Arabian Journal for Science and Engineering
https://doi.org/10.1007/s13369-022-07235-0

RESEARCH ARTICLE-COMPUTER ENGINEERING AND COMPUTER SCIENCE

Lightweight Two-Factor-Based User Authentication Protocol for IoT-Enabled Healthcare Ecosystem in Quantum Computing

Alawi A. Al-saggaf[1] · Tarek Sheltami[2] · Hoda Alkhzaimi[3] · Gamil Ahmed[2]

Received: 27 October 2021 / Accepted: 17 January 2022

Abstract
The healthcare ecosystem is migrating from legacy systems to the Internet of Things (IoT), resulting in a digital environment. This transformation has increased importance on demanding both secure and usable user authentication methods. Recently, a post-quantum fuzzy commitment scheme (PQFC) has been constructed as a reliable and efficient method of biometric template protection. This paper presents a new two-factor-based user authentication protocol for the IoT-enabled healthcare ecosystem in post-quantum computing environments using the PQFC scheme. The proposed protocol is proved to be secure using random oracle model. Furthermore, the functionality and security of the proposed protocol are analyzed, showing that memoryless-effortless, user anonymity, mutual authentication, and resistance to biometric templates tampering and stolen attacks, stolen smart card attack, privileged interior attack are fulfilled. The costs of storage requirement, computation, communication and storage are estimated. The results demonstrate that the proposed protocol is more efficient than Mukherjee et al., Chaudhary et al., and Gupta et al. protocols.

Keywords Internet of Things · IoT-enabled healthcare · Post-quantum cryptography · User authentication · Biometric · Lightweight authentication protocols

1 Introduction

The healthcare ecosystem is undergoing modernization is known as a digital transformation. The Internet of Things (IoT) offers many benefits for the healthcare sector. The IoT-enabled healthcare makes healthcare practical for an aging population, chronic diseases, automate patient care, health records assortment and analysis. The IoT-enabled healthcare provided a better environment for both physician and patient during the outbreak of COVID-19. The IoT-enabled healthcare ecosystem refers to the interconnection of smart devices and applications via the Internet. The IoT-enabled healthcare ecosystem enables the collection, monitoring, and analyzing patients' condition measurements, remotely [1, 2]. Figure 1 illustrates a typical IoT-enabled healthcare ecosystem, where a remote user (for instance, physicians and patient family) collect and monitor the patient's biomedical conditions for further processing. The wearable or implantable IoT medical devices are deployed in the patient's body, which is measures and collects the patient biomedical conditions. These biomedical conditions transfer to a smartphone connected to the IoT medical devices via an app. Then, the smartphone sends the biomedical conditions to the healthcare server for further analysis and decision.

Unlike the social and fiscal identities, the heath records such as genetic, conditions, or biometrics data cannot be revoked once it is compromised. The most significant threats that IoT-enabled healthcare poses are data security and privacy. Cybercriminals can misuse the patient's health records to claim in the patient's name, for instance, create fake IDs to buy drugs and medical equipment or file fraudulent Insurance. The IoT-enabled healthcare security is mainly for secure health records, communication, and user authentication. User authentication is a keystone in IoT-enabled healthcare security, which plays a crucial role in establishing

✉ Alawi A. Al-saggaf
alawi@kfupm.edu.sa

[1] Mathematical Sciences Department/DCC, Interdisciplinary Research Center of Intelligent Secure Systems Center, KFUPM, Dhahran 31261, Kingdom of Saudi Arabia

[2] Computer Engineering Department, Interdisciplinary Research Center of Smart Mobility and Logistics, KFUPM, Dhahran 31261, Kingdom of Saudi Arabia

[3] Center of Cyber Security and Interdisciplinary Studies, New York University Abu Dhabi, Abu Dhabi, UAE

Published online: 22 September 2022

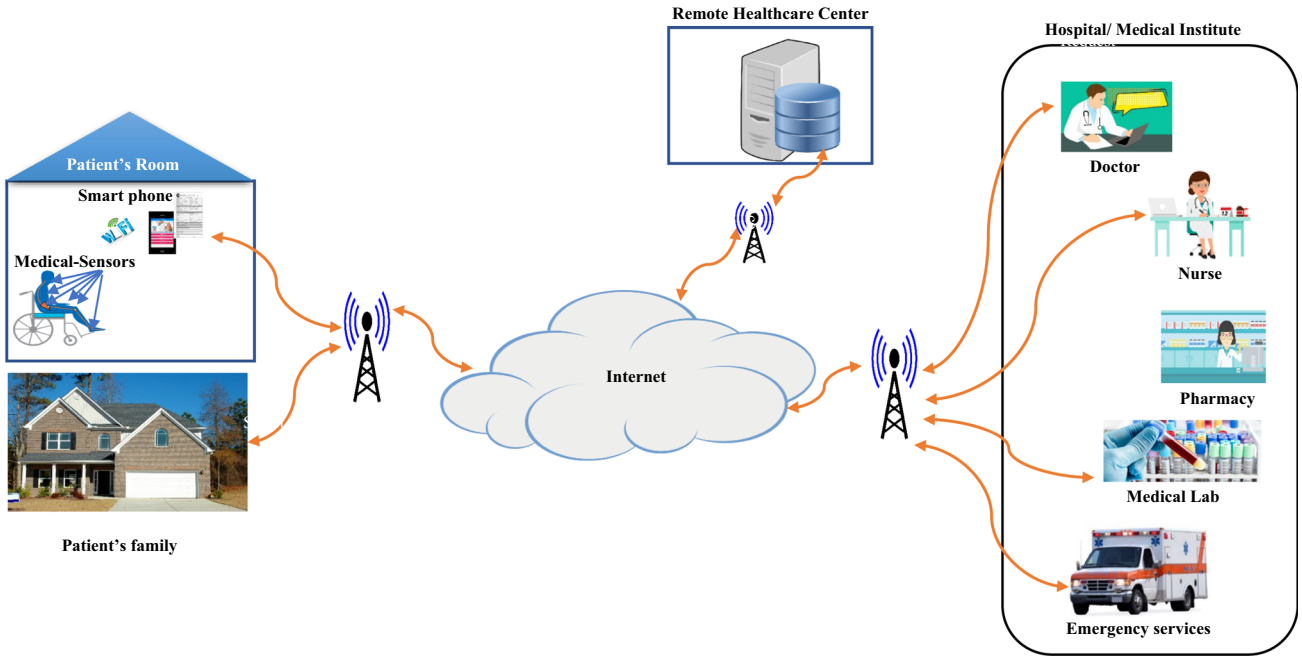

Fig. 1 A typical IoT-enabled healthcare ecosystem architecture

trust between IoT healthcare users and devices and preventing attacks [3].

