Journal of Ambient Intelligence and Humanized Computing (2023) 14:4853–4864
https://doi.org/10.1007/s12652-022-04370-2

ORIGINAL RESEARCH

Secure data authentication and access control protocol for industrial healthcare system

Daya Sagar Gupta[1] · Nabajyoti Mazumdar[2] · Amitava Nag[3] · Jyoti Prakash Singh[4]

Received: 2 December 2021 / Accepted: 30 July 2022 / Published online: 13 January 2023

Abstract
Because of recent COVID-19 epidemic, the Internet-of-Medical-Things (IoMT) has acquired a significant impetus to diagnose patients remotely, regulate medical equipment, and track quarantined patients via smart electronic devices installed at the patient's end. Nevertheless, the IoMT confronts various security and privacy issues, such as entity authentication, confidentiality, and integrity of health-related data, among others, rendering this technology vulnerable to different attacks. To address these concerns, a number of security procedures based on traditional cryptographic approaches, such as discrete logarithm and integer factorization problems, have been developed. All of these protocols, however, are vulnerable to quantum attacks. This paper, in this context, presents a data authentication and access control protocol for IoMT systems that can withstand quantum attacks. A comprehensive formal security assessment demonstrates that the proposed algorithm can endure both current and future threats. In terms of data computing, transmission, and key storage overheads, it also surpasses other related techniques.

Keywords Authentication · E-health · IoMT · Security and privacy · Lattice-based cryptography

1 Introduction

With unprecedented progress in technology, and medication, as well as the emergence of smart medical devices, the medical industry is evolving rapidly. Furthermore, advances in information technology have transformed a variety of medical facilities into virtual structures and applications that can be reached from a distance. The Internet of Things (IoT) and its integration into healthcare systems had a huge impact on public life and the medical industry. Noticeably, medical industries are turning to Internet of Medical Things (IoMT) applications to provide safer, faster, and more affordable healthcare (Firouzi et al. 2018; Kim 2015). IoMT systems are becoming more diverse and standard, making them suitable options for preventing, envisaging, and tracing evolving transferrable diseases such as COVID-19 (Alabdulatif et al. 2018). Wearable health-monitoring products, Wireless Body Area Networks, machine learning, and cloud-based health monitoring analysis are used in IoMT as a health-monitoring platform that provides real-time observation (Baranchuk et al. 2018). It is advantageous to provide an emergency alert technology to control the epidemic using IoMT specific functionality such as the collection of data, processing, exchange, and analytics. Security and privacy became an essential requisite for an IoMT application because it can have a negative impact on people's physiological, social, and biological states. Due to the restricted interface requirements and distributed architecture of the IoMT ecosystem, integrating security and privacy on IoMT devices is a difficult task. Furthermore, such instruments are at the network's edge and,

✉ Daya Sagar Gupta
dayasagar.ism@gmail.com

Nabajyoti Mazumdar
nabajyoti.ismdhanbad@gmail.com

Amitava Nag
amitava.nag@cit.ac.in

Jyoti Prakash Singh
jps@nitp.ac.in

[1] Department of Computer Science and Engineering, Rajiv Gandhi Institute of Petroleum Technology Jais, Amethi, UP 229304, India

[2] Department of Information Technology, Indian Institute of Information Technology Allahabad, Prayagraj, India

[3] Department of Computer Science and Engineering, Central Institute of Technology Kokrajhar, BTR, Kokrajhar, India

[4] Department of Computer Science and Engineering, National Institute of Technology Patna, Patna, India

in certain cases, are distant or embedded in the body, making them difficult to reach. Consequently, to make IoMT systems reliable, data protection and secure communication must conform to security standards. As per a recent study Aman et al. (2020), over 90% of all IoMT device communication is un-encrypted, meaning that 57% of IoT devices are susceptible to attacks that expose sensitive data. Cyber attacks are not only harmful to the system, but they can also be dangerous to people's lives. Any cyber-attack has the potential to be devastating, putting patients' lives in jeopardy (Yaacoub et al. 2020; Yaqoob et al. 2019). The recent emergence and proliferation of IoMT, especially during pandemics, could raise additional security concerns, making it even more difficult to safeguard the confidentiality of vital and sensitive patient information. Many IoT systems have no or poor authentication mechanisms due to hardware, energy usage, and other computing resource constraints, opening the door to cyber attacks (Gupta et al. 2020). Lightweight security methods including lightweight cryptography, lightweight hybrid anomaly detection, and lightweight multi-factor authentication are potentially feasible options for implementing stronger authentication in IoMT frameworks due to hardware restraints.

The smart e-health system is very useful during the time of global pandemics such as the ongoing COVID-19 outbreak in which remote monitoring of people in quarantine who are at high risk is essential to adhere social distance guidelines. In IoT-enabled health-care systems for COVID-19 monitoring and diagnosis, a wearable medical device equipped with several sensors are mounted in a patient's body in quarantine. Wireless technologies communicate and medical servers gather real-time physiological data on a patient's health (Baranchuk et al. 2018). The data collected at the medical server are then fetched by smart IoT devices like tablets, smart-phones, etc. The authorized doctors or nurses or relatives and friends of the patient are allowed to access those data and can take immediate decisions. Figure 1 exemplifies the IoT-enabled smart health-care system architecture for COVID-19 patients. These e-health systems must cater to different security and privacy requirements in order to easily identify a legitimate individual and ensure the privacy and confidentiality of data transmitted over a open wireless network.

1.1 Motivations and contributions

Secure communication and data authentication are extremely crucial among the various components of the IoMT system. Despite the fact that numerous studies have been conducted in this field, the majority of them have relied on traditional security procedures that have certain shortcomings. For example, Liu and Chung (2017) proposed an authentication

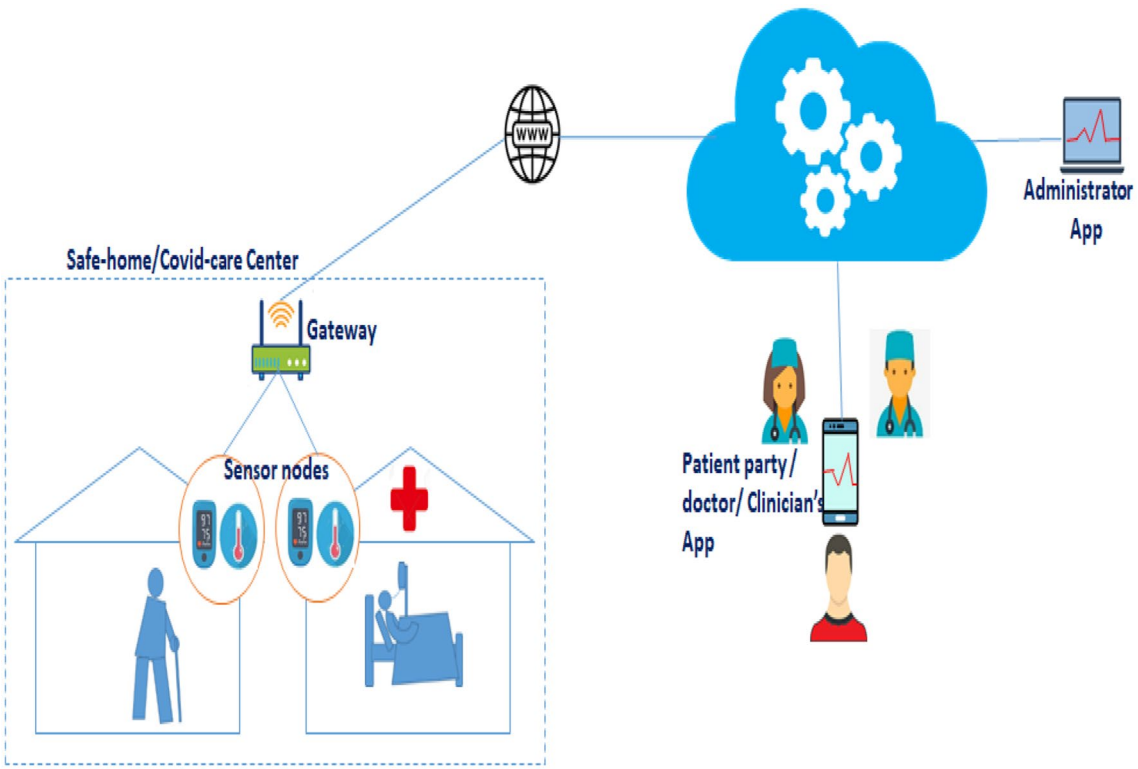

Fig. 1 The architecture of IoT based e-health system

protocol for e-health system which uses elliptic curve cryptography (ECC) and complex bilinear mapping (BP) in its design. Bilinear pairing on ECC is computationally expensive, making it incompatible for resource-constrained IoMT devices. Furthermore, most existing IoMT security protocols were designed employing conventional approaches, such as public-key cryptography (PKC), bilinear Diffie-Hellman problem (BDHP), identity-based cryptography (IBC), computational Diffie-Hellman problem (CDH), Chinese Remainder Theorem (CRT), and other DH type techniques (Kumar et al. 2012; Amin et al. 2018; Masud et al. 2020; Jan et al. 2021). Traditional security methods are vulnerable to a range of security attacks and incur significant costs in terms of communication, storage, and computing. Moreover, the aforementioned cryptographic methods, such as PKC, IBC, BP, CRT, ECC, BDH, and others, will be open to imminent quantum computing technologies. Shor (1999) have revealed that several cryptographic systems are diffident against computing power of quantum computers. However, it has been observed that lattice-based cryptographic designs are resistant to quantum workstations and ease the vulnerabilities found in classical cryptographic methods (Gupta et al. 2020, 2022). To address the issues raised above, the proposed protocol, referred to as PDAC-CoV, employs lattice as a tool to develop a data authentication and access control scheme for an IoMT network. The primary contributions of the designed PDAC-CoV protocol are as follows.

