The Journal of Supercomputing (2022) 78:16167–16196
https://doi.org/10.1007/s11227-022-04513-4

RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure

Vinod Kumar[1] · Mahmoud Shuker Mahmoud[2] · Ahmed Alkhayyat[3] · Jangirala Srinivas[4] · Musheer Ahmad[5] · Adesh Kumari[6]

Accepted: 6 April 2022 / Published online: 2 May 2022

Abstract

With the fast growth of technologies like cloud computing, big data, the Internet of Things, artificial intelligence, and cyber-physical systems, the demand for data security and privacy in communication networks is growing by the day. Patient and doctor connect securely through the Internet utilizing the Internet of medical devices in cloud-healthcare infrastructure (CHI). In addition, the doctor offers to patients online treatment. Unfortunately, hackers are gaining access to data at an alarming pace. In 2019, 41.4 million times, healthcare systems were compromised by attackers. In this context, we provide a secure and lightweight authentication scheme (RAPCHI) for CHI employing Internet of medical Things (IoMT) during pandemic based on cryptographic primitives. The suggested framework is more secure than existing frameworks and is resistant to a wide range of security threats. The paper also explains the random oracle model (ROM) and uses two alternative approaches to validate the formal security analysis of RAPCHI. Further, the paper shows that RAPCHI is safe against man-in-the-middle and reply attacks using the simulation programme AVISPA. In addition, the paper compares RAPCHI to related frameworks and discovers that it is relatively light in terms of computation and communication. These findings demonstrate that the proposed paradigm is suitable for use in real-world scenarios.

Keywords Cloud-healthcare infrastructure · Elliptic curve cryptography · Internet of medical things · Random oracle model · Security and privacy

✉ Adesh Kumari
adeshbhucker@gmail.com

Extended author information available on the last page of the article

1 Introduction

People choose an applicable medical system for high perfection of healthcare due to the quick growth of the Internet and its technology [1, 2]. Health centres provide medical services in remote regions in order to support the development of medical institutions and the medical sectors. The medical structure not only offers the necessary facilities, but it also improves medical care while maintaining the protection of patient data. Hospitals are working to develop their assistance so that patients may receive care that is easily accessible. When a patient enters the hospital, medical personnel immediately creates a medical report detailing their care in order to prevent mistakes. However, because this is not feasible everywhere, internet medical care has become a need in today's world. Blood pressure, heart rate, body temperature, ECG, electromyography, and other physiological data are all measured by the medical equipment. The employment of wireless-assisted technology has removed the bulk of physical, geographical, and organisational barriers, removing the need to pass over medical papers and information to the relevant authorities [3]. Patients save information in the cloud for secure retrieval in a cloud-based telecare medical information system (TMIS) in medical management. Because it is well recognised that the cloud environment is not completely secure, a robust authentication structure should be implemented to handle security risks [4]. Both the patient and the doctor can share information over the cloud via TMIS. Following that the doctor gathers medical information from patients and uploads a diagnosis report to the cloud as if they had specifically participated. The medical report is a very important aim in TMIS to maintain security and privacy. In a CHI, it is not possible to acknowledge it openly. In terms of security and privacy, data transmitted between the cloud, the patient, and the doctor are a major concern that must be addressed in this system. The medical report falls under the heading of "essential information" and is vulnerable to theft. It might be a delicate decline in one's life [5], and therefore, it is an important to provide a secure authentication framework so that an attacker cannot look into patients' medical records [6].

IoMT, Internet of Things, Internet of Service, Artificial Intelligence, Cyber-Physical Systems (CPS), and Multi-access Edge-based Cloud Computing are some of the technical contexts in which CHIs operate. Due to many advantages of cloud computing platform in an IoMT driven smart healthcare system and extensive information processing, such as the requirement of mobility support, heterogeneity distributed architecture, and other factors, data security and privacy, authentication, and key agreement protocols in cloud environments are no longer secure in IoMT healthcare systems. A user's data security, privacy, and physical control over the communication system are all compromised under this paradigm. Illegal data and data breath actions such as copy, deletion, alteration, and distribution can pose a number of security risks in these systems [7–9]. Data integrity, authenticity, secrecy, and other aspects of the cloud system may be affected by an attacker. As a result, it is a critical to develop a new solution against malicious attackers in order to build a safe and efficient environment.

Smart CHI is a technology that enables for the transfer of patient data across two or more sites. During COVID-19 pandemic, there are many users using many application of CHI. Hackers are obtaining access to data at an alarming pace. In 2019, healthcare systems were hacked 41.4 million times. In July 2020, *640,000* patient records were hacked at Florida Orthopedic Institute. In June 2020, Elite Emergency Physicians will have served *550,000* patients. It is necessary to preserve the data integrity of a patient in this system. CHI is playing an important role in medical user care for preserving the required physical distance during the ongoing COVID-19 epidemic. To safeguard sensitive patient data, integrity, secrecy, authentication, and key agreement methods are required in the current situation [10].

IoMT is a new field of CPS that aims to create a ubiquitous patient monitoring system. The majority of CHI's demands are met by this technology. It also allows for more consistent and definite essential treatment before the patient's health worsens. It is a cutting-edge technology approach for saving human lives by lowering the cost of medical treatment while removing the need for physical contact between the doctor and the patient. It has benefited medical users during COVID-19, according to [11]. The authentication and key agreement protocol in CHI is designed to manage security and privacy, including computation, data hiding, message authentication, mutual authentication, integrity, confidentiality, anonymity, non-repudiation, session key security communication, watermarking, and presume property rights, among other things [12]. A CHI system based on IoMT is expected to deal with algorithms that are computationally efficient, content authentication and key agreement that is safe, and so on.

1.1 Related work

In cloud-medical system, user should have particular access of medical information and privilege. They store data in cloud and TMIS can be classified into several applications to client constraints and organized classifications. A cloud-based approach for healthcare systems was proposed by Padhy et al. [13]. Banerjee et al. [14] proposed a cloud-based emergency healthcare system that retrieves the patient's data centrally before any medical treatment begins. Li et al. [15] suggested a privacy-preserving strategy for TMIS employing a cloud environment in order to offer security, privacy, and medical resource access. Chatterjee et al. [16] proposed a secure biometric authentication protocol for TMIS with proper user authentication. In this protocol, authors had not discussed the user linkability and users relationship. Islam et al. [17] created a framework for user authentication and key agreement that is highly suited to modern information systems. Wazid et al. [18] proposed user authentication and session key agreement schemes with client anonymity for TMIS. It is suggested the patient's healthcare record should be secure from malicious attacks. RSA-based safe authentication mechanism with user anonymity was proposed by Sutrala et al. [19]. They also used a verification tool to assure the security of the medical communication system. Chen et al. developed a cloud-based TMIS authentication technique [20] in 2014. In 2015, Amin et al. offered design and investigation

authentication work for a healthcare system [21], He et al proposed robust authentication work for TMIS [22], and Zhou et al suggested a security-preserving cloud-supported wireless body area network approach [23]. Castiglione et al. developed a Software-as-a-Service (SaaS)-assisted cloud heterogeneous equipments communication system for TMIS resources used by clients [24]. Chiou et al. [25] exhibited Chen et al. framework [20] in 2016, claiming that it fails to provide actual telemedicine, communication authentication, or patient anonymity. Then, in a similar situation, Chiou et al. devised a modification technique. In 2017, Mohit et al. [26] challenged that Chiou et al.'s protocol cannot support in mobile stolen verifier attack and patient anonymity. In addition to, Mohit et al. suggested authentication work for healthcare system. Kumar et al. [6] and Li et al. [27] shown the drawbacks of Mohit et al. scheme. Most recently, Kumar et al. [28] reviewed Li et al. scheme and discussed demerits of [27]. In 2019, Chandrakar et al. [29] presented cloud-based authenticated protocol for healthcare monitoring system which is not secure against patient anonymity, data confidentiality, impersonation attack and patient password change. For wireless body area network, Chen and Peng proposed analysing and improving a mutual authentication and key agreement mechanism [30]. Chen et al. [31] presented an authorization mechanism for smart device usage in cloud environments in the year 2020. For RFID-based healthcare systems, Zhu et al. [32] proposed a lightweight authentication technique. Arunkumar and Kousalya [33] suggested a decentralised and safe lightweight E-health system based on blockchain technology. For TMIS, Amintoosi and Nikooghadam suggested an ECC-based authentication and key management mechanism that is probably safe [33]. In this protocol, they claimed that Khatoon et al.'s [34] scheme is vulnerable to known-session-specific temporary information attacks as well as perfect forward secrecy. Deebak and Turjman [35] proposed a protocol for CHI using IoMT. It does not contain patient password change phase, high computation and communication cost. Chen et al. [36] a RFID authentication protocol for epidemic prevention and epidemic emergency management systems. They claimed that the designed scheme can aid in the realisation of the safety and traceability of epidemic prevention materials, as well as improving the automation and decision-making efficiency of epidemic prevention. Hathaliy and Tanwar presented an exhaustive survey on security and privacy issues in Healthcare 4.0 [37]. The authors claim that different taxonomies used in Healthcare 4.0 to investigate various security and privacy issues are also presented in a structured manner. The benefits and drawbacks of various security and privacy techniques are then discussed. Awotunde et al. proposed the big data analytics of IoT-based cloud system framework: smart healthcare monitoring systems [38]. They discussed Raj et al. published a work entitle issues and challenges related to privacy and security in healthcare using IoT, Fog, and cloud computing [39]. According to them, the published paper also includes some methodology used in various research papers to address security and privacy issues in the IoT, fog, and cloud computing environments. Singh et al. [40] proposed IoT for sustaining a smart and secure healthcare system. The performance of work [40] is measured in terms of

latency, network utilisation, RAM utilisation, and energy consumption. On the other hand, the suggested classifier's accuracy, precision, specificity, sensitivity, and F1 score are all evaluated. The results show that the proposed framework and classifier consistently outperform conventional frameworks and classifiers.

1.2 Motivation and contribution

Because of their increasing utility, dependability, autonomy, efficiency, and safety, various scopes of CHI in IoMT are currently opening as research and technology advance. By allowing users to obtain programmes on demand, cloud computing is excellent at reducing infrastructure expenses. However, impersonation, stolen-verifier attacks, data non-repudiation, data confidentiality, anonymity, known-key security, replay attack, message authentication, privileged-insider attacks, parallel session, and man-in-the-middle attacks are all vulnerable to communication across entities in CHI. CHI's security and privacy were breached by hackers during the COVID-19 epidemic. As a result, in a cloud-based CHI environment, information, security, and privacy are top priorities. In recent years, protocols [20, 25–27, 29, 35, 41] have been proposed in healthcare communication systems. However, these are insufficient to address the system's fundamental security and privacy issues. As a result, many procedures have significant omissions. A secure and efficient structure is required to safeguard CHI's security and privacy at all times. In this paper, the authors introduce a novel RAPCHI: Robust authentication protocol method for IoMT-based CHI to assure the security and privacy of CHI. The proposed RAPCHI has a number of important characteristics, which are listed below:

- To ensure the security of CHI as an IoMT application, an authentication and key agreement are formed among the patient, cloud server, and doctor.
- Without keeping data in a cloud database system, a session key is formed between patient and doctor.
- Further, RAPCHI is also resistant to a variety of security threats and meets a number of security requirements.
- Based on the random oracle concept, we give two independent formal security analyses of RAPCHI.
- We use the AVISPA tool to simulate RAPCHI.
- The comparison study shows that during a pandemic, RAPCHI is more effective than other protocols in the same context.