Nowadays, knowledge-based authentication such as passwords and PINs plays a central role in IoT-based healthcare. With the exponential increase in using online services based on the traditional authentication method such as passwords, passwords become not only frustrating for users but also costly to maintain. According to the 2020 Verizon Data Breach Investigation Report, more than 80% of data breaches due to passwords phishing and authentication systems' security vulnerabilities [4]. Additionally, users will hold an increasing number of accounts with the average user memorizing 191 passwords, according to the LastPass report 2016.

Due to its advantages over traditional authentication methods, biometrics considered is a promising authentication method in the IoT era [5]. However, there are serious concerns about the security and privacy of the stored biometric template [6]. In the last decade, many researchers combined techniques from the areas of cryptography and error-correcting codes to secure the stored biometric template known as biometric template protection schemes [7–10]. However, error-correcting code is essential in the design of the traditional biometric template protection schemes, which degrade the security and performance of these schemes [11–13].

Currently, IoT systems rely on conventional cryptography algorithms based on integer factorization and discrete logarithm, for instance, Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC). However, conventional cryptographic algorithms are no longer secure by upcoming quantum computing [14]. Furthermore, these conventional cryptographic algorithms are inadequate for IoT devices because of their complex computation requirements [2]. Therefore, post-quantum cryptography primitives are a promising technique for securing communications between IoT users and devices. Due to its predominant features, such as resistance to quantum attacks, performance efficiency, work in classical computing, lattice-based cryptography becomes ahead in the post-quantum techniques [15].

Recently, a post-quantum fuzzy commitment scheme (PQFC) [16] has been ensuring both security and accuracy efficiencies for biometric template protection. To tackle issues with IoT-enabled healthcare ecosystems, we propose a new lightweight two-factor user authentication protocol for the IoT-enabled healthcare ecosystem based on the security of PQFC scheme. The proposed protocol using biometrics and smartcard for authentication. The following are the main findings of the work:

1. A new lightweight two-factor user authentication protocol for the IoT-enabled healthcare ecosystem using a post-quantum fuzzy commitment scheme.
2. Formal theoretical analysis shows that the proposed protocol is secure against upcoming quantum threats using random oracle models.
3. Our protocol is quantum-safe protocol.
4. The biometric template safeguarded the biometric matching performed indirectly
5. Our protocol is a memoryless-based user authentication protocol.

6. Our protocol achieves important security and privacy properties, such as resistance to tampering and stolen of stored biometric template, stolen smart card, and privileged interior attacks.
7. Our protocol provides good functionality features, such as memoryless-effortless, user anonymity, mutual authentication, renewable biometric, and lightweight protocol.
8. The computational, communication, and storage costs of the proposed scheme are evaluated and compared with existing related protocols.
9. The security and performance analysis shows that the proposed protocol is suitable for application in an IoT-enabled healthcare environment in comparison with the other existing competitive protocols.

The rest of the paper is organized as follows: Sects. 2 and 3 contain related work and preliminaries, respectively. The biometric-based PQFC authentication system is described in Sect. 4. The presented lightweight two-factor authentication protocol for IoT-enabled healthcare and corresponding formal security analysis is presented in Sects. 5 and 6, respectively. Section 7 discusses the security and functionality analysis of the proposed protocol. The performance evaluation is done in Sect. 8. Section 9 presents the conclusions.

2 Related Work

Recently, many authentication protocols for secure communication between IoT users and devices in IoT environments have been proposed. Some of them use traditional public-key cryptography like Rivest–Shamir–Adleman (RSA) and elliptic curve cryptography (ECC). [17–19]. However, these protocols are inadequate for IoT devices because of their complex computation operations. Furthermore, these approaches are no longer secure by upcoming quantum computing [14]. There are also less efficient and secure authentication protocols [20–23], which are based on traditional biometric template protection. However, error-correcting code is essential in the design of these traditional biometric template protection schemes, which cause a downgrade of the security and performance of the system.

Lattice-based cryptography techniques attracted many researchers to secure applications in IoT environments due to their security and functionality efficiencies [15]. Of late, several authentication protocols for IoT sectors have been proposed in the literature. Nan et al. [24] proposed a lattice-based public-key encryption based on Needham and Schroeder scheme [25] and then used to construct a lightweight authentication protocol for smart city environment. They claimed their protocol is secure against different attacks using informal security analysis. The protocol was implemented in Contiki platform and evaluated using Cooja-based emulation environment and Texas Instruments CC2538 hardware platform. Cao et al. [26] presented an access authentication and data distribution scheme for the 5G narrowband Internet of Things systems. The security of their protocol is based on the lattice-based homomorphic encryption. To demonstrate the security of their protocol, they used BAN logic and Scyther tools. Zhou and Wang proposed an anonymous NTRU-based authentication scheme for mobile users in roaming service in ubiquitous networks [27]. Mukherjee et al. designed a lattice-based conditional privacy-preserving authentication protocol for vehicular ad hoc networks [28]. They showed that their protocol ensures the message integrity, authentication and privacy preservation using ROM model.

Chaudhary et al. [29] proposed a lattice-based cryptosystem for smart healthcare in future smart cities. Then, they combined their cryptosystem with bilinear Diffie–Hellman to construct an authentication protocol for healthcare. However, the protocol is not lightweight because of using exponential operations and hence it's not suitable for IoT applications. Sahu et al. [30] presented a lightweight multi-party authentication and key-establishment protocol in IoT-based e-Healthcare service access net-work using lattice identity-based encryption. They tested the security of their protocol using Scyther tool. Gupta et al. [31] presented a lattice-based authentication and access control protocol for IoT-based healthcare. The security assumption of their based on the hardness of the LWE problem. They measured the protocol's performance in terms of storage requirement and computational and communication costs and then compared with the existing related protocols.

All the aforementioned authentication protocols for IoT environments are relying solely on the password, which is falling apart if the password is not kept secure. However, passwords can be easily shared, stolen, forgotten, or phishing. Therefore, the rapid development of emerging technologies such as IoT, cloud computing, blockchain, quantum computing, and e-services makes the current research on user authentication protocols based on post-quantum cryptography urgent.

Recently, a post-quantum fuzzy commitment scheme (PQFC) [16] guaranteeing the security and accuracy efficiencies for biometrics template protection. The author provides a theoretical and experimental analysis of PQFC scheme, showing that the PQFC scheme is a promising technique to provide secure and usable method for users in IoT-Enabled healthcare ecosystems.

3 Preliminaries

This section provides a mathematical preliminary which are essential for describing and analysis the proposed protocol.

