Acta Informatica Pragensia
2026, Volume 15, Issue 3, 638–660
Special Issue: Selected Extended Papers from International Conferences CITA, ICRAMI, and ADACIS
https://doi.org/10.18267/j.aip.321

PRAGUE UNIVERSITY OF ECONOMICS AND BUSINESS

Article Open Access

PQAC–BIoMT: Post-Quantum Authentication and Access Control Framework for Blockchain-Enabled IoMT Systems

Rachida Hireche [1], **Houssem Mansouri** [1], **Yasmine Harbi** [1], **Al-Sakib Khan Pathan** [2], **Saad Harous** [3]

[1] Networks and Distributed Systems Laboratory, Ferhat Abbas University Setif 1, Setif, Algeria
[2] Computer Science and Engineering Department, United International University, Dhaka, People's Republic of Bangladesh
[3] Department of Computer Science, University of Sharjah, Sharjah, United Arab Emirates

Corresponding author: Rachida Hireche (hireche.rachida@univ-setif.dz)

Editorial Record

First submission received:
February 8, 2026

Revision received:
May 19, 2026

Accepted for publication:
July 1, 2026

Special Issue Editors:
Waad Alhoshan
Imam Mohammad Ibn Saud Islamic University, Saudi Arabia

Subrata Chakraborty
University of New England, Australia

Hakim Bendjenna
Echahid Cheikh Larbi Tebessi University, Algeria

Academic Editor:
Zdenek Smutny
Prague University of Economics and Business, Czech Republic

This article was accepted for publication by the Academic Editor upon evaluation of the reviewers' comments.

How to cite this article:
Hireche, R., Mansouri, H., Harbi, Y., Pathan, A.-S. K., & Harous, S. (2026). PQAC–BIoMT: Post-Quantum Authentication and Access Control Framework for Blockchain-Enabled IoMT Systems. *Acta Informatica Pragensia*, 15(3), 638–660. https://doi.org/10.18267/j.aip.321

Abstract

Background: In recent years, the Internet of Medical Things (IoMT) has transformed the healthcare sector through real-time patient monitoring and continuous data collection. However, transmitting sensitive medical information over public networks exposes IoMT systems to significant security threats, while emerging quantum computing technologies challenge the reliability of traditional cryptographic systems.

Objective: The objective of this study is to propose PQAC-BIoMT, a secure and robust model for remote user authentication and access control in IoMT environments, capable of withstanding both conventional and quantum attacks.

Methods: This article proposes a decentralized authentication framework that integrates post-quantum cryptography using Kyber Public–Key Encryption (Kyber-PKE) into blockchain-based smart contracts. Fog computing nodes are used to reduce the authentication latency and improve the system scalability. A role-based authorization mechanism is integrated to link user identities to functional roles and enforce authorization to medical data and system resource access. Formal security verification is conducted using Burrows–Abadi–Needham (BAN) logic to validate the correctness of authentication, and the Automated Validation of Internet Security Protocols and Applications (AVISPA) tool is used to assess resistance to known attacks. PQAC-BIoMT is further evaluated through a comparative analysis of the computational load, energy consumption and security properties.

Results: Our security analysis demonstrates that PQAC-BIoMT effectively resists common attacks while providing quantum-resistant protection against them. The performance evaluation shows that the proposed scheme achieves relatively lower computational and energy overhead compared to existing approaches, making it suitable for resource-constrained IoMT devices.

Conclusion: The proposed PQAC-BIoMT scheme delivers a secure, quantum-resilient authentication and authorization mechanism for IoMT systems, enhancing both data protection and operational efficiency, which can support practical deployment in real-world IoMT applications.

Index Terms

E-healthcare; Internet of medical things; Security; Key management; Authentication; Authorization; Blockchain; Post-quantum cryptography.

1 INTRODUCTION

The internet of medical things (IoMT) revolutionizes healthcare by enabling continuous monitoring and real-time data collection from patients. By connecting medical devices, sensors and healthcare systems, IoMT enhances patient care, improves treatment accuracy and reduces medical risks (Papaioannou et al., 2022).

This technology not only promotes proactive health management but also enhances decision-making for healthcare providers, leading to improved quality of healthcare, increased patient safety and better outcomes.

In smart IoMT environments, medical devices generally collect and transmit patient data to cloud servers for processing and storage. Then, only authorized users are supposed to access these data to carry out actions and make decisions in various healthcare applications (Hao et al., 2025). Therefore, it is crucial to authenticate user devices to ensure that only authorized individuals can access healthcare cloud data (Puneeth and Parthasarathy, 2024). A number of existing schemes have been studied for this work and it is found that even though many do provide authentication services for user devices in IoMT systems, they show considerable limitations and multiple security vulnerabilities for data confidentiality, integrity and authentication (Hireche et al., 2022).

In the existing literature, IoMT authentication methods are generally classified into centralized and decentralized models (Ahmad and Jagatheswari, 2026). Decentralized solutions, especially those using blockchain technology, are increasingly recommended for IoMT systems due to their ability to adapt to the distributed architecture and diversity of these systems (Mansouri et al., 2024). Moreover, by integrating fog computing with blockchain, the authentication framework addresses the issue of "single point of failure" found in centralized cloud servers, offering a more efficient, scalable and low-latency authentication process between remote users and healthcare cloud servers (Alzoubi et al., 2022).

In recent years, the development of post-quantum cryptosystems has led to significant progress in the field of cryptography, surpassing the traditional systems. Although conventional cryptographic methods such as elliptic curve cryptography (ECC) and Rivest-Shamir-Adleman (RSA) have proven to be effective, their efficiency and security are increasingly challenged by the rise of quantum computing (Mikić et al., 2026; Hireche et al., 2022). Post-quantum cryptography offers resilient solutions capable of withstanding attacks from advanced quantum computers, thereby ensuring long-term protection of encrypted data. However, existing schemes often fail to simultaneously ensure post-quantum security, decentralized trust and lightweight operation suitable for resource-constrained IoMT devices. To address this issue, the proposed scheme uses the benefits of post-quantum cryptography, blockchain (Hireche et al., 2024; Gautham et al., 2025) and fog computing technologies to overcome the limitations of existing authentication methods.

This paper is an extended and substantially revised version of our conference paper previously accepted for presentation at ICRAMI 2025, which is cited herein as (Hireche et al., 2025). This version significantly extends the conference work by incorporating an authorization mechanism based on functional roles, strengthening the post-quantum security design using Kyber-PKE, and providing more comprehensive formal security analysis and performance evaluation.

Unlike most current security approaches for IoMT, which rely separately on blockchain, post-quantum cryptography or access control mechanisms, the proposed PQAC-BIoMT framework introduces a unified post-quantum authentication and authorization protocol specifically designed for decentralized IoMT environments. In the proposed scheme, the Kyber-PKE post-quantum cryptographic primitive is used to securely transmit secret parameters over public channels, which are then used to derive a shared session key used during the authentication process between the remote user and the cloud server, ensuring strong confidentiality while maintaining a low computational load. A blockchain-based security layer is deployed on fog nodes in the framework to support decentralized verification and distributed trust management at the edge of medical nodes. In addition, the proposed protocol integrates role-based authorization directly into the authentication workflow through validation of smart contract and mapping of identifiers to roles. In this way, it enables secure authorization of remote user access while providing a robust and scalable security solution for practical deployment of IoMT.

The remainder of this paper is structured as follows. Recent user authentication solutions in the context of IoMT are reviewed in Section 2. Section 3 discusses the foundational concepts behind this work. The proposed scheme is detailed in Section 4. Then, Section 5 provides a security analysis while Section 6 shows the comparative results against the existing methods. At the end, Section 7 concludes the paper with potential future research directions.

2 LITERATURE REVIEW

In the existing literature, a good number of remote user authentication and authorization schemes have been proposed that address the security issue in IoMT systems. Thus, to select the related works for this paper, a

structured literature search was conducted across several major scientific databases, which included ScienceDirect, IEEE Xplore, SpringerLink and Google Scholar. The selection process focused on peer-reviewed articles published in the period 2019-2025 based on their relevance to authentication and authorization mechanisms in IoMT systems. Table 1 presents a summary of the reviewed works along with their principal strengths and limitations.

A biometric-based user authentication scheme was introduced by Deebak et al. (2019) which ensures secure and anonymous communication in healthcare systems. This scheme aims to safeguard against unauthorized access by preventing adversaries from impersonating legitimate users or misusing smart handheld cards. However, the scheme faces limitations, including vulnerability to single point of failure and the lack of key exposure resistance.

Chandrakar et al. (2020) presented a cloud-based authentication protocol for e-healthcare monitoring systems, offering patients a secure platform to access high-quality medical services and receive treatment from doctors remotely with the aid of mobile devices. However, the scheme is susceptible to user impersonation attacks and it lacks protections for anonymity and traceability. A secure and efficient authentication framework based on ECC for a cloud-assisted smart medical system (SMS) was proposed by Kumari et al. (2020). In this approach, physicians can offer online treatment to patients through cloud-supported applications. However, it also remains vulnerable to single point of failure and lacks protection against anonymity and traceability.

A blockchain-based authentication scheme was proposed by Cui et al. (2020) for an IoT scenario to improve the security of multi-WSN (wireless sensor network) communications. The proposed method organized a blockchain network with different types of nodes in a hierarchical architecture. However, the scheme does not address the issue of mitigating certificate-related attacks.

Li (2023) proposed an enhanced three-factor authentication protocol for IoT to address the security weaknesses of the scheme of Mirsaraei et al. (2022), particularly with respect to untraceability, perfect forward secrecy and resistance to key compromise impersonation attacks. The protocol employs ECC to achieve these security properties while reducing computational and communication overhead. Its security is formally verified using the ROR (real-or-random) model and the ProVerif tool. Furthermore, performance evaluation based on the MIRACL library indicates significant improvements in both the computational and communication overhead. However, the scheme suffers from implementation complexity and high initial deployment costs.

A lightweight mutual authentication and key establishment protocol for cloud-assisted IoT systems was presented by Mahor et al. (2024). The scheme provides anonymity, untraceability, password updating and device revocation. Its formal security is verified using BAN logic and the AVISPA tool. However, it suffers from single point of failure issues and vulnerability to advanced attacks.

Harbi et al. (2024) introduced a lightweight and distributed multi-factor remote user authentication scheme for IoT that makes use of blockchain and fog computing technologies, providing secure user authentication through smart contracts, a fuzzy extractor technique and a lightweight cryptographic hash function. While the work had some strong assumptions, being a lightweight scheme, its design did not consider a post-quantum scenario.

To address the vulnerability of current cryptographic techniques to the potential capabilities of future quantum computing, Mansoor et al. (2024) proposed a scheme that integrates post-quantum cryptography (PQC) in IoT-based consumer health devices. They evaluated the application of PQC methods alongside TLS 1.3 (Transport Layer Security 1.3) to enhance authentication robustness within these systems. The work basically aimed to establish a foundation for more secure and reliable healthcare technology in the era of advanced consumer electronics.

A flexible and robust post-quantum authentication framework tailored for cloud-based healthcare applications was proposed by Bahache et al. (2024). This framework aims to defend against quantum-based attacks by utilizing the Kyber-PKE scheme. However, it is still vulnerable to single point of failure (SPOF) and does not provide resistance against key exposure.

