Indian Journal of Pure & Applied Physics
Vol. 64, July 2026, pp. 746-761
DOI: 10.56042/ijpap.v64i7.29889

Quantum-Resilient Blockchain Framework with ZKP-Based Access Control for Secure IoMT Healthcare Systems

Nikita Tiwari[a*], Pradeep Kumar Biswal[a] & Prakash Ranjan[b]

[a]Department of Computer Science and Engineering, Indian Institute of Information Technology, Bhagalpur 813 210, India
[b]Department of Electronics and Communication Engineering, Indian Institute of Information Technology, Bhagalpur 813 210 India

Received: 19th March 2026; accepted: 3rd June 2026

The rapid development of the Internet of Medical Things (IoMT) has also facilitated real-time monitoring of healthcare, yet creates major issues of security, privacy, and interoperability, particularly in terms of emerging threats of quantum computing. This paper introduces a quantum-resilient blockchain paradigm, which combines post-quantum cryptography (PQC), Zero-Knowledge Proofs (ZKPs), and Fast Healthcare Interoperability Resources (FHIR) into secure and interoperable healthcare data management. Key encapsulation is performed using lattice-based algorithms, including Kyber and NTRU, and Dilithium and Falcon are algorithms used to secure digital signatures against quantum attacks. An authentication system which is based on a ZKP, and role-based access control allows privatizing access to electronic health records without exposing sensitive data. The framework is deployed on a PBFT-based permissioned blockchain and tested in simulated IoMT settings and has low latency, high throughput, and efficient cryptographic performance. In general, the suggested system will provide a reconfigurable, secure, and future-oriented method to safeguard the healthcare information against quantum threats without compromising the interoperability of the heterogeneous systems.

Keywords: IoMT, Consensus mechanism, Practical byzantine fault tolerance (PBFT), Blockchain

1 Introduction

Modern healthcare has undergone a significant transformation due to the Internet of Medical Things' (IoMT) quick development, which enables remote patient monitoring, remote diagnostics, and intelligent clinical decision-making. Wearable sensors, implantable medical devices and smart monitoring systems are IoMT devices that produce vast amounts of sensitive health data which must be transmitted, processed and stored safely. Even though these technologies increase the availability of healthcare and operational efficiency, they also present serious security and privacy concerns. The IoMT environments operate in limited resources and heterogeneous infrastructures that are susceptible to a wide range of cyber threats such as data interception, unauthorized access, and information leakage[1]. The challenge of ensuring the safety and dependability of handling such sensitive medical information while ensuring interoperability across healthcare systems is thus a primary challenge[2].

Blockchain technology has become a promising solution in order to improve the level of data integrity, transparency, and trust in distributed healthcare systems[3]. Blockchain can secure the information of electronic health records (EHRs) by enabling the decentralized recording and verification of these health records using cryptographic algorithms and eliminate the chances of unauthorized modifications in healthcare data[4]. Tamper-resistant storage and traceable access to medical data are facilitated by the integration of blockchain in the IoMT infrastructures, which enhances accountability in healthcare data management[5]. Nevertheless, classical cryptographic keys like RSA and Elliptic Curve Cryptography (ECC) are being used in traditional blockchain systems, which have been insecure with quantum computing developments. As soon as the large-scale quantum computers become a feasible option, the confidentiality and integrity of healthcare data may be jeopardized by these commonly used cryptography methods[6,7].

In order to deal with these new threats, recent studies have centered on post-quantum cryptography (PQC), which uses cryptographic algorithms, constructed to be resistant to both classical and quantum adversaries. Lattice-based cryptographic schemes, such as Kyber, NTRU, Dilithium, and

*Corresponding author: E-mail: nikita.cse.2203006@iiitbh.ac.in

Falcon, have been of intense interest among the other PQC schemes because of their theoretical security insurances, as well as their practical implementation properties. Such algorithms have been identified as leading approaches in the NIST post-quantum standardization procedure and are more often deemed as being appropriate in attaining security of distributed systems like blockchain networks. With the integration of PQC with IoMT-based healthcare frameworks long term protection against quantum threats while maintaining acceptable computational performance in resource-constrained environments can be achieved[8,9].

Besides cryptographic protection, patient privacy and controlled access to healthcare data are also necessary requirements of the modern healthcare system. Medical sensitive data has to be exchanged between hospitals, doctors, insurance parties and research centers without revealing confidential medical information about patients. A good solution would be privacy preserving authentication schemes including Zero-Knowledge Proofs (ZKPs) which would allow entities to authenticate without disclosing the underlying credentials or sensitive data. The attainment of secure interoperability whilst remaining compliant with the healthcare regulations including HIPAA and GDPR can thus serve as a major research goal[10,11].

In this work, a post-quantum secure, and privacy-preserving blockchain architecture of interoperable IoMT healthcare systems is proposed. The offered framework combines lattice-based cryptographic schemes, such as Kyber, NTRU, Dilithium, and Falcon, to offer quantum-resistant encryption and authentication schemes. To enhance privacy and decentralized authorization, the system will use Zero-Knowledge Proof-based authentication with role-based access control generated by blockchain smart contract. Besides, the architecture incorporates an interoperability layer that is FHIR-compliant and allows sharing healthcare information safely and in a standardized way across distributed medical systems. Unlike existing studies that independently address blockchain security, post-quantum cryptography, privacy-preserving authentication, or healthcare interoperability, the proposed framework integrates all these components within a unified IoMT healthcare architecture. In this work, a quantum-resilient blockchain framework is proposed for secure IoMT healthcare systems. The framework integrates lattice-based post-quantum cryptographic algorithms, Zero-Knowledge Proof-based authentication, blockchain-enabled access control, and FHIR-compliant interoperability within a unified architecture. This integrated design provides quantum-resistant security, privacy-preserving authentication, decentralized access control, and interoperable healthcare data exchange suitable for resource-constrained IoMT environments.

2 Literature Review

The combination of blockchain technology and Internet of Medical Things (IoMT) systems has become a topic of research interest in recent years and especially on enhancing data security, privacy protection, and interoperability in healthcare. Several techniques investigated secure data transmission protocol, access control via blockchain, post-quantum cryptography, and the framework of interoperability of healthcare data exchange.

2.1 Security Mechanisms for IoMT Data Transmission

Researches on secure communication protocols for protecting healthcare data generated by the IoMT has been carried out over the years. Proposed a framework[12] for safe data transmission in IoMT scenarios namely the SA-IoMTH this framework proved by formal verification and experimental testing. Though the technique shows better security of communication, it does not handle the problems of scale as well as the new threat of quantum computing. In the same light, a work presented[13] a new energy-efficient encryption system aimed at the IoMT devices that are constrained by resources. Although the approach helps to lower the computational load when communicating with others, it is mainly concerned with link-layer security and lacks systems to protect data integrity and auditability by using distributed ledgers[14].

2.2 Blockchain-Based Access Control for Healthcare Systems

The concept of blockchain as a tool of secure and transparent healthcare information management has received extensive research. To regulate access to medical data, researchers came up with the MEDACCESSX framework[15]; a combination of role-based access control (RBAC) and attribute-based access control (ABAC) policies via smart contracts. In the same way[16], IoMT edge architectures based on blockchain have been reviewed, emphasizing the possibilities of decentralized systems to manage

healthcare data safely. A framework also presented the BACKM-EHA[17] framework, which is a healthcare-specific key management with blockchain-based key management. Although the scheme enhances the security of key distribution, it adds to the storage overhead and can operate at a relatively low performance in large-scale deployments. A dynamic trust-based access control model for IoMT systems has also been proposed. Even though the framework enhances adaptive access management, sustained behavioral surveillance of users brings about computational overhead, which is not potentially appropriate in IoMT resource-constrained settings[18].

