) must have to satisfy the *BAN* logic:

GL 1: $P \mid\equiv P \overset{SK_{PH}}{\longleftrightarrow} HC$

The patient (P) believes that there is a session key (SK_{PH}) established between patient (P) and healthcare (HC).

GL 2: $P \mid\equiv HC \mid\equiv P \overset{SK_{PH}}{\longleftrightarrow} HC$

P & HC believe that there is a session key (SK_{PH}) between them.

GL 3: $HC \mid\equiv P \overset{SK_{PH}}{\longleftrightarrow} HC$

HC believes that there is a session key (SK_{PH}) established between P & HC.

GL 4: $HC \mid\equiv P \mid\equiv P \overset{SK_{PH}}{\longleftrightarrow} HC$

HC & P believe that there is a session key (SK_{PH}) established between them.

GL 5: $D \mid\equiv HC \overset{SK_{DH}}{\longleftrightarrow} D$

Doctor (D) believes that there is a session key (SK_{DH}) established between HC & D.

GL 6: $D \mid\equiv HC \mid\equiv HC \overset{SK_{DH}}{\longleftrightarrow} D$

D & HC believe that there is a session key (SK_{DH}) established between them.

GL 7: $HC \mid\equiv HC \overset{SK_{DH}}{\longleftrightarrow} D$

HC believes that there is a session key (SK_{DH}) established between HC & D.

GL 8: $HC \mid\equiv D \mid\equiv HC \overset{SK_{DH}}{\longleftrightarrow} D$

HC & D believe that there is a session key (SK_{DH}) established between them.

Initially, the proposed protocol is transformed into an idealized form with four distinct messages ($MESG_i$) as:

$MESG_1$: $HC \rightarrow P : C_1 : \langle S_1, I, R_H, R_P \rangle_G$
$MESG_2$: $P \rightarrow HC : S_2, C_2 : \langle C_P, Sig_P, R_P \rangle_{S_1}$
$MESG_3$: $HC \rightarrow D : C_3, S_3 : \langle C_H, Sig_H, R_{H1} \rangle_{NID}$
$MESG_4$: $D \rightarrow HC : C_4, S_4 : \langle C_D, Sig_D, S_4, R_D \rangle_{K_3}$

Then, the following assumptions ($ASUM_i$) on the initial state are exercised to analyze the proposed scheme:

$ASUM_1 : P \mid\equiv \sharp(R_P, R_H)$: Patient believes that (R_P, R_H) is fresh i.e. (R_P, R_H) have not previously been sent in any message.

$ASUM_2 : HC \mid\equiv \sharp(R_P, R_H, R_D)$	: HC believes that (R_P, R_H, R_D) is fresh.
$ASUM_3 : D \mid\equiv \sharp(R_H, R_D)$	: D believes that (R_H, R_D) is fresh.
$ASUM_4 : P \mid\equiv P \overset{G}{\longleftrightarrow} HC$	: P believes that P & HC use the shared key G to communicate.
$ASUM_5 : HC \mid\equiv HC \overset{G}{\longleftrightarrow} P$	: HC believes that HC & P use the shared key G to communicate.
$ASUM_6 : HC \mid\equiv HC \overset{S_1}{\longleftrightarrow} P$	: HC believes that HC & P use the shared key S_1 to communicate.
$ASUM_7 : P \mid\equiv P \overset{S_1}{\longleftrightarrow} HC$	: P believes that P & HC use the shared key S_1 to communicate.
$ASUM_8 : D \mid\equiv D \overset{NID}{\longleftrightarrow} HC$	: D believes D & HC use the shared key NID to communicate.
$ASUM_9 : HC \mid\equiv HC \overset{K_3}{\longleftrightarrow} D$	: HC believes that HC & D use the shared key K_3 to communicate.
$ASUM_{10} : D \mid\equiv HC \Rightarrow R_D$	: D believes that HC has jurisdiction over R_D i.e. HC beliefs about R_D should be trusted.
$ASUM_{11} : HC \mid\equiv D \Rightarrow R_D$	: HC believes that D has jurisdiction over R_D
$ASUM_{12} : HC \mid\equiv P \Rightarrow R_P$	: HC believes that P has jurisdiction over R_P
$ASUM_{13} : P \mid\equiv HC \Rightarrow R_P$	: P believes that HC has jurisdiction over R_P
$ASUM_{14} : P \mid\equiv HC \Rightarrow R_H$	: P believes that HC has jurisdiction over R_H

The Patient (P) authenticates the Healthcare (HC)

The patient authentication of the healthcare can be derived by the assumptions with the following BAN logic:

$MESG_1$ send by healthcare to patient:

$MESG_1$: $HC \rightarrow P : \langle S_1, I, R_H, R_P \rangle_G$

From seeing rule, Assertion 1 can be derived as:

(Assertion 1): $P \lhd \langle S_1, I, R_H, R_P \rangle_G$

From assumption $ASUM_4$ and Message-meaning postulate (P_{MM}) on Assertion 1, it gives:

(Assertion 2): $P \mid\equiv HC \mid\sim \langle S_1, I, R_H, R_P \rangle$

From assumption $ASUM_1$ and Nonce-verification postulate (P_{NV}) applied on Assertion 2, it gives:

(Assertion 3): $P \mid\equiv HC \mid\equiv R_H, R_P$, where R_H, R_P is the necessary parameter of the session key.