1.3 Threat model for RAPCHI

We consider the Dolev-Yao (DY) [42] in RAPCHI. Any opponent E has the following assumptions and capabilities:

- The public network system is open to E. In the network system, he/she can create new messages, retrieve, inject, edit, replay, and discard any information.
- Intruders or public users of the underlying network infrastructure can both be E.
- E knows the public keys of all the users in public channel.

1.4 The paper organization

The remaining paper is constructed as follows. In Section 2, we express the preliminaries. In Section 3, we proposed RAPCHI framework for CHI. Section 4 describes security analysis. Section 5 describes performance analysis. Lastly, we discuss conclusion of the paper. Furthermore, we have given notations in Table 1.

Table 1 Notations

Symbol	Description
l	The security parameter
P	The Patient
$\mathcal{E}(F_q)$	Elliptic curve $\mathcal{E}$ over a prime finite field F_q
q	Large prime
H	The healthcare centre with secret key γ
ID_i	Unique identity of i^{th} participant
$h(\cdot)$	Collision free one-way hash function
D	The doctor
$E_k(M)$	Encryption of information M using key k
Sig_i	The signature of i^{th} participant
S	The cloud server
PK_i	Public key of i participant
$SK_{\chi\psi}$	The computing session key between entities χ and ψ
$S_K(J)$	Signature of J with using key K
$\chi \stackrel{?}{=} \psi$	Whether χ equals ψ
$V_K(J)$	Verification of signature J using key K
SK_i	The secret key of i^{th} participant
K_i	The executing key of i^{th} participant
PWi	The password of i^{th} participant
$D_k(M)$	Decryption of information M using key k
E	Adversary
ΔT	Maximum communication delay
ECC	Elliptic curve cryptography
G	Additive ECC-based group
g	Base point of G
s	The secret key of S
$i \cdots \Rightarrow j : \{M\}$	i sends information M to j via secure channel
$i \cdots \rightarrow j : \{M\}$	i sends information M to j via public channel

2 Preliminaries

2.1 One-way collision-resistant hash function

Definition Hash function converts arbitrary string length $x \in \{0,1\}^*$ in finite length string $h(x) \in \{0,1\}^l$. H_i is the hash function then, $H_i : \{0,1\}^* \rightarrow \{0,1\}^l$.

The following properties of best hash function as below [6]:

- If inputs x then output the digest $h(x)$.
- *One-way* If output $y = h(x)$. Then, it is hard to compute x.
- *Weak-collision resistance* If x is the input and $h(x) = h(y)$ is the output. Finding y is then computationally impossible..
- *Strong-collision resistance* If $h(x) = h(y)$ is the output. Finding pair (x, y) with $x \neq y$ then becomes computationally impossible.

It is a deterministic method that takes any string as input and returns a fixed-length string as output. Let $Adv_E^{HASH}(t_1)$ denote any E's benefices in obtaining collision. Then, we have $Adv_E^{HASH}(t_1) = Prob[(\varphi, \psi) \Leftarrow_R E : \varphi \neq \psi \; and \; h(\varphi) = h(\psi)]$, where $Prob[W]$ represents the probability of a random appearance W, and $(\varphi, \psi) \Leftarrow_R E$ expresses the pair (φ, ψ) is elected randomly by E. Here, E is made probabilistic, and the probability in advantage is calculated using any E with a computing time of t_1. The $h(.)$ is called collision-resistant, if $Adv_E^{HASH}(t_1) \leq \epsilon_1$, for any adequately slight $\epsilon_1 > 0$ [43].

2.2 Elliptic curve cryptography

Classically, cryptographic protocols are used to ensure the security and privacy of communicated data. An emerging trend for security and privacy, authors are using two cryptographic techniques 1) symmetric key cryptography and 2) public key cryptography. In this paper, we use the concepts of elliptic curve cryptography (ECC) which is the branch of public key cryptography. The basic information of ECC is explained as below:

Let q be the large prime then F_q be the prime finite field of order q. An equation of elliptic curve (EC) is given by $v^2 = u^3 + cu + d \;\; mod \;\; q$ with $c, d \in F_q$. The elliptic curve is said to be non-singular if $4c^3 + 27d^2 \;\; mod \;\; q \neq 0$. Then, G define as $G = \{(u, v) : u, v \in F_q; (u, v) \in \mathcal{E}\} \bigcup \{\Theta\}$, where the point Θ is known as the identity element of G. ECC contains the following properties:

1. If $X = (u, v) \in G$ then $-X = (v, -v)$ and $X + (-X) = \Theta$.
2. If $X = (u, v) \in G$ then scalar multiplication: $kX = X + X + X ..... + X \; (k - times)$.
3. If $X = (u_1, v_1)$, $Y = (u_2, v_2) \in G$. Then, $X + Y = (u_3, v_3)$, where $u_3 = \mu^2 - u_1 - u_2 \;\; mod \;\; q, v_3 = (\mu(u_1 - u_3) - v_1) \;\; mod \;\; q$ and

$$\mu = \begin{cases} \frac{v_2 - v_1}{u_2 - u_1} \ mod \ q \ \ if \ X \neq Y \\ \\ \frac{3u_1^2 + c}{2v_1} \ mod \ q \ \ if \ X = Y \end{cases}$$

For more information of elliptic curve group and its properties, we refer [44]. The comparison of key size in ECC, DSA, RSA, and Diffie–Hellman given in Table 2.

2.3 ECC-based computational hard problems

The following computational hard problems which are based on ECC:

- *Elliptic curve Discrete Logarithms problem (ECDLP)* The detail of ECDLP discussed in [6].
  Remark The symbol $x \Leftarrow_R T$ to express value x is taken randomly from T.
  Input: (R, S, r) for some $k, r \in_R Z_q^*$.
  Output Yes, if $S = rR$, means that, $k = r$, and result *No*, otherwise.
  Assume the following two handling:
  $D_{real} = \{x \Leftarrow_R Z_q^*, L = R, M = S = kR, N = k : (L, M, N)\}$.
  $D_{rand} = \{k, r \Leftarrow_R Z_q^*, L = R, M = S = kR, N = r : (L, M, N)\}$.
  The benefits of any probabilistic, polynomial-time 0/1-listed recognizer $\mathbb{D}$ in solving ECDLP on $\mathcal{E}(F_q)$ is explained as $Adv_{\mathbb{D},\mathcal{E}}^{ECDLP} = |Prob[(L, M, N) \leftarrow D_{real} : \mathbb{D}(L, M, N) = 1] - Prob[(L, M, N) \leftarrow D_{rand} : \mathbb{D}(L, M, N) = 1]|$, where the probability $Prob(.)$ is take on the random values k and r. $\mathbb{D}$ is called a (t_2, ϵ_2)- ECDLP recognizer for $\mathcal{E}$, if $\mathbb{D}$ executes at most in time t_2 such that $Adv_{\mathbb{D},\mathcal{E}}^{ECDLP}(t_2) \geq \epsilon_2$.
- *ECDLP assumption* There exits no $t_2 \geq \epsilon_2$-ECDLP recognizer for $\mathcal{E}$. On the otherhand, for every probabilistic, polynomial-time 0/1- listed recognizer $\mathbb{D}$, we have $Adv_{\mathbb{D},\mathcal{E}}^{ECDLP}(t_2) < \epsilon_2$, for any sufficient small $\epsilon_2 > 0$ [47].
- *Elliptic curve computational Diffie–Hellman problem (ECCDHP)* The detail of ECCDHP discussed in [6].

Table 2 Compassion of the key size [45, 46]

S.No.	ECC key Size (bits)	RSA key Size (bits)	Diffie–Hellman and DSA
1.	163	1024	L = 1024, N = 160
2.	256	3072	L = 3072, N = 256
3.	384	7680	L = 7680, N = 384
4.	512	15360	L = 15360, N = 512

N = Size of private key and L = Size of public

3 The RAPCHI framework

Figure 1 shows the proposed framework's architecture.

There are four participants in CHI such as Patient, Doctor, Cloud server, and Body sensor RAPCHI framework having following phases:

3.1 Initialization

S selects security parameter l, the nonsingular elliptic curve $\mathcal{E}(F_q)$ over F_q, elliptic curve additive group G with base point g, hash function $h : \{0,1\}^* \rightarrow Z_q^*$ and ECDLP which is intractable. S publishes public parameters $\{F_q, \mathcal{E}(F_q), G, g, h(.), l\}$.

3.2 Patient registration in cloud server

With the help of medical device, P gets registration by S via secure channel as below:

Step 1. To register with S, P inputs identity ID_P and password pw_P. Then, P generates random value $a_P \in Z_q^\star$ and selects as a secret key. Further, P executes $PWP = pw_P \oplus h(pw_P \| ID_P \| a_P)$ and $P \Rightarrow S : M_{PR1} = \{PWP, ID_P\}$.

Step 2. On getting M_{PR1}, S verifies ID_P and PWP in database. If, these are new, S computes $A_P = h(h(ID_P) \oplus h(PWP \| ID_P))$, generates random value $b_P \in Z_q^\star$, computes $P_1 = h(ID_P \| A_P \| b_P)$, $P_2 = h(P_1 \| ID_P \| A_P)$, $B_P = h(ID_P \| s \| P_1 \| A_P \| P_2)$, stores $\{A_P, B_P, P_1, P_2, g, G\}$ in database and $S \Rightarrow P : M_{RP2} = \{A_P, B_P, P_1, P_2, g, G\}$.