2.3 Post-Quantum Cryptography for IoMT and Blockchain Systems

As quantum computing develops at high rates, the classical cryptographic algorithms like RSA and ECC will soon be broken. In order to overcome this hurdle, researchers have investigated the concept of post-quantum cryptographic (PQC) in securing the distributed systems. Researchers also examined optimum applications on ARM-based IoT of the NTRU encryption scheme[19]. They show that they achieved better performance with compression schemes and secret sharing, but the optimizations add complexity of implementation and are less likely to scale effectively in larger distributed systems. A lattice-based signature scheme that aimed at decreasing the size of blockchain transactions in IoT networks has been introduced[20]. In spite of the fact that the approach enhances efficiency in blockchain transactions, it lacks a full access control mechanism and data management models unique to healthcare. Subsequently, the relevance of these methods to practice-based healthcare environment is low.

2.4 Blockchain and FHIR Integration for Healthcare Interoperability

Interoperability issue is among the most important in the digital healthcare system. An Open Blockchain Framework (OBF) has been proposed to implement blockchain in FHIR-based healthcare systems[21]. Although the given approach proves the economic viability of blockchain-based healthcare data exchange, it does not have effective tools to manage the consent on the fly and provide access control on a fine-grained basis. Also, some of the solutions available are vendor locked and inadequately integrated with sophisticated cryptographic security solutions.

In summary, the current studies have gone a long way to handle the issue of insecurity, access control, and interoperability in the IoMT-based healthcare system. Nevertheless, the majority of solutions handle each of these issues separately and are based on conventional methods of cryptography that might not stay safe with the potential threat of quantum computing. The given limitation shows the necessity of a complex framework that interconnects post-quantum cryptography-based security, privacy-preserving authentication solutions, and standardized healthcare interoperability in a single blockchain-based IoMT architecture. In contrast to prior studies that primarily focus on isolated security or interoperability mechanisms, the proposed work provides an integrated blockchain-IoMT framework combining PQC, ZKP-based authentication, and FHIR-enabled healthcare interoperability within a unified architecture. Table 1 discusses the summary of the related works and alignment of this work for the identified research work.

The reviewed studies demonstrate significant progress in securing IoMT healthcare systems through blockchain, access control mechanisms, post-quantum cryptography, and healthcare interoperability. However, existing approaches primarily address these issues independently. Most studies lack an integrated framework that simultaneously provides quantum-resistant security, privacy-preserving authentication, decentralized access control, and FHIR-compliant interoperability.

3 Methodology for the Proposed Work

The suggested framework is designed to offer safe, scalable, and interoperable management of healthcare information created by the IoMT devices. The framework facilitates end-to-end protection of data confidentiality and integrity with implementation of post-quantum cryptography in combination with blockchain, and is also capable of supporting regulatory-compliant data exchange among healthcare stakeholders.

3.1 Overview of the core components

The fundamental technologies of the proposed structure, namely blockchain, the Internet of Medical Things (IoMT), Apache Kafka and post- quantum cryptography (PQC) are described. All these components counteract major limitations. in electronic health record (EHR) management through facilitating decentralized, secure and sensitive health data can be

Table 1 — Summary of Related Work on IoMT and Blockchain Networks

Focus	Blockchain Integration	Post Quantum Security	Access Control Mechanism	Healthcare Interoperability	Limitations
Secure data transmission for IoMT Wazid *et al*. (2025)[12]	No	No	Lightweight authentication	No	Focuses only on communication security; does not address scalability or quantum-resistant cryptography
Energy-efficient encryption for IoMT devices Xu *et al*. (2024)[13]	No	No	Device-level security	No	Limited to link-layer protection; lacks blockchain auditability and privacy-preserving access control
Smart-contract based healthcare access control (MEDACCESSX) Shi *et al*. (2025)[15]	Yes	No	RBAC + ABAC	No	High policy complexity; limited scalability for real-time healthcare systems
Blockchain-enabled IoMT edge architecture Pelekoudas-Oikonomou *et al*. (2022)[16]	Yes	No	Role Based Access Control	No	Consensus scalability issues and energy overhead
Blockchain-based key management for healthcare Wazid and Gope (2023)[17]	Yes	No	Key-based authentication	No	Increased storage overhead and limited performance evaluation
Trust-based dynamic access control in IoMT Awan *et al*. (2023)[18]	Yes	No	Trust-driven authorization	No	Continuous monitoring introduces computational overhead
NTRU optimization for IoT devices Al-Doori and Al-Gailani (2023)[19]	No	Yes	Cryptographic authentication	No	Focuses only on cryptographic optimization; lacks system-level healthcare integration
Lattice-based signatures for blockchain transactions Yuan *et al*. (2023)[20]	Yes	Yes	Signature Verification	No	Does not address healthcare access control or interoperability
Blockchain-FHIR integration framework Carter *et al*. (2020)[21]	Yes	No	Basic Authorization	Yes	Limited privacy-preserving mechanisms and weak cryptographic security
Secure IoMT healthcare data sharing (Proposed Framework)	Yes	Yes	ZKP + RBAC-based privacy-preserving access control	Yes	-

handled in a scaled manner, as well as real-time processing is supported and heterogeneity and cross-fertility among heterogeneous healthcare systems. Core components of this system are discussed below.

3.1.1 Internet of Medical Things

Internet of Medical Things (IoMT) is a network that links a set of connected medical machines, sensors, and wearable monitors, which constantly record and send information about patient health in real time. The technologies are crucial to contemporary healthcare systems as they allow patient monitoring throughout, promptly identifying the existence of abnormalities, and designing individualized treatment options based on data-driven decisions[22]. In this model, fastening to every device, an ECG monitor, a glucose meter, or a heart rate sensor, a distinct patient identifier is linked. Such connection guarantees the correct tracking of patient-specific data and contributes to the creation of contextual clinical insights depending on the specifics of health profiles of people. Such devices send raw health measurements to a local Edge Gateway, whereby the data is initially encrypted with Post-Quantum Cryptographic (PQC) methods to produce confidentiality as well as protection against possible quantum attacks. Hospital information systems or cloud-based dashboards at the backend receive these Kafka topics and use them to receive alerts, fill real time monitoring dashboards, and facilitate clinical decision-making processes. This multi-tiered architecture facilitates a secure, scalable and streaming-capable system to integrate IoMT

Table 2 — Summary of Related Work on IoMT and Blockchain Networks

Algorithm	Function	Security Level	Key Size (bytes)	Runtime (ms)
Kyber512	Key Encryption	NIST Level 1	800 / 768	1.1 / 0.9
Dilithium2	Digital Signature	NIST Level 1	12 528 / 2420	4/ 1.3

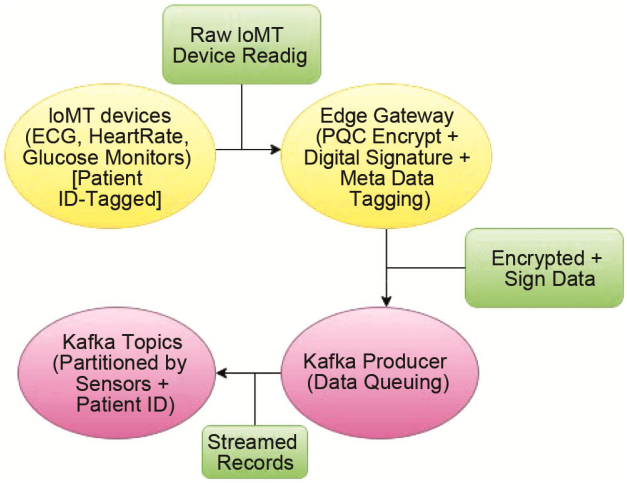

Fig. 1 — IoMT Architecture for Secure and Real-Time Patient Data Streaming

technologies into current healthcare systems. Fig 1 represents the architecture of the IoMT layer without blockchain or access control elements.