Satpathy et al. (2025) proposed a mutual authentication scheme for IoT-fog-cloud environments, using ECC to improve security and reduce energy consumption. Formal security is analysed using the ProVerif tool while the performance assessment performed with the iFogSim simulator demonstrates significant reductions in energy consumption, latency and execution time. However, it leads to authentication delays due to increased communication between fog nodes and cloud servers.

Khajehzadeh et al. (2025) introduced a lightweight three-factor authentication and authorization scheme for IoMT systems. The approach integrates biohash technique with a private blockchain supported by smart contracts to protect users' biometric credentials. Its security is formally analysed using the real-or-random (ROR) model and validated with the ProVerif tool. In addition, a Python-based implementation was developed to evaluate its effectiveness on key network performance metrics. However, the on-chain storage of medical data on the blockchain introduces significant latency and storage overhead, which negatively affects system scalability and real-time usability.

Hireche et al. (2026) proposed a lightweight blockchain-based protocol for mutual authentication and session key establishment in wireless body area networks (WBANs). Biometric-based sensor management and smart contract-driven revocation mechanisms are integrated in the proposal to enable the rapid removal of compromised entities from the system. For security validation, the authors used BAN logic and AVISPA while performance evaluation was conducted through Ethereum implementation and Hyperledger Caliper benchmarking. Their experimental results demonstrated reduced latency and improved throughput. Nevertheless, the framework relies on conventional ECC, which can be considered the weak point as it may become vulnerable in the quantum computing era.

Ashwini and Puneeth (2026) proposed a blockchain-based framework designed to ensure the security and interoperability of electronic health records (EHRs) in healthcare systems using Hyperledger Fabric and Ethereum blockchains. In this system, the authors basically combined ECC and proxy re-encryption to enable healthcare providers to control access to confidential data. This framework incorporates cryptographic mechanisms based on ECC, including ECIES and ECDSA, in an attempt to secure data exchange and access control in distributed healthcare systems. The experiments conducted by the authors demonstrated a reduced computational load and improved interoperability. However, this framework focuses primarily on sharing EHRs and relies on conventional ECC cryptography. This means that it remains vulnerable to quantum computing attacks.

After analysing the state of the art, to overcome the limitations of the previous studies, the present work proposes a robust scheme based on post-quantum cryptography for blockchain-enabled e-healthcare systems. The objective is to provide secure user authentication, session key establishment and effective access control to protect medical data.

Table 1. *Comparative analysis of reviewed studies: strengths and limitations.*

Study	Technologies and tools	Main strengths	Main limitations
Deebak et al. (2019)	Biometric-based authentication	Anonymous communication and resists impersonation and smart card misuse attacks	Susceptible to SPOF and key exposure attacks
Chandrakar et al. (2020)	Cloud-based authentication protocol	Enabling secure remote access to medical services and supports mobile-based healthcare monitoring	Susceptible to user impersonation attacks and does not provide anonymity and traceability guarantees
Kumari et al. (2020)	ECC-based authentication framework	Enables secure and efficient authentication in cloud-assisted smart medical systems; supports online treatment via cloud applications	Vulnerable to SPOF, lacks anonymity and traceability
Li (2023)	ECC-based three-factor authentication protocol	Provides security features including untraceability, perfect forward secrecy and resistance to key compromise impersonation attacks with reduced overhead	Involves high implementation complexity and incurs considerable initial deployment costs
Mahor et al. (2024)	Hash function and XOR operations	Provides anonymity, untraceability, password updating and device revocation	Vulnerable to SPOF and susceptible to advanced attacks
Harbi et al. (2024)	Blockchain and fog computing technologies, smart contract, fuzzy extractors and lightweight cryptographic primitives	Lightweight and secure multi-factor remote user authentication scheme	Scalability limitations and vulnerable to advanced attacks
Bahache et al. (2024)	Post-quantum cryptography Kyber-PKE), cloud-based deployment	Post-quantum security with Kyber-PKE, privacy-preserving authentication, computation and energy efficient	SPOF in system design and lacks protection against key exposure attacks

Study	Technologies and tools	Main strengths	Main limitations
Satpathy et al. (2025)	ECC-based mutual authentication scheme	Improves security while significantly reducing energy consumption and execution time	Causes authentication delays due to higher communication overhead between fog and cloud layers
Khajehzadeh et al. (2025)	Biohash-based and private blockchain-based authentication	Provides lightweight three-factor authentication and authorization with secure protection of biometric data	Incurs significant storage overhead and latency due to on-chain data storage, affecting scalability and real-time performance
Hireche et al. (2026)	Blockchain and fog computing technologies, biometric and system revoked list-based authentication	Blockchain and fog computing technologies; biometric and system revocation list-based authentication	Lack of post-quantum resistance, absence of integrated authorization and access control
Ashwini and Puneeth (2026)	Hyperledger Fabric, Ethereum, HEC-PRE, ECIES, ECDSA, IPFS	Securing and improving interoperability of HER sharing; authorization; reduced computational overhead	Focused mainly on EHR sharing; reliance on conventional ECC; lack of post-quantum resistance

3 PRELIMINARIES

The following subsections offer an outline of the network model, threat model, access control mechanism and theoretical foundations used in the proposed PQAC-BIoMT scheme.

3.1 Network model

The proposed model integrates three types of nodes: remote user, fog node and cloud server. Remote users include patients and medical staff such as doctors, nurses and physicians, who require access to medical device data. To enable remote users to securely access cloud-based health data, we propose a three-tier architecture that incorporates the remote user layer, the fog layer and the cloud layer, as illustrated in Figure 1.

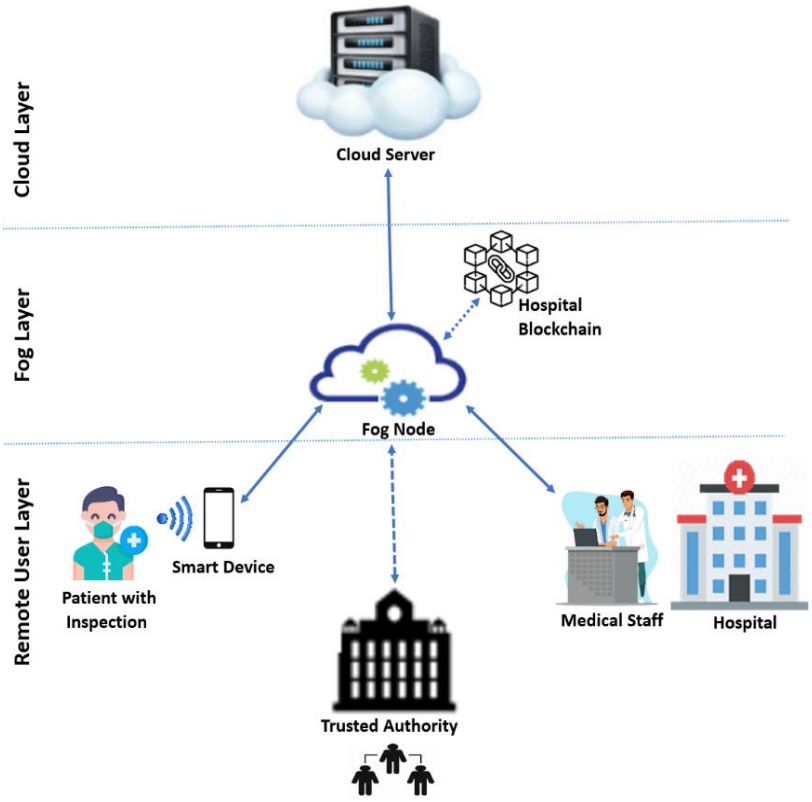

Figure 1. *Proposed model architecture.*

Remote user layer: this layer consists mainly of remote users' devices that need access to data generated by IoMT devices. The data are securely stored on a health cloud server.

Fog layer: The fog layer acts as a security intermediary between remote users and the cloud server. It consists of distributed fog nodes deployed at the network edge and connected through permissioned blockchain. The proposed PQAC-BIoMT framework adopts a lightweight permissioned blockchain architecture in which only authorized entities, including hospital staff, patients, fog nodes and cloud servers, participate in the transaction validation and smart contract execution. To support low-latency and lightweight operations suitable for IoMT environments, the framework adopts the practical byzantine fault tolerance (PBFT) consensus mechanism, which offers lower energy consumption and higher transaction throughput than the proof of work (PoW) and proof of stake (PoS) mechanisms (Manolache et al., 2022). Furthermore, smart contracts deployed on the hospital blockchain enable decentralized user verification and role-based access authorization during the authentication process.

Cloud layer: This layer comprises a cloud server responsible for processing and storing data gathered from IoMT devices, which is considered secure and reliable.

In this paper, our model outlines two scenarios that allow remote users to access patient data stored on the health cloud server:

- **Medical staff data access**: In this scenario, the medical staff requests access to historical medical data stored on the cloud server, typically captured periodically by the sensors. In addition, the personal healthcare data would be stored so that the physicians may update personal health records or upload new prescriptions. This scenario applies to remote diagnosis, medical record management and treatment follow-up.
- **Patient data access:** In this scenario, patients can check their updated medical prescriptions, diagnostic results and the physicians' observations uploaded by healthcare professionals.

3.2 Adversary model

Our research adopts the well-established Dolev-Yao (DY) (Dolev and Yao, 1983) and Canetti-Krawczyk (CK) (Canetti and Krawczyk, 2001) threat models, in which the communication between entities in the system is not secure, making it susceptible to manipulation by an adversary Ă. In our model, Ă can intercept and monitor transmissions over the communication channel, as well as control, modify and create messages based on Ă's initial knowledge. If the appropriate keys are known, Ă can encrypt or decrypt messages. In addition, the intruder is assumed to be able to break traditional number-theoretic cryptographic systems, such as RSA and ECC.

3.3 Access control mechanism

Healthcare environments naturally follow a role-oriented structure in which access privileges are determined by professional responsibilities. To regulate system privileges accordingly, the proposed PQAC-BIoMT scheme adopts a role-based access control (RBAC) framework. The trusted authority (TA) constructs a list of roles, denoted as RoleList, which defines a set of system roles (e.g., Patient, Doctor, Nurse, Physician, etc.) and specifies the access permissions associated with each role. These predefined roles also determine which users are authorized to access medical data and which patients' records they are permitted to access. Such role definitions and access policies constitute the foundation for regulating system operations and controlling data access in the subsequent phases of the protocol. The TA stores a copy of RoleList in the hospital blockchain (HBC). During the registration phase, the TA assigns each new user an appropriate role based on their identity credentials and stores the user's credentials together with the assigned role in HBC. By storing role definitions and user-role associations in HBC, the proposed scheme prevents unauthorized modification of access policies and enables transparent verification of user privileges.

3.4 Cryptographic foundations

The proposed scheme integrates advanced cryptographic techniques, including Kyber-PKE, fuzzy extractors and cryptographic hash functions.

Learning with error problem

Learning with errors (LWE), originally introduced by Regev (2009), is a mathematical problem that serves as a fundamental building block in the design of various post-quantum cryptographic primitives. The problem involves encoding secret information into a system of linear equations, each of which is

perturbed by a small random error. LWE operates over a finite field defined by a modulus q, where the goal is to recover the hidden secret from these noisy equations.