3.1 Statistical Distance

Let D_1 and D_2 be two probability distributions over a common measurable sample space Ω. Suppose further, the non-negative function $\varepsilon = \varepsilon(k)$ is negligible if, for all polynomials $p(k)$ we have that $\varepsilon(k) < p(k)^{-1}$ for sufficiently large k. The statistical distance SD between D_1 and D_2 is given by:

$$SD(D_1, D_2) = \sum_{x \in \Omega} |\Pr[D_1] - \Pr[D_2]| = \varepsilon \tag{1}$$

3.2 Collision Resistance Hash Function

A function $h : \{0, 1\}^* \rightarrow \{0, 1\}^k$ is called a collision resistant hash function [32] if the following properties hold: (1) compression: h maps an input x of arbitrary finite bit length to an output $h(x)$ of fixed bit length k. (2) easy to compute: Given h and an input as x, $h(x)$ is easy to compute, (3) pre-image resistance: For all specified output y, it is computationally infeasible to find any input x' such that $h(x') = y$, (4) collision resistant: it is computationally infeasible to find any two distinct inputs x, and x' have the same hash valued, i.e., $h(x) = h(x')$.

3.3 Lattice

Definition 1 A basis is defined as a set of linearly independent vectors $\mathrm{B} = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots.., \boldsymbol{b}_n\}$ of Euclidian vector space $\mathbb{R}^n$ that spans the full space.

Definition 2 A lattice $\mathcal{L}$ is a discrete additive subgroup of $\mathbb{R}^n$ whose elements generated by the integer linear combinations of the basis $\mathrm{B} = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots.., \boldsymbol{b}_n\}$.

$$\mathcal{L}(\mathrm{B}) := \left\{ \boldsymbol{v}_i = \sum_{i=1}^{n} z_i \boldsymbol{b}_i : \quad z_i \in \mathbb{Z} \right\} \tag{2}$$

3.4 lattice Computational Complexities

We now give definitions of well-known lattice computational problems used to construct lattice-based cryptography primitives.

LP1: Shortest Vector Problem (SVP): the shortest vector problem has three variants [33]:
P1) Find the length of the shortest nonzero vector in the lattice $\mathcal{L}(\mathrm{B})$.
P2) Find the shortest nonzero vector $\boldsymbol{v} \in \mathcal{L}(\mathrm{B})$ such that $\|\boldsymbol{v}\| \in \lambda(\mathcal{L})$.
P3) Find the basis $\mathrm{B} = \{\boldsymbol{b}_1, \boldsymbol{b}_2, \ldots.., \boldsymbol{b}_n\}$ in $\mathcal{L}$ in which $\max_i \|\boldsymbol{b}_i\|$ is the smallest possible up to a polynomial factor.

LP2: Approximation Shortest Vector Problem (SVP_γ) Given a basis B of the lattice of n- dimensional lattice $\mathcal{L} = \mathcal{L}(\mathrm{B})$, find a nonzero vector $\boldsymbol{v} \in \mathcal{L}$ such that $\|\boldsymbol{v}\| = \gamma(n).\lambda(\mathcal{L})$, for approximation factor $\gamma \geq 1$ taken as a polynomial of n [34].
LP3: Closet Vector Problem (CVP) [35]: Given a basis B of the lattice of n- dimensional lattice $\mathcal{L} = \mathcal{L}(\mathrm{B})$ and a vector u (not necessarily in the lattice), find a nonzero vector $\boldsymbol{v} \in \mathcal{L}$ that close to u.
LP4: Short Integer Solution (SIS) [36]: Given a matrix $\mathrm{A} \in \mathbb{Z}_q^{m \times n}$ whose columns are uniformly random vector in $\mathbb{Z}_q^n$, find a nonzero vector $\boldsymbol{w} \in \Lambda_q^{\perp}(\mathrm{A})$.
LP5: Decisional Approximate SVP $\left(\mathrm{G_{AP}SVP}_\gamma\right)$: Given a basis B of an n- dimensional lattice $\mathcal{L} = \mathcal{L}(\mathrm{B})$ and a number d. In YES instance $\lambda(\mathcal{L}) \leq d$ or No instance $\lambda(\mathcal{L}) > \gamma(n).d$.
LP6: Shortest Independent Vectors Problem $\left(\mathrm{SIVP}_\gamma\right)$ [36]: Given a basis B of an n- dimensional lattice $\mathcal{L} = \mathcal{L}(\mathrm{B})$. The goal is to output a set of n linearly independent lattice vectors of length at most $\gamma(n).\lambda(\mathcal{L})$.
LP7: Learn with Error (LWE) problem: We briefly describe the Learn with Error (LWE) that used to construct an efficient lattice-based cryptography. Regev [36] introduced a reduction from worst-case lattice problems such as GAPSVP and SIVP to a learning with error problems. The author proved that the solution to the LWE problem implies that there is a quantum algorithm to GAPSVP and SIVP.

LWE distribution: For some integer $k \geq 1$, let m, $n =$ poly(k), and q (prime) are positive integers and let $\mathcal{X}$ be a distribution on $\mathbb{Z}_q$. The LWE distribution $\mathcal{A}_{s,b_i} \subseteq \mathbb{Z}_q^n \times \mathbb{Z}_q$ is sampled using the vector $s \in \mathbb{Z}_q^n$ called secret and the matrix $\mathrm{A} \in \mathbb{Z}_q^{m \times n}$ whose columns are vectors uniformly chosen random, $\boldsymbol{a_i} \xleftarrow{R} \mathcal{U}\left(\mathbb{Z}_q^n\right)$, for $i = 1,2,\ldots,k$, choosing $\mathrm{e} \in \mathbb{Z}_q^n$ and the output is: $b_i = \langle \boldsymbol{a_i}, \mathbf{s} \rangle + e_i \in \mathbb{Z}_q$ for all $i = 1,2,\ldots,n$.

4 The Biometric-Based PQFC Authentication System

In this section, we briefly describe the biometric-based PQFC authentication system [16], which is relies on the worst-case hardness shortest vector problem (SVP) of lattice cryptography. Let us now describe the construction of the biometric-based PQFC authentication system which consists of two main stages: enrollment and verification. The process of the system is described below:

4.1 Setup Stage

Positive integers m, n, and p (prime number) are chosen randomly. Then, generate the matrix $\mathrm{A} \in \mathbb{Z}_q^{m \times n}$ whose columns are vectors in the lattice $\mathcal{L}(\mathrm{B})$.

4.2 Enrollment Stage

First, the user chooses a vector randomly $v \in Z_p^n$ and generates a biometric reference template $x_r \in Z_2^m$ using a specific software. The vector v and the template x_r are input to the PQFC function to generate the biometric reference commitment β_r:

$$\beta_r = F(v, u) = \mathrm{A} \times_q v +_{q,2} u_r, \tag{3}$$

where $\times_q$ applies matrix multiplication modulo q and $+_{q,2}$ applies vector addition modulo q and the result goes through modulo 2.