- To make the proposed scheme resilient against future quantum attacks, it is built on the notion of lattice cryptography that uses small integer solution (SIS) and inhomogeneous small integer solution (ISIS).
- The conceptual implementation of the suggested PDAC-CoV protocol is validated using a formal security framework based on the random oracle model (ROM).
- The proposed scheme ensures the IoMT network's security requirements, such as patient anonymity, replay attacks, mutual authentication, impersonation, access control, and quantum security.
- Because it primarily involves addition as well as multiplication among vectors and matrices, the suggested approach is relatively simple and efficient, and also it can be effortlessly applied in an IoMT scenario.

1.2 Structure of paper

This article is also structured in the subsequent way. The Sect. 2 contains recent works. Various definitions and ideas to be utilised in the designing the protocol is presented in Sect. 3. The suggested PDAC-CoV protocol is explained in Sect. 4. The Sect. 5 discusses the correctness and probable analysis of the PDAC-CoV protocol. The suggested protocol's performance evaluation and comparative findings are discussed in Sect. 6. The paper is concluded at Sect. 7.

2 Related work

An IoT-based e-Health system is used in modern healthcare institute such as hospitals, laboratories, clinics, smart homes etc., to provide a smart e-health service to the patient or patient party by performing healthcare activities such as remote monitoring, diagnosing and surgeries (Aman et al. 2020). Kumar et al. (2012) and Lin et al. (2009) have suggested authentication protocols for e-health systems, and named them as E-SAP and SAGE respectively. The proposed schemes are considered to be secure in the context of a global eavesdropping attack. In the paper Das and Goswami (2013), proposed a stable remote user authentication protocol for wireless medical sensor networks (WMSNs). (Automated Validation of Internet Security Protocols and Applications) AVISPA was used to demonstrate the application's security. Gupta and Biswas (2018) has designed a post-quantum encryption as well as signature scheme which is lightweight and may be applicable in IoMT scenario. Amin et al. (2015) designed a privacy-preserving authentication scheme for e-health systems. To prove its security, they used (Burrows–Abadi–Needham) BAN logic and AVISPA. They also compared their proposal to other protocols and demonstrated that it outperforms protocols in similar categories. However, Li et al. (2016) investigated Amin et al. (2015) article further and discovered an untraceability issue in the proposal. Likewise, He et al. (2015) have presented a robust authentication protocol for WMSNs based e-healthcare system and demonstrated its efficiency over (Kumar et al. 2012). For WMSNs, Liu and Chung (2017) suggested a user authentication and encryption protocol based on bilinear pairing. They demonstrated that their strategy protects against a wide number of attacks. Li et al. (2017) simplified several difficulties in the protocol (Liu and Chung 2017) and invented an enhanced protocol that can be used in IoT environments for e-health systems. They also stated that their proposed scheme is sufficiently robust to provide verifiable protection in the random oracle model, and that it outperforms related protocols in terms of efficiency. Amin et al. (2018) developed an architecture for WMSNs and introduced a mutual authentication protocol for mobile nodes. They used BAN logic and AVISPA to demonstrate the security of their proposal. Chaudhary et al. (2018) designed an encryption scheme for the IoMT system. Using encryption, they claimed that the proposal satisfies authentication among various entities. Aghili et al.

(2019) proposed an enhanced authentication protocol for IoT-based e-health systems. They assessed the security of their protocol using ProVerif analysis, demonstrating that it is robust enough to withstand all known attacks. SAHU et al. (2021) proposed lattice-based multi-party authentication scheme for IoMT environment. Cao et al. (2019) suggested an authentication protocol for IoT-enabled systems that included fast data transmission. Since their protocol employs lattice cryptography, it is resilient to quantum attacks. Al-Turjman and Deebak (2020) proposed a privacy-aware energy-efficient framework (P-AEEF) protocol with low communication cost. Mukherjee et al. (2019) developed an authentication protocol using lattices for the Vehicular Ad hoc Network (VANET). Kumar et al. (2020) designed a lattice-based signcryption scheme for electric vehicles.

3 Lattice

Due to inherent robustness, lattices are becoming a significant tool for ongoing and prospective cryptography. In the context of quantum computers, hard problems on a lattice can enhance cryptography schemes (Gupta and Biswas 2018).

Definition 1 (Lattice). A lattice represented by $\mathcal{L}$ can indeed be defined as follows given a set of vectors $\mathbf{u_1}, \mathbf{u_2} \cdots \mathbf{u_m} \in \mathcal{R}^n$:

$$\mathcal{L}(\mathbf{u_1}, \mathbf{u_2} \cdots \mathbf{u_m}) = \left\{ \sum_{i=1}^{n} g_i \mathbf{u_i} \, : \, g_i \in Z^+ \right\}$$

Such $\mathbf{u_1}, \mathbf{u_2} \cdots \mathbf{u_m}$ vectors ought to be linearly independent and are referred to as basis vectors (Gupta et al. 2022). The minimal distance of $\mathcal{L}$ is the shortest non-zero vector in $\mathcal{L}$ and can be computed using the expression below.

$$\mathcal{D}_{min}(\mathcal{L}) = \min_{\mathbf{v} \in \mathcal{L} \setminus \{0\}} \| \mathbf{v} \|$$

Lemma 1 *A lattice $\mathcal{L}$ obligate at least one basis to construct $\mathcal{L}$.*

The basis of $\mathcal{L}$ can be symbolized by a matrix $\mathbf{U} = [\mathbf{u_1}, \mathbf{u_2} \cdots \mathbf{u_m}] \in Z^{n \times m}$. The matrix $\mathbf{U}$ is termed as *basis matrix*, where the columns are set of basis vectors. Thus, a lattice $\mathcal{L}$ can be precise by the subsequent equation given bellow:

Definition 2 Consider $\mathbf{U} = [\mathbf{u_1}, \mathbf{u_2} \cdots \mathbf{u_m}] \in Z^{n \times m}$ be a basis matrix, the generated lattice $\mathcal{L}$ by $\mathbf{U}$ in $\mathcal{R}^n$ can be stated as $\mathcal{L}(\mathbf{U}) = [\mathbf{Uc} \, : \, \mathbf{c} \in Z^m]$ where $\mathbf{Uc}$ represent a usual matrix-vector multiplication.

The shortest vector problem (SVP) and closest vector problem (CVP) are well-known to be two basic hard assumptions in a lattice $\mathcal{L}$. In SVP, the problem is to find a short non-zero vector on a known lattice $\mathcal{L}$ with the minimum Euclidian norm, while in CVP, the problem is to find the closest vector to a known vector in $\mathcal{L}$. *appr*SVP and *appr*SVP are two more extensions of SVP and CVP, respectively.

Definition 3 (Shortest Vector Problem (SVP)). For a given lattice $\mathcal{L}(\mathbf{U})$ and its basis matrix $\mathbf{U} \in Z^{n \times m}$, it is quiet difficult to find a non-zero vector $\mathbf{h} \in \mathcal{L}(\mathbf{U})$ for $\| \mathbf{h} \| = \mathcal{D}_{min}(\mathcal{L})$.

Definition 4 (Closest Vector Problem (CVP)). For a given lattice $\mathcal{L}(\mathbf{U})$, its basis matrix $\mathbf{U} \in Z^{n \times m}$ and a vector $\mathbf{j} \notin \mathcal{L}$, it is quiet difficult to find a non-zero vector $\mathbf{h} \in \mathcal{L}(\mathbf{U})$ such that $\| \mathbf{j} - \mathbf{h} \| = \mathcal{D}_{min}(\mathcal{L})$.