Definition 1 (LWE): Let $n, t, q \in \mathbb{N}$ such that $n \geq t$ and $q \geq 2$ and let χ be a probability distribution over $\mathbb{Z}_q$. Consider a secret vector $s = (s_1, \ldots, s_t)^T \in \mathbb{Z}_q^t$, a matrix $A \in \mathbb{Z}_q^{n \times t}$ selected uniformly at random and an error vector $e \in \mathbb{Z}_q^t$ drawn from the distribution χ^n. The LWE problem is defined as follows: (i) ***Search-LWE:*** Given A and $b = As + e$, the goal is to determine the secret vector s; and (ii) ***Decision-LWE:*** Given A and b, distinguish with a non-negligible advantage between $b = As + e$, where e is sampled from χ^n and b sampled uniformly from $\mathbb{Z}_n^q$.

Module learning with errors (MLWE)

Module learning with errors (MLWE) is a structured generalization of the LWE problem, where vectors over integers are replaced with vectors over polynomial rings. This structure enables more lightweight implementations while maintaining provable security based on worst-case lattice problems over module lattices (Boudgoust et al., 2023).

Definition 2 (MLWE) : Let $q \geq 2$, $n \in \mathbb{N}$, k be the module rank and m the number of samples. Let the ring $R_q = \mathbb{Z}_q[x]/(x^n + 1)$ and let χ be a probability distribution over R_q. Consider a secret vector $s \in R_q^k$, a matrix $A \in R_q^{m \times k}$ chosen uniformly at random and an error vector $e \in R_q^k$ drawn from the distribution χ^m. Define $b = As + e$. The MLWE problem is defined as follows: (i) ***Search-MLWE:*** given A and b, recover the secret s; and (ii) **Decision-MLWE**: given A and b, distinguish with non-negligible advantage between the case where $b = As + e$, where e is sampled from χ^n and the case where b is sampled uniformly at random from R_q^m.

Kyber public-key encryption scheme (Kyber-PKE)

The Kyber public-key encryption scheme (Kyber-PKE) is a lattice-based cryptosystem constructed from the module learning with errors (MLWE) problem (Definition 2). It is parameterized by integers $n, k, q, \eta_1, \eta_2, d_u, d_v$ where $n = 256$ and $q = 3329$. The scheme consists of three algorithms: key generation ($KeyGen$), encryption (Enc) and decryption (Dec) (Nguyen et al., 2025).

***KeyGen* ():** To generate a key pair, a matrix $A \in \mathbb{Z}_q^{k \times k}$ is sampled uniformly at random, consistent with the MLWE formulation. A secret vector $s \in R_q^k$ and an error vector $e \in R_q^k$ are sampled from B_{n_1}. The public key is then computed as $b = As + e$ and the resulting key pair (public and secret keys) is $(pk = (A, b), sk = s)$.

***Enc* (m, pk):** To encrypt a message $m \in (0,1)^l$ using the public key $pk = (A, b)$, a fresh random vector $r \in R_q^k$ from B_{n_1} *and* error vectors $e_1 \in R_q^k$ and $e_2 \in R_q^k$ are sampled from B_{n_2}. Two vectors u and v are computed as follows: $u = A^T r + e_1$ and $v = A^T r + e_2 + encode(m)$ and the ciphertext is $c = (c_1, c_2)$, where $c_1 = Comp_q(u, d_u)$ and $c_2 = Comp_q(v, d_v)$.

***Dec* (c, sk):** To decrypt a ciphertext $c = (c_1, c_2)$, the components are first decompressed: $u := Decomp_q(c_1, d_u)$ and $v := Decomp_q(c_2, d_v)$. The plaintext is then recovered by computing $m = decode(v - s^T u)$.

Kyber-PKE is adopted in the proposed PQAC-BIoMT scheme to securely protect the transmitted parameters over public channels used for session key establishment between the remote user and cloud server. Since Kyber-PKE is based on the MLWE (module learning with errors) assumption, it ensures post-quantum security while maintaining a low computational burden, which is well-suited for resource-constrained medical devices. Furthermore, compared to alternative post-quantum mechanisms, such as NTRU, SABER and FrodoKEM, Kyber-PKE achieves a good balance between security and computational efficiency. In particular, its compact ciphertexts and lightweight encryption/decryption operations significantly reduce the communication and processing costs during session key generation in the authentication phase of the proposed scheme.

Fuzzy extractor

A fuzzy extractor is a cryptographic mechanism that enables the derivation of a reliable secret from biometric measurements, which are affected by noise and variations. It allows a consistent key to be reconstructed from an approximate biometric input with the aid of publicly stored auxiliary data and a predefined tolerance level (Dodis et al., 2004). As illustrated in Figure 2, this mechanism enhances biometric-based authentication in IoMT systems by supporting secure key generation without storing raw biometric templates (Shetty et al., 2022). A fuzzy extractor operates through two core functions:

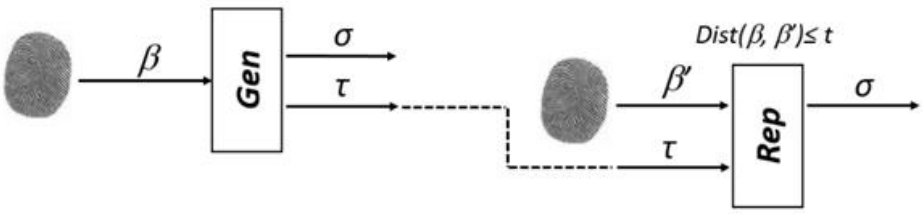

Figure 2. *Process flow of fuzzy extractor mechanism.*

Gen(β) = (σ, τ) is a probabilistic algorithm that takes the biometric data ***β*** as input and outputs a uniformly random secret key ***σ ∈ {0, 1}^{l}*** and a public reproduction parameter ***τ***, where ***l*** denotes the bit length of the extracted key.

Rep(β', τ) = σ is a deterministic algorithm that takes a noisy biometric sample ***β'*** and the public reproduction parameter ***τ*** as inputs and reproduces the original secret key ***σ***, provided that the Hamming distance satisfies ***d(β , β ') ≤ T***, where ***T*** is a predefined error-tolerance threshold.

4 PROPOSED SCHEME

The proposed scheme is composed of three main phases: initialization, registration and authentication. Table 2 presents a summary of the major notations used in this scheme.

Table 2. *Proposed PQAC-BIoMT scheme notations.*

Notation	Description
TA	Trusted authority
HBC	Hospital blockchain
CS, FN, U	Cloud server, fog node and user
ID_h, ID_{fn}, ID_u	Identity of the hospital, fog node and the user
EHR_u RoleList	Electronic health record of user List of user roles
MID_u	Masked identity of the user
HID_u, HPW_u	Hash identity and hash password of the user
Bio_u, PW_u	Biometrics and password of the user
Gen(), *Rep*()	Fuzzy extractor functions
σ_u, τ_u	Biometric secret and public parameters of the user
MK, SK, PK	Master key, secret and public keys generated by Kyber-PKE
$Enc()_{PK}$, $Dep()_{SK}$	Kyber-PKE encryption and decryption algorithms
Ti	Current timestamps
h(.), ‖	Hash function and concatenation operation

4.1 Initialization phase

The trusted authority (TA) conducts an offline initialization process. In this phase, the TA generates two master keys (MKcs, MKfn) and registers the fog nodes linked to the blockchain of the hospital in CS. Furthermore, the parameters for the Kyber-PKE post-quantum cryptographic mechanism are established.

- TA generates a secret key SK_{cs} and public key PK_{cs} for CS and stores SK_{cs} in CS memory.
- TA assigns a unique identity ID_h to each hospital and establishes its blockchain (HBC). Smart contracts are then deployed on HBC.
- TA picks a unique identity ID_{fn} for each fog node, generates its secret key SK_{fn} and a public key PK_{fn} and computes its credentials $C_{fn} = h(h(ID_{fn}) \| MK_{cs})$.

- TA securely stores ($h(ID_h)$, C_{fn}, PK_{fn}) on the cloud server and (ID_h, C_{fn}, SK_{fn}, PK_{cs}) on the fog node, respectively.
- TA stores a copy of RoleList in HBC to ensure the immutability and verifiability of role definitions, which are used to enforce access control policies in the subsequent phases of the protocol.

4.2 User registration

The registration phase enables entities to join the IoMT system. During this phase, system participants, including patients with their sensing devices and healthcare professionals, enrol in the medical network by submitting their identity credentials and role-related attributes. All communications are carried out over a secure channel.
Initially, users register with the medical network by providing the required information through an offline mode. After verification, the TA assigns a unique identity (ID_u) to each user and associates the user with an appropriate role ($Role_u$) according to RBAC policy. Their corresponding electronic health record (EHR) is uploaded to the cloud server. The user then completes the registration process on the hospital blockchain (HBC) by executing the steps illustrated in Figure 3:

- Ui picks their ID_u and PW_u and inputs their personal biometric Bio_u on the smart device.
- Ui's smart device computes $Gen(Bio_u) = (\sigma_u, \tau_u)$, $HID_u = h(ID_u)$ and $HPW_u = h(PW_u \| \sigma_u)$.
- It also generates the timestamp T_1 and sends (HID_u, HPW_u, τ_u, T_1) to the TA via a secure channel.
- Upon receiving the registration request at time T_c, the TA checks if $|T_1 - T_c| < \Delta T$ and checks the legitimate of Ui.
- If the check is held, the TA computes $X = h(HID_u \| MK_{fn})$ and the credentials $C_u = (h(X \| HPW_u) \| Role_u)$ of Ui.
- Then, the TA calls registerUser method in the smart contract of HBC with the transaction $Tr(HID_u, HPW_u, C_u)$.
- If the registration is successful, the TA generates a secret key SK_u and public key PK_u for the user Ui.
- After that, it stores PK_u in FN and (PK_u, τ_u) in CS and sends (SK_u, PK_{fn}, PK_{cs}, C_u) to Ui via a secure channel.
- Finally, Ui computes $MID_u = h(HID_u \| HPW_u)$ and $MC_u = C_u \oplus \sigma_u$ and stores SK_u, PK_{fn}, PK_{cs}, MID_u, MC_u and τ_u in their smart card.