4.3 Verification stage

The user generates his/her biometric query template $x_q \in Z_2^m$ and then computes the biometric query commitment β_q as follows:

$$\beta_q = F(v, u) = \mathrm{A} \times_q v +_{q,2} x_q \tag{4}$$

The biometric query commitment β_q is matched against the stored β_r using, e.g., Hamming distance. If the matching score is within the system threshold, then the user is authenticated.

5 Lightweight Two-Factor User Authentication protocol for the IoT-Enabled Healthcare

The proposed protocol comprises four phases, namely the registration phase, the login phase, the authentication phase, and the biometric renewable phase. The protocol consists of three entities, namely (1) a user U_i, which is for instance physician, nurse, pharmacologist, or patient's family member, (2) a medical server *MS*, and (3) a patient P_j. The U_i must register and authenticate herself/himself with the medical server MS to access the patient's medical data. It is worth noting that the patient's medical data are collected and measured using smart devices implanted with the body of the patient. Then, these medical data transfer to the medical server MS. Details of the steps of these phases are described below.

5.1 Setup Phase

The main purpose of this phase is to generate the public parameter $\triangle$.; that is, *MS* takes a unary 1^k as input and executes the following steps:

S1: *MS* chooses a prime number p and two positive integers m and n.
S2: *MS* generates randomly a matrix $\mathrm{A} \in Z_p^{m \times n}$, which consists of $n-$ linearly independent vector of the lattice Λ_p And then chooses a cryptographic hash function $h : \{0, 1\}^* \rightarrow \{0, 1\}^k$.
S3: *MS* chooses randomly a master key vector $mk \in Z_p^{1 \times n}$ and computes public key $pk = \mathrm{A}.mk^T (\mathrm{mod}\ p) \in Z_p^{1 \times m}$.
S4: *MS* publishes the public parameters of the system $\triangle = \{m, n, p, \mathrm{A}, pk, h(\cdot)\}$ and keeping mk as a secret.

5.2 Registration Phase

When the user U_i needs to register with the medical server *MS*, she/he performs the following steps:

R1:U_i selects her/his unique identity D_i.
R2:U_i uses specific software to generate cryptographic key $k_i \in Z_2^l$ and generates a random number N, then computes $c_i = h(k_i||N)$.
R3:U_i presents her/his personal biometric data B_i on biometric reader and the biometric reference template $x_r \in Z_2^t$ extracted such that $m = t + l$. Then, U_i chooses randomly $v_i \in Z_p^n$ and computes the following:

$$\beta_r = \mathrm{A} \times_q v_i +_{q,2} (x_r||k_i), \tag{5}$$

$$r_i = h(c_i||\beta_i), \tag{6}$$

$$w_i = \mathrm{A} \times_q v_i, \tag{7}$$

$$Z_i = w_i \times_q pk^T, \tag{8}$$

$$\delta_i = h(w_i) \oplus h(ID_i||r_i) \tag{9}$$

R4: U_i sends the registration message $\{ID_i, r_i, Z_i, \delta_i\}$ to the medical server *MS*.
R5: *MS* computes $e_i = h(ID_i||mk) \oplus r_i$ and loads $\{r_i, Z_i, \delta_i, e_i, s\}$ on $U_i's$ smart card, then sends the smart card to the user U_i.
R6: Upon receiving the smart card, the user stores the random number N and β_r in her/his smart card.

5.3 Login Phase

Whenever the user U_i wants to access the health profile of the patient P_j, she/he must log in to the medical serer *MS* by performing the following steps:

L1: U_i inserts her/his smart card into the card reader and keys her/his identity ID_i.
L2: The smart card sends the login message request $\{Z_i, \delta_i, r_i\}$ to the medical server *MS*.
L3: Upon receiving the login request, the medical server *MS* computes $w'_i = (Z_i \cdot \mathrm{A}) \cdot mk^T \pmod p$ and sends w'_i to the user U_i via a public channel.
L4: Upon receiving w'_i, the user U_i presents her/his biometric data B_i on biometric reader and a biometric query template x_q extracted. The smart card calculates $\beta_q = w'_i +_{q,2} (x_q||0)$ and verifies $dist(\beta_q, \beta_r) \leq d_{th}$.
L5: If the above biometrics verification fails, the session will be terminated; otherwise, the smart card extracts $k'_i = \beta_r \oplus \beta_q$ and computes $r'_i = h\big(h(k'_i||N)||\beta_q\big)$, and then the smart card verifies $r_i = r'_i$.
L6: If the above key verification fails, the session will be terminated; otherwise, the smart card continued computing the following: $\theta_1 = e_i \oplus r'_i$, $\theta_2 = \theta_1 \oplus R_u$, $\theta_3 = h(s||R_u)$, $\theta_4 = c_i \oplus \theta_3$, $\theta_5 = h(\theta_2||\theta_3||\theta_4)$, and $\theta_6 = \theta_3 \oplus ID_i$.
L7: The smart card sends the message $\{\theta_1, \theta_2, \theta_4, \theta_5, \theta_6\}$ to the medical server for authentication.

5.4 Authentication Phase

When *MS* received the message $\{\theta_1, \theta_2, \theta_4, \theta_5, \theta_6\}$, the medical server *MS* and the user U_i perform the following steps to authenticate each other.

A1: *MS* computes $\theta_7 = \theta_2 \oplus \theta_1$ and $ID'_i = \theta_6 \oplus h(s||\theta_1 \oplus \theta_2)$.
A2: *MS* checks the format of ID'_i. If ID'_i is valid, *MS* computes and verifies $\theta_5 = h(\theta_2||\theta_8||\theta_4)$, if it does not hold, MS rejects the login request and terminates the session. Otherwise, *MS* accepts the user U_i log in and stores $\{ID_i, \theta_7\}$ in the database system to resist the reply and man-in-the-middle attacks.
A3: *MS* computes $\theta_9 = \theta_4 \oplus \theta_8$, $\theta_{10} = h(\theta_9||ID_s||s) \oplus \theta_8 \oplus R_s$, $\theta_{11} = h(\theta_1||\theta_9||s||R_s)$, then *MS* sends $\{\theta_{10}, \theta_{11}\}$ to the user U_i.
A4: U_i computes $\theta_{12} = h(c_i||ID_s||s) \oplus R_u$ and verifies $\theta_{11} = h(\theta_1||c_s||s||\theta_{12})$. If it does not hold, U_i terminates the session. Otherwise, the medical server *MS* is authenticated by the user U_i. Finally, the user and the medical server computes $h(c_i||\theta_3||\theta_{12}||ID_s) = K_{\text{sess}} = h(\theta_9||\theta_8||R_s||ID_s)$ respectively, which is taken as the session key K_{sess}.