3.1 *q-ary* lattice

A lattice $\mathcal{L}$ that satisfies $Z_q^n \subseteq \mathcal{L} \subseteq Z^n$ is said to be *q-ary* lattice for an integer modular $q \approx poly(m)$. The following is the definition of an *q-ary* lattice:

Definition 5 For a given a modular matrix $\mathbf{U} \in Z_q^{n \times m}$ for $(n < m)$ and $m \approx poly(n)$, two *q-ary* lattices $\Lambda_q^{\perp}$ and Λ_q can be inscribed as:

$$\Lambda_q^{\perp} = \{\mathbf{b} \in Z^m \, : \, \mathbf{Ub} = \mathbf{0} \bmod q\}$$

and

$$\Lambda_q = \{\mathbf{b} \in Z^m \, : \, \mathbf{a} = \mathbf{U^T d} \bmod q, \forall \, \mathbf{d} \in Z^n\}$$

Several lattice-based advances had exploited *q-ary* lattices and their difficult problems to construct a cryptosystem, according to several literature. There are two difficult challenges on *q-ary* lattices that are employed in the PDAC-CoV scheme proposal. These issues are described in the subsequent way.

Definition 6 (Small Integer Solution (SIS) problem). For a given modular matrix $\mathbf{U} \in Z_q^{n \times m}$ and $\beta \in Z^+$, it is quiet difficult to acquire a vector $\mathbf{v} \in Z^m \setminus \{0\}$ such that $\mathbf{Xv} = \mathbf{0}$ mod q with $\| \mathbf{v} \| \leq \beta$.

Definition 7 (Inhomogeneous Small Integer Solution (ISIS) problem). For a given modular matrix $\mathbf{U} \in Z_q^{n \times m}$, $\beta \in Z^+$ and a random vector $\mathbf{b} \in Z_q^n$, it is hard to acquire a vector $\mathbf{v} \in Z^m \setminus \{0\}$ such that $\mathbf{Xv} = \mathbf{t}$ mod q with $\| \mathbf{v} \| \leq \beta$.

According to the authors of (Ajtai 1996; Mukherjee et al. 2019), the SIS and ISIS problems are immune against quantum assault. Furthermore, advances in (Ajtai 1996; Gentry

et al. 2008; Micciancio and Regev 2007) shown that SIS/ISIS hard problems are known to be as difficult as SVP, SIVP, and other challenges.

Theorem 1 *For $m = poly(n)$, $\beta \in Z^+$, a prime modulus $q \geq \beta \cdot \sqrt{\omega(n \log n)}$ and a lattice $\mathcal{L}$, finding a average-case result of SIS/ISIS problems is at least as unbreakable as approximating worst-case solution for $SIVP_\gamma$ and $GapSVP_\gamma$ within a factor $\gamma = \beta \cdot \tilde{O}\sqrt{m}$(Gentry et al. 2008).*

4 Proposed PDAC-CoV protocol

In the proposed protocol, U_i be a user such as doctors, nurses, relatives etc who wishes to examine the medical condition of a quarantine patient P_j, P_j be a patient equipped with wearable medical equipment and base station from which the medical condition of P_j is transferred to *MS*, and *MS* is a medical server which store the medical related data of the patient. To access P_j's data, U_i must use his/her smart-card to be authenticated by *MS*. This *MS* is directly connected to a patient P_j through the base-stations and collects the physiological information of P_j. Whenever, U_i needs the patient's information from *MS*, it follows the proposed access control mechanism. The notations which are used given in Table 1. The PDAC-CoV protocol is governed by the following five phases, namely *Setup, Registration, Login, Verification,* and *Access control*.

1. Setup Phase The medical server *MS* executes *Setup* phase to generate system parameter list *param*. With an input 1^k, *MS* firstly choose a prime modulus q with an integer n. It selects a modular matrix $\mathbf{X} \in \mathbb{Z}_q^{n \times n}$ with two cryptographic hash functions $h_1 : \{0,1\}^* \rightarrow \{0,1\}^k$ and $h_2 : \mathbb{Z}_q^n \times \{0,1\}^* \rightarrow \{0,1\}^k$. It randomly selects $\mathbf{d} \in \mathbb{Z}_q^n$ as its private key. At last, it shares the system parameters $param = \langle n, q, \mathbf{X}, h_1(\cdot), h_2(\cdot)\rangle$ with other entities.
2. Registration Phase To register with *MS*, a user U_i must get a personalized smart-card securely. Firstly, U_i need to create his/her password Pw_i along with an ID_i. It, then selects a random integer $a_i \in \mathbb{Z}_q$ to compute the value $\alpha_i = h_1(ID_i||Pw_i||a_i)$. Now, it passes request for registration to *MS* with tuple $\langle ID_i, \alpha_i\rangle$ through a secure channel. The medical server *MS* searches ID_i in its database and if it exists, then flashes a message to select another identity. *MS* chooses a random integer $b \in \mathbb{Z}_q$ and calculates $\beta_i = h_2(\mathbf{d}||b||ID_i)$, $\gamma_i = \alpha_i \oplus \beta_i$. It, then calculates $\mathbf{Q_i} = \mathbf{P_i} \cdot \mathbf{d^T}$ where $\mathbf{P_i} = \mathbf{X^T} \cdot \mathbf{r_i}$ and $\mathbf{r_i} \in \mathbb{Z}_q^n$ are the public and private values of U_i. Now, *MS* create a smart-card with tuple $\langle m, n, q, \mathbf{X}, \mathbf{Q_i}, h_1(\cdot), h_2(\cdot), b, \gamma_i\rangle$ and sends to U_i securely. It may be worth noting that same "b" is used for every patients in the system. Now, U_i calculates $\beta_i = \gamma_i \oplus h_1(ID_i||Pw_i||a_i)$, $\delta_i = h_1(ID_i||Pw_i) \oplus a_i$ and $\xi_i = h_1(a_i||h_1(ID_i||Pw_i)||\beta_i)$ and writes $\langle \delta_i, \xi_i\rangle$ to his/her smart-card. Now, the content of U_i's smart-card is updated as $\langle m, n, q, \mathbf{X}, \mathbf{Q_i}, h_1(\cdot), h_2(\cdot), b, \gamma_i, \delta_i, \xi_i\rangle$. The registration phase of our PDAC-CoV protocol is depicted in Fig. 2.
3. Login Phase This phase is initiated by U_i to access the health data D_j of P_j. Firstly, U_i feeds his/her smart-card into the device and inserts ID_i and Pw_i. Now, the smart-card of U_i computes $a_i' = h_1(ID_i||Pw_i) \oplus \delta_i$, $\beta_i' = \gamma_i \oplus h_1(ID_i||Pw_i||a_i')$,$\xi_i' = h_1(a_i'||h_1(ID_i||Pw_i)||\beta_i')$, and checks whether $\xi_i' = \xi_i$. If it is true, the smart-card chooses a random vector $\mathbf{u_i} \in \mathbb{Z}_q^n$ and computes $\mathbf{S_i} = \mathbf{Q_i^T} \cdot \mathbf{u_i} \in \mathbb{Z}_q^n$, $\chi_i = h_1(t_1||ID_i||\beta_i')$ and $\varphi_i = h_1(s_i) \oplus (ID_i||\chi_i)$ where $s_i = \sum_{k=1}^{n}(\mathbf{S_i})_k \bmod q$. It, then sends $\langle \mathbf{u_i}, \varphi_i, t_1\rangle$ to *MS* over a public network where t_1 denotes the timestamp during the login phase.
4. **Verification Phase** On receipt of $\langle \mathbf{u_i}, \varphi_i, t_1\rangle$ at time t_2, *MS* checks the validity of message by checking timestamp duration as $(t_2 - t_1) < \Delta\, t$. Now, it computes $\mathbf{R_i} = \mathbf{P_i^T} \cdot \mathbf{u_i}$, and then $\mathbf{S_i'} = \mathbf{d} \cdot \mathbf{R_i}$. Then, it computes $s_i' = \sum_{k=1}^{n}(\mathbf{S_i'})_k \bmod q$ and finds ID_i and χ_i satisfying $(ID_i||\chi_i) = h_1(s_i') \oplus \varphi_i$. It checks whether ID_i is present in its database. Then, it calculate $\beta_i = h_2(\mathbf{d}||b||ID_i)$ and $\chi_i' = h_1(t_1||ID_i||\beta_i)$, and checks $\chi_i = \chi_i'$ to authenticate U_i. It, then sends a fresh timestamp t' to U_i. Now, U_i verifies t' as $(t'' - t')\,\Delta\, t'$ at current time t'' and then forwards t' to *MS*.