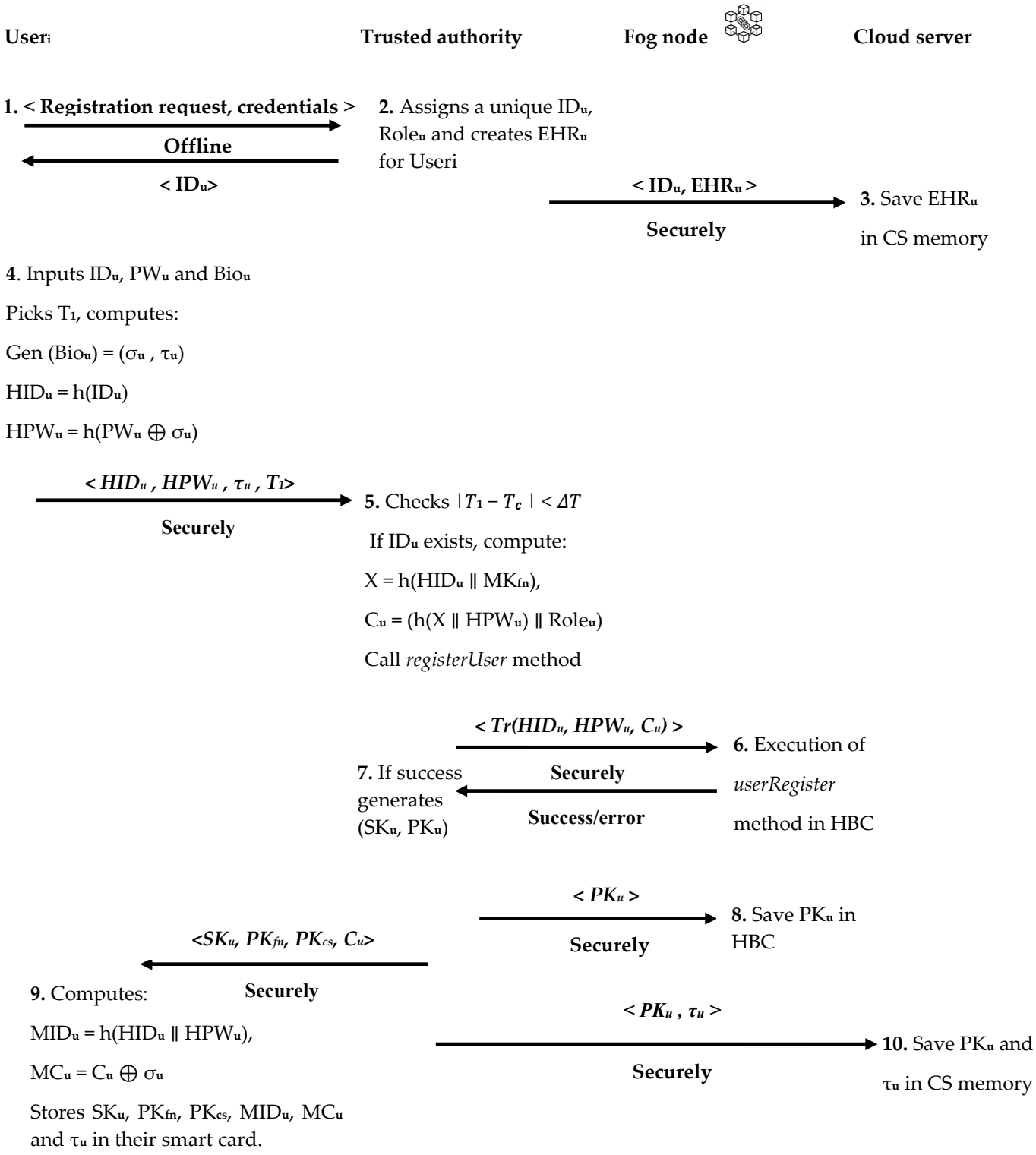

Figure 3. *Registration phase.*

4.3 Authentication phase

In the authentication process, the user (Ui) must verify their identity and prove their legitimacy to gain access to the patient's health data stored on the cloud server. Figure 4 illustrates this phase as following:

- Ui inserts their smart card in their smart device and inputs ID$_u$, PW$_u$ and their personal biometric Bio$_u$.
- Ui's smart device computes Rep(Bio$_u$, τ_u) = σ_u, HID$_u$ = h(ID$_u$), HPW$_u$ = h(PW$_u$ ‖ σ_u),

MID_u^* = h(HID_u ‖ HPW_u) and checks if MID_u^* = MID_u. If the check is held, Ui picks T_1 and computes C_u = $MC_u \oplus \sigma_u$, V_1 = h(C_u ‖ T_1), V_2 = h(τ_u ‖ HID_u ‖T_1) and encrypts E_1 = Enc(HID_u ‖ HPW_u ‖ V_1‖ T_1)$_{PK_{fn}}$. Then, it sends a message (E_1, V_2) to FN.

- FN receives the message at a time T_c. It decrypts D_1 = Dec(E_1)$_{SK_{fn}}$ and extracts HID_u, HPW_u, V_1 and T_1.
- Then, it checks if $|T_1 - T_c| < \Delta T$. If the checks is succeed, FN validates the mapping (HID_u, HPW_u, C_u) and verifies the existence of HID_u, HPW_u in HBC based on their associated role by calling the method UserValidate in the smart contract of HBC with Tr(HID_u, HPW_u, V_1, T_1). If the validation is successful, Ui is authenticated and the process continues. Otherwise, FN aborts the connection.
- FN generates T_2 and computes V_3 = h(C_{fn} ‖ T_2) and encrypts E_2 = Enc(HID_{fn} ‖ HID_u ‖ T_1 ‖T_2)$_{PK_{cs}}$. After that, it sends a message (E_2, V_2, V_3) to CS.
- CS decrypts D_2 = Dec(E_2)$_{SK_{cs}}$ and extracts HID_{fn}, HID_u, T_1 and T_2.
- Then, it checks if $|T_2 - T_c| < \Delta T$ and verifies the existence of HID_{fn} and HID_u in its DB. If the verification holds, it computes V_2^* = h(τ_u ‖ HID_u ‖ T_1) and V_3^* =h(C_{fn} ‖ T_2). if $V_2^* = V_2$ and $V_3^* = V3$ Ui and FN are authenticated. Otherwise, the process terminates.
- CS generates a random number R_{cs} and a timestamp T_3. Then, it calculates the session key SK = h(($HID_u \oplus HID_{fn}$) ‖ R_{cs} ‖ τ_u ‖ T_1).
- CS computes V_4 = h(C_{fn} ‖ T_3), V_5 = h(τ_u ‖ R_{cs} ‖ HID_u ‖ T_3) and encrypts E_3 = Enc(V_5 ‖ R_{cs} ‖ HID_{fn})$_{PK_u}$. After that, it sends a message (E_3, V_4, T_3) to FN.
- FN checks if $|T_3 - T_c| < \Delta T$ and computes V_4^* = h(C_{fn} ‖ T_3). If $V_4^* = V_4$ CS is authenticated. Otherwise, FN aborts the connection.
- FN generates T_4, computes V_6 = h(C_u ‖ HID_{fn} ‖ T_4) and sends a message (E_3, V_6, T_3, T_4) to the user Ui.
- Ui verifies if $|T_4 - T_c| < \Delta T$. Then, it decrypts D_3 = Dec(E_3)$_{SK_u}$ and extracts V_5, R_{cs} and HID_{fn}.
- Ui computes V_5^* = h(τ_u ‖ R_{cs} ‖ HID_u ‖ T_3) and V_6^* = h(C_u ‖ HID_{fn} ‖ T_4).
- Ui verifies if $V_5^* = V_5$ and $V_6^* = V_6$. If the verification is succeed, CS and NF are authenticated. Otherwise, the user Ui aborts the connection.
- Finally, Ui calculates the session key SK = h(($HID_u \oplus HID_{fn}$) ‖ R_{cs} ‖ τ_u ‖ T_1). Therefore, the user (Ui) can communicate securely with the cloud server (CS) using the session key (SK).

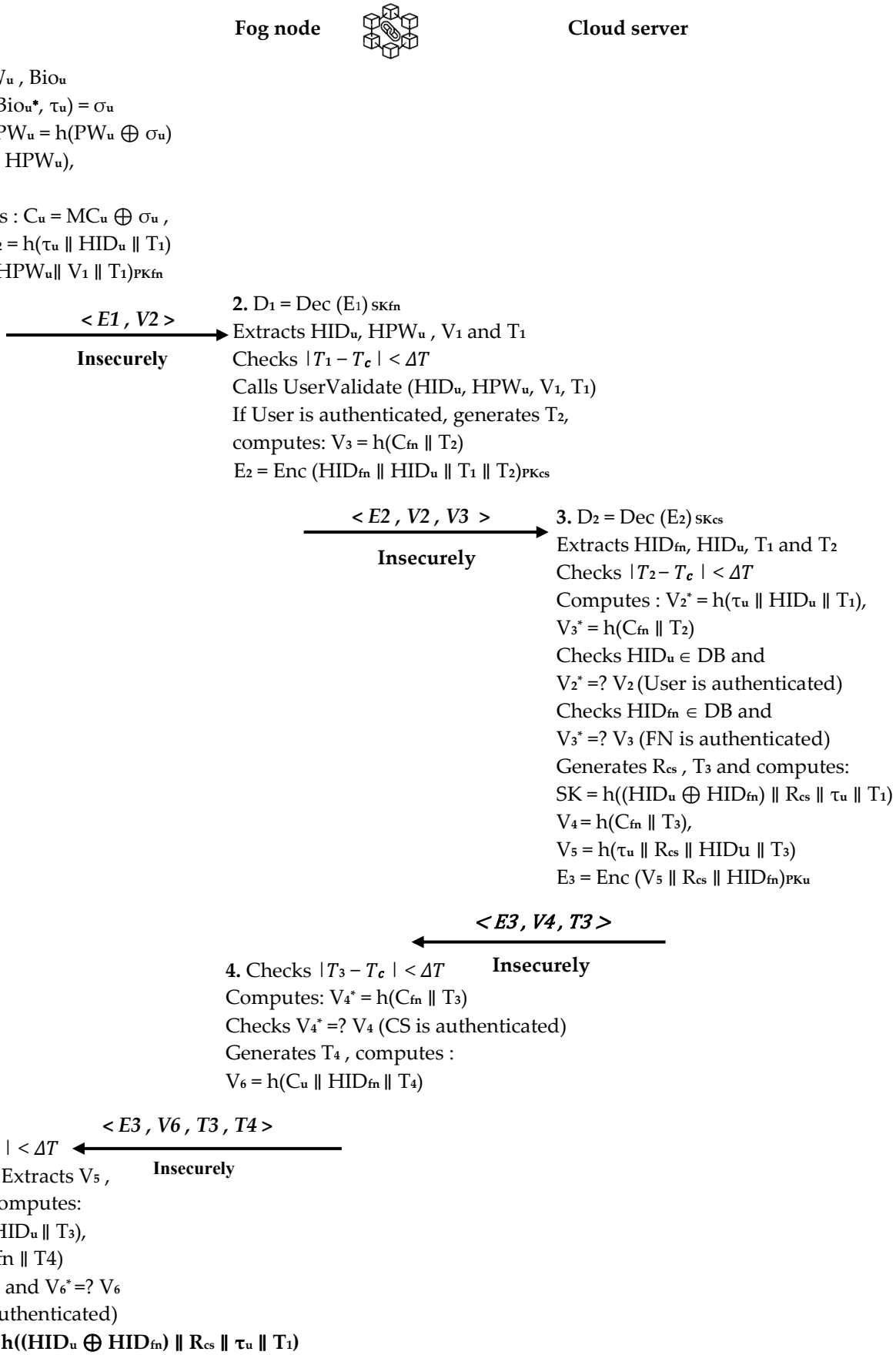

Figure 4. *Authentication phase.*

Algorithm 1. Smart contract of HBC.