As per assumption $ASUM_{14}$ and Jurisdiction postulate (P_{JD}) applied on Assertion 3, it yields:

(Assertion 4): $P \mid\equiv R_H, R_P$

The Patient believes that R_H, R_P is fresh (according to assumption $ASUM_1$) and it is another necessary parameter of the session key (SK_{PH}).

As per assumption $ASUM_1$ and Session keys postulate (P_{SK}) which is applied on Assertion 3. Then it gives:

(Assertion 5) : $P \mid\equiv P \overset{SK_{PH}}{\longleftrightarrow} HC$ **(GL 1)**

Then, we apply assumption $ASUM_2$, Nonce-verification postulate (P_{NV}) on Assertion 5, it gives:

(Assertion 6) : $P \mid\equiv HC \mid\equiv P \overset{SK_{PH}}{\longleftrightarrow} HC$ **(GL 2)**

The Healthcare (HC) authenticates the Patient (P)

The healthcare authentication of the patient can be shown by the following assumptions and postulates.

$MESG_2$ is sent by the patient to healthcare.

$MESG_2$: $P \rightarrow HC : S_2, C_2 : \langle C_P, Sig_P, R_P \rangle_{S_1}$

By seeing rule;

(Assertion 7): $HC \lhd S_2, C_2 : \langle C_P, Sig_P, R_P \rangle_{S_1}$

According to $ASUM_6$ and P_{MM} applied on Assertion 7, it gives:

(Assertion 8): $HC \mid\equiv P \mid\sim \langle C_P, Sig_P, R_P \rangle$

When we applied $ASUM_2$ and P_{NV} on Assertion 8, it gives:

(Assertion 9): $HC \mid\equiv P \mid\equiv R_P$, where R_P is the necessary parameter of the session key.

As per $ASUM_{12}$ and P_{JD} applied on Assertion 9 that gives:

(Assertion 10): $HC \mid\equiv R_P$

The Healthcare HC believes that R_P is fresh (according to assumption $ASUM_2$), which is a necessary parameter of the session key SK_{PH}.

As per $ASUM_2$ and P_{SK} applied on Assertion 9. It becomes:

(Assertion 11) : $HC \mid\equiv P \overset{SK_{PH}}{\longleftrightarrow} HC$ **(GL 3)**

As per $ASUM_2$ and P_{NV} on Assertion 11 that gives:

(Assertion 12) : $HC \mid\equiv P \mid\equiv P \overset{SK_{PH}}{\longleftrightarrow} HC$ **(GL 4)**

The Doctor (D) authenticates the Healthcare (HC) The doctor authentication of the healthcare can be shown by the following assumptions and postulates.

$MESG_3$: $HC \rightarrow D : C_3, S_3 : \langle C_H, Sig_H, R_{H1} \rangle_{NID}$

As per seeing rule;

(Assertion 13): $D \lhd \langle C_H, Sig_H, R_{H1} \rangle_{NID}$

As per $ASUM_8$ and P_{MM} on Assertion 13, it becomes:

(Assertion 14): $D \mid\equiv HC \mid\sim \langle C_H, Sig_H, R_{H1} \rangle$

By applying $ASUM_3$ and P_{NV} on Assertion 14, it gives:
(Assertion 15): $D \mid\equiv HC \mid\equiv R_{H1}$

As per $ASUM_{10}$ and P_{JD} on Assertion 15, it becomes:

(Assertion 16): $D \mid\equiv R_{H1}$

When $ASUM_3$ and the P_{SK} on Assertion 15, it yields:

$$\text{(Assertion 17)} : D \mid\equiv HC \overset{SK_{DH}}{\longleftrightarrow} D \qquad \textbf{(GL 5)}$$

As per $ASUM_3$ and P_{NV} on Assertion 17, it gives:

$$\text{(Assertion 18)} : D \mid\equiv HC \mid\equiv HC \overset{SK_{DH}}{\longleftrightarrow} D \qquad \textbf{(GL 6)}$$

The Healthcare (HC) authenticates the Doctor (D) The healthcare authentication of the doctor can be shown by the following assumptions and postulates as:

$MESG_4$: $D \rightarrow HC : C_4, S_4 : \langle C_D, Sig_D, S_4, R_D \rangle_{K_3}$

According to seeing rule;

(Assertion 19): $HC \triangleleft \langle C_D, Sig_D, S_4, R_D \rangle_{K_3}$

As per $ASUM_9$, P_{MM} applied over Assertion 19, it gives:

(Assertion 20): $HC \mid\equiv D \mid\sim \langle C_D, Sig_D, S_4, R_D \rangle$

As per $ASUM_2$, and P_{NV} on Assertion 20, it becomes:

(Assertion 21): $HC \mid\equiv D \mid\equiv R_D$

By Assertion 21, $ASUM_{11}$, and P_{JD}, it yields:

(Assertion 22): $HC \mid\equiv R_D$

As per $ASUM_2$, $E20$, and the P_{SJ} Assertion 21, it gives:

$$\text{(Assertion 23)} : HC \mid\equiv HC \overset{SK_{DH}}{\longleftrightarrow} D \qquad \textbf{(GL 7)}$$

Now by using $ASUM_2$, $E22$, and P_{NV} on Assertion 23, it becomes:

$$\text{(Assertion 24)} : HC \mid\equiv D \mid\equiv HC \overset{SK_{DH}}{\longleftrightarrow} D \qquad \textbf{(GL 8)}$$

The above discussion based on BAN logic gives the justification of mutual authentication and session key establishment in our proposed protocol.