Table 1 Notations and their description

Notation	Description
k	Security parameter
q	A prime modular, $q \approx poly(k)$
n	Positive integers
$\mathbf{X}$	Modular matrix, $\mathbf{X} \in Z_q^{m \times n}$
$\mathbf{d}$	Master secret key, $\mathbf{d} \in Z_q^n$
$\mathbf{Q_i}$	Public value, $\mathbf{Q_i} = \mathbf{P_i} \cdot \mathbf{d^T}$
$h_1(.), h_2(.)$	Cryptographic hash functions
U_i	User/Smart-card
MS	Medical server
P_j	Patient/Sensor node
ID_i & Pw_i	Identity and password of user
ID_{i_t}	Temporary identity of user
b	a secret value common for all patients, $b \in Z^q$
ϵ	A negligible function
t_i	Timestamp
D_j	Patient Health data
$\oplus$	XOR operation
$\|\|$	Concatenation operation

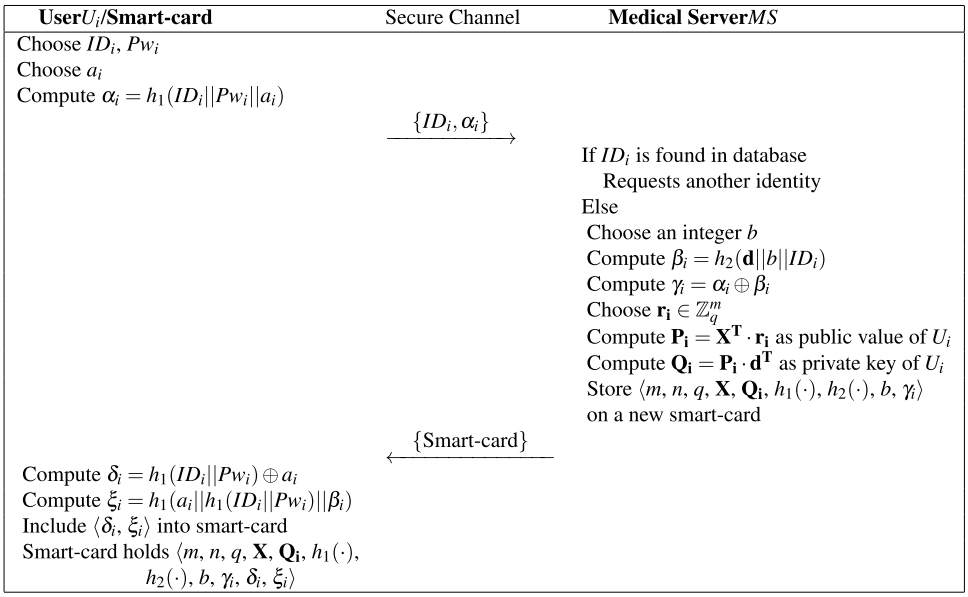

Fig. 2 Registration phase of proposed PDAC-CoV protocol

5. **Access Control Phase** After successful authentication, a user U_i can access the health data D_j of a patient P_j through the medical server MS. MS verifies the validity of t' as $(t''' - t') > \Delta t''$ at current time t''', where $\Delta t''$ is considered as idle session out time. If it happens, MS simply flashes an pop up message showing login again and terminates the session. Otherwise, it randomly picks $d_i \in \mathbb{Z}_q$ as an integer and calculates $\phi_i = h_1(d_i||ID_{i_t})$ for ID_{i_t} as a temporary identity of U_i. It calculates a message $M_i = h_1(s_i') \oplus (ID_i||ID_{i_t}||t_3||\phi_i)$ and $M_i' = h_1(ID_i||ID_{i_t}||t_3)$ for a permitted time t_3 and sends to U_i. It also transfers $\langle ID_{i_t}, t_3, d_i \rangle$ to P_j simultaneously over a secure channel. It may be worth noting that ID_{i_t} is only valid for "**Access control phase** ". On receipt of M_i and M_i', U_i calculates $(ID_i||ID_{i_t}||t_3||\phi_i) = h_1(s_i') \oplus M_i$. U_i then computes $M_i'' = h_1(ID_i||ID_{i_t}||t_3)$ and verifies whether $M_i' = M_i''$. After that U_i automatically authenticates S if fetched ID_i belongs to it. Next, U_i feeds his/her smart-card in the device and keeps ϕ_i and ID_{i_t} temporarily with it until this phase ended. U_i, then inserts his/her ID_i and Pw_i into the smart-card. Now, the smart-card of U_i calculates $a_i' = h_1(ID_i||Pw_i) \oplus \delta_i$, $\beta_i' = \gamma_i \oplus h_1(ID_i||Pw_i||a_i')$ and $\xi_i' = h_1(a_i'||h_1(ID_i||Pw_i)||\beta_i')$. It verifies $\xi_i' = \xi_i$ and computes $\pi_i = h_1(\phi_i) \oplus h_1(ID_{i_t}||b||t_4)$ on time t_4, and sends $\langle \pi_i, ID_{i_t}, t_4 \rangle$ to P_j. On receipt of $\langle \pi_i, ID_{i_t}, t_4 \rangle$ at time t_5, P_j verifies whether $(t_5 - t_4) < \Delta t$ and computes $\pi_i' = h_1(h_1(d_i||ID_{i_t})) \oplus h_1(ID_{i_t}||b||t_4)$. It, then verifies whether $\pi_i' = \pi_i$. If it holds true, P_j authenticates U_i. Next, to securely send the health data D_j, P_j calculates a session key $SK_{ij} = h_1(t_3 \oplus \phi_i \oplus b)$ and applies symmetric encryption algorithm to encrypt D_j as $E_{ji} = D_j \oplus SK_{ij}$. P_j then transfers E_{ji} to U_i through a public channel. On receipt of C_{ji}, U_i calculates $SK_{ij} = h_1(t_3 \oplus \phi_i \oplus b)$, and decrypts E_{ji} as $D_j = E_{ji} \oplus SK_{ij}$. The login, verification and access control phases of our PDAC-CoV protocol is depicted in Fig. 3.

5 Security analysis

This section discusses security aspects of the proposed PDAC-CoV protocol for the e-Health care system. The security analysis od PDAC-CoV is based on the random oracle model as discussed in Li et al. (2017), Gupta and Biswas (2017a, 2017b). The formal security model of our protocol is described below.

5.1 Provable security proofs

5.1.1 Security model

Let $\mathcal{P}$ be the set of participants and the execution of j^{th} instance of the protocol by $\mathcal{P}$ is denoted by $\Pi_{\mathcal{P}}^j$, where $\mathcal{P} \in \{U_i, MS, P_j\}$. Let $\mathcal{A}$ be a randomized probabilistic polynomial time-bounded (PPT) adversary who is allowed to execute the following oracle queries with the help of a challenger $\mathcal{C}$.

Send$(\Pi_{\mathcal{P}}^j, msg)$: After getting this oracle query with message msg, $\mathcal{C}$ executes the instance $\Pi_{\mathcal{P}}^j$ of the proposed protocol for msg and then returns the outcome to $\mathcal{A}$.

Hash$(\Pi_{\mathcal{P}}^j, msg)$: For this query, $\mathcal{C}$ returns a random hash value to $\mathcal{A}$ for the instance $\Pi_{\mathcal{P}}^j$ as per the following rules.