3.1.2 Post Quantum Cryptography

Post-Quantum Cryptography (PQC) protects data against potential threats from future quantum computers by employing cryptographic algorithms that are resistant to quantum attacks. As quantum computing technology continues to advance, traditional cryptographic systems such as RSA and ECC may become vulnerable to quantum-based cryptanalysis. Therefore, adopting PQC mechanisms is essential for ensuring long-term security in healthcare data management.

i Dilithium (Digital Signature)

Dilithium2 is used to provide quantum-resistant digital signatures for authenticating transactions and verifying the integrity of patient records. The CRYSTALS-Dilithium scheme is based on the Module-SIS and Module-LWE hardness assumptions, which provide strong security guarantees against quantum attacks. In the proposed architecture, Dilithium2 is responsible for signing and authenticating Electronic Health Record transactions, ensuring both data integrity and non-repudiation. The algorithm uses a public key of 1,312 bytes, a private key of 2,528 bytes, and produces signatures of 2,420 bytes. It meets the NIST Level-1 security standard while maintaining efficient performance suitable for edge computing environments. Experimental observations show that the signing and verification operations require approximately 1.4 milliseconds and 1.3 milliseconds, respectively. These characteristics provide a balance between computational efficiency and strong security, making Dilithium2 well suited for real-time healthcare data environments.

ii Kyber512 (Key Encapsulation Mechanism)

Kyber512 is used to secure the transmission of encrypted EHR data through an efficient post-quantum key exchange process between IoMT gateways and blockchain nodes. Kyber512 provides 128-bit post-quantum security and is based on the Module Learning with Errors (MLWE) problem, which forms the foundation of its resistance to quantum attacks. In this framework, Kyber512 is employed to generate symmetric session keys that are used to encrypt patient data before it is transmitted to the Kafka data stream. The algorithm uses a public key size of 800 bytes and produces ciphertexts of 768 bytes, while the derived shared key size is 32 bytes. Performance measurements show that Kyber512 achieves an encapsulation time of 1.1 milliseconds and a decapsulation time of 0.9 milliseconds, making it suitable for deployment in resource-constrained edge environments while still meeting the NIST Level-1 security requirements. Both cryptographic mechanisms are implemented at the Edge Gateway layer rather than directly on resource-constrained IoMT sensors, their details have been presented in Table 2. This design decision reduces computational overhead on medical devices while maintaining strong cryptographic protection for transmitted healthcare data. Furthermore, the use of PQC algorithms enhances regulatory compliance by strengthening privacy, integrity, and long-term security guarantees required in sensitive medical environments.

3.1.3 Blockchain Technology

The blockchain is a decentralized and distributed registry that ensures information stored in it has transparency, integrity, and immutability. Data is

encrypted into blocks that are cryptographically linked with secure hashing and hence blocking any unauthorized alteration or tampering. Due to these characteristics, blockchain has become a promising solution to addressing healthcare data management, wherein confidentiality, privacy, and traceability are required. In the suggested system, blockchain is the node that stores Electronic Health Records (EHRs) produced by IoMT devices in a secure way. A lightweight, Python-based customized blockchain is deployed instead of the traditional blockchain platforms like Ethereum or Hyperledger Fabric that can introduce some level of complexity to architecture and excessive computation overhead. This customized design puts the priority on using the resource with maximum efficiency and maintaining the basic characteristics of decentralization, immutability, and verifiability. To ensure safety of sensitive medical data against quantum-capable attackers in the future, the framework uses lattice-based Post-Quantum Cryptographic (PQC) algorithms. Particularly, digital signatures are done with Dilithium, and key encapsulation with Kyber, as opposed to legacy cryptography (RSA and ECC) that is susceptible to quantum attacks as described in the above section. The customized blockchain works in the framework in the following manner;

i *Transaction Request:* An action is taken, usually with the storage of encrypted data input by the devices of the IoMT.
ii *Network Distribution:* This is distributed around all the nodes on the peer-to-peer blockchain network.
iii *Block Validation:* Network nodes verify the transaction with the help of the PBFT consensus algorithm and provide authenticity and trust without too much computational load.
iv *Block Creation:* Once the validation has passed successfully a new block with the verified transaction data is created.
v *Addition of Blockchain:* The authenticated block is added to the existing blockchain rendering it irrevocable and giving it a verifiable audit trail.
vi Completion: The validated transaction gets propagated to the entire network and it ensures all the nodes involved are synchronized and consistent.

3.1.4 Smart Contract-Based Access Control and Revocation Mechanism

The framework is an integration of smart contracts and Zero-Knowledge Proofs (ZKPs) in order to enable the implementation of decentralized and privacy-sensitive access to Electronic Health Records (EHRs). These on-chain agents are smart contracts that automatically apply patient-defined authorization and revocation policies not revealing sensitive identities or metadata. Every patient is connected to a specific smart contract that is deployed on the blockchain. The contract has a Merkle tree of authorized healthcare provider public keys, which enables the verification to scale and retain privacy. The contract has three key operations: grant Access (providerpubkey) which adds a provider to the authorization list, revokeAccess (providerpubkey) which removes authorization, and verify ZKP (proof, publicInput) which verifies zk-SNARK proofs with a Groth16 verifier circuit. A healthcare provider producing a zk-SNARK proof does so in response to a request by the healthcare provider to access the proof, and the proof would prove that the healthcare provider has a public key in the patient Merkle tree of authorized entities. The evidence is forwarded to the smart contract to be verified. In case the contract is validated, an AccessGranted event is emitted. This event is detected by the patient node and produced a Kyber512-encrypted session key to be used to decrypt off-chain patient EHR (e.g. Kafka or IPFS).

In case access is compromised, the key of the provider is taken off the Merkle tree, and any further authentications are not possible. This ensures that the consent is controlled by the patient, that access is decentralized and auditable access logs are available and that only a minimal storage is required on-chain as only metadata and proof logs are stored. Groth16 to verification associated with zk-SNARK needs about 220,000 gas units, which is also efficient in executing it in the blockchain. The proposed mechanism offers several advantages for secure healthcare data management. It enables decentralized access control, allowing patients to directly manage access to their medical records through blockchain-based smart contracts. It also provides privacy-preserving authorization, as Zero-Knowledge Proofs (ZKPs) authenticate users without revealing their identities or cryptographic credentials. In addition, Kyber512 facilitates post-quantum secure key exchange by establishing secure session keys for encrypted communication. The immutable nature of blockchain further ensures auditability, maintaining tamper-resistant access logs that support regulatory compliance. Overall, the integration of smart contracts and Zero-Knowledge Proofs enables secure storage, patient-controlled consent management, and

privacy-preserving retrieval of electronic health records.

3.1.5 Zero-Knowledge Proofs (ZKPs)

Zero-Knowledge Proofs allow one party to demonstrate that they know a fact, but not the knowledge itself. ZKPs in the framework will offer decentralized access authorization and privacy-preserving authentication to EHRs. The system uses zk-SNARKs (Groth16 construction), which provides small proofs and is efficiently verified in a few seconds, which is ideal when executing smart contracts. In this protocol, a healthcare provider creates a demonstration that his/her public key is a part of the authorized Merkle tree of the patient without revealing the key. The evidence is sent to the blockchain smart contract and checked with Groth16 verifier. In case the verification is successful, a session-limited access token is granted by the contract and enables the retrieval and decryption of the EHR. With a size of around 192 bytes, the zk-SNARK proofs are small, and on-chain checking takes 58 ms, so authentication can be performed efficiently in real time in healthcare settings. The protocol is based on elliptic-curve pairings and uses the zk-SNARK security hypothesis and needs a trusted setup. This framework is used to provide confidential, scaled, and secure access to electronic health records in IoMT-based health care systems through a combination of ZKPs, smart contracts, and post-quantum cryptography. The system uses zk-SNARKs with a proof size of approximately 192 bytes and an on-chain verification time ranging from 5 to 8 milliseconds. It operates under security assumptions based on zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARKs) implemented over elliptic curve pairings and requires a trusted setup. This combination of zk-SNARKs and smart contracts ensures minimal overhead while enforcing strong privacy, making this system scalable and secure for real-time IoMT healthcare environments, its working is described in Fig. 2.