6.2. Authentication proof based on ROR model

In addition to BAN logic, this subsection presents formal security for session key using a famous Real-Or-Random (ROR) model [53]. To make the protocol free from the active and passive adversary, ROR model gives a significant contribution towards the validation of key assignments. Some different queries for the test purpose of the real attacks are taken into account as per Table 5. In ROR model, we have assumed that any two participants in a network can communicate over an insecure channel. Under these criteria, an adversary ($\mathcal{A}y$) has control over all communicated messages. Besides, $\mathcal{A}y$ may also intercept with $\mathcal{E}xe^t$ and the tth instance of an executing participant. The PDUP of proposed protocol includes two participants $\mathcal{E}xe^p_{P_i}$, $\mathcal{E}xe^h_{H_j}$, that indicates the instances p and h of P_i and H_j respectively. The verification of the proposed e-monitoring healthcare system can be validated by Theorem 1.

Theorem 1. *Let us consider the term $Adv^{\mathcal{A}y}_{HP}(t)$ represents $\mathcal{A}y$ dominance function to break the session key (SK_{PH}) of the proposed e-healthcare monitoring proposed (HP) in which $q_{\#}$, q_{send}, l, $|\#|$ and $|\mathcal{D}|$ represent the number of hash queries, send queries, number of bits, range of hash function, size of password dictionary $\mathcal{D}$ respectively. Then, the prominence of $\mathcal{A}y$ to crack the e-monitoring protocol (HP) to establish the session key as a function of relevant parameter is approximated as:*

$$Adv^{\mathcal{A}y}_{HP}(t) \leq \frac{q^2_{\#}}{|\#|} + \frac{2q_{send}}{|\mathcal{D}|} \tag{1}$$

Proof. The formal authentication proof of the proposed protocol follows similar proceedings as [9,54], and a few more. For verification purpose, four games (GAM_i) are introduced in which adversary ($\mathcal{A}y$) can win a game is described: $Adv^{\mathcal{A}y}_{GAM_i}$. Moreover, a benefit in the GAM_i is represented as: $Adv^{\mathcal{A}y}_{GAM_i} = Pr[Lead^{\mathcal{A}y}_{GAM_i}]$

- GAM_0: In this initial phase of the game, the bit "b" is selected and the real attack by $\mathcal{A}y$ against HP can be modeled as:

$$Adv^{\mathcal{A}y}_{HP}(t) = |2.Adv^{\mathcal{A}y}_{GAM_0} - 1| \tag{2}$$

- GAM_1: This game involves an eavesdropping attack in which $\mathcal{A}y$ can intersperse the communication message $M_2 = \langle C_1 \rangle$ and $M_3 = \langle S_2, C_2 \rangle$ during PDUP phase. Then, $\mathcal{A}y$ requires a test query at the end of the game. The test query output informs whether $\mathcal{A}y$ receives true session key between patient and healthcare or random value. If $\mathcal{A}y$ wants to compute the session key, it needs to know the secret values: $ID_P, ID_H, R_P, R_H, S_1$. As the session key is computed as $SK_{PH} = H(ID_P \parallel ID_H \parallel R_P \parallel R_H \parallel S_1)$. But $\mathcal{A}y$ cannot evaluate the session key without the aforementioned secret. Hence, eavesdropping cannot be possible in this GAM_1 and have same probability as that of GAM_0:

$$Adv^{\mathcal{A}y}_{GAM_1} = Adv^{\mathcal{A}y}_{GAM_0} \tag{3}$$

- GAM_2: An active attack by incorporating send and # queries are simulated in this game. In our proposed protocol the communicated messages (M_2, M_3) are protected through hash function. If $\mathcal{A}y$ tries to compute the session key (SK_{PH}) between P and HC: $\mathcal{A}y$ becomes unsuccessful due to the collision resistant feature of hash function. Finally, the birthday paradox for the two identical game (GAM_1 and GAM_2) results in the following inequality:

$$|Adv^{\mathcal{A}y}_{GAM_2} - Adv^{\mathcal{A}y}_{GAM_1}| \leq \frac{q^2_{\#}}{2|\#|} \tag{4}$$

- GAM_3: In this game, $\mathcal{A}y$ attempts to guess the identity of patient P_i (ID_P). Also, tries to use this information for the derivation of the session key between P and HC. Suppose $\mathcal{A}y$ has intercepted the messages (M_2, M_3), then it either gets the encrypted data or hash value of some parameters like random number R_P, R_D, Sig_H. To guess the identity of patient by ($\mathcal{A}y$) requires some secret credentials to decrypt it. Hence, the proposed systems allow only a limited number of wrong identity input that yields:

$$|Adv^{\mathcal{A}y}_{GAM_3} - Adv^{\mathcal{A}y}_{GAM_2}| \leq \frac{q_{send}}{|\mathcal{D}|} \tag{5}$$

After executing all four games, $\mathcal{A}y$ can only predict the correct bit b to win the game after the test. That concludes:

$$Adv^{\mathcal{A}y}_{GAM_3} = \frac{1}{2} \tag{6}$$

Now, by simplifying Eq. (2), (3), (6) provide the following set of the equation :

$$\begin{aligned}
&\frac{1}{2} = Adv^{\mathcal{A}y}_{HP}(t) = |Adv^{\mathcal{A}y}_{GAM_0} - \frac{1}{2}| \\
&Adv^{\mathcal{A}y}_{HP}(t) = |Adv^{\mathcal{A}y}_{GAM_1} - \frac{1}{2}| \\
&\frac{1}{2} Adv^{\mathcal{A}y}_{HP}(t) = |Adv^{\mathcal{A}y}_{GAM_1} - Adv^{\mathcal{A}y}_{GAM_3}|
\end{aligned} \tag{7}$$