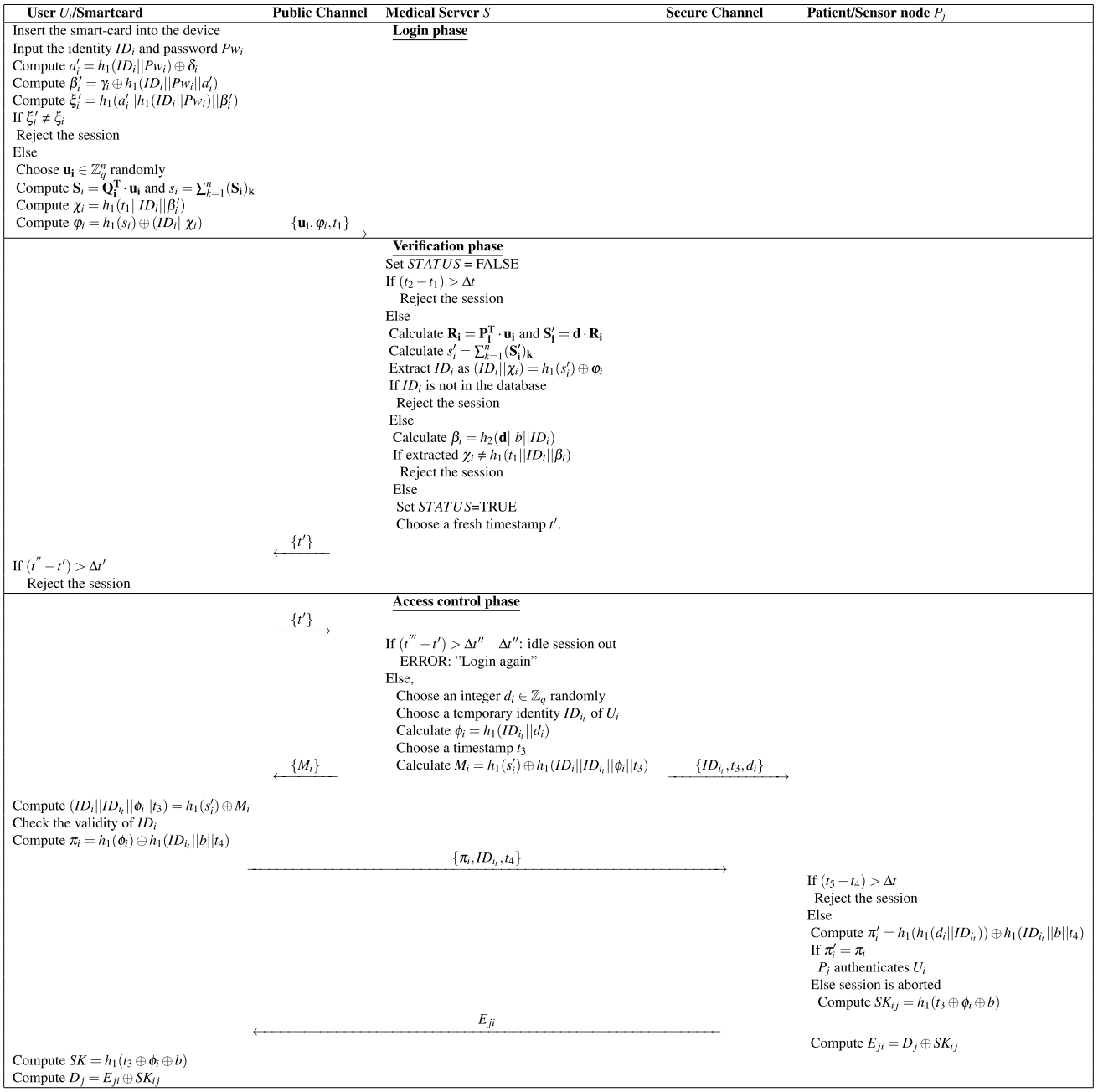

Fig. 3 Login, verification and access control phases

- h_1-*Query*: To respond this query, a list L_{h_1} is maintained by $\mathcal{C}$. Basically, L_{h_1} is initially kept empty and the content of this list is a tuple like (m_1, o) where m_1 is the input to h_1 and h_1 produces corresponding output as o. To answer the h_1-*Query* of $\mathcal{A}$ with an input m_1, $\mathcal{C}$ looks in the list L_{h_1} for a tuple (m_1, o). In case, the tuple (m_1, o) is in the list L_{h_1}, $\mathcal{C}$ outputs the corresponding output o to $\mathcal{A}$. Otherwise, a random $o \in \mathbb{Z}_q^*$ is selected by $\mathcal{C}$ as an output. In addition, $\mathcal{C}$ also inserts the newly generated tuple (m_1, o) into list L_{h_1}.
- H_2-*Query:* Similar to h_1-*Query*, To respond this query, a list L_{h_2} is maintained by $\mathcal{C}$. Basically, L_{h_2} is initially kept empty and the content of this list is a tuple like (m_2, o) where m_2 is the input to h_2 and h_2 produces corresponding output as o. To answer the h_2-*Query* of $\mathcal{A}$ with an input m_2, $\mathcal{C}$ looks in the list L_{h_2} for a tuple (m_2, o). In case, the tuple (m_2, o) is in the list L_{h_2}, $\mathcal{C}$ outputs the corresponding output o to $\mathcal{A}$. Otherwise, a random $o \in \mathbb{Z}_q^*$ is selected by $\mathcal{C}$ as an output. In addition, $\mathcal{C}$ also inserts the newly generated tuple (m_2, o) into list L_{h_2}.

Login $(\Pi^j_{U_i}, \mathcal{P})$: An adversary $\mathcal{A}$ runs a *Login-Query* with ID_i and Pw_i and generates login message $\langle \mathbf{u_i}, \varphi_i, t_1 \rangle$. $\mathcal{A}$ then submits this message to $\mathcal{C}$ as the answer.

Corrupt$(\Pi^j_{U_i}, \mathcal{P})$: For this query, $\mathcal{C}$ returns the password $Pw_{\mathcal{P}}$ of $\mathcal{P}$ for the instance $\Pi^j_{U_i}$ to $\mathcal{A}$. It may be noted that this oracle query satisfies the forward secrecy attack on the session key.

Reveal$(\Pi^j_{\Gamma \in \{U_i, P_j\}})$: After getting this query, $\mathcal{C}$ returns previously generated session key of an accepted state to $\mathcal{A}$. If it is not accepted, then $\mathcal{C}$ returns a random string. It may be noted that this oracle query satisfies the session key security attack.

Test$(\Pi^j_{\Gamma \in \{U_i, P_j\}})$: This oracle query is executed only once by the adversary $\mathcal{A}$. As a response to this query, $\mathcal{C}$ chooses a bit $c \in \{0, 1\}$ randomly and outputs it. If $c = 1$ is output, the session key is returned, otherwise, a random string is returned. It may be noted that this oracle query satisfies the semantic security of the session key.

The above queries satisfies the security against existential unforgeability under chosen message attack (EUF-CMA) of PDAC-CoV protocol. The adversary $\mathcal{A}$ asks these queries in an adaptive manner. To win this game, $\mathcal{A}$ has to successfully break the security authentication of PDAC-CoV protocol. Let $\mathcal{A}$ has violated the security of PDAC-CoV protocol then its advantage can be written as $\epsilon = Adv^{EUF-CMA}_{\mathcal{A},\, Auth}(k)$.

5.1.2 Security proof

The following theorem proofs the formal security of the PDAC-CoV protocol.

Theorem 2 *Let $\mathcal{A}$ be a PPT adversary who wishes to breaches (ϵ, τ)–EUF-CMA security of PDAC-CoV protocol. Then, $\mathcal{A}$ might break the SIS/ISIS problem in polynomial-time τ' with non-negligible advantage ϵ', where*:

$$\epsilon' \geq \epsilon \cdot \left(\frac{q_{hash}}{2^k}\right), \quad \tau' \geq \tau + O(T_{\mathbf{r}\cdot\mathbf{X}})$$

and q_{hash} represents the maximum number of hash queries and $T_{\mathbf{r}\cdot\mathbf{X}}$ denotes time needed to multiply $\mathbf{r} \in \mathbb{Z}^n_q$ with $\mathbf{X} \in \mathbb{Z}^{n\times n}_q$.

Proof Let the adversary $\mathcal{A}$ want to attack on the login massage $\langle \mathbf{u_i}, \varphi_i, t_1 \rangle$ of an authentic user U_i. In this regard, $\mathcal{C}$ helps $\mathcal{A}$ with a non-negligible advantage to break the SIS/ISIS problem on $\mathcal{L}$.To win the game played between $\mathcal{C}$ and $\mathcal{A}$, $\mathcal{A}$ needs to unmask the private key $\mathbf{d}$ from public values $\mathbf{X}$, and $\mathbf{Q_i} = \mathbf{P_i} \cdot \mathbf{d^T}$. Then, this game is began by $\mathcal{C}$ as follows.

- *Setup*: $\mathcal{C}$ runs the *Setup* phase of the proposed PDAC-CoV protocol and transfers system parameters $param = \langle n, q, \mathbf{X}, h_1(\cdot), h_2(\cdot) \rangle$ to $\mathcal{A}$ along with $\mathbf{Q_i}$.
- h_1-*Query*: In this query, a list L_{h_1} is maintained by $\mathcal{C}$. Basically, L_{h_1} is initially kept empty and the content of this list is a tuple $\langle t_1, ID_i, \beta'_i, s_i, \mu_i, \upsilon_i \rangle$. A query with $\langle t_1, ID_i, \beta'_i, s_i \rangle$ is initiated by $\mathcal{A}$. To answer this query, $\mathcal{C}$ searches the list L_{h_1} and outputs $\mu_i = h_1(t_1||ID_i||\beta'_i)$ and $\upsilon_i = h_1(s_i)$ to $\mathcal{A}$ if corresponding values are found. Otherwise, random values of $\mu'_i, \upsilon'_i \in \mathbb{Z}_q$ are chosen by $\mathcal{C}$ and returned to $\mathcal{A}$. In addition, $\mathcal{C}$ puts $\langle t_1, ID_i, \beta'_i, s_i, \mu'_i, \upsilon'_i \rangle$ into L_{h_1} as a new entry.
- h_2-*Query:* In this query, a list L_{h_1} is maintained by $\mathcal{C}$. Basically, L_{h_1} is initially kept empty and the content of this list is a tuple $\langle \Gamma, \beta, ID_i, \mu_i \rangle$. A query with $\langle \Gamma, \beta, ID_i \rangle$ is initiated by $\mathcal{A}$. To answer this query, $\mathcal{C}$ searches the list L_{h_2} and outputs $\mu_i = h_1(\Gamma||\beta_i||ID_i)$to $\mathcal{A}$ if corresponding values are found. Otherwise, random values of $\mu'_i \in \mathbb{Z}_q$ are chosen by $\mathcal{C}$ and returned to $\mathcal{A}$. In addition, $\mathcal{C}$ puts $\langle \Gamma, \beta, ID_i, \mu'_i \rangle$ into L_{h_2} as a new entry.
- *Login-Query*: This query is executed by $\mathcal{A}$ with $\langle ID_i, Pw_i \rangle$. In response $\mathcal{C}$ randomly picks $\mathbf{u_i} \in \mathbb{Z}^m_q$ and $\beta'_i \in \mathbb{Z}_q$, and then computes $\mathbf{S_i} = \mathbf{Q_i^T} \cdot \mathbf{u_i}$, $\chi_i = h_1(t_1||ID_i||\beta'_i)$ and $\varphi_i = h_1(s_i) \oplus (ID_i||\chi_i)$where $s_i = \sum_{k=1}^{n} (\mathbf{S_i})_k \bmod q$. After that, $\mathcal{C}$ sends $\langle \mathbf{u_i}, \varphi_i, t_1 \rangle$ to $\mathcal{A}$.