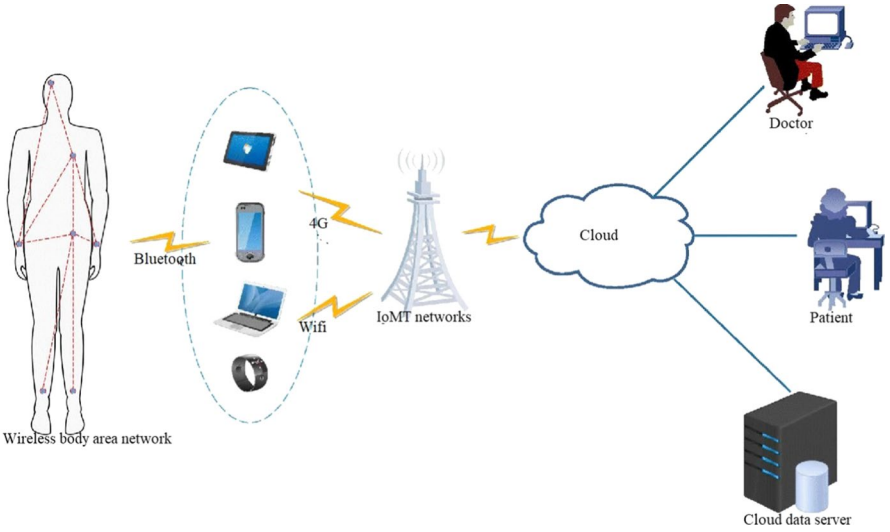

Fig. 1 Architecture for RAPCHI

Step 3. On collecting M_{RP2}, P sets public key $PK_P = a_P.g$ and stores parameters $\{A_P, B_P, P_1, P_2, g, G\}$ in database.

3.3 Doctor registration in cloud server

D gets registration via secure channel as below:

Step 1. To register with S, D inputs identity ID_D and $D \Rightarrow S : M_{RD1} = \{ID_D\}$.

Step 2. On collecting $\{ID_D\}$, S verifies ID_D in database. If, ID_D is new, S generates random number $b_D \in Z_q^\star$, computes $D_1 = h(ID_D \| b_D)$, $B_D = h(D_1 \| s \| b_D)$, stores $\{D_1, B_D, g, G\}$ in database and $S \Rightarrow D : M_{RD2} = \{D_1, B_D, g, G\}$.

Step 3. On getting M_{RD2}, S generates $a_D \in Z_q^\star$ and sets as a public key $PK_D = a_D.g$. Further, D stores parameters $\{D_1, B_D, g, G\}$ in database.

3.4 Patient login, authentication and key agreement phase

P uses the medical sensors device, forward regular medical record to S and get treatment by D via S. The process of this phase is explained as below:

Step 1. P login with ID'_P and pw'_P. Further, P computes $PWP' = pw'_P \oplus h(pw'_P \| ID'_P \| a_P)$, $A'_P = h(h(ID'_P) \oplus h(PWP' \| ID'_P))$ and verifies $A'_P \stackrel{?}{=} A_P$. After that P generates random number $x \in Z_q^\star$, computes $\alpha = x.g$, inserts medical data $M_P = (ID_P, Data_P)$, computes signature $Sig_P = S_{SK_P}(h(M_P))$, computes $H_1 = h(ID_P \| PK_D \| (ID_P \oplus T_1))$, $H_2 = h(A_P \| B_D \| (ID_P)$, encrypts $E_1 = E_{h(ID_P \| P_1 \| P_2)}(H_1, M_P, \alpha, Sig_P, T_1)$ by using key $h(ID_P \| P_1 \| P_2)$. Then, $P \rightarrow S : M_1 = \{E_1, H_2, T_1\}$.

Step 2. On collecting M_1, S verifies $T_2 - T_1 \leq \triangle T$ and $H_2^* \stackrel{?}{=} h(P_P \| B_P \| ID_D)$. Further, S computes $ID_{P1} = ID_P \oplus h(ID_1 \| ID_D \| B_D)$, $H_3 = h(ID_D \| B_D \| D_1 \| T_3)$, encrypts $E_2 = E_{h(ID_D \| B_D \| D_1)}(E_1, H_3, ID_{P1}, P_1, P_2, B_P)$ by using key $h(ID_D \| B_D \| D_1)$. Then, $S \rightarrow D : M_2 = \{E_2, T_3\}$.

Step 3. On getting M_2, D verifies $T_4 - T_3 \leq \triangle T$. Then, D decrypts $(E_1, H_3, ID_{P1}, P_1, P_2, B_P) = D_{h(ID_D \| B_D \| D_1)}(E_2)$ by using key $h(ID_D \| B_D \| D_1)$, verifies $H_3^* \stackrel{?}{=} h(ID_D \| B_D \| D_1 \| T_3)$, computes $ID_P^* = ID_{P1} \oplus h(ID_1 \| ID_D \| B_D)$, decrypts $(H_1, M_P, \alpha, Sig_P, T_1) = D_{h(ID_P^* \| P_1 \| P_2)}(E_1)$ by using key $(ID_P^* \| P_1 \| P_2)$, verifies $H_1^* \stackrel{?}{=} h(ID_P \| a_D.g \| (ID_P \oplus T_1))$ and $V_{PK_P}(Sig_P) \stackrel{?}{=} h(M_P)$. Further, D generates medical report $M_D = (ID_D, Data_D)$, computes signature $Sig_D = S_{SK_D}(h(M_D))$. Then, D generates random number $y \in Z_q^\star$, computes $\beta = y.g$, $MAC_D = h(ID_P^* \| ID_D \| B_P \| B_D \| T_5)$, session key $SK_{DP} = h(ID_P^* \| ID_D \| Sig_P \| Sig_D \| MAC_D \| B_D \| B_P \| \| y.\alpha \| T_5)$, $ID_{D1} = ID_D \oplus h(Sig_P \| B_P \| H_1^*)$, encrypts $E_3 = E_{h(H_1^* \| B_P \| P_2)}(ID_{D1}, MAC_D, Sig_D, M_D, B_D, \beta, T_5)$ by using key $h(H_1^* \| B_P \| P_2)$ and $D \rightarrow S : M_3 = \{E_3, T_5\}$.

Step 4. On collecting M_3, S verifies $T_6 - T_5 \leq \triangle T$ and $S \rightarrow P : M_4 = \{E_3, T_5, T_7\}$.

Step 5. Upon accepting M_4, P verifies $T_8 - T_7 \leq \bigtriangleup T$. Then, P computes $ID_D^* = ID_{D1} \oplus h(Sig_P \| B_P \| H_1)$, decrypts $(ID_{D1}, MAC_D, Sig_D, M_D, B_D, \beta, T_5) = D_{h(H_1 \| B_P \| P_2)}(E_3)$ by using key $h(H_1 \| B_P \| P_2)$ and verifies $V_{PK_D}(Sig_D) \stackrel{?}{=} h(M_D)$. Further, P computes $MAC_P = h(ID_P \| ID_D^* \| B_P \| B_D \| T_5)$ and verifies $MAC_P \stackrel{?}{=} MAC_D$. Furthermore, P computes session key $SK_{PD} = h(ID_P \| \ ID_D^* \| Sig_P \| Sig_D \| MAC_P \| B_D \| B_P \| x.\beta \| T_5)$.

Thus, common session key between P and D is $SK = SK_{PD} = SK_{PD}$. Hence, P gets treatment by authenticated D (Table 3).

3.5 Patient password change

The details of this phase is given as below:

Step 1. P login with ID'_P and pw'_P. P computes $PWP' = pw'_P \oplus h(pw'_P \| ID'_P \| a_P)$, $A'_P = h(h(ID'_P) \oplus h(PWP' \| ID'_P))$ and verifies whether holds $A'_P \stackrel{?}{=} A_P$ or not.

Step 2. P verifies the validity of the condition $A'_P \stackrel{?}{=} A_P$. Then, P selects new password pw_P^{NEW}. Further, P computes $PWP^{NEW} = pw_P^{NEW} \oplus h(pw_P^{NEW} \| ID_P \| a_P)$ and $A_P^{NEW} = h(h(ID_P) \oplus h(PWP^{NEW} \| ID_P))$.

Step 3. P replaces pw_P^{NEW} by pw_P, PWP^{NEW} by PWP, and A_P^{NEW} by A_P, respectively.

4 Security evaluation

In this session, we will look at RAPCHI's security in the following ways:

4.1 Formal security analysis by method I

Here, we apply the formal method of security evaluation under the approach of ROM, we prove that RAPCHI is safe. We take the proof of this approach by the mechanism of contradiction as [48]. We apply same investigation as [49–51]. In RAPCHI, we implement this method under the generic group method of secure communication environment. Assume that there are two oracles for any E:

- *Reveal* 1 Here, x is an arbitrary value, and $y = h(x)$ is a fixed length value [52].
- *Reveal* 2 Given $X \in \mathcal{E}(F_q)$ and the public key $Y = kX \in \mathcal{E}(F_q)$, this oracle will find as secret key k [52].

Table 3 Patient login, authentication and key agreement phase via public channel

Patient P with medical device	Cloud server S	Doctor D
Login with ID'_P and pw'_P		
Computes $PWP' = pw'_P \oplus h(pw'_P \| ID'_P \| a_P)$		
Computes $A'_P = h(h(ID'_P) \oplus h(PWP' \| ID'_P))$		
Verifies $A'_P \stackrel{?}{=} A_P$		
Generates $x \in Z_q^\star$		
Computes $\alpha = x.g$		
Generates $M_P = (ID_P, Data_P)$		
Computes $Sig_P = S_{SK_P}(h(M_P))$		
Computes $H_1 = h(ID_P \| PK_D \| (ID_P \oplus T_1))$		
Computes $H_2 = h(A_P \| B_D \| ID_P)$	Verifies $T_2 - T_1 \leq \triangle T$	
Encrypts $E_1 = E_{h(ID_P \| P_1 \| P_2)}(H_1, M_P, \alpha, Sig_P, T_1)$	Verifies $H_2^* \stackrel{?}{=} h(P_P \| B_P \| ID_D)$	
Sends $M_1 = \{E_1, H_2, T_1\}$	Computes $ID_{P1} = ID_P \oplus h(ID_1 \| ID_D \| B_D)$	
$\cdots\cdots\cdots\cdots\rightarrow$	Computes $H_3 = h(ID_D \| B_D \| D_1 \| T_3)$	Verifies $T_4 - T_3 \leq \triangle T$
(via public channel)	Encrypts $E_2 = E_{h(ID_D \| B_D \| D_1)}(E_1, H_3, ID_{P1}, P_1, P_2, B_P)$	Decrypts $(E_1, H_3, ID_{P1}, P_1, P_2, B_P) = D_{h(ID_D \| B_D \| D_1)}(E_2)$
	Sends $M_2 = \{E_2, T_3\}$	Verifies $H_3^* \stackrel{?}{=} h(ID_D \| B_D \| D_1 \| T_3)$
	$\cdots\cdots\cdots\cdots\rightarrow$	Computes $ID_P^* = ID_{P1} \oplus h(ID_1 \| ID_D \| B_D)$
	(via public channel)	Decrypts $(H_1, M_P, \alpha, Sig_P, T_1) = D_{h(ID_P^* \| P_1 \| P_2)}(E_1)$
		Verifies $H_1^* \stackrel{?}{=} h(ID_P \| a_D.g \| (ID_P \oplus T_1))$
		Verifies $V_{PK_P}(Sig_P) \stackrel{?}{=} h(M_P)$
		Generates $M_D = (ID_D, Data_D)$
		Computes $Sig_D = S_{SK_D}(h(M_D))$
		Generates $y \in Z_q^\star, \beta = y.g,$
		Computes $MAC_D = h(ID_P^* \| ID_D \| B_P \| B_D \| T_5)$
		Computes $SK_{DP} = h(ID_P^* \| ID_D \| Sig_P \| Sig_D \| MAC_D \| B_D \| B_P \| y.\alpha \| T_5)$