3.2 Component Interaction

The proposed system supports secure and privacy-preserving management of electronic health records (EHRs) by employing blockchain, post-quantum cryptography (PQC), Internet of Medical Things (IoMT) devices, and Zero-Knowledge Proofs (ZKPs). The IoMT devices such as wearable sensors and smart medical monitors continually collect the health data on the patients including vital signs and diagnostic measurements. To protect sensitive healthcare information during transmission, the obtained data is encrypted using lattice-based post-quantum algorithms to share keys with Kyber and validate information authenticity and integrity with digital signatures created using Dilithium or Falcon. The encrypted messages are next forwarded to a verified blockchain network; Nodes execute them with the help of a consent system. When validated, the health records are permanently stored on the blockchain and hence become readable, traceable and safe in the long-run against the potential of quantum attacks. Access to patient records is done with privacy-preserving access through the use of role-based access control policies that are executed with smart contracts and Zero-Knowledge Proofs (ZKP). Clients who want

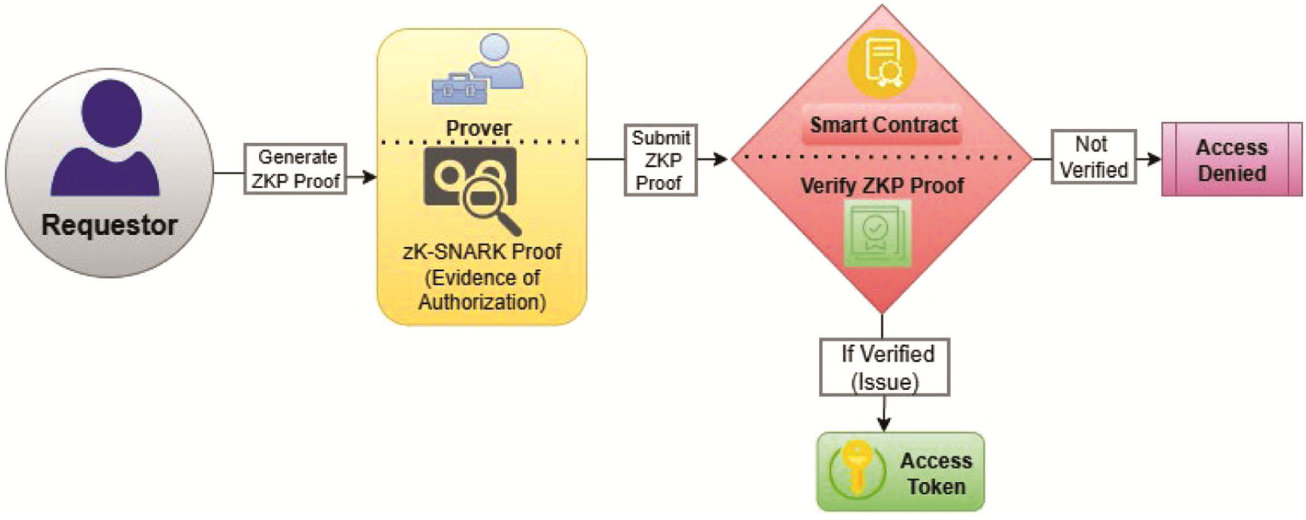

Fig. 2 — ZKP-based Authentication Flow in KB-IoMT

to access healthcare should produce cryptographic signatures indicating their authorization without disclosing confidential credentials. The system takes a layered architecture as shown in Fig. 3 with each layer playing specific role.

i *IoMT Device Layer*: Collects physiological data from wearable and implantable medical devices.
ii *Data Transmission and Security Layer:* This provides a secure communication scheme as it uses Kyber Key Encapsulation Mechanism (KEM) in data transfer over TLS and verifies messages by using lattice-based digital signature.
iii *Blockchain Layer:* Validates transactions using the Practical Byzantine Fault Tolerance (PBFT) consensus protocol, manages workloads through sharding, and stores data immutably on the blockchain.
iv *FHIR Integration Layer:* Converts blockchain-stored data into FHIR-compliant records, enabling standardized interoperability and secure access through APIs.
v *Application and Access Control Layer:* Uses Zero-Knowledge Proofs (ZKPs) for privacy-preserving authentication and Role-Based Access Control (RBAC) for fine-grained authorization, with patient consent managed through smart contracts.

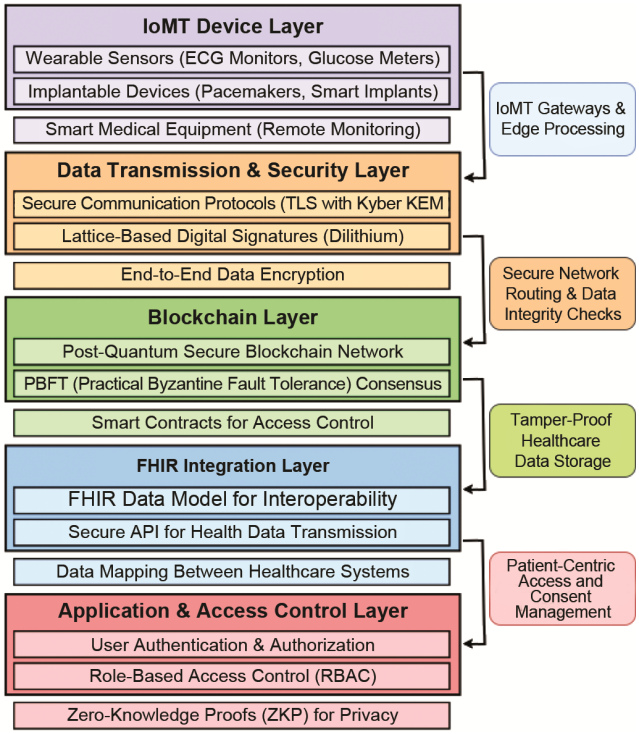

Fig. 3 — Layered Architecture of the KB-IoMT System

The smart contract checks these evidence and only trusted parties access the system, but an audit trail of every access point remains intact. In order to be interoperable among healthcare systems, the framework will integrate a Fast Healthcare Interoperability Resources (FHIR) layer that can adapt blockchain-stored records to standard healthcare data formats. The integration will allow safe and effective data transfer between hospitals, clinical systems, and healthcare applications without compromising the privacy of patients or regulatory standards.

3.4 Working Process and Algorithmic Flow

This section outlines the operational cycle of the suggested framework and provides the algorithmic process of the secure IoMT healthcare data management. The workflow combines post-quantum cryptography, blockchain authentication, privacy-preserving authentication, and FHIR-compliant healthcare data exchange to provide the electronic health record with safe and interoperable management. The workflow of transmitting and storing securely the IoMT healthcare data with the help of post-quantum cryptographic mechanisms is introduced in Algorithm 1. In the algorithm, a secure session key is created with the help of lattice-based key encapsulation schemes, including Kyber or NTRU, and the FHIR healthcare record is authenticated with the help of encrypted using this key. Decrypted digital signatures that are produced by Dilithium or Falcon provide protection to data integrity and authenticity prior to passing the transaction to the blockchain network. The validated transaction is then transacted on the blockchain consensus mechanism and fully written in the distributed ledger.