1. **Input:** HID_u, HPW_u, C_u, V_1, T_1
2. **Output:** Confirm Msg/Error Msg
3. **Begin**
4. **UserRole(C_u)**
5. $Role_u$: = RoleExtract(C_u) ▷ *Extract user role from user credentials C_u.*
6. **if** (Exist($Role_u$, RoleList)) **then** ▷ *Fetch user role in the list of the roles.*
7. UserList := RoleList.UserList ▷ *Choose the list of the user according to his role.*
8. **return** UserList
9. **else return** Error()
10. **EndUserRole**
11.
12. **RegisterUser(HID_u, HPW_u, C_u)**
13. UserList := UserRole(C_u)
14. **if** (!Exist(<HID_u, HPW_u>, UserList)) **then**
15. Add(<HID_u, HPW_u>, UserList) ▷ *Add the new user in the approved list*
16. *according to his role.*
17. CreateMapping(HID_u, HPW_u, C_u) ▷ *Create a mapping between the new user's*
18. *identity, password and credentials.*
19. **return** "The user is successfully registered."
20. **else return** Error()
21. **EndRegisterUser**
22.
23. **UserValidate(HID_u, HPW_u, V_1, T_1)**
24. ▷ *Fetches mapping (HID_u, HPW_u, C_u) where $V_1 = h(C_u \| T_1)$*
25. **if** (FetchMapping(HID_u, HPW_u, V_1, T_1)) **then**
26. UserList := UserRole(C_u)
27. **if** (Exist(<HID_u, HPW_u>, UserList)) **then**
28. **return** "The user is successfully authenticated."
29. **else return** Error()
30. **else return** Error()
31. **EndUserValidate**
32. **End**

5 SECURITY ANALYSIS

In this section, we evaluate the informal and formal security aspects of the PQAC-BIoMT scheme during the authentication phase.

5.1 Informal security analysis

Resistance to quantum attacks: Lattice-based cryptography is considered to be a leading candidate for post-quantum cryptography. By integrating Kyber-PKE into our model, we guarantee robust long-term security against both conventional and quantum threats, providing solid protection against constantly evolving attack vectors.

User impersonation attack: In our proposed scheme, if the attacker Ă steals user's smart card and tries to initiate an authentication request, Ă will not be able to succeed because Ă needs user's personal biometric data to validate the connection and proceed with authentication. As a result, our system is protected against user impersonation attacks.

Eavesdropping attack: Under the Dolev–Yao adversarial model, an attacker can passively intercept all messages exchanged over the public channel. However, all sensitive parameters are encrypted using Kyber-PKE and protected by one-way hash functions. Without the private keys or long-term secrets, the adversary cannot derive user identities or the session key from the intercepted messages. Thus, the proposed scheme is secure against eavesdropping attacks.

Man-in-the-middle (MITM) attack: In our framework, each transmitted message is encrypted with a fresh timestamp included to prevent replay and man-in-the-middle attacks. Additionally, the distributed nature of the blockchain and the use of smart contracts ensure secure and tamper-proof transaction execution, making such attacks exceedingly difficult.

Stolen smart card attack: Even if an adversary obtains the user's smart card, the stored parameters are protected by biometric data and one-way hash function. As the biometric information cannot be feasibly reconstructed from the stored values, the attacker would not be able to generate valid authentication messages. Therefore, the proposed scheme is resistant to stolen smart card attacks.

Sybil attack: A unique identity is assigned to each new user during the registration phase. Again, their credentials are securely recorded on the hospital's blockchain through the creation of a mapping block between the user's identity, password and related sensitive data. On top of that, the trusted authority (TA) assigns a specific role to each user based on the identity verified during the registration and both the credentials and the associated role are stored immutably on the blockchain. During the authentication phase, every user must prove its legitimacy by interacting with the corresponding smart contract using the registered credentials combined with biometric verification. This mechanism ensures that no identity theft or duplication is possible. This combination of a unique identity link, biometric authentication and storage on a tamper-proof blockchain significantly reduces the risk of creation of a Sybil identity or malicious duplication of identity.

Denial of service (DoS) attack: Smart contracts deployed on the blockchain and implemented in this system through distributed fog nodes are used to verify identities and authenticate legitimate users based on credentials recorded on the hospital's blockchain. These smart contracts perform lightweight deterministic verification without requiring a direct database query, which makes sure that invalid or unauthorized requests are rejected at the edge layer before they reach the cloud server. This early filtering mechanism reduces unnecessary communications and computational load on the cloud server; thereby limiting the impact of request floods and repeated false authentication requests. This design improves the resilience of the proposed system to DoS attacks.

Anonymity and untraceability: In the proposed system, timestamps with the Kyber-PKE mechanism encrypt and decrypt data, creating a chronological record of transactions that preserves user anonymity, enabling secure interaction within the system without revealing sensitive information. As a result, sessions cannot be linked together, guaranteeing both anonymity and untraceability across the entire network.

Confidentiality and integrity: Medical data security is ensured through a robust authentication protocol and a Kyber-PKE public key encryption scheme, which prevents unauthorized access and tampering while preserving the privacy of sensitive information. Furthermore, our system safeguards data integrity by hashing and securely storing confidential records and transactions on the hospital's blockchain. The recipient verifies the hash value to detect any alterations.

Perfect forward and backward secrecy: The proposed scheme achieves both perfect forward secrecy and backward secrecy by generating the session key dynamically for each authentication session using fresh random numbers and timestamps. Specifically, the session key is computed as $SK=h((HID_u \oplus HID_{fn}) \| R_{cs} \| \tau_u \| T_1)$, where R_{cs} and T_1 are freshly generated nonces and HID_u, HID_{fn} and τ_u are long-term secrets shared between the user and the cloud server. The compromise of long-term secrets does not enable an adversary to derive past session keys, as each session key depends on the fresh random value R_{cs} and timestamp T_1, which are never reused and are protected during transmission by Kyber-PKE encryption. Similarly, the disclosure of a current session key does not allow an attacker to compute future session keys, which will be generated using new independent nonces and timestamps in subsequent sessions. Therefore, the proposed protocol effectively guarantees both forward and backward secrecy.

Mutual authentication: The proposed scheme achieves mutual authentication among the user (U), fog node (FN) and cloud server (CS) using shared secrets (C_u, C_{fn}, τ_u), public-key encryption and fresh timestamps. The FN authenticates the user by verifying the credential C_u and the freshness of the timestamps T_1, which is received encrypted under the FN public key. The CS authenticates the FN using its credential C_{fn} and the timestamps T_2. Again, it authenticates the user using the secret τ_u and T_1, both of which are obtained from messages encrypted with the CS public key. The user authenticates the CS upon receiving the fresh random number R_{cs} and timestamp T_3, which are generated by the CS and encrypted under the user's public key. Thus, all the entities mutually verify each other's legitimacy before establishing a session key. This mechanism prevents impersonation and replay attacks.

Access control and authorization: The proposed scheme adopts a role-based access control (RBAC) mechanism to ensure that only authorized entities can access system services and sensitive medical data. During the registration phases, the TA assigns each user a unique identity and an appropriate role according to predefined access policies. In the authentication phase, an entity is authorized only if it successfully proves its legitimacy and holds a valid role that is consistent with the requested operation. Consequently, unauthorized entities would be unable to obtain system privileges or sensitive data without possessing valid credentials and the corresponding role.

Data availability and single point of failure (SPOF): The proposed scheme enhances data availability and eliminates SPOF by integrating blockchain technology into the fog layer architecture. In fact, blockchain provides an immutable and tamper-proof distributed ledger, where data are replicated across multiple fog nodes instead of being stored at a single centralized entity. This distributed storage mechanism makes sure that the failure or compromise of any individual node does not disrupt the normal operation of the system or lead to any significant data loss. Eventually, critical medical data still remain continuously accessible, even in the event of node failures or network disruptions. Furthermore, the inherent redundancy and consensus mechanisms of blockchain guarantee resilience against SPOF, improve the overall reliability and fault tolerance of the proposed system.

5.2 Formal security analysis

The formal security analysis of the proposed scheme is conducted using two well-established methods: BAN logic and the AVISPA tool. BAN logic is applied to demonstrate that a secure and mutually authenticated session key is successfully established between the user (U) and the cloud server (CS). In addition, the AVISPA tool is employed to verify the resistance of the proposed scheme against common security threats, such as replay attacks, impersonation attacks and MITM attacks (Armando et al., 2005).

5.2.1 Security proof using BAN logic

The objectives of the BAN logic analysis are to verify mutual authentication between the user and the cloud server and to ensure that both parties agree on a fresh session key (SK). Additional intermediate beliefs are derived to validate the authentication of the fog node.

The notations used in the BAN logic analysis of our proposed scheme are defined as follows:

- P |≡ X: Principal P believes statement X.
- P ◁ X: Principal P sees (receives) message X.
- P |∼ X: denotes that principal P once sent a message containing X; although the transmission time is unknown, it is assumed that P believed X at the time of sending.
- P |⇒ X: Principal P has jurisdiction over statement X and should be trusted on it.
- $\{X\}_{pk}$: Message X encrypted using the public key pk.
- $\langle X \rangle_k$: Message X protected using the key k (X is hashed with k).
- $P \leftrightarrow_k Q$: P and Q share a secret key k.
- $\rightarrow_{pk} P$: Principal P has k as a public key.
- #(X): The message or value X is fresh, i.e., it has not been sent in any previous protocol execution and is guaranteed to be new.
- (X, Y): X and Y are one part of the formula (X, Y).

Inference rules: The following inference rules of BAN logic are employed to analyse the authentication and session key establishment properties of the proposed protocol:

1. **Message meaning rule (MMR):** If P believes a key is shared with Q and P sees a message encrypted with that key, then P believes that Q once said the message.

$$\frac{P \mid\equiv (P \leftrightarrow_k P), P \triangleleft \langle X \rangle_k}{P \mid\equiv Q \mid\sim X}$$

2. **Public key confidentiality rule (PKCR):** If a message is encrypted using P's public key pk, then only P can decrypt it using its private key pk-1.

$$\frac{P \mid\equiv (\rightarrow_{pk} P), P \triangleleft \{X\}_{pk}}{P \mid\equiv only\ P\ can\ obtain\ X}$$

3. **Nonce verification rule (NVR):** If P believes X is fresh and believes that Q once said X, then P believes that Q currently believes X.

$$\frac{P \mid\equiv \#(X), P \mid\equiv\ Q \mid\sim X}{P \mid \equiv Q \mid \equiv X}$$

4. **Jurisdiction rule (JR):** If P believes that Q has authority over statement X and that Q believes X, then P also believes X.

$$\frac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv\ Q \mid\equiv X}{P \mid\equiv X}$$

5. **Belief rule (BR):** Belief in a compound statement implies belief in each individual component.

$$\frac{P \mid\equiv Q \mid\equiv (X, Y)}{P \mid\equiv Q \mid\equiv X}$$

6. **Freshness rule (FR):** If one part of a message is fresh, the entire message is considered fresh.

$$\frac{P \mid\equiv\ \#(X)}{P \mid\equiv \#(X, Y)}$$

Initial assumptions: The protocol participants share the following initial beliefs:

A1: U, CS |≡ (→$_{PKfn}$ FN)

A2: U, FN |≡ (→$_{PKcs}$ CS)

A3: FN, CS |≡ (→$_{PKu}$ U)

A4: U |≡ (U ↔$_{Cu}$ FN)

A5: FN |≡ (U ↔$_{Cu}$ FN)

A6: FN |≡ (FN ↔$_{Cfn}$ CS)

A7: CS |≡ (FN ↔$_{Cfn}$ CS)

A8: U |≡ (U ↔$_{\tau u}$ CS)

A9: CS |≡ (U ↔$_{\tau u}$ CS)

A10: U |≡ #(T1), FN |≡ #(T2), FN |≡ #(T4), CS |≡ #(T3), CS |≡ #(Rcs), U |≡ FN ⇒ #(T3)

A11: U |≡ CS ⇒ (U ↔$_{SK}$ CS)

Idealized form: In our scheme, the messages conveyed through an insecure communication channel consist of:

M1: U → FN: <E1, V2>

M2: FN → CS: <E2, V2, V3>

M3: CS → FN: <E3, V4, T3>

M4: FN → U: <E3, V6, T3, T4>

Based on the real protocol execution, the idealized form of the exchanged messages is defined as follows:

IM1: U → FN: {(U |~ ((U ↔$_{Cu}$ FN), T1)}$_{PKfn}$

IM2: FN → CS: {FN |~ ((U ↔$_{\tau u}$ CS), (FN ↔$_{Cfn}$ CS), T1, T2)}$_{PKcs}$

IM3: CS → FN: {CS |~ ((U ↔$_{\tau u}$ CS), Rcs, T3)}$_{PKu}$, ⟨ CS |~ ((FN ↔$_{Cfn}$ CS) , T3) ⟩$_{Cfn}$

IM4: FN → U: { CS |~ ((U ↔$_{\tau u}$ CS), Rcs, T3)}$_{PKu}$, ⟨ FN |~ ((U ↔$_{Cu}$ FN), T4)⟩$_{Cu}$

Goals: In order to verify the mutual authentication of the new scheme, we have to achieve the following goals.