Again by applying triangular inequality, it yields:

$$\begin{aligned}
|Adv^{\mathcal{A}y}_{GAM_1} - Adv^{\mathcal{A}y}_{GAM_3}| &\leq |Adv^{\mathcal{A}y}_{GAM_1} - Adv^{\mathcal{A}y}_{GAM_2}| \\
&\quad + |Adv^{\mathcal{A}y}_{GAM_2} - Adv^{\mathcal{A}y}_{GAM_3}| \\
&\leq \frac{q^2_{\#}}{2|\#|} + \frac{q_{send}}{|\mathcal{D}|}
\end{aligned} \tag{8}$$

Now, Eqs. (7) and (8) give the following expression:

$$\frac{1}{2} Adv^{\mathcal{A}y}_{HP}(t) \leq \frac{q^2_{\#}}{2|\#|} + \frac{q_{send}}{|\mathcal{D}|} \tag{9}$$

Table 5
Queries with description present in ROR model.

Queries	Description
Execution $(\mathcal{E}xe^p_{P_i}, \mathcal{E}xe^h_{H_j})$	Adversary $(\mathcal{A}y)$ can attain all transmitted messages between $\mathcal{E}xe^p_{P_i}, \mathcal{E}xe^h_{H_j}$ and maybe possible reasons for the eavesdropping attack.
Reveal $(\mathcal{E}xe^t)$	$\mathcal{A}y$ can also access the session key between $(\mathcal{E}xe^t)$ and its partner.
Sent $(\mathcal{E}xe^t, MESG)$	In this query, an active attack by $\mathcal{A}y$ can send a message to any instance $\mathcal{E}xe$ and receive the answer for $\mathcal{E}xe^t$.
Test $(\mathcal{E}xe^t)$	$\mathcal{A}y$ asks $\mathcal{E}xe^t$ for the session key but $\mathcal{E}xe^t$ gives probabilistic outcome.
$(q_{\#})$	Cryptographic hash function is accessible by all the participants and $\mathcal{A}y$

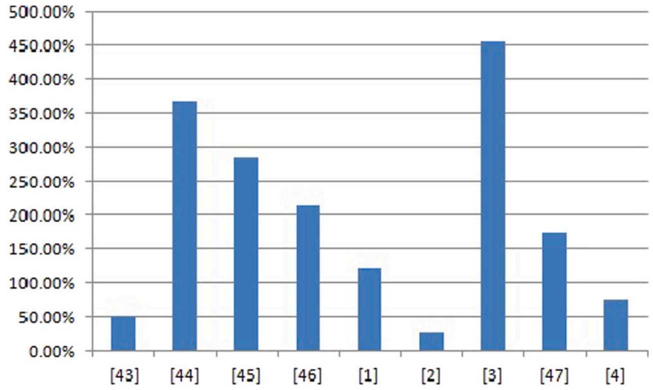


Fig. 8. Comparison (in percent) of Communication cost with respect to proposed scheme.

Finally, multiplying Eq. (9) by factor 2 results:

$$Adv^{\mathcal{A}y}_{HP}(t) \leq \frac{q^2_{\#}}{|\#|}\frac{2q_{send}}{|\mathcal{D}|} \tag{10}$$

The final expression validates Theorem 1. □

7. Performance evaluation

This section presents a comparative study of communication, storage and computation cost of the proposed healthcare monitoring protocol with other schemes [1–4,43–47]. The involvement/ availability of communication and computation cost in the respective protocols are evaluated for different phases such as the healthcare update phase (HUP), patient data upload phase (PDUP), treatment phase (TP), report delivery phase (RDP), and emergency phase (EP).

7.1. Communication cost

For a fair comparison, communication overheads of existing protocol evaluated based on the literature [1–3]. The bit sizes of different entities are considered as: identity 48 bits, time-stamp 48 bits, generated random number 48 bits, symmetric encryption/decryption operation 128 bits, cryptographic hash function 160 bits, executing/verifying a signature 512 bits.

Table 6 describes a brief comparison of communication costs. It is found that among all the presented healthcare protocols, the proposed protocol has the lowest communication cost. As the number of communicated message is only seven, transmitted between the patient, healthcare, doctor (three party) 1. transmitted between patient and healthcare: $\{C_0\}$, $\{C_1\}$, $\{S_2, C_2\}$, 2. transmitted between healthcare and doctor: $\{C_3, S_3\}$, $\{C_4, S_4\}$ and 3. transfer between the patient and healthcare: $\{C_5, S_5\}$, $\{C_7, S_6\}$. Therefore, the total communication cost of our protocol is: $(128 + 128 + 160 + 128) + (160 + 128 + 128 + 160) + (128 + 160 + 128 + 160) = 1696$ bits.

In addition, Table 6, also shows storage cost offers a marginally better storage cost than the [1,45,46], [2–4,47]. But the overall cost (communication and storage cost) in the proposed design has less than the existing literature. Besides, a comparative statement of communication expenditure for related schemes in terms of percentage is shown in Fig. 8 and given below:

- Chen et al. [43] use 2576 bits, which is nearly 51.88% greater than our communication cost.
- Chen et al. [44] use 7952 bits, which is nearly 368.86% greater than our communication cost.
- Chiou et al. [45] use 6528 bits, which is nearly 284.90% greater than our communication cost.
- Mohit et al. [46] use 5312 bits, which is nearly 213.20% greater than our communication cost.
- Li et al. [1] use 3776 bits, which is nearly 122.64% greater than our communication cost.
- Kumar et al. [2] use 2128 bits, which is nearly 25.47% greater than our communication cost.
- Chandrakar et al. [3] use 9440 bits, which is nearly 456.60% greater than our communication cost.
- Chen et al. [47] use 4640 bits, which is nearly 173.58% greater than our communication cost.
- Kumari et al. [4] use 2976 bits, which is nearly 75.47% greater than our communication cost.