Table 3 (continued)

Patient P with medical device	Cloud server S	Doctor D
		Computes $ID_{D1} = ID_D \oplus h(Sig_P \| B_P \| H_1^*)$
		Encrypts $E_3 = E_{h(H_1^* \| B_P \| P_2)}(ID_{D1}, MAC_D, Sig_D, M_D, B_D, \beta, T_5)$
	Verifies $T_6 - T_5 \leq \triangle T$	Sends $M_3 = \{E_3, T_5\}$
Verifies $T_8 - T_7 \leq \triangle T$	Sends $M_4 = \{E_3, T_5, T_7\}$	$\leftarrow \cdots\cdots\cdots\cdots\cdots$
Computes $ID_D^* = ID_{D1} \oplus h(Sig_P \| B_P \| H_1)$	$\leftarrow \cdots\cdots\cdots\cdots\cdots$	(via public channel)
Decrypts $(ID_{D1}, MAC_D, Sig_D, M_D, B_D, \beta, T_5)$ $= D_{h(H_1 \| B_P \| P_2)}(E_3)$	(via public channel)	
Verifies $V_{PK_D}(Sig_D) \stackrel{?}{=} h(M_D)$		
Computes $MAC_P = h(ID_P \| ID_D^* \| B_P \| B_D \| T_5)$		
Verifies $MAC_P \stackrel{?}{=} MAC_D$		
Computes $SK_{PD} = h(ID_P \| ID_D^* \| Sig_P \| Sig_D \| MAC_P \| B_D \| B_P \| x.\beta \| T_5)$		

Algorithm1 $EXP1_{E,\ RAPCHI}^{HASH,\ ECDLP}$

1. Eavesdrop the login request with information ID'_P, pw'_P
2. Executes $PWP' = a'_p \oplus h(pw'_p \| ID'_P \| a_P)$, $A'_P = h(h(ID'_P) \oplus h(PWP' \| ID'_P))$
3. Call $Reveal$ 1 oracle on input A_P to recover ID_P, PWP, a_P as $(ID'_P, PWP'_P, a'_P) \leftarrow (A_P)$
4. **if** $(PWP' = PWP)$ then
5. Accept ID'_P as true identity ID_P of P
6. E guesses random number x
7. Call $Reveal$ 2 oracle on take α to recover $x'_P \leftarrow Reveal\ 2(\alpha)$
8. Computes $x'_P.g$ using base g point which is public.
9. Eavesdrop in authentication request message in authentication and key agreement phase
10. Call $Reveal$ 2 oracle on take $x.y.g$ recovers $x' \leftarrow x$ and $y' \leftarrow y$, then $(x'.y') \leftarrow (x.y.g)$
11. Call $Reveal$ 1 oracle on input MAC_P to recover $ID_P, ID^*_D, B_P, B_D, T_5$ as $(ID_P \| ID^*_D \| B_P \| B_D \| T_5) \leftarrow (MAC_P)$
12. Computes $MAC'_P = h(ID'_P \| ID'_D \| B'_P \| B'_D \| T'_5)$
13. E guesses $Sig'_P = Sig_P$, $Sig'_D = Sig_D$ and $T'_5 = T_5$
14. **if**$(MAC'_P = MAC_P)$
15. Accepted SK_{PD} as correct session key as SK_{DP} between P and D.
16. **return** 1(Success)
17. **else**
18. **return** 0(Failure)
19. end if
20. **else**
21. **return** 0 (Failure)
22. **end if**

Theorem 1 *Under ECDLP assumption, RAPCHI is safe against any E for determining ID_P and SK_{PD} between a patient and the doctor, if h(.) nearly acts such a random oracle.*

Proof Here, we want to compose E which has the capacity to determine both ID_P of P and SK_{PD} between P and D. Any E uses the random oracles *Reveal* 1 and *Reveal* 2 in order to test the algorithm, say $EXP_{E,RAPCHI}^{HASH,ECDLP}$ prepared in Algorithm. For the proposed framework RAPCHI, define the success probability for $EXP_{E,RAPCHI}^{HASH,ECDLP}$ as $Succ = 2Prob[EXP_{E,RAPCHI}^{HASH,ECDLP} = 1] - 1$, where $Prob[W]$ presents the probability on a game W. For the experiment, the benefit function becomes $Adv(et, qR_1, qR_2) = Max_E\{Succ\}$, where the maximal is seized overall E with queries qR_1, qR_2 done to *Reveal* 1 and *Reveal* 2 oracles and execution time *et*, respectively. RAPCHI is said to be provably safe against an E for determining ID_P and SK_{PD}, if $Adv(et, qR_1, qR_2) < \epsilon$, for any adequately slight $\epsilon > 0$. As an experiment, if E has the capability to change $h(.)$ and deals with ECDLP, she/he can simply determine both ID_P and SK_{PD} and achieve the game. However, by Subsect. 2.3, it is a findable computing unattainable issue to revert $h(\Delta)$, means that, $Adv_E^{HASH}(t_1)$, for any adequately slight $\epsilon > 0$. Also, in subsection 2.3, it is computationally unattainable to determine k from R and $S = kR$ in $\mathcal{E}(F_q)$, means that $Adv_{\mathbb{D},\mathcal{E}}^{ECDLP}(t_2) < \epsilon_2$, for any sufficient slight $\epsilon_2 > 0$. Hence, we contain $Adv(et_1, qR_1, qR_2) \leq \epsilon$, as $Adv(et_1, qR_1, qR_2)$ depends into other advantages $Adv_E^{HASH}(t_1)$ and $Adv_{\mathbb{D},\mathcal{E}}^{ECDLP}(t_2) < \epsilon_2$. □

Theorem 2 *Under the assumption that h(.) nearly performs such an oracle, RAPCHI is provably safe against attacker E for acquire pw_P of a valid patient P, even if her/his registration phase is breakable.*

Proof This proof is also same as Theorem 1. We wish to make any E who will contain the capacity to rid the password pw_P of a valid P, even if her/his registration. By Threat model [42] and Sect. 2.1 E can extract all information of P. Any E uses the Reveal oracle for Algorithm 2, say $EXP2_{E,RAPCHI}^{HASH}$ for RAPCHI. The progressive probability for $EXP2_{E,RAPCHI}^{HASH}$ as $Succ2 = 2Prob[EXP2_{E,RAPCHI}^{HASH} = 1] - 1$, and the experiment's advantage $Adv(et, qR_1, qR_1) = Max_E\{Succ2\}$, where the maximal is seized overall E with the queries qR_1, qR_2 made to the *Reveal* 1 oracles and execution time et_1, respectively. The RAPCHI is said to be provably safe against E for determining pw_P, if $Adv(et, qR_1) < \epsilon_1$, for any adequately slight $\epsilon > 0$. As experiment 2, if E has the capability to change $h(.)$ and achieve the game. However, by subsection 2.1, it is a possible for computing unattainable issue to invert $h(\Delta)$, means that, $Adv_E^{HASH}(t_1)$, for any adequately slight $\epsilon > 0$, means that $Adv(et_1, qR_1) \leq \epsilon$, since $Adv(et_1, qR_1)$ depends on other advantages $Adv_E^{HASH}(t_1) < \epsilon_1$. □

Algorithm2 $EXP2_{E,\ RAPCHI}^{HASH}$

1. Extract all the information $\{A_P, a_P, PWP_P\}$
2. Call $Reveal$ oracle on take A_P to recover ID_P, PWP as $(ID'_P, PWP'_P) \leftarrow (A_P)$
3. Eavesdrop the login request with information $\{A_P, a_P, PWP_P\}$
4. **if** $(PWP' = PWP)$ then
5. Accept ID'_P as true identity ID_P of P
6. Call $Reveal$ oracle on take A_P to recover ID_P and PWP as $(h(ID'_P) \oplus h(PWP'\|ID'_P) \leftarrow A_P$
7. **if**$(ID'_P = ID_P)$ and $(PWP' = PWP)$
8. Accepted pw'_P as correct session key as pw_P of P.
9. **return** 1(Success)
10. **else**
11. **return** 0(Failure)
12. end if
13. **else**
14. **return** 0 (Failure)
15. **end if**

4.2 Formal security by method II

Here, we adopt the random oracle model II for RAPCHI from [53–56].

Theorem 3 *The RAPCHI employees a group G under addition with a base point g of order q. According to the assumption of hash output digest of length l bit which performs an exact random oracle. Therefore, we have*

$$ADV_{E,\ succ}^{RAPCHI} \leq \frac{q_h^2}{2^l} + \frac{q_s}{2^{l-1}} + \frac{(q_s + q_e)^2}{2^{l+1}} + 2q_h(ADV_{E,\ succ}^{RAPCHI}(q)) + \frac{2q_s}{\bigvee} + \frac{2q_s}{\bigwedge}. \quad (1)$$

For a probabilistic polynomial time-bounded technique,$ADV_{E,\ succ}^{RAPCHI}$ which is the probability of success. Any E is trying to hack the semantic security (SS) of RAPCHI and $ADV_{E,\ succ}^{ECCDHP}$ is denoted a chance of success for E to find the solution of

the ECCDHP. The password dictionary is represented by $\bigvee$, *while the identity dictionary is represented by* $\bigwedge$ *in this competition. Where* q_h *times* H, q_e *times Execute queries and* q_s *times Send queries for* E *to breach the communication of entities in RAPCHI.*