The privacy preserving access control mechanism used in the proposed framework is described by Algorithm 2. A Zero-Knowledge Proof (ZKP) is produced when a healthcare provider requests to access patient data in order to prove that he is authorized according to the established access policy without disclosing sensitive credentials. The smart contract authenticates the proof and checks the role of the requester and then gives access. Any access request and authorization result is recorded on the blockchain to achieve transparency, accountability, and regulatory compliance. Algorithm 3 is the algorithm to retrieve and deliver healthcare records in a standard format. Once successfully authorized, the

Algorithm 1 — Hybrid Post-Quantum Security Workflow for IoMT Data Transmission and Blockchain Storage

Input: FHIR record r, device identity DevID, current time t
Output: Encrypted, signed, and immutably stored blockchain transaction

1 Initialization
Session key Ks ← ∅
Metadata meta ← (DevID, t, nonce)
2 Key Establishment
If kem_scheme = Kyber then
Ks ← Kyber.Encap/Decap()
Else
Ks ← NTRU.Encap/Decap()
3 Data Encryption
Serialize healthcare record
p ← SerializeFHIR(r)
Encrypt data using authenticated encryption
c ← AEAD_Encrypt(Ks, p, meta)
4 Digital Signature Creation
If sig_scheme = Dilithium then
σ ← Dilithium.Sign(c || meta)
Else
σ ← Falcon.Sign(c || meta)
5 Packet Assembly and Transmission
M ← <meta, c, σ, sig_scheme, kem_scheme>
Send message M through secure communication channel
6 Receiver Verification
Verify signature σ
If verification fails
Return Reject
7 Data Decryption
Decrypt payload using session key Ks
Parse FHIR record r
8 Blockchain Transaction Creation
τ ← BuildTx(r, DevID, t, hash(M))
9 Consensus Execution
Execute blockchain consensus procedure
Validate transaction across network nodes
10 Block Creation and Storage
Append validated transaction to new block B
Store block B in blockchain ledger
11 Finalization
Store transaction metadata
(hash(B), DevID, t)

Return Success

Algorithm 2 — ZKP-Based Privacy-Preserving Access Control for Secure EHR Retrieval

Input: User identity U, claimed role R, access policy P, patient identifier PID.
Output: Authorized access to FHIR-compliant healthcare record

1 Access Request Initialization
User U submits a request to access patient record PID
2 Policy Retrieval
Retrieve access policy P and role permissions from the blockchain smart contract
3 Credential Commitment
Generate cryptographic commitment:
com ← Commit(skU)
4 Zero-Knowledge Proof Generation
Generate proof:
π ← ZKP. Prove(skU, R, P)
5 Proof Submission
Submit the tuple <U, R, PID, π> to the blockchain smart contract
6 Proof Verification
valid ← ZKP. Verify(π, R, P)
7 Access Decision
If valid = false
Return Reject
8 Role Validation
If role R satisfies policy P
Access Granted
Else
Return Reject
9 Secure Session Establishment
Generate session key Ks using Kyber-KEM.
10 Data Retrieval
Retrieve encrypted healthcare record corresponding to PID
11 Decryption
Decrypt the record using session key Ks.
12 FHIR Mapping
Convert the healthcare record to FHIR format:
FHIR_record ← MapFHIR(EHR)
13 Audit Logging
Store access log entry (U, PID, timestamp) on blockchain
14 Return Result
Provide authorized user with the FHIR-compliant healthcare record

Algorithm 3 — FHIR-Based Healthcare Data Retrieval and Interoperable Data Exchange

Input: Authorized request Req, patient identifier PID
Output: FHIR-compliant healthcare record

1 Access Request Reception
Receive authorized request Req for patient record PID
2 Permission Verification
Verify access permission using smart contract policies
3 Blockchain Record Lookup
Retrieve transaction hash corresponding to PID from blockchain ledger
4 Off-Chain Data Retrieval
Fetch encrypted healthcare record associated with retrieved hash
5 Secure Decryption
Obtain session key Ks from secure channel
Decrypt encrypted healthcare data
6 Record Parsing
Extract medical data fields from decrypted electronic health record
7 FHIR Mapping
Map healthcare data into standardized FHIR resources
Example resources include:
Patient Resource
Observation Resource
DiagnosticReport Resource
Medication Resource
8 FHIR Structure Generation
Construct structured FHIR record
9 Schema Validation
Validate generated record against FHIR data schema
10 Secure Data Delivery
Deliver FHIR-compliant healthcare record to authorized user
11 Audit Logging
Record access activity in blockchain audit log
12 Return FHIR Record

system recovers the encrypted healthcare information of the patient identifiable in blockchain-linked storage. Decryption of the data and its mapping to Fast Healthcare Interoperability Resources (FHIR) structures: Patient, Observation, Diagnostic Report. This procedure allows interoperable data sharing amongst disparate health systems as well as maintaining the safety and integrity of data.

4 Experimental Setup and Result Analysis

In order to measure the efficiency of the presented framework, the experimental environment was created to model the scenario of an Internet of Medical Things (IoMT) healthcare system with blockchain and post-quantum cryptography tools, which is secure. The experiments aimed at examining the computational efficiency of post-quantum cryptographic algorithms, the system latency under conditions of secure transmission of healthcare data, and the viability of privacy-preserving access control in the blockchain-based architecture. It was implemented on a local computing environment, which was running Windows 11, has Intel Core i5 (3.0 GHz) processor, 16 GB RAM, and 512 GB SSD. The proposed structure was realized with Python and blockchain nodes were hosted in permissioned network to simulate distributed verification and healthcare data storage. Open-source PQC libraries that implement Kyber and NTRU in key encapsulation and encryption, Dilithium and Falcon in digital signature generation and verification were used to implement post-quantum cryptographic operations. These algorithms were chosen because they are identified during the NIST Post-Quantum Cryptography standardization procedure and because they can be used in resource-constrained IoMT environments.

To recreate the aspect of real-time healthcare data creation, a series of software-defined IoMT sensors were created to produce physiological data including heart rate, ECG signals and glucose levels. All records generated were based on the Fast Healthcare Interoperability Resources (FHIR) standard so that they could be compatible with healthcare information systems. The simulated IoMT devices have relayed encrypted electronic medical records to the blockchain network, with the transactions being verified and stored in the distributed registry. An access control mechanism that preserves privacy was introduced based on the Zero-Knowledge Proof (ZKP) authentication scheme and the role-based access control policies were applied based on the blockchain smart contracts. The patient records requested by the healthcare providers had to produce cryptographic proofs that proved their authorization. The smart contract established the validity and allowed the access before storing the requests as an unchangeable audit trail in the blockchain.

The experimental assessment was aimed at the measurement of key performance measures that are applicable to healthcare IoMT security systems. These measures were encryption and decryption time, key-generation overhead, and time of verifying digital signatures, and the time it takes to perform a transaction in the blockchain when storing and retrieving values in the storage. The experimentation was performed under varying loads of the transaction in order to examine the system scalability and testing the feasibility of practicality of post-quantum cryptography, privacy-preserving authentication and blockchain-based data management integration into secure IoMT healthcare settings.

4.1 Post-Quantum Cryptographic Performance Metrics and Analysis

Cryptographic layer of framework provides security in the transmission as well as authentication of the data using post-quantum encryption functions and digital signature functions. In particular, Kyber and NTRU are encryption-based, and Dilithium and Falcon are applicable to the digital signature. All these algorithms guarantee security in the long term against quantum capable adversaries. To determine their efficiency, this section will analyse some of the most important cryptographic operations, such as encryption and decryption time, key generation overhead, and signature verification performance. The major performance indicators that will be used in this assessment are;

i *Encryption and Decryption Time (Te, Td):* Measures the computational cost of encrypting and decrypting IoMT-generated healthcare data.
ii *Key Generation Time (Tk):* Represents the time required to generate public–private key pairs.
iii *Signature Verification Time (Tv):* Indicates the efficiency of validating digital signatures during device authentication or user verification.

Kyber and NTRU differ in their underlying mathematical structures, which directly affect computational complexity. Kyber is based on the Module Learning With Errors (MLWE) problem and utilizes the Number Theoretic Transform (NTT) to accelerate polynomial multiplication. This approach significantly reduces encryption and decryption costs, making Kyber suitable for resource-constrained IoMT environments. The complexity of Kyber encryption and decryption is:

$$Te(Kyber) = O(nlogn),\ Td(Kyber) = O(nlogn) \quad \ldots (1)$$

In contrast, NTRU relies on polynomial ring structures and convolution operations. Although it offers strong security guarantees, its encryption complexity can be comparatively higher for certain parameter sets.

$$Te(NTRU) = O(n^2),\ Td(NTRU) = O(n) \quad \ldots (2)$$

Experimental results obtained from the implementation show encryption and decryption times of 1.1 ms and 0.9 ms for Kyber, and 2.0 ms and 0.7 ms for NTRU, respectively as shown in Fig. 4. The figure highlights that practical system-level deployment introduces manageable overhead while maintaining feasible cryptographic performance for real-time healthcare communication. These values are slightly higher than benchmark results reported in isolated studies (Kyber: 0.20/0.25 ms, NTRU: 0.25/0.20 ms) Chen (2022)[23].