It is found that communication cost of Chandrakar et al. [3] scheme is 456.60% greater (highest) and Kumar et al. [2] is 25.47% greater (lowest) than our communication cost.

From Table 6 and Fig. 8, it is obvious that the communication cost of our protocol is very less in comparison to the other methods [43,44], [1–4,45–47].

7.2. Computation cost

The other functionality feature in terms of computation cost of the proposed protocol with existing schemes is also evaluated. To measure the performance of all protocol, a common platform for mobile phone Android 4.4.4KTU84P (1.8 GHz processor and 2 GB RAM) and windows 7 computer with a configuration of Intel Core Quad CPU (Q8300@2.50 GHz and 2 GB RAM) is used as per the literature [45]. It is found that the complexity of bit-wise XOR operation exhibits very little time in comparison to addition (+) and subtraction (-). Hence, the complexity of XOR and concatenation are considered as Big-O(1) or constant time. In addition, other cryptographic operations such as hash function, symmetric encryption, signature involve multiple steps to generate the output bits [55,56]. Hence, bit-wise XOR and concatenation operation are neglected in this proposed protocol.

A complete comparison of computation cost is shown in Table 7 in which the different execution time in each phase is illustrated. The description of the different execution time are given below [45]:

$T_{Sig} \approx 0.3317$ s: Execution time for a signature operation.

$T_A \approx 0.3057$ s: Execution of asymmetric encryption/ decryption operation.

$T_S \approx 0.0087$ s: Execution time for symmetric encryption or decryption operation.

$T_P \approx 0.0621$ s: Execution time for a bilinear pairing operation.

$T_H \approx 0.0005$ s: Execution time of one-way hash function.

$T_M \approx 0.0503$ s: Execution time for multiplication.

Table 6
Communication and storage cost comparison in *bits*.

Schemes ↓ Phases →		Communication	Cost	(CC)			Storage Cost	Total
	HUP	PDUP	TP	RDP	EP	Total:CC	SC	(CC+SC)
Chen et al. [43]	816	816	944	N/A	N/A	**2576**	768	**3,344**
Chen et al. [44]	1936	2064	2192	N/A	1760	**7952**	1280	**9,232**
Chiou et al. [45]	704	1600	2112	2112	N/A	**6528**	1648	**8,176**
Mohit et al. [46]	592	1744	1792	1184	N/A	**5312**	2144	**7,456**
Li et al. [1]	592	1232	720	1232	N/A	**3776**	2240	**6,016**
Kumar et al. [2]	496	496	544	592	N/A	**2128**	2192	**4,320**
Chandrakar et al. [3]	800	1120	5296	2224	N/A	**9440**	3776	**13,216**
Chen et al. [47]	1456	N/A	3008	176	N/A	**4640**	1760	**6,400**
Kumari et al. [4]	528	528	688	528	704	**2976**	2414	**5,390**
Proposed	N/A	544	576	576	N/A	**1696**	1408	**3,104**

HUP:Healthcare upload phase; PDUP:Patient data upload phase; TP:Treatment phase; RDP: Report Delivery phase; EP: Emergency phase.

Table 7
Computation cost comparison in seconds.