Proof We believe E is capable of cracking the RAPCHI mechanism. In addition, the ECCDHP may be used to find a polynomial time-bounded method $\sum$ [57], i.e. from a random input (g, xg, yg), *sum* returns xyg within polynomial time bounds, where $x, y \in Z_q^*$. Here, we consider a sequence of games $G_j (0 \leq j \leq 5)$ [55, 56], and in the simulation of the game G_j, E can compute the exact attack against RAPCHI by computing G_0, but E has no security. Further, we define the term game $\eta_j (0 \leq j \leq 5)$ where E defeats G_j in breaking into the RAPCHI's communication system. Furthermore, we believe that the event Π, which separates η_i, may occur while E is being calculated, causing $\sum$ to detect Π. Unless Π is present, neither G_j nor G_{j+1} can be distinguished. As a result, we have

$$| Pr[\eta_{j+1}] - Pr[\eta_j] | \leq Pr[\Pi] \tag{2}$$

G_0 : The execution of G_0 is akin to the ROR model of a real-world security attack. As a result, in this oracle, all P and D outcomes are modelled as expected. When G_0 is computed, E can guess which bit in the Test question is related to τ, which is the exact bit. Therefore, we have

$$ADV_{E,succ}^{RAPCHI} = \ | 2Pr[\eta_0] - 1 | \tag{3}$$

G_1 : Here, G_1 is similar to G_0 without the hash oracle H is calculated by E by maintaining a list L_H^P, which runs the (Hin, $Hout$). If E inputs Hin_{NEW}, $\sum$ and find output $Hout_{NEW}$. Then, a new list of tuple (Hin_{NEW}, $Hout_{NEW}$) in L_H^P. Otherwise, $\sum$ randomly prefers a number $Hout_{NEW} \in F_q^\star$, returns to E and considers new tuples ($Hin_{NEW}, Hout_{NEW}$) in L_H^P. Here, *Execute*, *Send*, *Corrupt*, *Reveal*, and $Test - queries$ are polished in the same way that genuine attacks are calculated. So that's it.

$$Pr[\eta_1] = Pr[\eta_0] \tag{4}$$

G_2 : In this contest, G_2 is similar to except if a collision occurs during the simulation of the values, G_1 will be exited $M_1 = \{E_1, H, T_1\}, M_2 = \{E_2, T_3\}$, $M_3 = \{E_3, T_5\}$ and $M_2 = \{E_3, T_5, T_7\}$ which are based on the birthday attack. Probability of collisions of the simulated hash oracle is at most $\frac{q_h^2}{2q}$. In the contents simulation, the possibility of collisions is $\frac{(q_s+q_e)^2}{2^{l+1}}$. Thus, we have

$$| Pr[\eta_2] - Pr[\eta_1] | \leq \frac{q_h^2}{2q} + \frac{(q_s + q_e)^2}{2^{l+1}} \tag{5}$$

G_3 : Here, suppose E is guessed attributes Sig_P, H_1, H_2 without hash query. Further, G_3 is similar to G_2 with P and S occurrence refuses authenticated numbers. Thus, we have

$$| Pr[\eta_3] - Pr[\eta_2] | \leq \frac{q_s}{2^l} \tag{6}$$

G_4 : In this contest, E accurately guessed attributes H_2^*, H_3, ID_{P1} without hash query. Further, G_4 is similar to G_3 with S and D occurrence refuses authenticated values. Thus, we have

$$| Pr[\eta_4] - Pr[\eta_3] | \leq \frac{q_s}{2^l} \tag{7}$$

G_5 : In this game, E accurately guessed the authenticated attributes $H_3^*, ID_P^*, H_1^*, V_{PK_P}(\quad Sig_P), Sig_D = S_{SK_D}(h(M_D)), MAC_D, SK_{DP}, ID_{D1}, MAC_D$ without hash query. Further, G_5 is similar to G_4 with S and D occurrence refuses authenticated values. Thus, we have

$$| Pr[\eta_5] - Pr[\eta_4] | \leq \frac{q_s}{2^l} \tag{8}$$

G_6 : In this event, E accurately guessed attributes E_3, T_5, T_7 without hash query. Further, G_6 is similar to G_5 with S and P occurrence refuses a legitimated values. Thus, we have

$$| Pr[\eta_6] - Pr[\eta_5] | \leq \frac{q_s}{2^l} \tag{9}$$

G_7 : In this game, E is session key $SK_U = SK_S = SK$ with find the values xyg. As a result, when using the *ECCDHP*'s random self-reducibility, G_6 and G_6 are comparable in execution. Thus E applied queries with random values $(g,\ xg,\ yg)$ to compute $ECCDHP(xg, yg) = xyg$, where $x, y \in Z_q^\star$ .Therefore, we have

$$| Pr[\eta_7] - Pr[\eta_6] | \leq q_h ADV_{E,\ succ}^{ECCDHP}(q) \tag{10}$$

G_8 : This game is identical to the previous game except for the addition of a $Test - query$. If E asks a $H - query$ with information $\{ID_P, ID_D^*, Sig_P, Sig_D, MAC_P, B_D, B_P, x,\ \beta, T_5\}$, the game will end. By running the $H - query$ with a probability at most $\frac{q_h^2}{2l}$, E can obtain the session key $SK = SK_U = SK_S$. Thus, we have

$$| Pr[\eta_9] - Pr[\eta_8] | \leq \frac{q_h^2}{2q} \tag{11}$$

If E will not get a session key without perfect input which contains different parameters, thus $Prob[\eta_9] = \frac{1}{2}$. Furthermore, it specifies that the password $Corrupt - query(Corrupt(U, 1))$ has not been made in [53] if the $Corrupt(U, 2)query$ has been made. The probability of applying off-line password guessing attack and identity guessing attacks are $\frac{q_s}{\bigvee}$ and $\frac{q_s}{\bigwedge}$ by E. Thus, from equations (3) – (11), we obtained

$$ADV_{E,\,succ}^{ESEAP} \leq \frac{q_h^2}{2^l} + \frac{q_s}{2^{l-1}} + \frac{(q_s + q_e)^2}{2^{l+1}} + 2q_h(ADV_{E,\,succ}^{ECCDHP}(q)) + \frac{2q_s}{X} + \frac{2q_s}{Y}. \tag{12}$$

Hence, the theorem is established. □

4.3 Informal security analysis

The following security aspects and properties are discussed in this session for RAPCHI analysis:

4.3.1 Patient anonymity

We express P anonymity in RAPCHI which is given as below:

- S computes P' partial identity $ID_{P1} = ID_P \oplus h(ID_1 \| ID_D \| B_D)$, encrypts ID_{P1} by $E_2 = E_{h(ID_D \| B_D \| D_1)}(E_1, H_3, ID_{P1}, P_1, P_2, B_P)$ with using key $(h(\ ID_D \| B_D \|\ D_1)$ and sends to D. Further, D decrypts $(E_1, H_3, ID_{P1}, P_1, P_2,\ B_P) = D_{h(ID_D \| B_D \| T_2)}$ (E_2) using key $h(ID_D \| B_D \| D_1)$ and computes anonymous identity of P as $ID_P^* = ID_{P1} \oplus h(ID_1 \| ID_D \| B_D)$. Furthermore, D uses ID_P^* in authentication phase of RAPCHI.

Thus, our protocol provides P anonymity.

4.3.2 Doctor anonymity

We describe D anonymity in RAPCHI as below:

- D computes his/her partial identity $ID_{D1} = ID_D \oplus h(Sig_P \| B_P \| H_1^*)$ and sends to P. Further, P computes D's anonymous identity as $ID_D^* = ID_{D1} \oplus h(Sig_P \| B_P \| H_1^*)$ and uses ID_P^* in RAPCHI.

Thus, our protocol provides D anonymity.

4.3.3 Man-in-the-middle attack

In RAPCHI, each step of authentication phase having time-stamp status $T_i - T_j \leq \bigtriangleup T$ and hash conditions $H_i^* = H_i$. If possible, any E enters in

authentication and key agreement phase after checks $T_i - T_j \leq \bigtriangleup T$ then, verifies $H_i' \stackrel{?}{=} H_j$. This condition is not achievable to verify by the definition of hash function which is secure. Further, E cannot verify P's signature $V_{PK_P}(Sig_P) \stackrel{?}{=} h(M_P)$ and D's signature $V_{PK_D}(Sig_D) \stackrel{?}{=} h(M_D)$. Thus, E will unsuccessful in authentication and key agreement phase. Therefore, RAPCHI secures against this attack.

4.3.4 Replay attack

Every time we utilise the time-stamp condition $T_i - T_j \leq \bigtriangleup T$ in RAPCHI, we use random values as a counter-measure. In RAPCHI, the valid time length is $\bigtriangleup T$. Furthermore, the hash value, encryption, decryption, various keys, and session keys are all computed using the current time value and a random number. It is well known that in a network system, an ECC-based one-way hash function is secure. Hence, the replay attack is not possible in RAPCHI.

4.3.5 Known-key security property

The session keys are expressed in the following way by RAPCHI:

- P executes session key $SK_{PD} = h(ID_P \| ID_D^* \| Sig_P \| Sig_D \| MAC_P \| B_D \| B_P \| x.\beta \| T_5)$.
- D executes session key $SK_{DP} = h(ID_P^* \| ID_D \| Sig_P \| Sig_D \| MAC_D \| B_D \| B_P \| y.\alpha \| T_5)$.

RAPCHI presents session key in communication system. Even if E finds the past key, she/he cannot execute it. Thus, RAPCHI maintains this property.

4.3.6 Data confidentiality

It is a way to send secure data in communication system without E. In RAPCHI, the following are the details of encryption and description:

– P encrypts $E_1 = E_{h(ID_P \| P_1 \| P_2)}(H_1, M_P, \alpha, Sig_P, T_1)$ by using key $h(ID_P \| P_1 \| P_2)$ and uploads to S. Further, S encrypts $E_2 = E_{h(ID_D \| B_D \| D_1)}(E_1, H_3, ID_{P1}, P_1, P_2, B_P)$ by using key $h(ID_D \| B_D \| D_1)$ and forwards to D. After that, D decrypts $(E_1, H_3, ID_{P1}, P_1, P_2, B_P) = D_{h(ID_D \| B_D \| D_1)}(E_2)$ by using key $h(ID_D \| B_D \| D_1)$ and $(H_1, M_P, \alpha, Sig_P, T_1) = D_{h(ID_P^* \| P_1 \| P_2)}(E_1)$ by using key $ID_P^* \| P_1 \| P_2)$. Furthermore, D encrypts $E_3 = E_{h(H_1^* \| B_P \| P_2)}(ID_{D1}, MAC_D, Sig_D, M_D, B_D, \beta, T_5)$ by using key $h(H_1^* \| B_P \| P_2)$ and uploads to S. In addition to, S sends E_3 to P. Then, P decrypts $(ID_{D1}, MAC_D, Sig_D, M_D, B_D, \beta, T_5) = D_{h(H_1 \| B_P \| P_2)}(E_3)$ by using key $h(H_1 \| B_P \| P_2)$.

Thus, if E tries to find communicated message at the time of communication, E encrypts information which cannot be decrypted without the hash value and generated key. By the definition of hash function, it assumed to be secure and one way. So

that, it is hard to compute generated key and hash value. Therefore, RAPCHI maintains the confidentiality.

4.3.7 Data non-repudiation

The details of this attribute in RAPCHI are given as:

- P makes digital signature $Sig_P = S_{SK_P}(h(M_P))$ and verifies D's digital signature $V_{PK_D}(Sig_D) \stackrel{?}{=} h(M_D)$.
- D verifies P's digital signature by $V_{PK_D}(Sig_P) \stackrel{?}{=} h(M_P)$. After that, D makes digital signature $Sig_D = S_{SK_D}(h(M_D))$.