The observed differences arise because this system evaluates cryptographic operations within a full-stack IoMT environment, which includes several additional processing layers such as:

i TLS 1.3 with Kyber-KEM for quantum-secure communication sessions.
ii FHIR-based interoperability validation for healthcare data.
iii Real-time message serialization and API interactions.

These components introduce additional overhead but are essential for ensuring interoperability, security, and regulatory compliance in real-world healthcare systems. Consequently, the measured results represent practical system performance rather than isolated cryptographic benchmarks. These

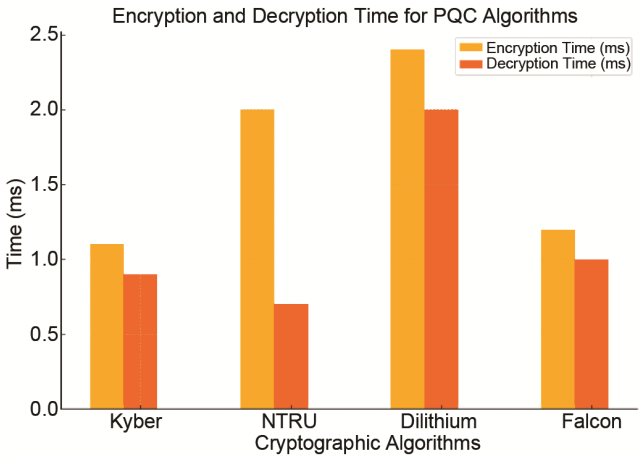

Fig. 4 — Encryption and Decryption Time for Post-Quantum Cryptographic Algorithms

findings demonstrate that the proposed framework can integrate post-quantum cryptographic protection within practical IoMT healthcare environments while maintaining acceptable computational performance. This is particularly important for latency-sensitive medical applications, where secure real-time communication and interoperability must be achieved without introducing excessive processing delays.

4.2 Key Generation Efficiency

Key generation is particularly important in IoMT environments due to limited computational resources. For lattice-based cryptographic schemes, key generation complexity can be expressed as:

$$Tk = O(n^2) \quad \ldots (3)$$

Experimental results as shown in Fig. 5 from KB-IoMT show Kyber and NTRU requiring 1.8 ms and 2.2 ms, respectively. Fig 5 demonstrates that the proposed framework can support efficient post-quantum key generation despite additional network and interoperability overheads in practical IoMT deployments. References in the literature indicate the generation of the Kyber key at 0.15 ms and NTRU at 0.20 ms[23]. These differences arise due to overhead from Python-based APIs, network latency, and system-level interactions in our real-time environment.

The obtained results indicate that the proposed framework can efficiently support post-quantum key management operations within practical IoMT healthcare systems despite additional real-world deployment overheads. Efficient key generation is essential for enabling secure session establishment, device authentication, and continuous healthcare data exchange in resource-constrained and latency-sensitive medical environments.

4.3 Digital Signature Performance

The system uses Dilithium and Falcon for digital signatures. Falcon employs FFT-based sampling, which provides efficient verification complexity.

$$Tv = O(n\log n) \quad \ldots (4)$$

Verification times recorded in KB-IoMT were 2.5 ms (Dilithium) and 0.7 ms (Falcon) as shown in Fig. 6, compared to 1.10 ms and 0.15 ms respectively in benchmark environments[24]. The Fig. 6 further indicates that Falcon achieves lower verification latency compared to Dilithium, making it suitable for latency-sensitive healthcare authentication scenarios. The slightly higher values in our results reflect the additional consensus, transaction logging, and cryptographic integration into the blockchain workflow. This is particularly significant for healthcare IoMT environments where rapid and trustworthy authentication of medical transactions is necessary to maintain data integrity, secure clinical communication, and timely healthcare decision-making without compromising long-term quantum resistance.

The results summarized in Table 3 demonstrate that the proposed framework achieves practical post-quantum cryptographic performance suitable for secure IoMT healthcare applications. Although the observed execution times are slightly higher than standalone benchmark values, the increase reflects the integration of cryptographic operations with blockchain validation, networked transaction signing, and real-time device authentication. These results

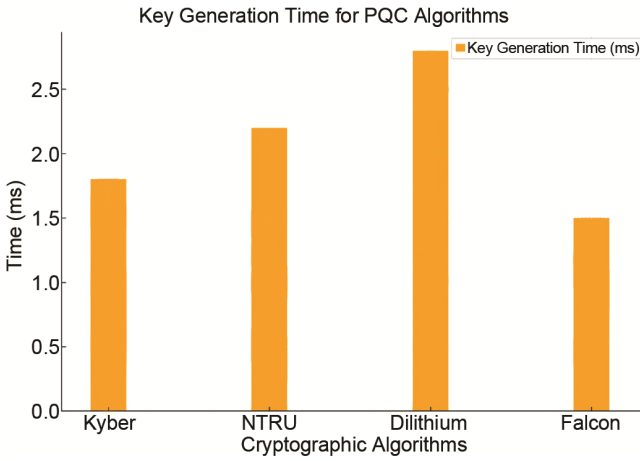

Fig. 5 — Key Generation Time for Post-Quantum Cryptographic Algorithms (Kyber, NTRU)

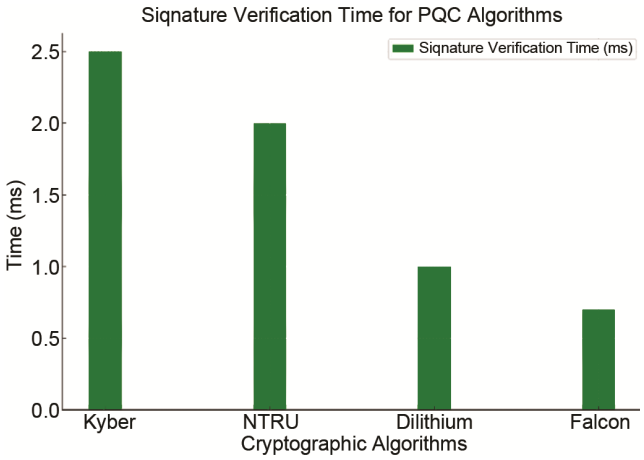

Fig. 6 — Signature Verification Time for Post-Quantum Cryptographic Algorithms (Dilithium, Falcon)

Table 3 — Performance Comparison of PQC Schemes

Metric	KB-IoMT Implementation	Reference Values
Encryption Time (ms)	Kyber: 1.1; NTRU: 2.0	Kyber: 0.20; NTRU: 0.25 [23]
Decryption Time (ms)	Kyber: 0.9; NTRU: 0.7	Kyber: 0.25; NTRU: 0.20 [23]
Key Generation Time (ms)	Kyber: 1.8; NTRU: 2.2	Kyber: 0.15; NTRU: 0.20 [23]
Signature Verification Time (ms)	Dilithium: 2.5; Falcon: 0.7	Dilithium: 1.10; Falcon: 0.15 [24]

therefore represent realistic system-level performance when post-quantum security, FHIR-based inter-operability, and blockchain infrastructure operate together.