5.5 Biometric Revocation Phase

To re-register her/his same biometric B_i,U_i performs a biometric revocation phase as follows:

V1: U_i inserts her/his smart card, keys identity ID_i, and presents her/his biometrics B_i in the biometric reader, which generates a biometric template x_r^{new} that will be used for a biometric verification approach as described in steps L2–L5 in the login phase. the cryptographic key k'_i is retrieved, and the user will generate a new cryptographic key k_i^{new}.
V2: If this verification fails, the session will be terminated. Otherwise, the smart card computes $e'_i = e_i \oplus r'_i$, $\beta_r^{\text{new}} = \mathrm{A}^T \times_q v_i^{\text{new}} +_{q,2} (x_r^{\text{new}}||k_i^{\text{new}})$, $c_i^{\text{new}} = h(k_i^{\text{new}}||N)$, $r_i^{\text{new}} = h\big(c_i^{\text{new}}||\beta_r^{\text{new}}\big)$, $e_i^{\text{new}} = e_i \oplus r_i^{\text{new}}$, $w_i^{\text{new}} = \mathrm{A}^T \times_q v_i^{\text{new}}$, $Z_i^{\text{new}} = pk \times_q w_i^{\text{new}}$, and $\delta_i^{\text{new}} = h\big(w_i^{\text{new}}\big) \oplus h(ID_i||r_i^{\text{new}})$.
V3: Finally, e_i^{new}, r_i^{new}, β_r^{new}, Z_i^{new}, and δ_i^{new} are stored in U_i smart card.

6 Security Analysis

In this section, a formal security analysis of the proposed protocol is given using the random oracle model (ROM). Theorem 1 shows that the adversary A^Q can breaches the proposed protocol by learn the biometric reference template x_r and the cryptographic key k_i from F_i only with negligible probability. Theorem 2 proves that the adversary A^C is able to breach the proposal protocol if he/she is able to invert the one-way hash function. To this end, we simulate two random oracle model.

6.1 Quantum Random Oracle Model

This model specifies as a game that a probabilistic polynomial-time algorithm (possibly quantum) A^Q adversary plays with a challenger. The game works as follows:

The challenger takes unary $\big(1^k\big)$ and generates vectors $v \in Z_p^m$ and $x \in Z_2^n$, and sends it to the adversary A^Q as input.

The adversary A^Q takes v and x as input to the function $F(v, x)$ and is allowed to make queries q_F to the challenger. The adversary outputs a value F, which is sent to the challenger.

The challenger then looks at (v, x), F, and the queries q_F made by the adversary A^Q. Finally, the challenger outputs 1 or 0.

6.2 Classical Random Oracle Model

This model specifies as a game that a probabilistic polynomial-time algorithm A^C adversary plays with a challenger. The game works as follows:

The challenger takes unary $\left(1^k\right)$ and generates a value x and sends it to the adversary A^C as its input.

The adversary A^C takes x as input to the hash function $h(.)$ and is allowed to make queries q_h to the challenger. The adversary then outputs a value y, which it sends to the challenger.

The challenger then looks at x and y and the queries q_h made by the adversary A^C. Finally, the challenger outputs 1 or 0.

Theorem 1 Assume that $D^{R'(\mathrm{A},.)}$ and $D^{R(.)}$ are two distributions of outputs of a probabilistic polynomial-time algorithm adversary A^Q. The first distribution for the oracle of chosen matrix $\mathrm{A} \in Z_p^{m\times n}$ and the second distribution is taken over the true oracles with q_F quantum oracle queries. Then, the distributions $D^{R'(\mathrm{A},.)}$ and $D^{R(.)}$ are statistically close (at most $\varepsilon < p^{-n}2^{-m}q_F$).

Proof of Theorem 1 Let R be a random oracle, $D^{R(\mathrm{A},.)}\left(1^k\right)$ and $D^{R(.)}\left(1^k\right)$ are two random oracle distributions taken over sample space Ω, which are the output of possible quantum adversary A^Q.

For m and n being positive integers ($m > n$), which are polynomial of the security parameter k, let p be a prime number. For $v \in Z_p^m$ and $x \in Z_2^n$ chosen randomly, we define the statistical distance between the two distributions as follows:

$$\begin{aligned} &SD\left(D^{R(\mathrm{A},.)}\left(1^k\right),\ D^{R(,.)}\left(1^k\right)\right) \\ &= \sum \left| Pr_{(x,v)\leftarrow D^{R(\mathrm{A},.)}(1^k)}\left[A^Q(x,\ v)=1\right]\right. \\ &\quad \left. - Pr_{(x,v)\leftarrow D^{R(.)}(1^k)}\left[A^Q(x,\ v)=1\right]\right| \end{aligned} \tag{10}$$

where $Pr_{(x,v)\leftarrow D^{R(\mathrm{A},.)}(1^k)}\left[A^Q(x,\ v)=1\right] = \sum_v pr[v]Pr[F|v]$ and $x = [x_r|k_i]$.

Fix $x_0 \in Z_2^n$ such that $F(x_0,\ v_0) = F_0$ for some $v_0 \in Z_p^m$, and then the following probability can be computed as follows:

$$Pr[F_0|v_0] = \begin{cases} \frac{1}{2^m} & v_0 \in \varphi(F_0) \\ 0 & elsewhere \end{cases} \tag{11}$$

where $\varphi(F)$ is the set of all preimages of the function F. We defined the size of φ as the number of quantum queries q_F.

Now, we are computing the probability of the distribution:

$$\begin{aligned} &Pr_{(x,\ v)\ \leftarrow D^{R(\mathrm{A},.)}(1^k)}\left[A^Q\ (x,\ v)=1\right] \\ &= \sum_v pr\ [v]\ Pr[F|v] = \sum_{v\in\varphi(F)} \frac{1}{p^m}\frac{1}{2^2} = \frac{q_F}{2^n.p^m} \end{aligned} \tag{12}$$

Then, we are ready to estimate the probability between the two distributions.

$$\begin{aligned} \varepsilon &= \sum \left| Pr_{(x,\ v)\leftarrow D^{R(\mathrm{A},.)}(1^k)}\left[A^Q(x,\ v)=1\right]\right. \\ &\quad \left. - Pr_{(x,\ v)\leftarrow D^{R(.)}(1^k)}\left[A^Q(x,\ v)=1\right]\right| \\ &< \sum_{v\in\varphi(F)} \frac{1}{p^m}\frac{1}{2^2} = \frac{1}{p^m}\frac{1}{2^2}\left|q_F^{'} - q_F\right| \end{aligned}$$

□

Theorem 2 Suppose that for $k_i \in Z_2^l$, N, and F_i are generated randomly. If a probabilistic polynomial-time algorithm (classical) A^C adversary breaches the security of the proposed protocol, then the adversary is able to invert the one-way hash function $h(z)$ on a random input $z \in D \subseteq \{0,\ 1\}^n$ in polynomial time with a non-negligible probability $\varepsilon' > 2^{-k-n}q_h$.