Thus, P checks the health information. If, the medical information is incorrect, the authenticated party cannot be denied. The non-repudiation arguments are saved in S. Therefore, RAPCHI protests data non-repudiation.

4.3.8 Message authentication

The details of it describe in RAPCHI as below:

- S gets M_2, verifies $T_2 - T_1 \leq \bigtriangleup T$ and hash function $H_2^* \stackrel{?}{=} h(P_P \| B_P \| ID_D)$. Similarly, S accepts message M_3 and checks the validity by confirming times-stamps condition $T_6 - T_5 \leq \bigtriangleup T$.
- D receives message M_2, verifies $T_4 - T_3 \leq \bigtriangleup T$, $H_3^* \stackrel{?}{=} h(ID_D \| B_D \| D_1 \| T_3)$, $H_1^* \stackrel{?}{=} h(ID_P \| a_D.g \| (ID_P \oplus T_1))$ and $V_{PK_P}(Sig_P) \stackrel{?}{=} h(M_P)$.
- P receives message M_4, checks $T_8 - T_7 \leq \bigtriangleup T$, $V_{PK_D}(Sig_D) \stackrel{?}{=} h(M_D)$ and $MAC_P \stackrel{?}{=} MAC_D$.

If any E endeavours change any charge in data of P, S and D will recognize it. Therefore, RAPCHI protests against the message authentication attack.

4.3.9 Impersonation attack

The details of an impersonation attack describe in RAPCHI as below:

- Any E attempts to masquerade as an authenticated P and tries to compute $Sig_P = S_{SK_P}(h(M_P))$, $H_1 = h(ID_P \| PK_D \| (ID_P \oplus T_1))$, $H_2 = h(A_P \| B_D \| ID_P)$, encrypts $E_1 = E_{h(ID_P \| P_1 \| P_2)}(H_1, M_P, \alpha, Sig_P, T_1)$ by using key $h(ID_P \| P_1 \| P_2)$. Then, P sends $M_1 = \{E_1, H_2, T_1\}$ to S . E cannot compute Sig_P, H_1, H_2, and $h(ID_P \| P_1 \| P_2)$ by the definition explanation of hash function and digital signature. Thus, E cannot impersonate as authenticated P.
- Any E attempts to masquerade as an authenticated D. On getting M_2, D decrypts $(E_1, H_3, ID_{P1}, P_1, P_2, B_P) = D_{h(ID_D \| B_D \| D_1)}(E_2)$ by using key $h(ID_D \| B_D \| D_1)$, com-

putes $ID_P^* = ID_{P1} \oplus h(ID_1 \| ID_D \| B_D)$, decrypts $(H_1, M_P, \alpha, Sig_P, T_1) = D_{h(ID_P^* \| P_1 \| P_2)}(E_1)$ by using key $ID_P^* \| P_1 \| P_2)$. Further, D generates medical report $M_D = (ID_D, Data_D)$, computes signature $Sig_D = S_{SK_D}(h\ (M_D))$. Then, D generates random value $y \in Z_q^\star$, computes $\beta = y.g$, $MAC_D = h(ID_P^* \| ID_D \| B_P \| B_D \| T_5)$, session key $SK_{DP} = h(ID_P^* \| ID_D \| Sig_P \| Sig_D \| MAC_D \| B_D \| B_P \| y.\alpha \| T_5)$, $ID_{D1} = h(Sig_P \| B_P \| H_1^*)$, encrypts $E_3 = E_{h(H_1^* \| B_P \| P_2)}(ID_{D1}, MAC_D, Sig_D, M_D, B_D, \beta, T_5)$ by using key $h(H_1^* \| B_P \| P_2)$ and D sends $M_3 = \{E_3, T_5\}$ to S. E cannot compute these parameters as discussed above. Thus, E cannot impersonate as an authenticated D.

- Any adversary E attempts to masquerade as an authenticate S and eavesdrop the transmitted M_2 and M_4. Further, S $ID_{P1} = ID_P \oplus h(ID_1 \| ID_D \| B_D)$, $H_3 = h(ID_D \| B_D \| D_1 \| T_3)$, encrypts $E_2 = E_{h(ID_D \| B_D \| D_1)}(E_1, H_3, ID_{P1}, P_1, P_2, B_P)$ by using key $h(ID_D \| B_D \| D_1)$. E cannot compute these parameters as discussed above. Thus E cannot impersonate as authenticated S.

Hence, RAPCHI is secured against this attack.

4.3.10 Session key security

RAPCHI contains two session keys which are computed between P and D. The details of session key are shown in RAPCHI as below:

- D computes $SK_{DP} = h(ID_P^* \| ID_D \| Sig_P \| Sig_D \| MAC_D \| B_D \| B_P \| y.\alpha \| T_5)$ and P computes $SK_{PD} = h(ID_P \| ID_D^* \| Sig_P \| Sig_D \| MAC_P \| B_D \| B_P \| x.\beta \| T_5)$. E cannot execute SK_{DP} or SK_{PD}, where $MAC_P = MAC_D$. With the help of impersonation attack, MAC_D and MAC_P cannot be executed by E. Furthermore, for given (g, α, β), it is impossible for an attacker G to compute xyg using ECCDHP in ECC for $x, y \in Z_q^*$ and g is the base point of G. As a result, the authenticated participant is the only one who can build SK.

Hence, RAPCHI could defend the session key.

5 Simulation study using AVISPA tool

AVISPA is a tool for evaluating the proposed protocols' security against passive/active attacks, man-in-the-middle attacks, and reply assaults. AVISPA's back-end servers, such as the On-the-Fly Modeler (OFMC), constraint-Logic (Cl-AtSe) attacker search, SAT-based Model-Checker (SATMC), and Tree Automata based on Automatic Approximations for the evaluation of security protocols, include an integrated automated validation security analysis (TA4SP) [45, 58]. It can examine the capability of the RAPCHI under security attacks. As a result, we decided to investigate RAPCHI's security and confidentiality against active and passive attacks. The analysis results are depicted in Fig. 2. RAPCHI is secure in communication channel.

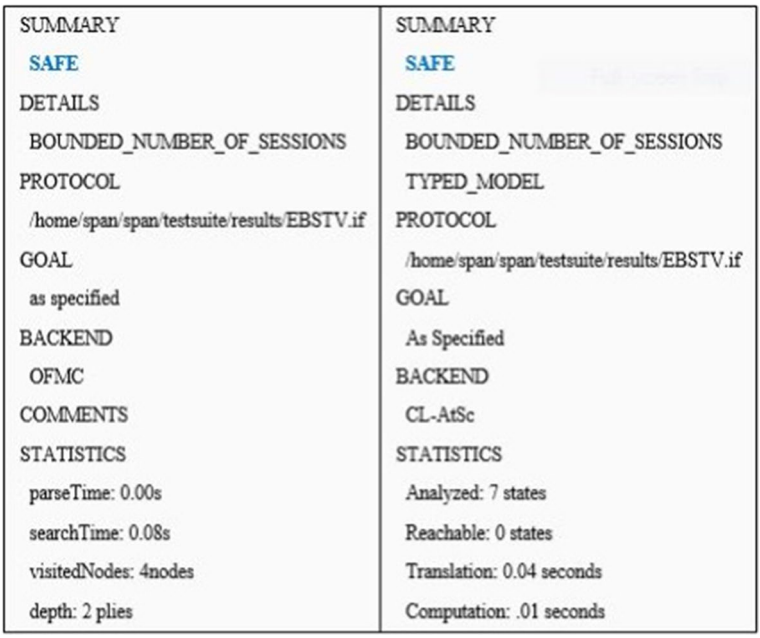

Fig. 2 Results of AVISPA using the OFMC and CL-AtSe back-ends

AVISPA's outcome is that one of the four back-ends is used: CL-AtSe, OFMC, TA4SP and SATMC. The results reveal that the private parameters between P and D are kept secret. It also protects against both passive and active attacks. In the execution of RAPCHI, the parameters cannot be determined by E in public channel.

It is worth noting that we did not use the TA4SP and SATMC simulation results because they do not support running bitwise XOR ($\oplus$) operations.

6 Performance analysis

In this part, we compare RAPCHI's security and functionality aspects, as well as communication and computation costs, to other frameworks such Mohit et al. [26], Chen et al.[20], Li et al.[27], Chen et al. [41], Chiou et al. [25], Chandrakar et al. [29] and Deebak and Turjman [35]. The details of this phase following as:

6.1 Comparison of the security and functionality attributes

In Table 4, we compare security and functionality attributes of RAPCHI with related frameworks below as:

Table 4 Comparison of different attributes

Protocol	$\Gamma 1$	$\Gamma 2$	$\Gamma 3$	$\Gamma 4$	$\Gamma 5$	$\Gamma 6$	$\Gamma 7$	$\Gamma 8$	$\Gamma 9$	$\Gamma 10$	$\Gamma 11$	$\Gamma 12$	$\Gamma 13$	$\Gamma 14$	$\Gamma 15$	$\Gamma 16$
Chen et al. [20]	√	×	×	√	×	√	√	√	√	×	√	×	×	×	×	×
Mohit et al. [26]	√	×	×	√	×	√	√	√	×	√	×	×	×	×	×	×
Chen et al. [41]	√	×	×	√	√	√	√	×	×	√	×	×	×	×	×	×
Li et al. [27]	√	×	×	√	√	√	√	×	×	√	√	√	×	×	×	×
Chiou et al. [25]	√	×	×	√	×	√	√	√	×	√	×	×	×	×	×	×
Chandrakar et al.[29]	√	×	√	√	√	×	√	√	×	√	√	√	×	×	×	×
Deebak and Turjman [35]	√	√	√	√	√	√	√	√	√	√	√	×	√	×	×	√
RAPCHI	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√	√

$\Longrightarrow \sqrt{}$: Attribute protected by the protocol, ×: Attribute not protected by the protocol, $\Gamma 1$: Man-in-the-middle attack, $\Gamma 2$: Patient anonymity, $\Gamma 3$: Doctor anonymity, $\Gamma 4$: Replay attack, $\Gamma 5$: Known-key security property, $\Gamma 6$: Data confidentiality, $\Gamma 7$: Data non-repudiation, $\Gamma 8$: Message authentication, $\Gamma 9$: Impersonation attack, $\Gamma 10$: Session key security, $\Gamma 11$: Patient unlinkability, $\Gamma 12$: Doctor unlinkability, $\Gamma 13$: Patient password change, $\Gamma 14$: Low Computation cost, $\Gamma 15$: Low communication cost and $\Gamma 16$: Secure protocol