4.5 Blockchain Consensus and Scalability Analysis

The transaction finality time T_f in the Practical Byzantine Fault Tolerance (PBFT) consensus mechanism can be expressed as the sum of three major components: network propagation delay, computation delay, and consensus delay.

$$T_f = T_{network} + T_{computation} + T_{consensus} \quad \ldots (5)$$

Here, $T_{network}$ represents the time required for messages to propagate across blockchain nodes, $T_{computation}$ denotes the time required for cryptographic verification of transactions, and $T_{consensus}$ corresponds to the delay introduced by PBFT consensus rounds. The traditional PBFT protocol in experimental testing on a locally-deployed testing blockchain based on Python, demonstrates the ability to execute about 500 transactions per second (TPS). With the addition of sharding and Layer-2, the throughput can be boosted to around 1500-1700 TPS with simulated *conditions*. A maximum throughput of 2300 TPS was achieved at controlled workloads and small network latencies and transaction payloads as indicated in Fig. 7 shows that sharding and Layer-2 mechanisms significantly improve scalability and responsiveness compared to traditional PBFT implementations. Smaller blockchain networks with fewer than 10 nodes recorded transaction finality of about 50-70 ms, but these latency values could rise in larger or more heterogeneous IoMT settings. In general, the suggested framework exhibits much higher throughput and latency characteristics than traditional blockchain-based infrastructures like Ethereum and Hyperledger Fabric, and it is evident that PBFT-based designs can be employed to provide the best response time to IoMT healthcare applications at the cost of security and computational resources. The results further indicate that PBFT-based blockchain architectures, when enhanced with sharding and Layer-2 mechanisms, can provide

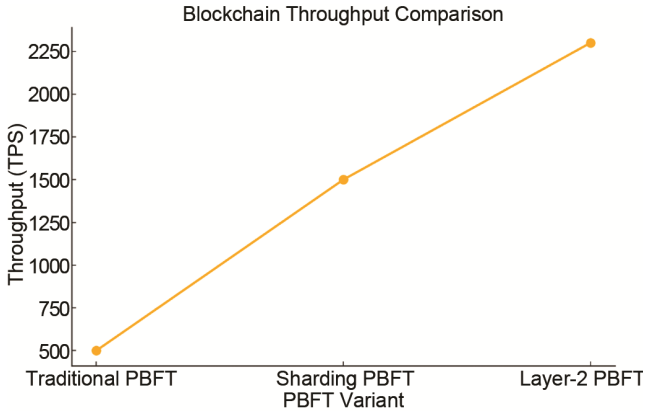

Fig. 7 — Blockchain Throughput Comparison (TPS) for PBFT Variants

scalable and responsive healthcare data management while maintaining strong security.

4.6 Scalability Factor Analysis

Scalability is a critical factor in blockchain deployment for real-time applications such as the Internet of Medical Things (IoMT). The scalability factor S_f is defined as the ratio between the throughput of the optimized system and that of the traditional implementation.

$$S_f = \frac{TPS_{Optimized}}{TPS_{Traditional}} \quad \ldots (6)$$

Experimental findings show that the framework has a scaling factor of about 4.5x of the traditional PBFT implementation. Much of this improvement is due to the inclusion of sharding mechanisms that in itself can add about 2.8× scalability by spreading the transaction processing load among several blockchain partitions. The other performance enhancement is by means of optimized consensus communication and an efficient integration of data streaming. These findings show that the proposed architecture is able to adequately sustain the large transaction throughput demanded by real-time IoMT healthcare settings as shown in Fig. 8. The figure highlights the effectiveness of distributed transaction processing in improving scalability for large-scale IoMT healthcare environments. This scalability improvement is particularly important for large-scale healthcare

infrastructures involving continuously connected IoMT devices, where increasing patient data volume and simultaneous medical transactions require efficient and responsive blockchain-based processing without significant performance degradation.

4.7 Fault Tolerance Analysis

The experimental results emphasize the effectiveness of integrating lattice-based cryptography with blockchain for securing IoMT transactions. The KB-IoMT system achieves robust quantum-resistant security, high transaction throughput, and improved scalability, making it a viable and efficient solution for secure healthcare data exchange in post-quantum environments as shown in Fig. 9. All performance evaluations were conducted on a single-machine, multi-process simulation using Python with synthetic data generation.

Although the setup reflects the intended interaction patterns and cryptographic workflows, large-scale deployment in real-world heterogeneous networks (e.g., with Raspberry Pi or embedded IoMT devices) may exhibit different results. This scalability improvement is particularly important for large-scale healthcare infrastructures involving continuously connected IoMT devices, where increasing patient data volume and simultaneous medical transactions require efficient and responsive blockchain-based processing without significant performance degradation. Future testing in distributed environments with real hardware and network latencies will provide further validation.

4.8 Security Analysis

The security evaluation of this system focuses on its ability to protect IoMT-generated medical data against various cyber threats, as illustrated in Fig. 10. To address the risk of quantum attacks, the system uses lattice-based cryptographic algorithms whose security relies on hard mathematical problems such as the Shortest Vector Problem (SVP) and Closest Vector Problem (CVP), which remain infeasible to solve even with quantum computers.

To prevent Man-in-the-Middle (MITM) attacks, the framework employs TLS secured with the Kyber Key Encapsulation Mechanism (KEM), ensuring quantum-resistant communication between IoMT devices and blockchain nodes. Sybil and replay attacks are mitigated using the PBFT consensus mechanism, which validates transactions across distributed nodes and prevents malicious participants from gaining control or reusing previous transactions. PBFT is

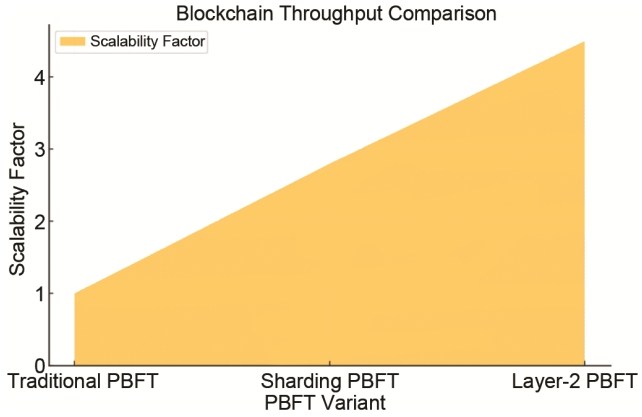

Fig. 8 — Blockchain Scalability Factor Comparison

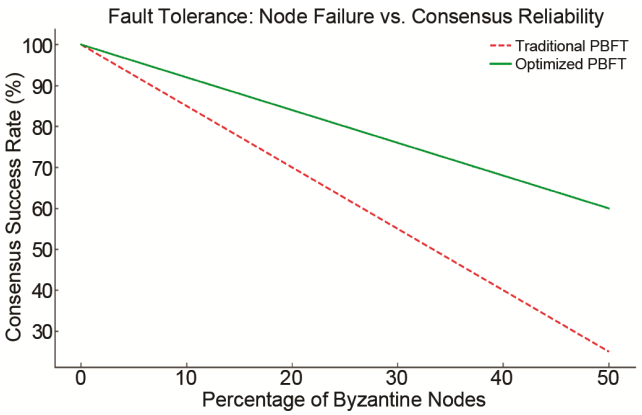

Fig. 9 — Fault Tolerance: Node Failure vs. Consensus Reliability

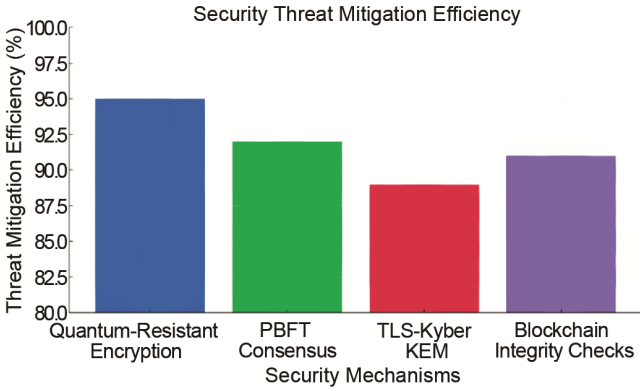

Fig. 10 — Security Threat Mitigation Efficiency

preferred over PoS-based approaches because it provides deterministic finality and strong tolerance to malicious nodes, which is essential for maintaining healthcare data integrity. Sharding is also implemented in the system to enhance scalability, spreading the transaction workloads on several partitions to boost the throughput by a long way without huge latency overhead. Also cryptographic integrity checks with consensus validation safeguard

the network against double-spending as well as Byzantine node failure such that transactions are safe and resistant to alteration in the distributed ledger.