The adversary $\mathcal{A}$ continuously asks above queries a number of times and at last, outputs a tuple $\langle \mathbf{u'_i}, \varphi'_i, t_1 \rangle$ to $\mathcal{C}$. Let q_{hash} be the maximum number of hash queries and q_s be the maximum number of login queries issued by $\mathcal{A}$ to $\mathcal{C}$. Consider that $\mathcal{A}$ has an advantage of ϵ to impersonate an authentic user U_i, so that $\mathcal{C}$ may accept the forged login message $\langle \mathbf{u'_i}, \varphi'_i, t_1 \rangle$. Now, it is given that $\mathbf{u_i}$ and $\mathbf{P_i} = \mathbf{X} \cdot \mathbf{r_i}$ which is available to $\mathcal{A}$ where $\mathbf{d}$, $\mathbf{Q_i}$ and $\mathbf{S_i}$ are unknown. However, $\mathcal{A}$ is able to compute $\mathbf{R_i} = \mathbf{P_i^T} \cdot \mathbf{u_i}$. Thus, given $(\mathbf{X}, \mathbf{u_i}, \mathbf{P_i}) = (\mathbf{X}, \mathbf{u_i}, \mathbf{X^T} \cdot \mathbf{r_i})$, $\mathcal{C}$ can compute $\mathbf{d} \cdot \mathbf{P_i^T} \cdot \mathbf{u_i} = \mathbf{d} \cdot \mathbf{r_i^T} \cdot \mathbf{X} \cdot \mathbf{u_i}$ by using algorithm executed by $\mathcal{A}$. Hence, $\mathcal{C}$ can solve the ISIS problem with advantage

$$\begin{aligned}
&\epsilon' \\
\geq & q \cdot \epsilon \cdot \frac{q_s}{q} \cdot \mathbf{Pr}\left[\beta'_i = h_2(\mathbf{d}||b||ID_i); \chi_i = h_1(t_1||ID'_i||\beta'_i); (ID_i||\chi_i) = h_1(s'_i) \oplus \varphi'_i\right] \cdot \frac{1}{q_s} \\
\geq & \epsilon \cdot q \cdot \frac{q_s}{q} \cdot \frac{q_{hash}}{2^k} \cdot \frac{1}{q_s} \\
= & \epsilon \cdot \left(\frac{q_{hash}}{2^k}\right)
\end{aligned}$$

5.2 Further security discussions

This section mentions some of the important security aspects, such as user anonymity, replay attack, server impersonation, user impersonation, sensor node impersonation, stolen smart-card, off-line password guessing, session key, entity privacy, password disclosure attacks. we show that the new PDAC-CoV protocol resists all the aforementioned attacks.

5.2.1 Anonymity of the user

The proposed PDAC-CoV protocol is designed to provide the user anonymity property. The real identity ID_i of the user U_i is covered in each transmission and it is difficult for any adversary $\mathcal{A}$ to find the real identity ID_i through any attack. The login phase of the proposed protocol masks the real identity ID_i of U_i in $\varphi_i = h_1(s_i) \oplus (ID_i||\chi_i)$ in which $\mathcal{A}$ cannot unmask ID_i without the secret values (s_i), $\chi_i)$. Further, a temporary identity ID_{i_t} of U_i is used in subsequent phases to hide the real identity ID_i of U_i. This ID_{i_t} is randomly chosen in each session. Thus, the proposed PDAC-CoV proposed supports user anonymity.

5.2.2 Replay attack

In our PDAC-CoV approach, the time-stamps and randomized values are supposed to preclude the replay attack. In the login phase, $\langle \mathbf{u_i}, \varphi_i, t_1 \rangle$ is sent which include timestamp t_1. At verification end, the validity of time-stamp is tested to avoid the replay attacks. Similarly, next subsequent phases prevent the replay attack by including a new timestamp. Further, these timestamps are also inserted in the encrypted messages $\varphi_i = h_1(s_i) \oplus (ID_i||h_1(t_1||ID_i||\beta_i'))$ and $\pi_i = h_1(\phi_i) \oplus h_1(ID_{i_t}||b||t_4)$ to confirm the validity of timestamps. As a result, the receiver of any message validates the timestamp's freshness before verifying its correctness in the current message. As a result, the proposed PDAC-CoV protocol precludes replay attacks.

5.2.3 Server impersonation attack

To impersonate the medical server *MS*, an adversary $\mathcal{A}$ must compute the valid response message M_i. However, the real identity ID_i, password Pw_i and the random value d_i is unknown to $\mathcal{A}$. Due to the lack of these values, $\mathcal{A}$ is unable to compute M_i. Thus, $\mathcal{A}$ cannot impersonate *MS* to U_i. Hence, the PDAC-CoV protocol resists the server impersonation attack.

5.2.4 User impersonation attack

In this attack, an adversary $\mathcal{A}$ attempts to impersonate U_i either by creating a fabricated login credential or by eavesdropping the login message to prove his/her authenticity to *MS*. In our PDAC-CoV protocol, ID_i, Pw_i and $\mathbf{Q_i}$ is unknown to $\mathcal{A}$. Due to this reason, $\mathcal{A}$ is unable to create a valid and fabricated login message $\langle \mathbf{u_i}, \varphi_i, t_1 \rangle$ and thus cannot impersonate U_i to *MS*. Hence, our PDAC-CoV protocol resists the user impersonation attack. Similarly, the patient P_j can also authenticate U_i since only U_i can compute the value π_i which can be verified by P_j as $\pi_i' = \pi_i$.

5.2.5 Sensor node impersonation attack

In the proposed protocol, only a sensor node, which is implanted in the body of the patient P_j, could compute the common session key $SK = h_1(t_3 \oplus \phi_i \oplus b)$, which is used for encryption of data D_j as $E_{ji} = D_j \oplus SK_{ij}$. An adversary $\mathcal{A}$ can compute the same session key since the values $(\phi_i$, $b)$ are not known to him/her. Thus, U_i can authenticate P_j by generating the same common session key *SK*.

5.2.6 Stolen smart-card attack

In this attack, an adversary $\mathcal{A}$ somehow get the U_i's smart-card and using the information stored on it, he/she tries to obtain other secret information to be used to create a valid login message. $\mathcal{A}$ could obtain the parameter $\langle m, n, q, \mathbf{X}, \mathbf{Q_i}, h_1(\cdot), h_2(\cdot), b, \gamma_i, \delta_i, \xi_i \rangle$ stored on it. Now, $\mathcal{A}$ wishes to successfully login to *MS*. However, he/she could not guess ID_i and Pw_i, thus the values $a_i' = h_1(ID_i||Pw_i \oplus \delta_i$, $\beta_i' = \gamma_i \oplus h_1(ID_i||Pw_i||a_i')$ and $\xi_i' = h_1(a_i'||h_1(ID_i||Pw_i)||\beta_i')$ are unknown. Hence, the verification $\xi_i' = \xi_i$ fails. Moreover, guessing the parameters ID_i and Pw_i of U_i is hard due to the collision resistance property of hash functions. Hence, the stolen smart-card attack is prevented in the proposed PDAC-CoV protocol.

5.2.7 Off-line password guessing attack

In this attack, an adversary $\mathcal{A}$ tries to guess the password of U_i from the known parameter (stolen smart-card or login and verification messages). In our PDAC-CoV protocol, the password Pw_i is always combined with ID_i to calculate any private message. Thus, only knowing the Pw_i, $\mathcal{A}$ can not compute a private message. Thus, the proposed PDAC-CoV protocol provides robustness against the off-line password guessing attack.

5.2.8 Session key security

When an adversary $\mathcal{A}$ attempts to crack the session key SK transferred between U_i and P_j. $\mathcal{A}$ could perhaps attempt it either by targeting the shared messages during the login phase or by using stored parameter of the smart-card. The session key in our suggested approach is obtained as $SK = h_1(t_3 \oplus \phi_i \oplus b)$, which has ϕ_i and b as confidential parameters and t_3 as a freshness parameter. With the hacked smart-card and public messages, $\mathcal{A}$ is unable to compute the right session key.