- Chen et al.'s protocol [20] fails against $\Gamma 2$, $\Gamma 3$, $\Gamma 5$, $\Gamma 10$, $\Gamma 12$, $\Gamma 13$, $\Gamma 14$, $\Gamma 15$ and $\Gamma 16$.
- Mohit et al.'s protocol [26] fails against $\Gamma 2$, $\Gamma 3$, $\Gamma 5$, $\Gamma 9$,$\Gamma 11$, $\Gamma 12$ $\Gamma 13$, $\Gamma 14$, $\Gamma 15$ and $\Gamma 16$.
- Chen et al's. protocol [41] fails against $\Gamma 2$, $\Gamma 3$, $\Gamma 8$, $\Gamma 9$, $\Gamma 11$, $\Gamma 12$, $\Gamma 13$, $\Gamma 14$, $\Gamma 15$ and $\Gamma 16$.
- Li et al.'s protocol [27] fails $\Gamma 2$, $\Gamma 3$, $\Gamma 8$, $\Gamma 9$, $\Gamma 13$, $\Gamma 14$, $\Gamma 15$ and $\Gamma 16$.
- Chiou et al.'s protocol [25] fails against $\Gamma 2$, $\Gamma 3$, $\Gamma 5$, $\Gamma 9$,$\Gamma 11$, $\Gamma 12$, $\Gamma 13$, $\Gamma 14$, $\Gamma 15$ and $\Gamma 16$.
- Chandrakar et al.'s protocols [29] fails against $\Gamma 2$, $\Gamma 6$, $\Gamma 9$, $\Gamma 13$, $\Gamma 14$, $\Gamma 15$ and $\Gamma 16$.
- Deebak and Turjman protocol [35] fails against $\Gamma 12$, $\Gamma 14$ and $\Gamma 15$.

In this context, RAPCHI satisfies all above security attributes.

6.2 Comparison of the computation cost

We have taken several cryptographic operations those based on the information applicable in [6, 25, 26] to test the execution cost of the presented scheme which are related frameworks. The RAPCHI used time for computing to verify/execute a signature ($T_{Sign} \approx 0.3317$ *Sec*), asymmetric decryption/encryption ($T_A \approx 0.3057$ *Sec*), multiplication ($T_M \approx 0.0503$ *Sec*), bilinear pairing ($T_P \approx 0.0621$ *Sec*), symmetric decryption/encryption ($T_S \approx 0.0087$ *Sec*) and hash function is ($T_H \approx 0.0005$ *Sec*).

The communication overhead concatenation operation ($\|$) and XOR operation ($\oplus$) are generally known to be minimal. Table 5 shows the computation cost of the proposed framework and related frameworks as follows:

- The computation cost Chen et al.'s protocol [20] is $3T_{Sign} + 3T_M + 6T_P + 15T_S + 6T_H + 10T_A$ which is ≈ 4.7091 Sec.

Table 5 Comparison of computation and communication cost

Protocol	Total cost	Execution time	Communication cost
Chen et al. [20]	$3T_{Sign} + 3T_M + 6T_P + 15T_S + 6T_H + 10T_A$	≈ 4.7091 Sec	2576 bits
Mohit et al. [26]	$6T_{Sign} + 9T_S + 35T_H$	≈ 2.086 Sec	5312 bits
Chen et al. [41]	$6T_{Sign} + 12T_M + 15T_P + 15T_S + 22T_H + 2T_A$	≈ 4.379 Sec	7952 bits
Li et al. [27]	$7T_{Sign} + 15T_S + 36T_H$	≈ 2.4704 Sec	3776 bits
Chiou et al. [25]	$5T_{Sign} + 4T_M + 13T_P + 10T_S + 33T_H$	≈ 2.7705 Sec	6528 bits
Chandrakar et al. [29]	$10T_{Sign} + 18T_S + 59T_H$	≈ 3.5031 Sec	9440 bits
Deebak and Turjman [35]	$8T_{Sign} + 17T_S + 51T_H + T_{mul}$	≈ 2.9503 Sec	7646 bits
RAPCHI	$4T_{Sign} + 6T_S + 2T_M + 24T_H$	≈ 1.4916 Sec	752 bits

- The computation cost Mohit et al.'s protocol [26]is $6T_{Sign} + 9T_S + 35T_H$ which is ≈ 2.086 Sec.
- The computation cost Chen et al.'s protocol [41] is $6T_{Sign} + 12T_M + 15T_P + 15T_S + 22T_H + 2T_A$ which is ≈ 4.379 Sec.
- The computation cost Li et al.'s protocol [27] is $7T_{Sign} + 15T_S + 36T_H$ which is ≈ 2.4704 Sec.
- The computation cost Chiou et al.'s protocol [25]is $5T_{Sign} + 4T_M + 13T_P + 10T_S + 33T_H$ which is ≈ 2.7705 Sec.
- The computation cost Chandrakar et al.'s protocol [29] is $10T_{Sign} + 18T_S + 59T_H$ which is ≈ 3.5031 Sec.
- The computation cost of Deebak and Turjman protocol [35] is $8T_{Sign} + 17T_S + 51T_H + T_{mul}$ which is ≈ 2.9503 Sec.
- The computation cost of RAPCHI is $4T_{Sign} + 6T_S + 2T_M + 24T_H$ which is ≈ 1.4916 Sec.

Thus, RAPCHI is more efficient and secure in CHI. Figure 3 details of computation cost. As a result, as compared to other CHI protocols, RAPCHI is both secure and cost-effective in terms of computation cost.

6.3 Comparison of the communication cost

The communication cost of RAPCHI is compared to that of equivalent frameworks in this section. For this, we use the method of the Mohit et al. [26] protocol. There are several cryptographic components, including produced random numbers, time stamps, and a 48-bit identity length; 128-bit symmetric encryption/decryption, asymmetric encryption/decryption, and modular multiplication/inversion operations; length of cryptographic hash function and bilinear pairing to be 160-bits and length

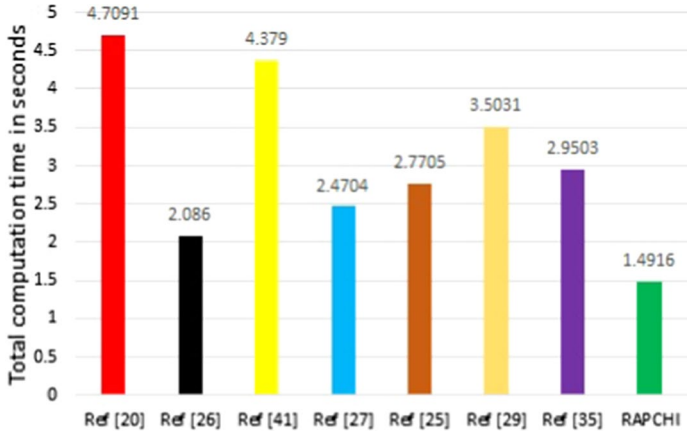

Fig. 3 Computation cost comparison

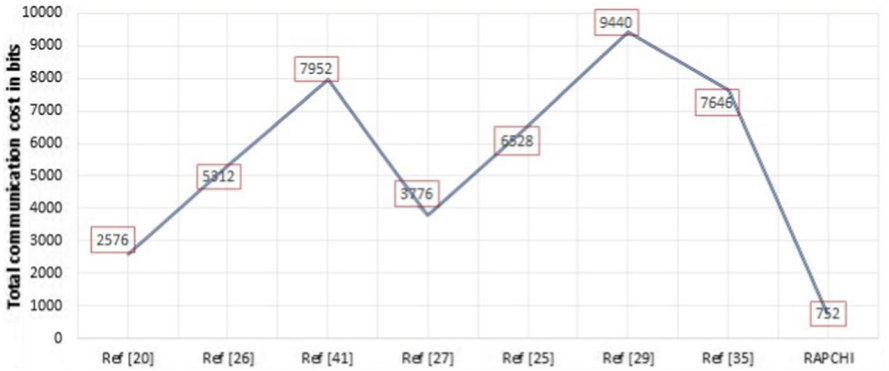

Fig. 4 Communication cost comparison

of executing/verifying a signature is 512-bits. Table 5 displays the communication cost of RAPCHI and other comparable related frameworks in details as below:

- The communication cost Chen et al.'s protocol [20] is 2576 bits.
- The communication cost Mohit et al.'s protocol [26]is 5312 bits.
- The communication cost Chen et al.'s protocol [41] is 7952 bits.
- The communication cost Li et al.'s protocol [27] is 3776 bits.
- The communication cost Chiou et al.'s protocol [25]is 6528 bits.
- The communication cost Chandrakar et al.'s protocol [29] is 9440 bits.
- The communication cost of Deebak and Turjman protocol [35] is 7646 bits.
- The communication cost of RAPCHI is 752 bits.

Figure 4 details of communication cost. As a result, RAPCHI has a lower communication cost than other protocols CHI.

7 Conclusions

In this work, we have proposed a secure and lightweight authentication mechanism for IoMT-based CHI. The study demonstrates formal security analysis using two distinct ROM-based techniques. We also used the simulation software AVISPA to demonstrate that RAPCHI is not vulnerable to replay and man-in-the-middle attacks. Furthermore, informal security analysis based on various security attributes and properties such as replay attack, data confidentiality, man-in-the-middle attack, patient anonymity, doctor anonymity, data non-repudiation, known-key property, patient unlinkability, impersonation attack, session key security, message authentication, and doctor unlinkability is demonstrated. Furthermore, we compared the proposed framework to existing frameworks in a similar environment, demonstrating that RAPCHI is more secure and efficient in terms of computation and communication cost. As a result, our proposed framework could be more useful in

IoT-based cloud-healthcare infrastructure. It is also a real-world application that protects humans from attackers through online treatment.