Proof of Theorem 2 Assume that A^C runs a random oracle algorithm to retrieve user cryptographic key k_i from the one-way hash function h with a number of queries q_h. We define the adversary advantages as the probability $Adv_{A^C}(D) = Pr_{z\leftarrow D}\left[A^C(z)=1\right]$. This advantage is determined by the number of queries q_h for the classical random oracle model. Then, the advantage probability is computed as follows:

$$\begin{aligned} Adv_{A^C}(D) &= Pr_{z\leftarrow D}\left[A^C(z)=1\right] = Pr_{z\leftarrow D}[z : h(z)=y] \\ &= \sum_z Pr[y]\cdot Pr[z|y] \le \sum_z \frac{1}{2^k}\cdot\frac{1}{2^n} \le \frac{q_h}{2^{k+n}}. \end{aligned}$$

□

7 Security and Functionality Features

In this section, we discuss the security and functionality features of our proposed protocol and compare with the related lattice-based authentication protocols [28, 29, 31] as shown in Table 1.

F1: Quantum attack resistant: The IoT is encountering security and privacy threats. However, with quantum computing, these security and privacy threats will increase more and more. The security of the proposed protocol is based on PQFC scheme, which is provable secure against quantum attacks.

F2: Tampering with stored biometric templates attack: This property applies when an attacker gets access to the system database or the token, temporarily or permanently cannot

Table 1 Comparisons of security and functionality features of the proposed protocol with the related protocols

Protocol	Security and functionality features									
	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10
[29]	■	▬	▬	□	▬	■	▬	□	□	□
[28]	■	▬	▬	□	▬	■	▬	□	□	■
[31]	■	▬	▬	■	■	■	▬	□	□	■
Our protocol	■	■	■	■	■	■	■	■	■	■

■: Satisfied, □: Not satisfied, ▬: Not elaborated

modify the template in the system database/token to gain server authentication. In the proposed protocol, the attacker needs to break the SVP problem to obtain the biometric reference template.

F3: Biometric template thefts resistant: This property applies to an attacker that gets access to the database system or token and obtain the user's biometric template; she/he can use it for other purposes. In our protocol, the user's biometric template is protected using PQFC scheme. Hence, there is no clear stored template to be stolen.

F4: Privileged insider attack resistant: Insider attacker with privileged access to the database server can pose a serious threat to the server database. One of the breaches can lead to stealing/tampering with the stored biometric templates in the database. The proposed protocol offers an opportunity for the user to hide her/his biometric template from privileged insiders in the registration phase by allowing her/him to send it to authentication server in encrypted format, which will prevent an inside attacker from getting it.

F5: Smart card/token attack resistant: Assume that the user's smart card is lost or stolen. An attacker having the smart card has no way to obtain secret information stored in the smartcard. If the attacker retrieves the information $\sqsupseteq$, the attacker has to find v by solving lattice SVP problem to gain information, which is contradiction to shortest vector problem (SVP).

F6: Man-in-the-Middle attack resistant: In the man-in-the-middle attack, the attacker sits in the middle and negotiates the cryptographic parameters with the user and server to gain access as a legitimate. In the registration phase of the proposed protocol, the user sends request to the authentication server. The server replies by sending the message including the matrix $\boldsymbol{A}$; assume the man-in-the-middle attacker intercepts the server message and replaces the matrix $\boldsymbol{A}$ by $\hat{\boldsymbol{A}}$; the user will compute $F^r_{\mathcal{U}_i} = \left(\hat{\boldsymbol{A}} \cdot v \bmod q + t^r_{\mathcal{U}_i}\right) \bmod 2$ and send to the server. Then, the man-in-the-middle attacker cannot learn the biometric template $t^r_{\mathcal{U}_i}$ from $F^r_{\mathcal{U}_i}$, only if she/he solves the LWE lattice problem.

F7: Renewable biometric template: Unlike passwords, biometrics are limited and once it compromised cannot be revoked. A biometric is the principle means of authentication in our protocol. If the biometric template is compromised by any attacks, it can be used again with new registration parameters.

F8: Memoryless-effortless: An authentication protocol that does not require any users to remember any secret per service called memoryless-effortless. By this definition, the proposed authentication protocol is memoryless-effortless

F9: User anonymity: An important security property of authentication protocol for IoT applications is the confidentiality of the user's identity. It is desirable to keep user's identity hiding from attackers. In the proposed protocol, the plaintext user's identity $ID_{\mathcal{U}_i}$ is neither stored in the user's smart card nor sent in the login and authentication messages over secure or insecure channels. If the attacker is able to retrieve the values e_i and r_i from the user's smart card, it is obvious that an attacker is determining $ID_{\mathcal{U}_i}$ which is equivalent to find the collision in the hash function h.

F10: Lightweight: A protocol with less computational and communication complexities is called a lightweight protocol.

8 Performance Analysis

In this section, we evaluate the performance of our protocol based on the following metrics: the storage requirements, communication costs, and computational complexities. Furthermore, we have compared the proposed protocol with the recent related protocols for IoT systems [28, 31]. Table 2 shows the computational costs comparison between the proposed protocol and the protocols in [28, 31]. Let T_{Mp}, T_{Vp}, T_{add}, and T_h denote the operation time required to execute the matrix multiplication modulo p, vector multiplication modulo p, vector addition modulo p, and one-way hash function, respectively. The total computational time cost of our protocol is $\mathbf{4}\boldsymbol{T}_{\mathbf{Mp}} + \mathbf{2}\boldsymbol{T}_{\mathbf{add}} + \mathbf{19}\boldsymbol{T}_{\boldsymbol{h}}$. Furthermore, we have estimated the execution time of the above mentioned operations as $T_{\text{Mp}} = 4$ ms, $T_{\text{Vp}} = 1$ ms, $T_{\text{add}} = 2$ ms, and $T_h = 0.0023$ ms. The tasks are executed using MATLAB 2020b on PC workstation with Intel(R) Core(TM) i7-10,700

Table 2 Comparisons of computational costs of our protocol with the related protocols

Protocol	[28]	[31]	Our protocol
Initialization phase	T_{Mp}	T_{Mp}	T_{Mp}
Registration phase	–	$4T_h$	$2T_{\text{Mp}} + T_{\text{add}} + 5T_h$
Login phase	$2T_{\text{Mp}} + 2T_{\text{Vp}} + 2T_{\text{add}} + 3T_h$	$T_{\text{Mp}} + T_{\text{Vp}} + 5T_h$	$T_{\text{Mp}} + T_{\text{add}} + 5T_h$
Authentication phase	$1T_{\text{Mp}} + 2T_{\text{Vp}} + 2T_{\text{add}} + T_h$	$T_{\text{Vp}} + 16T_h$	$9T_h$
Total cost	$\boldsymbol{4T_{\text{Mp}} + 4T_{\text{Vp}} + 4T_{\text{add}} + 4T_h}$	$\boldsymbol{2T_{\text{Mp}} + 2T_{\text{Vp}} + 25T_h}$	$\boldsymbol{4T_{\text{Mp}} + 2T_{\text{add}} + 19T_h}$
Total time cost (ms)	28.0092	10.0575	20.0437