5.2.9 Entity privacy

An adversary $\mathcal{A}$ may try to obtain the information for U_i (user's ID_i and Pw_i). In our PDAC-CoV protocol, this type of information is always transferred as encrypted messages or as digest value of a collision resistance hash function. Due to these factors, $\mathcal{A}$ can not get the information about ID_i and Pw_i. Thus, our PDAC-CoV protocol supports privacy.

5.2.10 Password disclosure attack

In this attack, an adversary $\mathcal{A}$ want to guess the password Pw_i of U_i. The password Pw_i is included in the message $\alpha_i = h_1(ID_i||Pw_i||a_i)$, which is sent to MS over any public network. It can be easy for any insider adversary to get α_i and ID_i, but extraction of Pw_i from these values is difficult because α_i depends on a secret value a_i. Further, in the next subsequent phase of PDAC-CoV protocol, neither transferred message nor smart-card includes the password Pw_i of U_i. Thus, the proposed PDAC-CoV protocol is immune to the password disclosure attack.

6 Performance evaluation

In this section, the performance of proposed PDAC-CoV protocol is measured in terms of computational, communication, storage and energy cost. In addition, a comparative analysis with similar competing works has been also included to show the betterment of the proposed PDAC-CoV protocol. For our computation, we have taken the values as $n = O(k \log q)$ where $q = O(k^2)$. These taken value for PDAC-CoV protocol insures its security. Moreover, we have chosen $n = k \log q$ and $q = k^2$ in our analysis to keep it simple and lower cost operations like hash functions are ignored during comparison.

- **Computation cost:** The computation cost of different operations used in the proposed work for a particular user is computed. In the computation of $\mathbf{P_i} = \mathbf{X^T} \cdot \mathbf{r_i}$, the order of execution is $O(n^2 \cdot |q^2|) = O(k^2 \log^4 k)$ for $|q| = \log q$. The $|q^2|$ denotes the multiplication cost of two numbers in $\mathbb{Z}_q^*$. Similarly, $\mathbf{Q_i} = \mathbf{P_i} \cdot \mathbf{d^T}$ and $\mathbf{S_i} = \mathbf{Q_i^T} \cdot \mathbf{u_i}$ has a order of execution as $O(n \cdot |q^2|) = O(k \log^3 k)$ and $O(n^2 \cdot |q^2|) = O(k^2 \log^4 k)$ respectively. Thus, if $n = k \log q$ with $q = k^2$, the total computation cost incurred during the execution of our PDAC-CoV protocol is $2n^2 \cdot |q^2| + n \cdot |q^2|$.
- **Communication and storage costs:** The transmission overhead of our PDAC-CoV protocol is evaluated with the consideration that the overhead of timestamps are negligible. In our PDAC-CoV protocol, the sent messages include $\langle \mathbf{u_i}, \varphi_i \rangle$, $\langle \boldsymbol{\pi}_i, ID_i \rangle$, M_i, $\langle ID_{i_i}, d_i \rangle$ and E_{ji} which has a total communication cost as $n \cdot |q| + 7|q|$. Next, the storage cost for storing the values $\mathbf{d}$ and $\mathbf{X}$ is $(n^2 + n) \cdot |q|$.

Further, It may be noted that the protocols based on the DH problem uses exponential operations under modulus operation (say q_1). This modulus q_1 depends on a security parameter k_1 where $q_1 \approx 2^{k_1}$. The cost incurred in DH-type protocols is $|q_1^3|$ in $\mathbb{Z}_{q_1}^*$ which is huge in comparison with lattice based operations. Similarly, T_{pt} which is a point addition on an elliptic curve group incurs more cost than matrix operations. The computation, communication and storage overhead of lattice operations used in our PDAC-CoV protocol are $3n^2 \cdot |q^2|$, $n \cdot |q| + 7|q|$ and $(n^2 + n) \cdot |q|$ respectively. Most of the IoMT systems as seen in prior art mainly based on PKC, CRT, IBC, BDH, ECC, BP, and

Table 2 Computation costs of related protocols (based on lattice operations only)

Protocol	Order of execution	Total cost
Chaudhary et al. (2018)	$O(n^2 \cdot \|q^2\| + \log^3 q_1)$	$4n^2 \cdot \|q^2\| + 8 \log^3 q_1 = 48k^2 \log^4 k + 8 \log^3 q_1$
Cao et al. (2019)	$O(n^2 \cdot \|q^2\|)$	$22n^2 \cdot \|q^2\| = 352k^2 \log^4 k$
Mukherjee et al. (2019)	$O(n^2 \cdot \|q^2\|)$	$3n^2 \cdot \|q^2\| + 2n \cdot \|q\| = 48k^2 \log^4 k + 8k \log^2 k$
Kumar et al. (2020)	$O(n^2 \cdot \|q^2\|)$	$6n^2 \cdot \|q^2\| + 2n \cdot \|q\| + 7T_{pt} = 96k^2 \log^4 k + 8k \log^2 k + 7T_{pt}$
PDAC-CoV	$O(n^2 \cdot \|q^2\|)$	$2n^2 \cdot \|q^2\| + m \cdot \|q^2\| = \mathbf{32k^2 \log^4 k + 8k \log^3 k}$

Table 3 Storage and communication comparisons of the competitive protocols

Protocol	Type and Primitive	Length (in bits)
Chaudhary et al. (2018)	Storage: $\langle \mathbf{A}, \mathbf{B}, \mathbf{C} \rangle \in \mathbb{Z}_q^{n \times n}, \langle \mathbf{k}, \mathbf{l}, \mathbf{m}, \mathbf{n} \rangle \in \mathbb{Z}_q^n, g \in \mathbb{Z}_{q_1}^*$	$(3n^2 + 4n) \cdot \lvert q \rvert + \lvert q_1 \rvert \approx 24k^2 \log^3 k + 16k \log^2 k + \log q_1$
	Communication: $e, \langle k_1, k_2 \rangle, m, \langle R, S, ID \rangle, \langle T, U, ID, v \rangle$	$(n^2 + 3n + 1) \cdot \lvert q \rvert + 4\lvert q_1 \rvert \approx 8k^2 \log^3 k + 12k \log^2 k + 2 \log k + 4 \log q_1$
Cao et al. (2019)	Storage: $\langle \mathbf{A}, \mathbf{B} \rangle \in \mathbb{Z}_q^{n \times n}, \langle \mathbf{d}, \mathbf{e}, \mathbf{p}, \mathbf{s}, \mathbf{u}, \mathbf{v} \rangle \in \mathbb{Z}_q^n$	$(2n^2 + 6n) \cdot \lvert q \rvert \approx 16k^2 \log^3 k + 24k \log^2 k$
	Communication: $\langle 3m, 3\sigma \rangle$	$(9n + 3) \cdot \lvert q \rvert \approx 36k \log^2 k + 6 \log k$
Mukherjee et al. (2019)	Storage: $\mathbf{d} \in \mathbb{Z}_q^n, \mathbf{A} \in \mathbb{Z}_q^{n \times n}$	$(n^2 + n) \cdot \lvert q \rvert \approx 8k^2 \log^3 k + 4k \log^2 k$
	Communication: $\langle m, Ans, \mathbf{R}, \mathbf{S} \rangle$	$(3n + 2) \cdot \lvert q \rvert \approx 12k \log^2 k + 4 \log k$
Kumar et al. (2020)	Storage: $\langle \mathbf{R_q}, \mathcal{N}_{\mathbf{ag}} \rangle \in \mathbb{Z}_q^{n \times n}, \langle \mathbf{s}, \mathbf{e_1}, \mathbf{e_2} \rangle \in \mathbb{Z}_q^n, G, K_{opagg-} \in \mathbb{F}_{q_1}$	$(2n^2 + 3n) \cdot \lvert q \rvert + 2\lvert q_1 \rvert \approx 16k^2 \log^3 k + 12k \log^2 k + 2 \log q_1$
	Communication: $\langle \mathbf{R}, s, c \rangle$	$(n^2 + 2) \cdot \lvert q \rvert \approx 8k^2 \log^3 k + 4 \log k$
PDCA-CoV	Storage: $\mathbf{d} \in \mathbb{Z}_q^n, \mathbf{X} \in \mathbb{Z}_q^{n \times n}$	$(n^2 + n) \cdot \lvert q \rvert \approx \mathbf{8k^2} \log^3 \mathbf{k} + \mathbf{4k} \log^2 \mathbf{k}$
	Communication: $\langle \mathbf{u_i}, \varphi_i \rangle, \langle \boldsymbol{\pi}_i, ID_i \rangle, M_i, \langle ID_i, d_i \rangle, E_{ji}$	$(n + 7) \cdot \lvert q \rvert \approx \mathbf{4k} \log^2 \mathbf{k} + \mathbf{14} \log \mathbf{k}$

others. These schemes will be exposed to future quantum computing technologies and thus, can not resist quantum attack. Hence, We consider related quantum-secured protocols to estimate the security level and performance efficiency of the proposed protocol. In line, the similar computation has been done with competing lattice-based state-of-the-arts (Kumar et al. 2020; Cao et al. 2019; Chaudhary et al. 2018; Mukherjee et al. 2019) which are also used for the data protection and authentication in IoMT and resists the quantum attack. Tables 2 and 3 show detailed comparisons with existing schemes, and based on the analyses, it is noticed that the PDAC-CoV outperforms other quantum-secured protocols (Kumar et al. 2020; Cao et al. 2019; Chaudhary et al. 2018; Mukherjee et al. 2019) in IoMT communication.