G1: FN |≡ U |≡ (U ↔$_{Cu}$ FN)

G2: CS |≡ FN |≡ (FN ↔$_{Cfn}$ CS)

G3: CS |≡ U |≡ (U ↔$_{\tau u}$ CS)

G4: CS |≡ (U ↔$_{SK}$ CS)

G5: U |≡ (U ↔$_{SK}$ CS)

G6: U |≡ CS |≡ (U ↔$_{SK}$ CS)

The analysis proves the goals above for mutual authentication and session-key agreement between the user (U) and the cloud server (CS), based on the inference rules, initial assumptions and idealized form as follows:

- From IM1 and A1, FN decrypts IM1: FN ◃ {U |~ ((U ↔$_{Cu}$ FN), T1)}$_{PKfn}$
- Using the public key confidentiality rule, FN concludes:
  FN |≡ U |~ ((U ↔$_{Cu}$ FN), T1)
- From A10 and applying **NVR** and **BR**, we obtain:
  $$\frac{FN \mid\equiv \#(T1),\ \ FN \mid\equiv U \mid\sim ((U \leftrightarrow\_Cu\ FN),\ \ T1)}{FN \mid\equiv U \mid\equiv ((U \leftrightarrow\_Cu\ FN),\ \ T1)}$$
  Thus, FN |≡ U |≡ (U ↔$_{Cu}$ FN) **(G1 achieved)**
- From IM2 and A2, CS decrypts IM1: CS ◃ { FN |~ ((U ↔$_{\tau u}$ CS)**, (** FN ↔$_{Cfn}$ CS)**,** T1, T2)}$_{PKcs}$
- Using the public-key confidentiality rule, CS concludes:
  CS |≡ FN |~ ((U ↔$_{\tau u}$ CS)**, (**FN ↔$_{Cfn}$ CS)**,** T1, T2)
- By extracting FN's statement from IM2 and applying **A10** and **NVR**, **CS** concludes:
  $$\frac{CS \mid\equiv \#(\boldsymbol{T2}),\ \ CS \mid\equiv FN \mid\sim ((\ FN \leftrightarrow\_Cfn\ CS),\ \ T2)}{CS \mid\equiv FN \mid\equiv ((\ FN \leftrightarrow\_\boldsymbol{Cfn}\ CS),\ \ T2)}$$
- By applying BR, we obtain: CS |≡ FN |≡ **(**FN ↔$_{Cfn}$ CS**) (G2 achieved)**
- By extracting U's statement from **IM2** and applying **A10** and **NVR**, **CS** gets:
  $$\frac{CS\ \mid\equiv\ \#(T2),\ \ CS\ \mid\equiv\ U\ \mid\sim\ ((U \leftrightarrow\_\tau u\ CS),\ \ T2)}{CS\ \mid\equiv\ U\ \mid\equiv\ (\ (U \leftrightarrow_{\tau u}\ \ CS),\ \ T2)}$$
- By applying BR, we get: CS |≡ U |≡ (U ↔$_{\tau u}$ CS) **(G3 achieved)**
- The session key is computed as: SK = h((HID$_u$ ⊕ HID$_{fn}$) ‖ R$_{cs}$ ‖ τ_u ‖ T$_1$)
  Since the session key SK is derived from the fresh nonce R$_{cs}$ and T$_1$ (A10) and
  CS |≡ U |≡ (U ↔$_{\tau u}$ CS), CS believes that Ks is a secure session key shared with U.
  Thus, CS |≡ (U ↔$_{SK}$ CS) **(Gl4 achieved)**
- From **A11** and **G4**, we apply **JR**:
  $$\frac{U\ \mid\equiv CS \Rightarrow (U \leftrightarrow\_\boldsymbol{SK}\ CS),\ \ CS \mid\equiv (U \leftrightarrow\_\boldsymbol{SK}\ CS)}{U \mid\equiv (U \leftrightarrow\_\boldsymbol{SK}\ CS)} \Rightarrow$$ U |≡ (U↔$_{SK}$ CS) **(G5 achieved)**

Since U receives the fresh nonce R$_{cs}$ (A10) encrypted under its public key (A3) and believes that CS knows all session-key components (τ_u, T$_1$ from A9 and IM2 verified earlier), U concludes that CS believes in the established session key shared with U.

Therefore: U |≡ CS |≡ (U ↔$_{SK}$ CS) **(G6 achieved)**

The above analysis formally confirms that, in PQAC-BIoMT, the user (U) and the cloud server (CS) mutually authenticate and successfully establish a shared session key (SK).

5.2.2 Security proof using AVISPA tool

The AVISPA tool has been used to formally validate the proposed protocol. AVISPA is a well-established framework for detecting security vulnerabilities in cryptographic protocol designs. It enables the identification of authentication flaws and potential attacks, such as replay, MITM and impersonation attacks, under the Dolev-Yao (DY) threat model (Armando, 2005). The protocol is specified using the high-level protocol specification language (HLPSL) and analysed through the security protocol animation platform (SPAN).

The verification results obtained using the OFMC and CL-AtSe backends are illustrated in Figures 5 and 6, respectively. These results indicate that the proposed scheme is secure and it satisfies its intended security objectives. In particular, it meets the security goals defined in the HLPSL specification guarantee: (i) the secrecy of sensitive parameters MK, SK, ID$_{fn}$, σ_u, ID$_u$ and PW$_u$; (ii) mutual authentication among the communicating entities, namely the user (U), fog node (FN) and cloud server (CS); and (iii) resistance against replay, MITM and impersonation attacks.

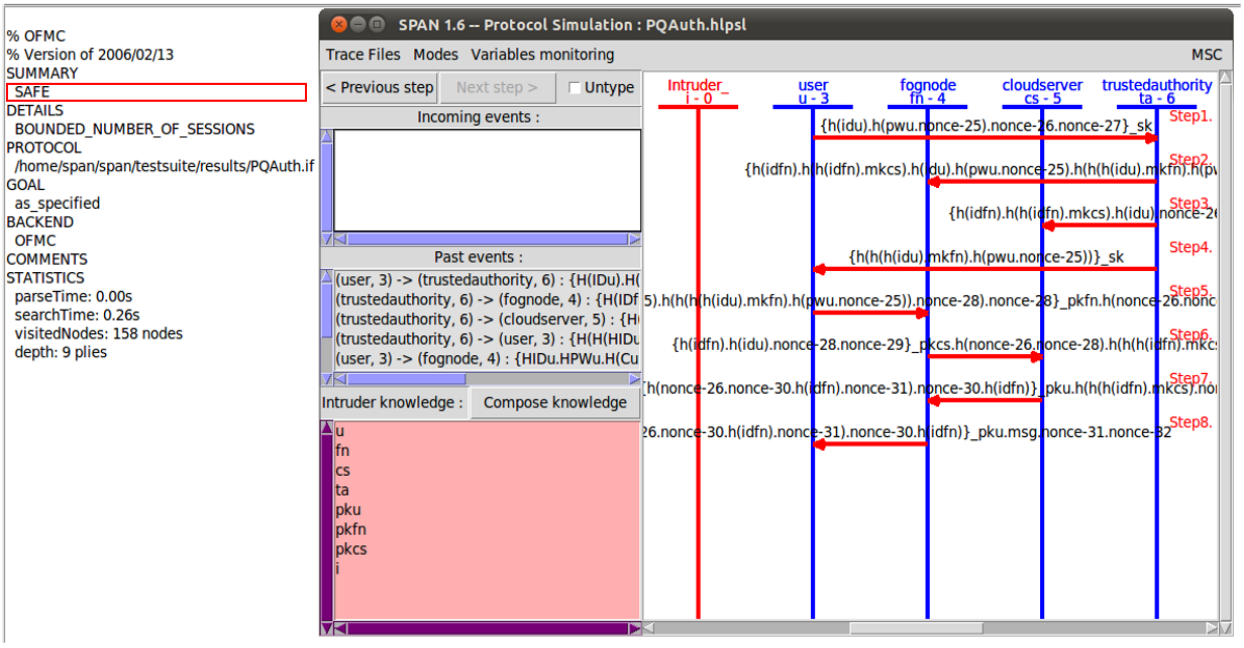

Figure 5. *Results of formal security validation using OFMC.*

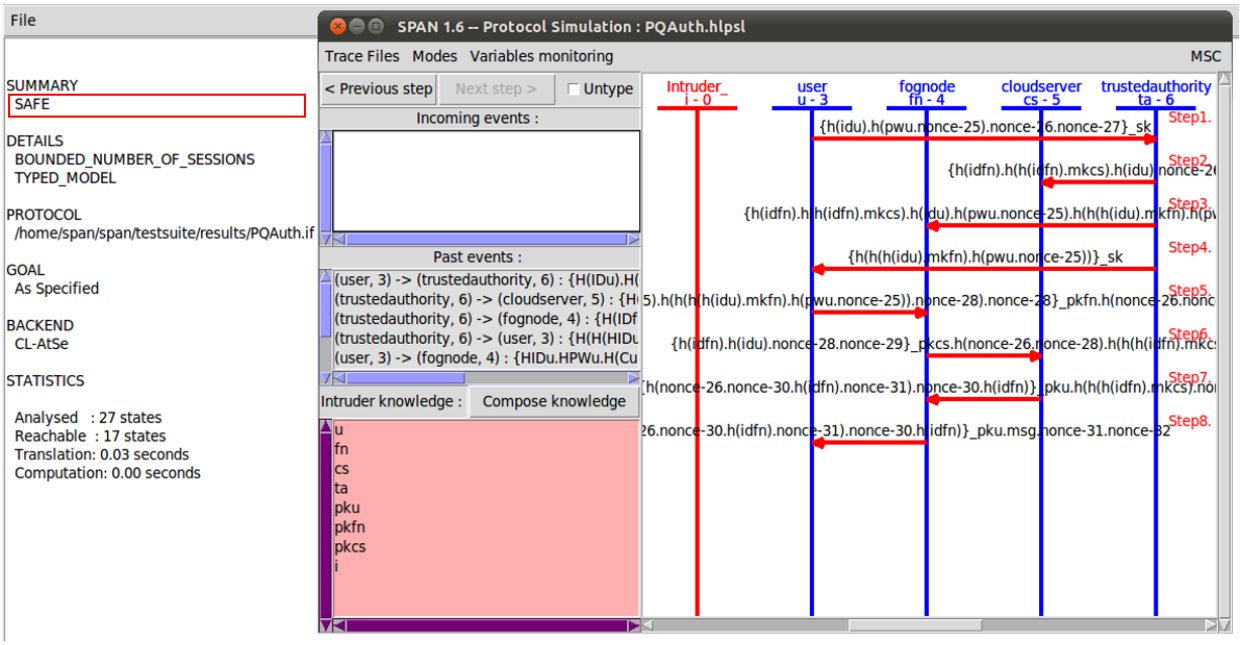

Figure 6. *Results of formal security validation using CL-AtSe.*

6 COMPARATIVE ANALYSIS

This section evaluates the performance and security properties of the proposed authentication and access control framework in comparison with recent methods (Deebak et al., 2019; Chandrakar et al., 2020; Kumari et al., 2020; Li, 2023; Mahor et al., 2024; Harbi et al., 2024; Bahache et al., 2024; Satpathy et al., 2025; Khajehzadeh et al., 2025). The comparative study focuses on computational overhead, energy consumption and supported security features during the authentication phase.