Table 3 Comparisons of computational complexities of our protocol with the related protocols

Protocol	Primitive	Complexity overhead	Computational Cost
[28]	$PUB,\ sk,\ R,\ S,\ ANS$	$O\left(mn\left\|p^2\right\|\right)$	$16k\log^2(k)\left(4k\log^2(k) + 2\log(k) + 1\right)$
[31]	$PU,\ t_i,\ v_i,\ v_i^{'}$	$O\left(mn\left\|p^2\right\|\right)$	$16k\log^3(k)(2k\log(k) + 1)$
Our protocol	$pk,\ F_r,\ w_i,\ Z_i,\ w_i^{'}$	$O\left(mn\left\|p^2\right\|\right)$	$8k\log^2(k)\left(8k\log^2(k) + 1\right)$

Table 4 Comparisons of storage and communication costs of our protocol with the related protocols

Protocol		Data storage/exchange	Data length
[28]	Communication	$\{M_i,\ ANS_i,\ R_i,\ S_i\}$	$2\log k(6k\log(k) + 1)$
	Storage	$d \in Z_p^{1\times n},\ A \in Z_p^{m\times n},$ $PUB \in Z_p^{1\times m},\ sk_i \in Z_p^{1\times n},$ $4h(.)$	$2\log k\left(4k^2\log^2 k + 6k\log k + 4\right)$
[31]	Communication	$\{t_i,\ \varphi_i\},\ \{\pi_i,\ ID_i\},\ \{R_i\}$ $\{ID_i,\ b_i\},\left\{C_{ij}\right\}$	$2\log k(2k\log(k) + 7)$
	Storage	$d \in Z_p^{1\times n},\ X \in Z_p^{m\times n},$ $PU \in Z_p^{1\times m}, 6h(.)$	$2\log k\left(4k^2\log^2 k + 4k\log k + 6\right)$
Our protocol	Communication	$\{ID_i,\ Z_i,\ \beta_i,\ r_i\},\ \left\{w_i'\right\},$ $\{\theta_1,\ \theta_2,\ \theta_4,\ \theta_5,\ \theta_6\}$	$2\log k(2k\log(k) + 11)$
	Storage	$mk \in Z_p^{1\times n},\ A \in Z_p^{m\times n},$ $pk \in Z_p^{1\times m}, 7h(.)$	$2\log k\left(4k^2\log^2 k + 4k\log k + 7\right)$

CPU @ 2.90 GHz 2.90 GHz RAM 16.0 GB. Thus, the total execution time for the proposed protocol is 20.0437 ms.

For computational complexity comparison, we followed the parameters reported in [31] as follows: assume that $m = n = O(k\log p)$, $p = O\left(k^2\right)$ and $|p| = \log(p)$. The computational complexity for the operations: matrix multiplication modulo p, vector multiplication modulo p, and vector addition modulo p is $O\left(\text{mn}\left|p^2\right|\right)$, $O\left(m\left|p^2\right|\right)$, and $O(m|p|)$, respectively. Thus, the total computational complexity of the proposed protocol is $8k\log^2(k)\left(8k\log^2(k) + 1\right)$. Table 3 shows the comparison result of our protocol with the related protocols.

Furthermore, the storage requirement and the communication cost comparisons between the proposed protocol and the related protocols [28, 31] are evaluated and shown in Table 4. In the evaluation, we consider the login and authentication phases in the comparison. Note that the registration phase is not performed frequently. In all protocols, we assume the length of the identity, output size of the hash function, and number in Z_p are $|p| = 2logk$. Thus, the total communication cost of our protocol sending messages $\{ID_i,\ Z_i,\ \beta_i,\ r_i\}$, $\left\{w'_i\right\}$, and $\{\theta_1,\ \theta_2,\ \theta_4,\ \theta_5,\ \theta_6\}$ is $(m + 11)|p| = 2\log k(2k\log(k) + 11)$. The storage requirements of our protocol and the related protocols [28, 31] are computed. The total storage cost for storing master

key $mk \in Z_p^{1\times n}$, matrix $A \in Z_p^{m\times n}$, public key $pk \in Z_p^{1\times m}$, and seven hash value is $(n+mn+m+7)|p| = 2\log k\left(4k^2\log^2 k + 4k\log k + 7\right)$.

9 Conclusion

This paper proposed a new lightweight two-factor-based user authentication protocol for the IoT-enabled healthcare ecosystem. We evaluated the security of the proposed protocol through the formal security analysis using random oracle model (ROM), showing that our protocol is secure against today and upcoming quantum attacks. The proposed protocol achieved the following functionality and security properties: memoryless-effortless, user anonymity, mutual authentication, and resistance to tampering and stolen of biometric template, stolen smart card, privileged interior attacks.

The proposed protocol was evaluated in terms of the performance metrics: storage requirement, computation and communication. The results demonstrated that our protocol is more efficient than Mukherjee et al., Chaudhary et al., and Gupta et al. protocols. The overhead of the computational costs of our protocol becomes larger naturally since the proposed protocol exploits these computations to provide several significant security and functionality properties.

The overall performance demonstrates that the proposed protocol is suitable for the Internet of Things applications.

Acknowledgements The authors thank King Fahd University of Petroleum & Minerals for providing facilities for this research.