References

1. Abor PA, Agrizzi D (2012) Healthcare Governance and Patients' Perception of Service Quality. In: Annual Conference on Innovations in Business & Management, London, pp 21–23
2. Ramez WS (2012) Patients' perception of health care quality, satisfaction and behavioral intention: an empirical study in bahrain. International Journal of Business and Social Science, Centre for Promoting Ideas, US, 3(18):
3. Wu J, Li H, Cheng S, Lin Z (2016) The promising future of healthcare services: when big data analytics meets wearable technology. Inform Manag 53(8):1020–1033
4. Li C-T, Lee C-C, Weng C-Y (2014) A secure chaotic maps and smart cards based password authentication and key agreement scheme with user anonymity for telecare medicine information systems. J Med Syst 38(9):77
5. Tan Z et al (2013) An efficient biometrics-based authentication scheme for telecare medicine information systems. Network 2 2(3):200–204
6. Kumar V, Jangirala S, Ahmad M (2018) An efficient mutual authentication framework for healthcare system in cloud computing. J Med Syst 42(8):142
7. Habibzadeh H, Dinesh K, Shishvan OR, Boggio-Dandry A, Sharma G, Soyata T (2019) A survey of healthcare internet of things (hiot): a clinical perspective. IEEE Internet Things J 7(1):53–71
8. Dourado CM, da Silva S.P.P., da Nobrega RVM, Rebouças Filho PP., Muhammad K, de Albuquerque VHC (2020) An open ioht-based deep learning framework for online medical image recognition. IEEE J Sel Areas Commun 39(2):541–548
9. Tanveer M, Zahid AH, Ahmad M, Baz A, Alhakami H (2020) Lake-iod: lightweight authenticated key exchange protocol for the internet of drone environment. IEEE Access 8:155645–155659
10. Parah SA, Kaw JA, Bellavista P, Loan NA, Bhat G, Muhammad K, Victor A (2020) Efficient security and authentication for edge-based internet of medical things. IEEE Internet Things J. https://doi.org/10.1109/JIOT.2020.3038009
11. Hayajneh T, Vasilakos AV, Almashaqbeh G, Mohd BJ, Imran MA, Shakir MZ, Qaraqe KA (2014) Public-Key Authentication for Cloud-Based wbans. In: Proceedings of the 9th International Conference on Body Area Networks, pp 286–292
12. Choo K-KR, Gritzalis S, Park JH (2018) Cryptographic solutions for industrial internet-of-things: research challenges and opportunities. IEEE Trans Industr Inf 14(8):3567–3569
13. Padhy RP, Patra MR, Satapathy SC (2012) Design and implementation of a cloud based rural healthcare information system model. Univ J Appl Comput Sci Technol 2(1):149–157
14. Banerjee A, Agrawal P, Rajkumar R (2013) Design of a cloud based emergency healthcare service model. Int J Appl Eng Res 8(19):2261–2264
15. Li C-T, Lee C-C, Wang C-C, Yang T-H, Chen S-J (2015) Design Flaws in a Secure Medical Data Exchange Protocol Based on Cloud Environments. In: International Conference on Algorithms and Architectures for Parallel Processing, Springer, pp 435–444
16. Chatterjee S, Roy S, Das AK, Chattopadhyay S, Kumar N, Reddy AG, Park K, 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
17. Islam SH, Khan MK, Li X (2015) Security analysis and improvement of 'a more secure anonymous user authentication scheme for the integrated epr information system'. PLoS ONE 10(8):e0131368
18. 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. Sec Commun Netw 9(13):1983–2001
19. Sutrala AK, Das AK, Odelu V, Wazid M, Kumari S (2016) Secure anonymity-preserving password-based user authentication and session key agreement scheme for telecare medicine information systems. Comput Methods Prog Biomed 135:167–185
20. Chen C-L, Yang T-T, Chiang M-L, Shih T-F (2014) A privacy authentication scheme based on cloud for medical environment. J Med Syst 38(11):143

21. Amin R, Islam SH, Biswas G, Khan MK, Obaidat MS (2015) Design and analysis of an enhanced patient-server mutual authentication protocol for telecare medical information system. J Med Syst 39(11):137
22. He D, Kumar N, Chen J, Lee C-C, Chilamkurti N, Yeo S-S (2015) Robust anonymous authentication protocol for health-care applications using wireless medical sensor networks. Multimedia Syst 21(1):49–60
23. Zhou J, Cao Z, Dong X, Xiong N, Vasilakos AV (2015) 4s: A secure and privacy-preserving key management scheme for cloud-assisted wireless body area network in m-healthcare social networks. Inf Sci 314:255–276
24. Castiglione A, Pizzolante R, De Santis A, Carpentieri B, Castiglione A, Palmieri F (2015) Cloud-based adaptive compression and secure management services for 3d healthcare data. Futur Gener Comput Syst 43:120–134
25. Chiou S-Y, Ying Z, Liu J (2016) Improvement of a privacy authentication scheme based on cloud for medical environment. J Med Syst 40(4):101
26. Mohit P, Amin R, Karati A, Biswas G, Khan MK (2017) A standard mutual authentication protocol for cloud computing based health care system. J Med Syst 41(4):50
27. Li C-T, Shih D-H, Wang C-C (2018) Cloud-assisted mutual authentication and privacy preservation protocol for telecare medical information systems. Comput Methods Prog Biomed 157:191–203
28. Kumar V, Ahmad M, Kumari A (2019) A secure elliptic curve cryptography based mutual authentication protocol for cloud-assisted tmis. Telematics Inform 38:100–117
29. Chandrakar P, Sinha S, Ali R (2019) Cloud-based authenticated protocol for healthcare monitoring system. J Ambient Intell Human Comput, 1–17
30. Chen R, Peng D (2019) Analysis and improvement of a mutual authentication scheme for wireless body area networks. J Med Syst 43(2):19
31. Chen C-L, Huang P-T, Deng Y-Y, Chen H-C, Wang Y-C (2020) A secure electronic medical record authorization system for smart device application in cloud computing environments. HCIS 10:1–31
32. Zhu F, Li P, Xu H, Wang R (2020) A novel lightweight authentication scheme for rfid-based healthcare systems. Sensors 20(17):4846
33. Arunkumar B, Kousalya G (2020) Blockchain-based decentralized and secure lightweight e-health system for electronic health records. In: Intelligent Systems, Technologies and Applications, Springer, pp 273–289
34. Khatoon S, Rahman SMM, Alrubaian M, Alamri A (2019) Privacy-preserved, provable secure, mutually authenticated key agreement protocol for healthcare in a smart city environment. IEEE Access 7:47962–47971
35. Deebak BD, Al-Turjman F (2020) Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. IEEE J Sel Areas Commun 39(2):346–360
36. Chen X, Zhang X, Geng D, Zhou L, Chen J, Lu F (2021) A rfid authentication protocol for epidemic prevention and epidemic emergency management systems. J Healthcare Eng
37. Hathaliya JJ, Tanwar S (2020) An exhaustive survey on security and privacy issues in healthcare 4.0. Comput Commun 153:311–335
38. Awotunde JB, Jimoh RG, Ogundokun RO, Misra S, Abikoye OC (2022) Big data analytics of iot-based cloud system framework: Smart healthcare monitoring systems. In: Artificial Intelligence for Cloud and Edge Computing, Springer, pp 181–208
39. Raj H, Kumar M, Kumar P, Singh A, Verma OP (2022) Issues and challenges related to privacy and security in healthcare using iot, fog, and cloud computing. Empowering Physicians with IoT-Enabled Technologies, Advanced Healthcare Systems, pp 21–32
40. Singh PD, Dhiman G, Sharma R (2022) Internet of things for sustaining a smart and secure healthcare system. Sustain Comput Inform Syst 33:100622
41. Chen C-L, Yang T-T, Shih T-F (2014) A secure medical data exchange protocol based on cloud environment. J Med Syst 38(9):112
42. Dolev D, Yao A (1983) On the security of public key protocols. IEEE Trans Inf Theory 29(2):198–208

43. Sarkar P (2010) A simple and generic construction of authenticated encryption with associated data. ACM Trans Inform Syst Sec (TISSEC) 13(4):33
44. Hankerson D, Menezes A.J., Vanstone S (2006) Guide to elliptic curve cryptography. Springer, New York
45. Kumar V, Ahmad M, Mishra D, Kumari S, Khan MK (2020) Rseap: Rfid based secure and efficient authentication protocol for vehicular cloud computing. Vehicul Commun 22:100213
46. Stallings W (2006) Cryptography and network security, 4/E. Pearson Education India, UK
47. Das AK, Paul NR, Tripathy L (2012) Cryptanalysis and improvement of an access control in user hierarchy based on elliptic curve cryptosystem. Inf Sci 209:80–92
48. Chuang Y-H, Tseng Y-M (2010) An efficient dynamic group key agreement protocol for imbalanced wireless networks. Int J Network Manage 20(4):167–180
49. Chatterjee S, Das AK, Sing JK (2014) An enhanced access control scheme in wireless sensor networks., Adhoc Sensor Wirel Netw, 21(1)
50. Das AK, Goswami A (2015) A robust anonymous biometric-based remote user authentication scheme using smart cards. J King Saud Univ-Comput Inform Sci 27(2):193–210
51. Odelu V, Das AK, Goswami A (2014) A secure effective key management scheme for dynamic access control in a large leaf class hierarchy. Inf Sci 269:270–285
52. Das AK (2015) A secure user anonymity-preserving three-factor remote user authentication scheme for the telecare medicine information systems. J Med Syst 39(3):30
53. Kumari A, Jangirala S, Abbasi MY, Kumar V, Alam M (2020) Eseap: Ecc based secure and efficient mutual authentication protocol using smart card. J Inform Sec Appl 51:102443
54. Bellare M, Rogaway P (1993) Random Oracles are Practical: A Paradigm for Designing Efficient protocols. In: Proceedings of the 1st ACM Conference on Computer and Communications Security, ACM, pp 62–73
55. Shoup V (2004) Sequences of games: a tool for taming complexity in security proofs. IACR Cryptology ePrint Archive 2004:332
56. Xu J, Zhu W-T, Feng D-G (2009) An improved smart card based password authentication scheme with provable security. Comput Stand Interfaces 31(4):723–728
57. Mishra D, Das AK, Mukhopadhyay S (2016) A secure and efficient ecc-based user anonymity-preserving session initiation authentication protocol using smart card. Peer-to-peer Netw Appl 9(1):171–192
58. Wazid M, Das AK, Odelu V, Kumar N, Conti M, Jo M (2017) Design of secure user authenticated key management protocol for generic iot networks. IEEE Internet Things J 5(1):269–282

Authors and Affiliations

Vinod Kumar[1] · Mahmoud Shuker Mahmoud[2] · Ahmed Alkhayyat[3] · Jangirala Srinivas[4] · Musheer Ahmad[5] · Adesh Kumari[6]

Vinod Kumar
vinod.iitkgp13@gmail.com; vinod@pgdav.du.ac.in

Mahmoud Shuker Mahmoud
Mahmoud.shukur@muc.edu.iq

Ahmed Alkhayyat
ahmedalkhayyat85@gmail.com

Jangirala Srinivas
sjangirala@jgu.edu.in; getsrinunow1@gmail.com

Musheer Ahmad
musheer.cse@gmail.com; mahmad9@jmi.ac.in

[1] Department of Mathematics, PGDAV College, University of Delhi, New Delhi 110065, India

[2] Al-Mansour University College, Baghdad, Iraq

[3] Department of Computer Technical Engineering, College of Technical Engineering, The Islamic University, Najaf, Iraq

[4] Jindal Global Business School, O. P. Jindal Global University, Sonipat, Haryana 131001, India

[5] Department of Computer Engineering, Jamia Millia Islamia, New Delhi 110025, India

[6] Department of Mathematics, Dyal Singh College, University of Delhi, New Delhi 110003, India