7 Concluding remarks

Given the recent emergence and widespread use of IoMT, notably during COVID-19 pandemics, it seems more logical to develop a secure IoMT-based system to protect the confidentiality of vital and sensitive patient data. The vast majority of existing IoMT security mechanisms have been found to be vulnerable to a variety of attacks, including quantum attacks. This article proposes a lattice-based data authentication and access control protocol for IoMT systems in this regard. The proposed protocol employs lattice as a mechanism to withstand a future quantum attack. For its lightweight nature, the scheme is appropriate for resource-constrained IoMT environments. The protocol has proven to be resilient to the majority of traditional security attacks, as well as future quantum attacks. The proposed scheme can be used in resource-constrained quantum environments due to its efficiency and ease of implementation. The proposed protocol has been subjected to verifiable security analysis. Furthermore, the performance evaluation demonstrates that the proposed approach is suitable for implementation in an IoT device. In the future, researchers may investigate the mobility characteristics of IoMT devices to evaluate how they affect patient data confidentiality, especially in terms of ensuring continuous connectivity across multiple IoT platforms.

References

Aghili SF, Mala H, Shojafar M, Peris-Lopez P (2019) LACO: Lightweight three-factor authentication, access control and ownership transfer scheme for e-health systems in IoT. Futur Gener Comput Syst 96:410–424

Ajtai M (1996) Generating hard instances of lattice problems. In: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, ACM, pp. 99–108

Alabdulatif A, Khalil I, Forkan ARM, Atiquzzaman M (2018) Real-time secure health surveillance for smarter health communities. IEEE Commun Mag 57(1):122–129

Alassaf N, Gutub A (2019) Simulating light-weight-cryptography implementation for iot healthcare data security applications. Int J E-Health Med Commun (IJEHMC) 10(4):1–15

Alassaf N, Alkazemi N, Gutub A (2003) Applicable light-weight cryptography to secure medical data in iot systems, Arabia

Al-Turjman F, Deebak B (2020) Privacy-aware energy-efficient framework using the internet of medical things for covid-19. IEEE Internet Things Mag 3(3):64–68

Aman AHM, Hassan WH, Sameen S, Attarbashi ZS, Alizadeh M, Latiff LA (202) IoMT amid COVID-19 pandemic: Application, architecture, technology, and security. J Netw Comput Appl

Amin R, Islam SH, Biswas GP, Khan MK, Li X (2015) Cryptanalysis and enhancement of anonymity preserving remote user mutual authentication and session key agreement scheme for e-health care systems. J Med Syst 39(11):140

Amin R, Islam SH, Biswas GP, Khan MK, Kumar N (2018) A robust and anonymous patient monitoring system using wireless medical sensor networks. Futur Gener Comput Syst 80:483–495

Baranchuk A, Refaat MM, Patton PP, Chung MK, Krishnan K, Kutyifa V, Upadhyay G, Fisher JD, Lakkireddy DR, Cardiology AC et al (2018) Cybersecurity for cardiac implantable electronic devices: what should you know? J Am Coll Cardiol 71(11):1284–1288

Cao J, Yu P, Xiang X, Ma M, Li H (2019) Anti-quantum fast authentication and data transmission scheme for massive devices in 5G NB-IoT system. IEEE Internet Things J 6(6):9794–9805

Chaudhary R, Jindal A, Aujla GS, Kumar N, Das AK, Saxena N (2018) Lscsh: Lattice-based secure cryptosystem for smart healthcare in smart cities environment. IEEE Commun Mag 56(4):24–32

Das AK, Goswami A (2013) A secure and efficient uniqueness-and-anonymity-preserving remote user authentication scheme for connected health care. J Med Syst 37(3):9948

Firouzi F, Farahani B, Ibrahim M, Chakrabarty K (2018) Keynote paper: From EDA to IoT ehealth: Promises, challenges, and solutions. IEEE Trans Comput Aided Des Integr Circuits Syst 37(12):2965–2978

Gentry C, Peikert C, Vaikuntanathan V (2008) Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the fortieth annual ACM symposium on Theory of computing, pp. 197–206

Gupta DS, Islam SH, Obaidat MS, Karati A, Sadoun B (2020) Laac: Lightweight lattice-based authentication and access control protocol for e-health systems in IoT environments. IEEE Syst J

Gupta DS, Karati A, Saad W, Da Costa DB (2022) Quantum-defended blockchain-assisted data authentication protocol for internet of vehicles. IEEE Trans Veh Technol

Gupta DS, Biswas G (2017) An ecc-based authenticated group key exchange protocol in ibe framework. Int J Commun Syst 30(18):e3363

Gupta DS, Biswas G (2017) On securing bi-and tri-partite session key agreement protocol using ibe framework. Wireless Pers Commun 96(3):4505–4524

Gupta DS, Biswas G (2018) Design of lattice-based elgamal encryption and signature schemes using sis problem. Trans Emerg Telecommun Technol 29(6):e3255

Gupta DS, Biswas G (2018) A novel and efficient lattice-based authenticated key exchange protocol in c-k model. Int J Commun Syst 31(3):e3473

Gupta DS, Islam SH, Obaidat MS, Vijayakumar P, Kumar N, Park Y (2020) A provably secure and lightweight identity-based two-party authenticated key agreement protocol for iiot environments. IEEE Syst J 15(2):1732–1741

Gupta DS, Ray S, Singh T, Kumari M (2022) Post-quantum lightweight identity-based two-party authenticated key exchange protocol for internet of vehicles with probable security. Comput Commun 181:69–79

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. Multimed Syst 21(1):49–60

Jan MA, Khan F, Mastorakis S, Adil M, Akbar A, Stergiou N (2021) LightIoT: Lightweight and secure communication for energy-efficient IoT in health informatics. IEEE Trans Green Commun Netw

Kim J (2015) Energy-efficient dynamic packet downloading for medical IoT platforms. IEEE Trans Industr Inf 11(6):1653–1659

Kumar P, Lee S-G, Lee H-J (2012) E-SAP: efficient-strong authentication protocol for healthcare applications using wireless medical sensor networks. Sensors 12(2):1625–1647

Kumar G, Saha R, Rai MK, Buchanan WJ, Thomas R, Geetha G, Hoon-Kim T, Rodrigues JJ (2020) A privacy-preserving secure framework for electric vehicles in IoT using matching market and signcryption. IEEE Trans Veh Technol 69(7):7707–7722

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

Li C-T, Wu T-Y, Chen C-L, Lee C-C, Chen C-M (2017) An efficient user authentication and user anonymity scheme with provably security for IoT-based medical care system. Sensors 17(7):1482

Lin X, Lu R, Shen X, Nemoto Y, Kato N (2009) SAGE: a strong privacy-preserving scheme against global eavesdropping for ehealth systems. IEEE J Sel Areas Commun 27(4):365–378

Liu C-H, Chung Y-F (2017) Secure user authentication scheme for wireless healthcare sensor networks. Comput Electr Eng 59:250–261

Masud M, Gaba GS, Alqahtani S, Muhammad G, Gupta B, Kumar P, Ghoneim A (2020) A lightweight and robust secure key establishment protocol for internet of medical things in covid-19 patients care. IEEE Internet Things J

Micciancio D, Regev O (2007) Worst-case to average-case reductions based on gaussian measures. SIAM J Comput 37(1):267–302

Mukherjee S, Gupta DS, Biswas GP (2019) An efficient and batch verifiable conditional privacy-preserving authentication scheme for vanets using lattice. Computing 101(12):1763–1788

Sahu AK, Sharma S, Puthal D (2021) Lightweight multi-party authentication and key-agreement protocol in iot based e-healthcare service. ACM Trans Multimed Comput Commun Appl (TOMM)

Samkari H, Gutub A (2019) Protecting medical records against cybercrimes within hajj period by 3-layer security. Recent Trends Inf Technol Appl 2(3):1–21

Shambour M, Gutub A (2021) Personal privacy evaluation of smart devices applications serving hajj and umrah rituals. J Eng Res

Shor PW (1999) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev 41(2):303–332

Yaacoub J-PA, Noura M, Noura HN, Salman O, Yaacoub E, Couturier R, Chehab A (2020) Securing internet of medical things systems: limitations, issues and recommendations. Futur Gener Comput Syst 105:581–606

Yaqoob T, Abbas H, Atiquzzaman M (2019) Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices-a review. IEEE Commun Surv Tutor 21(4):3723–3768