Schemes ↓ Phases →	HUP	PDUP	TP	RDP	EP	Total
Chen et al. [43]	$1T_{Sig} + 1T_M + 2T_P$ $4T_S + 2T_H + 3T_A$	$1T_M + 2T_P + 4T_S$ $2T_H + 3T_A$	$2T_{Sig} + 1T_M + 2T_P$ $7T_S + 2T_H + 4T_A$	N/A	N/A	$3T_{Sig} + 3T_M + 6T_P$ $15T_S + 6T_H + 10T_A$ $\approx$ **4.7091**
Chen et al. [44]	$1T_{Sig} + 4T_M + 4T_P$ $2T_S + 6T_H + 1T_A$	$1T_{Sig} + 4T_M + 2T_P$ $3T_S + 6T_H + 1T_A$	$2T_{Sig} + 4T_M + 4T_P$ $4T_S + 6T_H$	N/A	$2T_{Sig} + 3T_P + 6T_S$ $4T_H$	$6T_{Sig} + 12T_M + 15T_P$ $15T_S + 22T_H + 2T_A$ $\approx$ **4.379**
Chiou et al. [45]	$1T_{Sig} + 3T_P + 2T_S$ $7T_H$	$1T_{Sig} + 4T_P + 2T_S$ $12T_H$	$2T_{Sig} + 4T_M + 4T_P$ $4T_S + 6T_H$	$1T_{Sig} + 2T_P + 2T_S$ $8T_H$	N/A	$5T_{Sig} + 4T_M + 13T_P$ $10T_S + 33T_H$ $\approx$ **2.7705**
Mohit et al. [46]	$1T_{Sig} + 3T_S + 11T_H$	$2T_{Sig} + 2T_S + 10T_H$	$2T_{Sig} + 2T_S + 9T_H$	$1T_{Sig} + 2T_S + 5T_H$	N/A	$6T_{Sig} + 9T_S + 35T_H$ $\approx$ **2.086**
Li et al. [1]	$1T_{Sig} + 3T_S + 11T_H$	$2T_{Sig} + 4T_S + 10T_H$	$3T_{Sig} + 6T_S + 10T_H$	$1T_{Sig} + 2T_S + 8T_H$	N/A	$7T_{Sig} + 15T_S + 39T_H$ $\approx$ **2.4719**
Kumar et al. [2]	$1T_{Sig} + 5T_S + 10T_H$	$2T_{Sig} + 6T_S + 11T_H$	$3T_{Sig} + 6T_S + 12T_H$	$1T_{Sig} + 6T_S + 5T_H$	N/A	$7T_{Sig} + 23T_S + 37T_H$ $\approx$ **2.5405**
Chandrakar et al. [3]	$1T_{Sig} + 4T_S + 10T_H$	$2T_{Sig} + 7T_S + 9T_H$	$5T_{Sig} + 5T_S + 32T_H$	$2T_{Sig} + 2T_S + 8T_H$	N/A	$10T_{Sig} + 18T_S + 59T_H$ $\approx$ **3.503**
Chen et al. [47]	$4T_{Sig} + 4T_A + 2T_S + 2T_H$	N/A	$8T_{Sig} + 8T_A + 4T_S + 2T_H$	$2T_A$	N/A	$12T_{Sig} + 14T_A + 6T_S + 4T_H$ $\approx$ **8.3144**
Kumari et al. [4]	$4T_{Sig} + 4T_A + 2T_S + 2T_H$	$2T_{Sig} + 8T_S + 15T_H$	$2T_{Sig} + 8T_S + 13T_H$	$1T_{Sig} + 8T_S + 6T_H$	$6T_S + 10T_H$	$6T_{Sig} + 37T_S + 56T_H$ $\approx$ **2.3401**
Proposed	N/A	$1T_{Sig} + 7T_S + 14T_H$	$4T_{Sig} + 8T_S + 16T_H$	$1T_{Sig} + 6T_S + 6T_H$	N/A	$6T_{Sig} + 21T_S + 36T_H$ $\approx$ **2.1909**

In the proposed protocol, computation cost of messages is $6T_{Sig}$ + $21T_S$ + $36T_H$= 2.1909 s which is transmitted between the patient, healthcare and doctor. However, the related schemes [1–4,43–45,47] require 4.7091, 4.379, 2.7705, 2.419, 2.5405, 3.503, 8.3144, 2.3401 secs, respectively. Moreover, the proposed protocol utilizes slightly more computation overhead than [46].

In addition, a detailed comparison in terms of percentage increase of computation cost with the proposed scheme is shown in Fig. 9 and given below:

- The total execution time of Chen et al. [43] computation cost is 4.7091 s, which is nearly 114.93% greater than our computation cost.
- The total execution time of Chen et al. [44] computation cost is 4.379 s, which is nearly 99.87% greater than our computation cost.
- The total execution time of Chiou et al. [45] computation cost is 2.7705 s, which is nearly 26.45% greater than our computation cost.
- The total execution time of Mohit et al. [46] computation cost is 2.086 s, which is nearly 5% less than our computation cost.
- The total execution time of Li et al. [1] computation cost is 2.419 s, which is nearly 10.41% greater than our computation cost.
- The total execution time of Kumar et al. [2] computation cost is 2.5405 s, which is nearly 15.95% greater than our computation cost.
- The total execution time of Chandrakar et al. [3] computation cost is 3.503 s, which is nearly 59.88% greater than our computation cost.
- The total execution time of Chen et al. [47] computation cost is 8.3144 s, which is nearly 279.49% greater than our computation cost.
- The total execution time of Kumari et al. [4] computation cost is 2.3401 s, which is nearly 6.809% greater than our computation cost.

From Table 7 and Fig. 9, it is obvious that the computation cost of our protocol is very less in comparison to the other methods [43,44], [1–4,45,47] but slightly greater then [46], but it does not satisfy patient anonymity, impersonation attack.

Therefore, the proposed e-healthcare monitoring scheme is an efficient protocol compared to computation and communication functionality features.

8. Conclusion

This research article presents a secure and compact authentication protocol for e-Healthcare monitoring with private cloud services. To achieve this purpose, we have developed a new three-phase scheme, specifically Patient Data Upload Phase (PDUP), Treatment Phase (TP), and Report Delivery Phase (RDP), in addition to the registration phase for e-healthcare monitoring of recovered patients. The proposed scheme is well tested for various security aspects that comprise both informal security analysis “Man-in-the-middle attack, patient anonymity, doctor

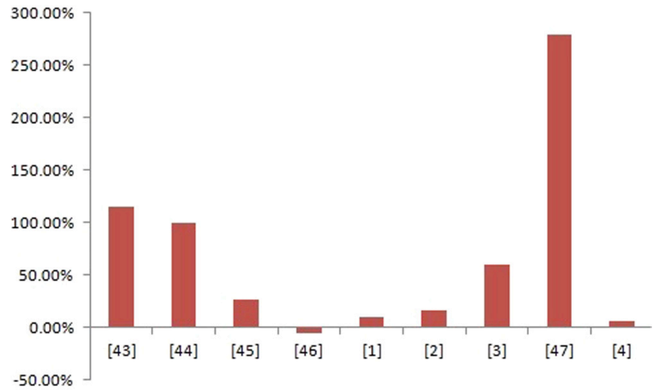


Fig. 9. Comparison (in percent) of computation cost with respect to proposed scheme.

anonymity, patient unlikability, impersonation attack, known key security, session key security, message authentication, data confidentiality, data non-repudiation" and formal security analysis "BAN logic and ROR model". In addition, the performance effectiveness of the proposed protocol is also evaluated in terms of computation, communication, storage cost, and a fair comparison with existing scientific literature. A comparative study of the proposed scheme with others gives efficient functionality features and a lightweight authentication scheme. Finally, this type of development in e-healthcare monitoring through TMIS may provide a step forward towards humanizing effectively and privacy convenience treatment for recovered patients with any severe disease.