Table 3 summarizes the cryptographic primitives employed in the analysis, along with their corresponding execution times and energy costs. These values are adopted from prior experimental studies (Bahache et al., 2024; Tasopoulos et al., 2023) and are used as the basis for estimating the overall performance of each scheme.

Table 3. *Assessment of cryptographic primitives.*

Crypto-operation	Abbreviation	Computation time (ms)	Energy costs (mJ)
Scalar point multiplication (Curve BN-P254)	T_{SM}	261.066	1.127
Fuzzy extractor	T_{FE}	261.066	0.198
Biohash function	T_{BF}	261.066	0.198
Signature/verification	T_{Sig}	988.830	6.541
Symmetric decrypt/encrypt (AES-128)	T_S	0.288	0.019
Hash function (SHA-256)	T_H	0.154	0.00102
Kyber-PKE encryption	K_{Enc}	6.694	0.443
Kyber-PKE decryption	K_{Dec}	0.672	0.0445

Table 4 presents the total performance measures of the compared schemes. Again, Figure 7 highlights the computational costs and energy consumption of the proposed system compared to other methods.

Table 4. *Comparison of performance measures.*

Reference	Computational costs	Computation time (ms)	Energy costs (mJ)
Deebak et al. (2019)	TFE + 18TH + 6TSM + 2TS	1830.81	7.02
Chandrakar et al. (2020)	12TH + TS + 2TSig	1979.80	13.11
Kumari et al. (2020)	15TH + 8TS + 2TSig	1982.27	13.24
Li (2023)	18TH + TFE + 2TSM	785.97	2.47
Mahor et al. (2024)	14TH + 3TSM + TS	785.64	3.41
Harbi et al. (2024)	TFE + 19TH	263.99	0.22
Bahache et al. (2024)	TFE + 19TH + 4KEnc + 4KDec	293.46	2.17
Satpathy et al. (2025)	22TH + 8TSM + 4TS	2093.07	9.11
Khajehzadeh et al. (2025)	15TH + TBH	263.38	0.21
PQAC-BIoMT	TFE + 16TH + 3KEnc + 3KDec	285.63	1.68

The results indicate that PQAC-BIoMT achieves one of the lowest computation times (285.63 ms) and energy consumptions (1.68 mJ) among all the evaluated schemes. This improvement is mainly attributed to the use of lightweight cryptographic primitives combined with Kyber-PKE, which provides more efficient public-key operations than the traditional ECC- and signature-based mechanisms adopted in many of the other studies (Deebak et al., 2019; Chandrakar et al., 2020; Kumari et al., 2020; Li, 2023; Mahor et al., 2024; Satpathy et al., 2025). These schemes incur significantly higher overhead, with computation times exceeding 1800 ms and energy consumption greater than 7 mJ, rendering them unsuitable for resource-constrained IoMT devices. In addition, the proposed PQAC-BIoMT framework limits the use of blockchain to remote user authentication, smart contract execution and access control operations, while medical records are maintained off-chain within healthcare cloud servers. This design choice preserves the security and traceability benefits of blockchain technology while avoiding excessive storage overhead and additional latency.

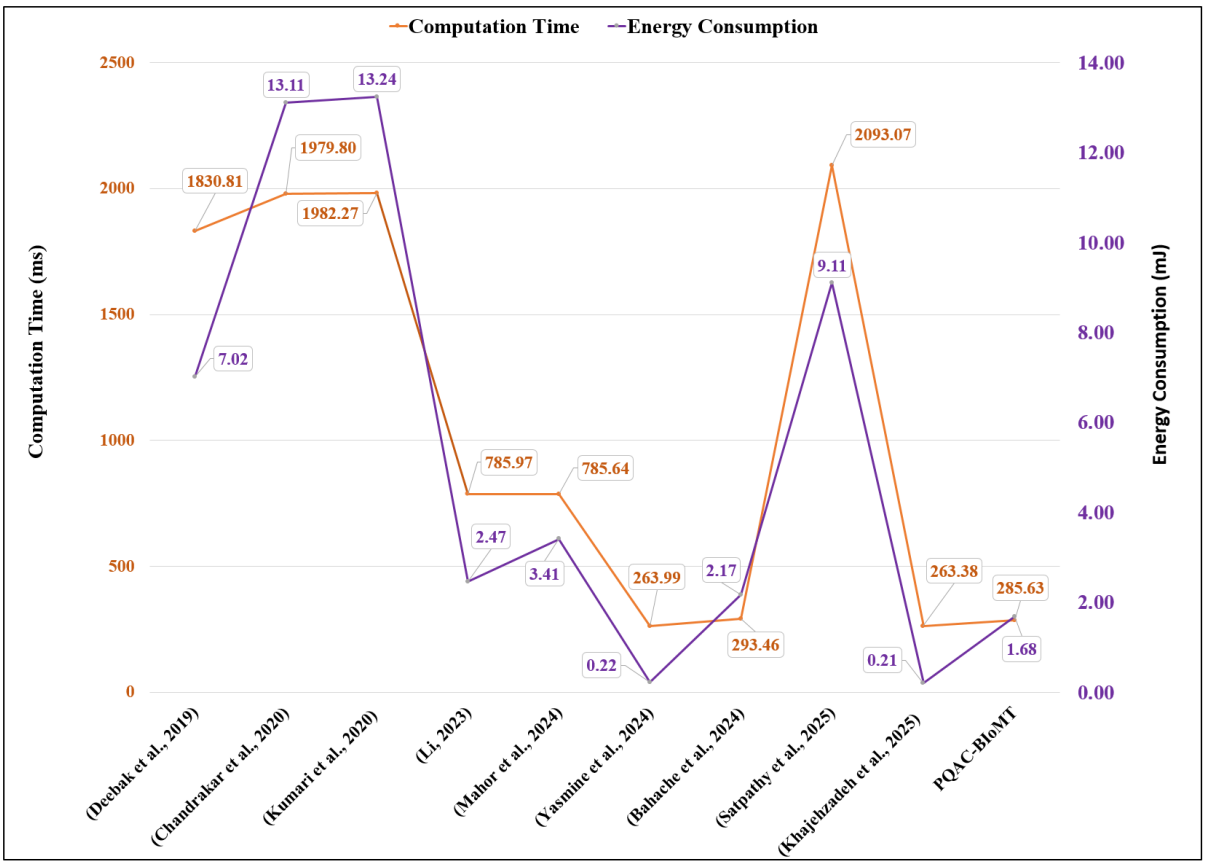

Figure 7. *Comparison of computation time and energy consumption.*

Compared to more recent lightweight approaches (Li, 2023; Mahor et al., 2024; Bahache et al., 2024), PQAC-BIoMT achieves comparable efficiency while additionally providing post-quantum security, which is not supported by Li (2023) and Mahor et al. (2024). Although Harbi et al. (2024) and Khajehzadeh et al. (2025) reported slightly shorter raw computation times, they did not integrate post-quantum encryption and offered limited security coverage.

Table 5 evaluates the security properties of the compared schemes against essential security features.

Table 5. *Comparison of security features.*

Reference	SF1	SF2	SF3	SF4	SF5	SF6	SF7	SF8	SF9	SF10
Deebak et al. (2019)	×	√	√	√	×	×	×	√	×	√
Chandrakar et al. (2020)	×	×	√	√	×	√	√	×	×	√
Kumari et al. (2020)	×	√	√	√	×	√	√	×	×	√
Li (2023)	×	√	√	√	×	×	√	√	√	√
Mahor et al. (2024)	×	×	√	√	×	×	×	√	×	√
Harbi et al. (2024)	×	√	√	√	√	√	√	√	×	√
Bahache et al. (2024)	√	√	√	√	×	×	×	√	×	√
Satpathy et al. (2025)	×	√	√	×	×	√	√	√	×	√
Khajehzadeh et al. (2025)	×	√	√	√	√	×	√	√	√	√
PQAC-BIoMT	√	√	√	√	√	√	√	√	√	√

Notes: √: supported, ×: not supported, SF1: resistance to quantum attacks, SF2: user impersonation attack, SF3: MiTM, SF4: Sybil attack, SF5: blockchain, SF6: data availability and SPOF, SF7: key exposure, SF8: anonymity and traceability, SF9: access control and authorization, SF10: confidentiality and integrity.

Table 5 shows that PQAC-BIoMT provides the most comprehensive security coverage among all compared schemes. Earlier approaches (Deebak et al., 2019; Chandrakar et al., 2020; Kumari et al., 2020) addressed only a limited set of conventional attacks and lacked several essential security features, leaving them vulnerable to cryptanalytic threats and centralized failures. Although Li (2023) and Mahor et al. (2024) offered resistance to impersonation and confidentiality, their schemes do not eliminate the risk of single point of failure.

The proposed scheme distributes the authentication process across fog nodes by integrating blockchain, thereby improving fault tolerance and service availability. Again, the smart contracts ensure tamper-resistant and auditable authentication. The blockchain-based approach of Bahache et al. (2024) enhances decentralization and traceability but does not mitigate key exposure (SF7) situations. Moreover, the use of Kyber-PKE in the scheme enables resistance to quantum attacks, which is not supported by other related schemes (Deebak et al., 2019; Chandrakar et al., 2020; Kumari et al., 2020; Li, 2023; Mahor et al., 2024; Harbi et al., 2024; Satpathy et al., 2025; Khajehzadeh et al., 2025). PQAC-BIoMT also enforces access control and authorization through role-based permissions – a feature supported only by Li (2023) and Khajehzadeh et al. (2025) among the compared schemes.

Overall, the results obtained demonstrate that the PQAC-BIoMT provides relatively stronger security guarantees compared to the existing approaches while maintaining low computational and energy overhead. By combining post-quantum cryptography, blockchain-based decentralization and role-oriented authorization, the scheme achieves an improved trade-off between security, efficiency and scalability, making it suitable for practical deployment in resource-constrained IoMT environments, where low energy consumption, resistance to emerging threats and reliable access control are the critical requirements.

7 CONCLUSION AND FUTURE WORK

In this paper, we presented a secure and scalable authentication framework for IoMT environments that addresses both conventional and quantum attacks. By combining Kyber-based post-quantum encryption with blockchain-enabled smart contracts and fog computing, the proposed scheme achieves decentralized and robust authentication while eliminating single points of failure. In addition, an authorization mechanism that binds authenticated identities to functional roles was incorporated to enforce controlled access to medical services and data. Formal verification using BAN logic and the AVISPA tool confirms the correctness of the authentication process and the resistance of the scheme against common security attacks. Performance and security comparisons with recent approaches demonstrate that the proposed framework provides improved robustness with acceptable computational and energy overhead, making it suitable for resource-constrained IoMT devices.