Funding This work is a part of the project supported by the King Fahd University of Petroleum and Minerals under Grant SR191031.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

1. Alsubaei, F., Abuhussein, A., Shiva, S.: A framework for ranking IoMT solutions based on measuring security and privacy. In: Advances in Intelligent Systems and Computing (2019)
2. Sun, Y.; Lo, F.P.W.; Lo, B.: Security and privacy for the internet of medical things enabled healthcare systems: a survey. IEEE Access. (2019). https://doi.org/10.1109/ACCESS.2019.2960617
3. Yang, W.; Wang, S.; Zheng, G.; Yang, J.; Valli, C.: A privacy-preserving lightweight biometric system for internet of things security. IEEE Commun. Mag. (2019). https://doi.org/10.1109/MCOM.2019.1800378
4. Campbell, M.: Putting the Passe into passwords: how passwordless technologies are reshaping digital identity. Computer (Long. Beach. Calif) (2020). https://doi.org/10.1109/MC.2020.2997278
5. Karimian, N., Wortman, P.A., Tehranipoor, F.: Evolving authentication design considerations for the Internet of biometric things (IoBT). In: 2016 International Conference on Hardware/Software Codesign and System Synthesis, CODES+ISSS 2016 (2016)
6. Riaz, N.; Riaz, A.; Khan, S.A.: Biometric template security: an overview. Sens. Rev. **38**(1), 120–127 (2018). https://doi.org/10.1108/SR-07-2017-0131
7. Al-Saggaf, A.A.: Secure method for combining cryptography with Iris biometrics. J. Univers. Comput. Sci. **24**(4), 341–356 (2018)
8. Hao, F.; Anderson, R.; Daugman, J.: Combining crypto with biometrics effectively. IEEE Trans. Comput. (2006). https://doi.org/10.1109/TC.2006.138
9. Christian, R.; Andreas, U.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP J. Inf. Secur. **2011**(3), 1–25 (2011). https://doi.org/10.1186/1687-417X-2011-3
10. Juels, A., Wattenberg, M.: Fuzzy commitment scheme. In: Proceedings of the ACM Conference on Computer and Communications Security (1999)
11. Rathgeb, C.; Uhl, A.: Statistical attack against fuzzy commitment scheme. IET Biom. (2012). https://doi.org/10.1049/iet-bmt.2011.0001
12. Ignatenko, T.; Willems, F.M.J.: Information leakage in fuzzy commitment schemes. IEEE Trans. Inf. Forensics Secur. (2010). https://doi.org/10.1109/TIFS.2010.2046984
13. Tams, B.: Decodability attack against the fuzzy commitment scheme with public feature transforms. 1–19 (2014)
14. Shor, P.W.: Polynomial time algorithms for discrete logarithms and factoring on a quantum computer. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) (1994)
15. Asif, R.: Post-quantum cryptosystems for internet-of-things: a survey on lattice-based algorithms. IoT (2021). https://doi.org/10.3390/iot2010005
16. Al-Saggaf, A.A.: A post-quantum fuzzy commitment scheme for biometric template protection: an experimental study. IEEE Access. (2021). https://doi.org/10.1109/ACCESS.2021.3100981
17. Mumtaz, M., Akram, J., Ping, L.: An RSA based authentication system for smart IoT environment. In: Proceedings—21st IEEE International Conference on High Performance Computing and Communications, 17th IEEE International Conference on Smart City and 5th IEEE International Conference on Data Science and Systems, HPCC/SmartCity/DSS 2019 (2019)
18. Xu, G.; Qiu, S.; Ahmad, H.; Xu, G.; Guo, Y.; Zhang, M.; Xu, H.: A multi-server two-factor authentication scheme with un-traceability using elliptic curve cryptography. Sensors (Switzerland) (2018). https://doi.org/10.3390/s18072394
19. Soni, P.; Pal, A.K.; Islam, S.H.: An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system. Comput. Methods Programs Biomed. (2019). https://doi.org/10.1016/j.cmpb.2019.105054
20. Ayub, M.F.; Mahmood, K.; Kumari, S.; Sangaiah, A.K.: Lightweight authentication protocol for e-health clouds in IoT based applications through 5G technology. Digit. Commun. Netw. (2020). https://doi.org/10.1016/j.dcan.2020.06.003
21. Rehman, H.U.; Ghani, A.; Chaudhry, S.A. et al.: A secure and improved multi server authentication protocol using fuzzy commitment. Multimed. Tools Appl. **80**, 16907–16931 (2021). https://doi.org/10.1007/s11042-020-09078-z
22. Mohammed, A.J.; Yassin, A.A.: Efficient and flexible multi-factor authentication protocol based on fuzzy extractor of administrator's fingerprint and smart mobile device. Cryptography (2019). https://doi.org/10.3390/cryptography3030024
23. Taher, B.H.; Jiang, S.; Yassin, A.A.; Lu, H.: Low-overhead remote user authentication protocol for IoT based on a fuzzy extractor and feature extraction. IEEE Access **7**, 256 (2019). https://doi.org/10.1109/ACCESS.2019.2946400

24. Li, N.; Liu, D.; Nepal, S.: Lightweight mutual authentication for IoT and its applications. IEEE Trans. Sustain. Comput. (2017). https://doi.org/10.1109/TSUSC.2017.2716953
25. Needham, R.M.; Schroeder, M.D.: Using encryption for authentication in large networks of computers. Commun. ACM (1978). https://doi.org/10.1145/359657.359659
26. Cao, J.; Yu, P.; Xiang, X.; Ma, M.; Li, H.: Anti-quantum fast authentication and data transmission scheme for massive devices in 5G NB-IoT system. IEEE Internet Things J. (2019). https://doi.org/10.1109/JIOT.2019.2931724
27. Zhou, Y.; Wang, L.: A lattice-based authentication scheme for roaming service in ubiquitous networks with anonymity. Secur. Commun. Netw. (2020). https://doi.org/10.1155/2020/2637916
28. Mukherjee, S.; Gupta, D.S.; Biswas, G.P.: An efficient and batch verifiable conditional privacy-preserving authentication scheme for VANETs using lattice. Computing (2019). https://doi.org/10.1007/s00607-018-0689-3
29. Chaudhary, R.; Jindal, A.; Aujla, G.S.; Kumar, N.; Das, A.K.; Saxena, N.: LSCSH: lattice-based secure cryptosystem for smart healthcare in smart cities environment. IEEE Commun. Mag. (2018). https://doi.org/10.1109/MCOM.2018.1700787
30. Sahu, A.K.; Sharma, S.; Puthal, D.: Lightweight multi-party authentication and key-agreement protocol in IoT based e-healthcare service. ACM Trans. Multimed. Comput. Commun. Appl. (2020). https://doi.org/10.1145/3398039
31. Gupta, D.S.; Islam, S.H.; Obaidat, M.S.; Karati, A.; Sadoun, B.: LAAC: lightweight lattice-based authentication and access control Protocol for E-health systems in IoT environments. IEEE Syst. J. (2020). https://doi.org/10.1109/jsyst.2020.3016065
32. Dang, Q.: Changes in federal information processing standard (FIPS) 180–4, secure hash standard. Cryptologia (2013). https://doi.org/10.1080/01611194.2012.687431
33. Ajtai, M.: Generating hard instances of lattice problems. In: Proceedings of the Annual ACM Symposium on Theory of Computing (1996)
34. Peikert, C.: A decade of lattice cryptography. Found. Trends Theor. Comput. Sci. (2016). https://doi.org/10.1561/0400000074
35. Micciancio, D., Regev, O.: Lattice-based cryptography. In: Post-Quantum Cryptography (2009)
36. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM. (2009). https://doi.org/10.1145/1568318.1568324