CRediT authorship contribution statement

Prerna Mohit: Conception and design of study, Writing - original draft.

References

[1] Li C-T, Shih D-H, Wang C-C. Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. Comput Methods Programs Biomed 2018;157:191–203.

[2] Kumar V, Ahmad M, Kumari A. A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted TMIS. Telemat Inform 2019;38:100–17.

[3] Chandrakar P, Sinha S, Ali R. Cloud-based authenticated protocol for healthcare monitoring system. J Ambient Intell Humaniz Comput 2019;1–17.

[4] Kumari A, Kumar V, Abbasi MY, Kumari S, Chaudhary P, Chen C-M. CSEF: Cloud-based secure and efficient framework for smart medical system using ECC. IEEE Access 2020;8:107838–52.

[5] Karthigaiveni M, Indrani B. An efficient two-factor authentication scheme with key agreement for IoT based E-health care application using smart card. J Ambient Intell Humaniz Comput 2019;1–12.

[6] Savitha V, Karthikeyan N, Karthik S, Sabitha R. A distributed key authentication and OKM-ANFIS scheme based breast cancer prediction system in the IoT environment. J Ambient Intell Humaniz Comput 2020;1–13.

[7] Sahoo SS, Mohanty S, Majhi B. A secure three factor based authentication scheme for health care systems using IoT enabled devices. J Ambient Intell Humaniz Comput 2020;1–16.

[8] Jiang Q, Ma J, Yang C, Ma X, Shen J, Chaudhry SA. Efficient end-to-end authentication protocol for wearable health monitoring systems. Comput Electr Eng 2017;63:182–95.

[9] Srinivas J, Das AK, Kumar N, Rodrigues J. Cloud centric authentication for wearable healthcare monitoring system. IEEE Trans Dependable Secure Comput 2018.

[10] Ali R, Pal AK, Kumari S, Sangaiah AK, Li X, Wu F. An enhanced three factor based authentication protocol using wireless medical sensor networks for healthcare monitoring. J Ambient Intell Humaniz Comput 2018;1–22.

[11] Chatterjee K. An improved authentication protocol for wireless body sensor networks applied in healthcare applications. Wirel Pers Commun 2019;1–19.

[12] Alzahrani BA, Irshad A, Albeshri A, Alsubhi K. A provably secure and lightweight patient-healthcare authentication protocol in Wireless Body Area networks. Wirel Pers Commun 2020;1–23.

[13] Li X, Peng J, Obaidat MS, Wu F, Khan MK, Chen C. A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems. IEEE Syst J 2019;14(1):39–50.

[14] Selvam L, Renjit JA. On developing dynamic and efficient cryptosystem for safeguarding healthcare data in public clouds. J Ambient Intell Humaniz Comput 2020.

[15] Kaufman LM. Can public-cloud security meet its unique challenges? IEEE Secur Privacy 2010;8(4):55–7.

[16] Saheb T, Izadi L. Paradigm of IoT big data analytics in healthcare industry: a review of scientific literature and mapping of research trends. Telemat Inform 2019.

[17] Shen J, Liu D, Liu Q, Sun X, Zhang Y. Secure authentication in cloud big data with hierarchical attribute authorization structure. IEEE Trans Big Data 2017.

[18] Nikou S, Agahari W, Keijzer-Broers W, de Reuver M. Digital healthcare technology adoption by elderly people: A capability approach model. Telemat Inform 2019;101315.

[19] Peris-Lopez P, Hernandez-Castro JC, Estevez-Tapiador JM, Ribagorda A. Emap: An efficient mutual-authentication protocol for low-cost rfid tags. In: OTM Confederated International Conferences "on the Move To Meaningful Internet Systems". Springer; 2006, p. 352–61.

[20] Das AK. A secure and efficient user anonymity-preserving three-factor authentication protocol for large-scale distributed wireless sensor networks. Wirel Pers Commun 2015;82(3):1377–404.

[21] Alkhater N, Walters R, Wills G. An empirical study of factors influencing cloud adoption among private sector organisations. Telemat Inform 2018;35(1):38–54.

[22] Akbarzadeh A, Bayat M, Zahednejad B, Payandeh A, Aref MR. A lightweight hierarchical authentication scheme for internet of things. J Ambient Intell Humaniz Comput 2019;10(7):2607–19.

[23] Mohit P, Amin R, Biswas G. Design of authentication protocol for wireless sensor network-based smart vehicular system. Veh Commun 2017;9:64–71.

[24] Kumar V, Ahmad M, Mishra D, Kumari S, Khan MK. RSEAP: RFID based secure and efficient authentication protocol for vehicular cloud computing. Veh Commun 2020;22:100213.

[25] Wu Z-Y, Lee Y-C, Lai F, Lee H-C, Chung Y. A secure authentication scheme for telecare medicine information systems. J Med Syst 2012;36(3):1529–35.