4.9 ZKP Access Control Performance and FHIR Interoperability Evaluation

The privacy-preserving authentication mechanism based on Zero-Knowledge Proofs was evaluated by measuring the computational overhead introduced during authorization requests. The results indicate that the proof verification process introduces only minor processing delay compared to traditional authentication methods. Since the verification occurs through smart contracts, the additional overhead remains manageable and does not significantly affect system responsiveness. To evaluate interoperability, healthcare records generated by IoMT devices were converted into FHIR-compliant data structures such as Patient, Observation, and Diagnostic Report resources. The generated records were successfully validated against FHIR schemas, demonstrating the capability of the framework to support standardized healthcare data exchange across heterogeneous systems.

5 Discussion

The development of post-quantum cryptography (PQC) in blockchain technology can greatly increase security through its ability to introduce resilience. The proposed system uses lattice-based cryptographic schemes like Kyber, NTRU, Dilithium, and Falcon to provide confidentiality, authentication and integrity in IoMT transactions. The findings suggest that although PQC enhances security assurances, it also creates computational overhead, which can affect the performance of a system. Nevertheless, the overheads are being countermeasure by the optimizations of PBFT, such as sharding, and Layer-2 solutions, ensuring high throughput and low latency and reducing the risk posed by a quantum threat to the network. As demonstrated by the analysis of the experiment, the KB-IoMT system continues to provide the best performance in terms of transaction finality and scalability with PQC-related overheads through the processing of parallel consensus and off-chain execution of transactions.

Despite the security and interoperability advantages offered by the proposed framework, practical IoMT deployments may face several operational constraints. Many IoMT devices possess limited computational capability, memory resources, and battery power, which can affect the execution efficiency of advanced cryptographic operations, particularly post-quantum algorithms and blockchain-related processes. Additionally, healthcare IoT environments often experience network variability, bandwidth fluctuations, and intermittent connectivity that may influence real-time data synchronization and transaction propagation. Although the proposed Kafka-assisted architecture helps reduce communication latency and improve data streaming efficiency, lightweight optimization and adaptive resource-management strategies may still be required for large-scale deployments involving highly constrained edge devices. These considerations highlight the importance of balancing security, scalability, and computational efficiency in practical IoMT ecosystems.

The practicability of the proposed framework deployment in the real world raises other concerns. It needs effective data transmission protocols and FHIR compatibility to be integrated with blockchain and IoMT devices to ensure a smooth integration with healthcare infrastructures. Network issues, resource usage within the IoMT devices, and regulatory processes become obstacles that must be overcome in order to implement the same practically. Also, the cross-platform compatibility and standardized cryptographic frameworks should be investigated to facilitate its adoption. The future outlook of this study consists of additional optimization of PQC algorithm to improve the efficiency of computations with the preservation of strong security models. The incorporation of AI-based anomaly detection mechanisms might significantly enhance the ability to detect threats and make the system flexible to react in advance to the threat. Moreover, a further provision of the FHIR standard to be integrated seamlessly with the blockchain would contribute to the increased applicability of the system to the real-world healthcare environment, as it would provide the standardization of the data exchange, better interoperability, as well as greater security to the operations of electronic health records management. Generally, this system is a scalable, secure, and quantum-resistant architecture of the future of healthcare blockchain applications, and the further development of cryptographic optimization and AI-assisted security measures is likely to enhance the performance and adoption.

6 Conclusion

This study presents a secure blockchain-enabled framework for Internet of Medical Things (IoMT)

healthcare systems that integrates post-quantum cryptographic mechanisms, privacy-preserving access control, and standardized healthcare data interoperability. The proposed architecture employs lattice-based cryptographic algorithms, including Kyber and NTRU for secure key encapsulation and encryption, and Dilithium and Falcon for digital signatures, ensuring long-term protection of electronic health records against emerging quantum computing threats. The framework provides tamper-resistant storage, data integrity, and transparent verification of transaction records of healthcare data produced by the IoMT devices by integrating these quantum-resistant mechanisms and blockchain-based data management. Besides this the combination of Zero-Knowledge Proof (ZKP)-based authentication and role-based access control allows sharing of data in a secure and privacy-respecting way among the authorized organizations in the healthcare industry. The proposed framework distinguishes itself from existing approaches through the unified integration of quantum-resistant cryptography, decentralized privacy-preserving authentication, blockchain-based healthcare security, and standardized interoperability support for IoMT ecosystems.

Moreover, the implementation of Fast Healthcare Interoperability Resources (FHIR) standard simplifies exchange of structured and interoperable healthcare data using the heterogeneous medical systems. Through experimental analysis, the proposed framework has been shown to support effective cryptographic performance at the same time ensuring a high level of security that is appropriate in actual IoMT healthcare setting. In general, the suggested architecture provides a quantum resistant and scalable solution to secure healthcare data management that incorporates the blockchain immutability, post-quantum cryptography protection, privacy preserving authentication, and interoperable healthcare data exchange. The next step in the future is to make optimization of the implementation of post-quantum cryptography and develop intelligent security protocols in order to make blockchain-based healthcare infrastructures even more robust and scalable.

References

1 Kumar A, Gupta R, Kumar S, Dutta K & Rani M, *Securing IoMT-Based Healthcare System: Issues, Challenges, and Solutions*, Artificial Intelligence and Cybersecurity in Healthcare, (2025) 17–56.

2 Nasayreh A, Khalid H M, Alkhateeb H K, Al-Manaseer J, Ismail A & Gharaibeh H, *Comput Secur*, 150 (2025) 104288.

3 Chaurasia B K, Tiwari N & Pateria N, *Sci Rep*, 16 (2026) 14581.

4 Verma A, Tiwari N & Chourasia B K, in *2024 IEEE International Conference on Intelligent Signal Processing and Effective Communication Technologies (INSPECT)*, IEEE, (2024) 1–6.

5 Tiwari N, Ranjan P, Biswal P K *et al*., *Multimed Tools Appl*, 84 (14) (2025) 13571.

6 Sahraoui S & Bachir A, *Digit Commun Netw*, 11 (4) (2025) 1246.

7 Yalamuri G, Honnavalli P & Eswaran S, *Procedia Comput Sci*, 215 (2022) 834.

8 Jenefa A, Josh F, Taurshia A *et al*., *Proc 2nd Int Conf Automation, Computing and Renewable Systems (ICACRS)*, IEEE, (2023) 1799–1804.

9 Gitonga C K, *Eur J Inf Technol Comput Sci*, 5 (2025) 1.

10 Saripalle R, Runyan C & Russell M, *J Biomed Inform*, 94 (2019) 103188.

11 Saini V, Reddy S G, Kumar D *et al*., *IoT Edge Comput J*, 1 (2021) 28.

12 Wazid M, Nautiyal S, Das A K *et al*., *Security Privacy*, 8 (2025) e468.

13 Xu T, Zhu G, Zhao L *et al*., *Proc Int Conf Power, Electrical Engineering, Electronics and Control (PEEEC)*, IEEE, (2024) 568–573.

14 Agrawal A K & Bharti M, in *Harnessing the Internet of Things (IoT) for a Hyper-Connected Smart World* (Apple Academic Press), (2022) 243–258.

15 Shi G, Qi M, Zhong Q *et al*., *Sensors*, 25 (2025) 1857.

16 Pelekoudas-Oikonomou F, Zachos G, Papaioannou M *et al*., *Sensors*, 22 (2022) 2449.

17 Wazid M & Gope P, *ACM Trans Internet Technol*, 23 (2023) 1.

18 Awan S M, Azad M A, Arshad J *et al*., *Information*, 14 (2023) 129.

19 Al-Doori M J & Al-Gailani M F, *Int J Intell Eng Syst*, 16 (5) (2023) 462.

20 Yuan B, Wu F & Zheng Z, *PLoS One*, 18 (2023) e0279429.

21 Carter G, Chevellereau B, Shahriar H *et al*., *Blockchain Healthc Today*, 3 (2020) 1.

22 Agrawal A K, *Advances Manuf Ind Eng*, (2021) 975.

23 Chen A C H, Cryptology ePrint Archive, Paper 2022/1619, (2022).

24 Vidaković M & Miličević K, *Algorithms*, 16 (2023) 518