Despite the promising security and performance results of the proposed system, several practical challenges could arise during real-world deployment. The integration of the framework into existing health infrastructure systems may require additional interoperability and management considerations. Furthermore, resource-limited medical devices may encounter constraints when performing post-quantum cryptographic operations. Therefore, achieving an effective balance between security, scalability and operational efficiency remains a significant challenge for the practical deployment in IoMT systems.

Future work will investigate the optimization of consensus and smart contract execution to further reduce authentication latency in large-scale IoMT deployments. In addition, adaptive security mechanisms based on intelligent resource management will be explored to dynamically adjust authentication and authorization policies according to network conditions and user behaviour.

ADDITIONAL INFORMATION AND DECLARATIONS

Conflict of Interests: The authors declare no conflict of interest.

Author Contributions: R.H.: Writing – Original draft, Conceptualization, Investigation, Formal analysis, Validation. H.M.: Supervision, Methodology, Formal analysis, Writing – reviewing and editing. Y.H.: Conceptualization, Writing – reviewing and editing. A.-S.K.P.: Supervision, Writing –reviewing and editing. S.H.: Writing – Reviewing and editing.

Statement on the Use of Artificial Intelligence Tools: The authors declare that they didn't use artificial intelligence tools for text or other media generation in this article.

Data Availability: Additional data that support the findings of this study are available from the corresponding author.

REFERENCES

Ahmad, A., & Jagatheswari, S. (2026). PQ-ABS: Post-Quantum Aggregate Blind Signature-Based Anonymous Authentication for Blockchain-Enabled IOMT. *IEEE Transactions on Information Forensics and Security*, 21, 1542–1551. https://doi.org/10.1109/tifs.2026.3657031

Alzoubi, Y. I., Al-Ahmad, A., & Kahtan, H. (2022). Blockchain technology as a Fog computing security and privacy solution: An overview. *Computer Communications*, 182, 129–152. https://doi.org/10.1016/j.comcom.2021.11.005

Ashwini, D. Y., & Puneeth, R. P. (2026). Blockchain-Based framework for enhancing interoperability and security in EHR Exchange using lightweight ECC Proxy Re-Encryption. *Acta Informatica Pragensia*, 15(1), 90–108. https://doi.org/10.18267/j.aip.290

Armando, A., Basin, D., Boichut, Y., Chevalier, Y., Compagna, L., Cuellar, J., Drielsma, P. H., Heám, P. C., Kouchnarenko, O., Mantovani, J., Mödersheim, S., Von Oheimb, D., Rusinowitch, M., Santiago, J., Turuani, M., Viganò, L., & Vigneron, L. (2005). The AVISPA tool for the automated validation of internet security protocols and applications. In *Computer Aided Verification, CAV 2005*, (pp. 281–285). Springer. https://doi.org/10.1007/11513988_27

Bahache, A. N., Chikouche, N., & Akleylek, S. (2024). Securing Cloud-based Healthcare Applications with a Quantum-resistant Authentication and Key Agreement Framework. *Internet of Things*, 26, 101200. https://doi.org/10.1016/j.iot.2024.101200

Boudgoust, K., Jeudy, C., Roux-Langlois, A., & Wen, W. (2022). On the Hardness of Module Learning with Errors with Short Distributions. *Journal of Cryptology*, 36(1), Article 1. https://doi.org/10.1007/s00145-022-09441-3

Canetti, R., & Krawczyk, H. (2001). Analysis of key-exchange protocols and their use for building secure channels. In *EUROCRYPT 2001*, (pp. 453–474). Springer-Verlag. https://doi.org/10.1007/3-540-44987-6_28

Chandrakar, P., Sinha, S., & Ali, R. (2020). Cloud-based authenticated protocol for healthcare monitoring system. *Journal of Ambient Intelligence and Humanized Computing*, 11(8), 3431–3447. https://doi.org/10.1007/s12652-019-01537-2

Cui, Z., Xue, F., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A hybrid BlockChain-Based identity authentication scheme for Multi-WSN. *IEEE Transactions on Services Computing*, 13(2), 241–251. https://doi.org/10.1109/tsc.2020.2964537

Deebak, B. D., Al-Turjman, F., Aloqaily, M., & Alfandi, O. (2019). An Authentic-Based Privacy Preservation Protocol for smart e-Healthcare systems in IoT. *IEEE Access*, 7, 135632–135649. https://doi.org/10.1109/access.2019.2941575

Dodis, Y., Reyzin, L., & Smith, A. (2004). Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In *EUROCRYPT 2004*, (pp. 523–540). Springer. https://doi.org/10.1007/978-3-540-24676-3_31

Dolev, D., & Yao, A. (1983). On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2), 198–208. https://doi.org/10.1109/tit.1983.1056650

Gautham, G. K., R, P. K., Rajan, A. A., V, V., & M, M. I. P. (2025). Healthchain: protecting healthcare data through blockchain with zero-knowledge proof and biometric-based access control. *Journal of Cyber Security Technology*, *10*(1), 1–26. https://doi.org/10.1080/23742917.2025.2523760

Hireche, R., Mansouri, H., & Pathan, A. K. (2022). Security and Privacy Management in Internet of Medical Things (IOMT): a synthesis. *Journal of Cybersecurity and Privacy*, 2(3), 640–661. https://doi.org/10.3390/jcp2030033

Hireche, R., Mansouri, H., Harbi, Y., & Pathan, A. K. (2024). Robust Group Authentication Using Quantum Cryptography and Smart Contract for IoMT. In 2*024 International Conference on Information and Communication Technologies for Disaster Management (ICT-DM)*. IEEE. https://doi.org/10.1109/ICT-DM62768.2024.10798936

Hireche, R., Mansouri, H., Harbi, Y., Pathan, A. K., & Harous, S. (2025). Secure Post-Quantum Cryptography-based Authentication for Blockchain-Enabled IoMT Systems. In *International Conference on Recent Advances in Mathematics and Informatics, (ICRAMI 2025).* IEEE. https://doi.org/10.1109/ICRAMI64946.2025.11472719

Hireche, R., Mansouri, H., Harbi, Y., & Pathan, A. S. K. (2026). Lightweight and resilient blockchain-enabled mutual authentication and key establishment protocol for smart health devices in IoMT. *International Journal of Ad Hoc and Ubiquitous Computing*, 51(3), 159–187. https://doi.org/10.1504/ijahuc.2026.152540

Manolache, M. A., Manolache, S., & Tapus, N. (2022). Decision Making using the Blockchain Proof of Authority Consensus. *Procedia Computer Science*, 199, 580–588. https://doi.org/10.1016/j.procs.2022.01.071

Hao, L., Wang, R., Wang, X., Yue, X., Tariq, N., & Sajid, A. (2025). Post-quantum-inspired scalable blockchain architecture for internet hospital systems with lightweight privacy-preserving access control. *PLoS ONE*, 20(12), e0332887. https://doi.org/10.1371/journal.pone.0332887

Harbi, Y., Aliouat, Z., Harous, S., & Gueroui, A. M. (2024). Lightweight blockchain-based remote user authentication for fog-enabled IoT deployment. *Computer Communications*, 221, 90–105. https://doi.org/10.1016/j.comcom.2024.04.019

Khajehzadeh, L., Barati, H., & Barati, A. (2025). L2AI: lightweight three-factor authentication and authorization in an IoMT blockchain-based environment with unsecure channel communication. *Cluster Computing*, 28(13), 865. https://doi.org/10.1007/s10586-025-05569-6

Kumari, A., Kumar, V., Abbasi, M. Y., Kumari, S., Chaudhary, P., & Chen, C. (2020). CSEF: Cloud-Based Secure and Efficient Framework for Smart Medical System Using ECC. *IEEE Access*, 8, 107838–107852. https://doi.org/10.1109/access.2020.3001152

Li, Y. (2023). A secure and efficient three-factor authentication protocol for IoT environments. *Journal of Parallel and Distributed Computing*, 179, 104714. https://doi.org/10.1016/j.jpdc.2023.104714

Mahor, V., Padmavathy, R., & Chatterjee, S. (2024). Secure and lightweight authentication protocol for anonymous data access in cloud assisted IoT system. *Peer-to-Peer Networking and Applications*, 17(1), 321–336. https://doi.org/10.1007/s12083-023-01590-x

Mansoor, K., Afzal, M., Iqbal, W., Abbas, Y., Mussiraliyeva, S., & Chehri, A. (2024). PQCAIE: Post quantum cryptographic authentication scheme for IoT-based e-health systems. *Internet of Things*, 27, 101228. https://doi.org/10.1016/j.iot.2024.101228

Mansouri, H., Hireche, R., Benrebbouh, C., & Pathan, A. K. (2024). A review of blockchain in internet of Medical Things. In *Cryptology and Network Security with Machine Learning*, (pp. 397–412). Springer. https://doi.org/10.1007/978-981-97-0641-9_28

Mikić, M., Srbakoski, M., & Praška, S. (2026). Post-quantum stealth address protocols. *Journal of Cyber Security Technology*, (in press). https://doi.org/10.1080/23742917.2025.2611820

Mirsaraei, A. G., Barati, A., & Barati, H. (2022). A secure three-factor authentication scheme for IoT environments. *Journal of Parallel and Distributed Computing*, 169, 87–105. https://doi.org/10.1016/j.jpdc.2022.06.011

Nguyen, H., Huda, S., Nogami, Y., & Nguyen, T. T. (2025). Security in Post-Quantum Era: A Comprehensive Survey on Lattice-Based Algorithms. *IEEE Access*, 13, 89003–89024. https://doi.org/10.1109/access.2025.3571307

Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J., & Lymberopoulos, D. (2022). A survey on Security Threats and Countermeasures in Internet of Medical Things (IOMT). *Transactions on Emerging Telecommunications Technologies*, 33(6), e4049. https://doi.org/10.1002/ett.4049

Puneeth, R. P., & Parthasarathy, G. (2024). Blockchain-Based Framework for Privacy Preservation and Securing EHR with Patient-Centric Access Control. *Acta Informatica Pragensia*, 13(1), 1–23. https://doi.org/10.18267/j.aip.225

Regev, O. (2009). On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM*, 56(6), 1–40. https://doi.org/10.1145/1568318.1568324

Satpathy, S. P., Mohanty, S., & Pradhan, M. (2025). A sustainable mutual authentication protocol for IoT-Fog-Cloud environment. *Peer-to-Peer Networking and Applications*, 18(1), Article 35. https://doi.org/10.1007/s12083-024-01843-3

Shetty, S., S, A. V., & Mahale, A. (2022). Comprehensive Review of Multimodal Medical data Analysis: open issues and future research Directions. *Acta Informatica Pragensia*, 11(3), 423–457. https://doi.org/10.18267/j.aip.202

Tasopoulos, G., Dimopoulos, C., Fournaris, A. P., Zhao, R.K., Sakzad, A., & Steinfeld, R. (2023). Energy consumption evaluation of post-quantum TLS 1.3 for resource-constrained embedded devices. In *Proceedings of the 20th ACM International Conference on Computing Frontiers*, (pp. 366–374). https://doi.org/10.1145/3587135.3592821

Acta Informatica Pragensia is published by the Prague University of Economics and Business, Czech Republic | eISSN: 1805-4951