[26] Debiao H, Jianhua C, Rui Z. A more secure authentication scheme for telecare medicine information systems. J Med Syst 2012;36(3):1989–95.

[27] Wei J, Hu X, Liu W. An improved authentication scheme for telecare medicine information systems. J Med Syst 2012;36(6):3597–604.

[28] Khan MK, Kumari S. An authentication scheme for secure access to healthcare services. J Med Syst 2013;37(4):9954.

[29] Amin R, Biswas G. A secure three-factor user authentication and key agreement protocol for tmis with user anonymity. J Med Syst 2015;39(8):78.

[30] Mishra D, Mukhopadhyay S, Chaturvedi A, Kumari S, Khan MK. Cryptanalysis and improvement of Yan et al.'s biometric-based authentication scheme for telecare medicine information systems. J Med Syst 2014;38(6):24.

[31] Wazid M, Das AK, Kumari S, Li X, Wu F. Design of an efficient and provably secure anonymity preserving three-factor user authentication and key agreement scheme for TMIS. Secur Commun Netw 2016;9(13):1983–2001.

[32] Li X, Peng J, Kumari S, Wu F, Karuppiah M, Choo K-KR. An enhanced 1-round authentication protocol for wireless body area networks with user anonymity. Comput Electr Eng 2017;61:238–49.

[33] Sowjanya K, Dasgupta M, Ray S. An elliptic curve cryptography based enhanced anonymous authentication protocol for wearable health monitoring systems. Int J Inf Secur 2020;19(1):129–46.

[34] Liu J, Zhang L, Sun R. 1-RAAP: An efficient 1-round anonymous authentication protocol for wireless body area networks. Sensors 2016;16(5):728.

[35] Chandrakar P, Om H. A secure and robust anonymous three-factor remote user authentication scheme for multi-server environment using ECC. Comput Commun 2017;110:26–34.

[36] Ali R, Pal AK. Three-factor-based confidentiality-preserving remote user authentication scheme in multi-server environment. Arab J Sci Eng 2017;42(8):3655–72.

[37] Li X, Niu J, Karuppiah M, Kumari S, Wu F. Secure and efficient two-factor user authentication scheme with user anonymity for network based e-health care applications. J Med Syst 2016;40(12):268.

[38] Shen J, Gui Z, Ji S, Shen J, Tan H, Tang Y. Cloud-aided lightweight certificateless authentication protocol with anonymity for wireless body area networks. J Netw Comput Appl 2018;106:117–23.

[39] Amin R, Islam SH, Biswas G, Khan MK, Kumar N. A robust and anonymous patient monitoring system using wireless medical sensor networks. Future Gener Comput Syst 2018;80:483–95.

[40] Ever YK. Secure-anonymous user authentication scheme for e-healthcare application using wireless medical sensor networks. IEEE Syst J 2018;13(1):456–67.

[41] Qi M, Chen J. Anonymous biometrics-based authentication with key agreement scheme for multi-server environment using ECC. Multimedia Tools Appl 2019;78(19):27553–68.

[42] Kasyoka P, Kimwele M, Mbandu Angolo S. Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system. J Med Eng Technol 2020;44(1):12–9.

[43] Chen C-L, Yang T-T, Shih T-F. A secure medical data exchange protocol based on cloud environment. J Med Syst 2014;38(9):1–12.

[44] Chen C-L, Yang T-T, Chiang M-L, Shih T-F. A privacy authentication scheme based on cloud for medical environment. J Med Syst 2014;38(11):1–16.

[45] Chiou S-Y, Ying Z, Liu J. Improvement of a privacy authentication scheme based on cloud for medical environment. J Med Syst 2016;40(4):1–15.

[46] Mohit P, Amin R, Karati A, Biswas G, Khan MK. A standard mutual authentication protocol for cloud computing based health care system. J Med Syst 2017;41(4):50.

[47] Chen C-L, Huang P-T, Deng Y-Y, Chen H-C, Wang Y-C. A secure electronic medical record authorization system for smart device application in cloud computing environments. Hum-Centr Comput Inform Sci 2020;10:1–31.

[48] Mo J, Shen W, Pan W. An improved anonymous authentication protocol for wearable health monitoring systems. Wirel Commun Mob Comput 2020;2020.

[49] Dolev D, Yao A. On the security of public key protocols. IEEE Trans Inform Theory 1983;29(2):198–208.

[50] Katz J, Lindell Y. Introduction to modern cryptography. CRC Press; 2014.

[51] Dodis Y, Reyzin L, Smith A. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: International conference on the theory and applications of cryptographic techniques. Springer; 2004, p. 523–40.

[52] Burrows M, Abadi M, Needham RM. A logic of authentication. Proc R Soc Lond Ser A Math Phys Eng Sci 1989;426(1871):233–71.

[53] Abdalla M, Fouque P-A, Pointcheval D. Password-based authenticated key exchange in the three-party setting. In: International workshop on public key cryptography. Springer; 2005, p. 65–84.

[54] Das AK, Wazid M, Yannam AR, Rodrigues JJ, Park Y. Provably secure ECC-based device access control and key agreement protocol for IoT environment. IEEE Access 2019;7:55382–97.

[55] Granlund T. Instruction latencies and throughput for AMD and Intel x86 Processors. Technical report, KTH; 2012.

[56] Barman S, Shum HP, Chattopadhyay S, Samanta D. A secure authentication protocol for multi-server-based e-healthcare using a fuzzy commitment scheme. IEEE Access 2019;7:12557–74.