IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 22 September 2024, accepted 24 November 2024, date of publication 9 December 2024,
date of current version 26 December 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3513153

RESEARCH ARTICLE

Hyperledger Fabric-Based Post Quantum Cryptography for Healthcare Application Using Discrete Event Simulation

TAMARA ZHUKABAYEVA[1], (Member, IEEE), ATEEQ UR REHMAN[2], (Member, IEEE), NARGIS TARIQ[3], (Member, IEEE), AND ELHADJ BENKHELIFA[2], (Senior Member, IEEE)

[1]Faculty of Information Technology, L. N. Gumilyov Eurasian National University, Astana 010000, Kazakhstan
[2]Department of Computing, Smart Systems, AI, and Cybersecurity Research Centre, University of Staffordshire, ST4 2DE Stoke-on-Trent, U.K.
[3]Department of Information Technology, The University of Haripur, Haripur 22620, Pakistan

Corresponding author: Elhadj Benkhelifa (e.benkhelifa@staffs.ac.uk)

This work was supported by the Science Committee of the Ministry of Education and Science of the Republic of Kazakhstan under Grant AP23489127.

ABSTRACT The centralized data sharing challenges in healthcare have spurred the adoption of distributed methods, including blockchain technology, to enhance security and privacy. This paper proposes a blockchain-based healthcare system leveraging post-quantum cryptography (PQC) to secure sensitive patient data, stored on a permissioned blockchain. Discrete event simulation (DES) is used in the simulation to represent and assess three critical processes: blockchain transactions, patient data requests, and data encryption. We examine the dynamics of blockchain transaction processing, encryption effectiveness, and data access inside the suggested architecture through simulation. The results highlight how post-quantum encryption and blockchain technology can strengthen healthcare data management by resolving important concerns about patient data sharing's integrity and confidentiality.

INDEX TERMS Hash-based cryptography, post-quantum cryptography, healthcare, IoT and the Hyperledger fabric.

I. INTRODUCTION

The healthcare sector is one of the most critical industries today, requiring robust security measures to protect sensitive data, particularly electronic health records (EHRs). EHRs have revolutionized healthcare by enabling digital data storage and controlled data access, resulting in improved efficiency and quality of care [1], [2]. Blockchain technology, with its decentralized data storage and tamper-proof features, has emerged as a powerful tool for securing EHRs. However, its adoption in healthcare faces challenges related to scalability, privacy, and security [3].

With the advent of quantum computing, new vulnerabilities have been introduced, as traditional cryptographic techniques may no longer offer adequate protection. Post-quantum cryptography (PQC) has gained significant attention as a means to address these challenges, creating opportunities for more secure and efficient systems in the healthcare sector [4]. To protect systems against such attacks, quantum computation and lattice-based cryptography are utilized [1]. The Verilog programming language and Zynq UltraScale FPGAs are used to revise the lattices based on the third round of the NIST PQC standardization process, providing a more secure solution [5]. Similarly, combining the CRYSTAL-Kyber and ASCON algorithms strengthens IoMT against quantum threats, demonstrating efficacy in real-world healthcare settings [6]. A framework using quantum-safe blockchain is a suitable option for securely and efficiently storing and accessing EHRs, even in systems with hundreds of thousands of users [1].

In this regard, the MediSecureNet model has been proposed as a secure healthcare solution that integrates

The associate editor coordinating the review of this manuscript and approving it for publication was Razi Iqbal.

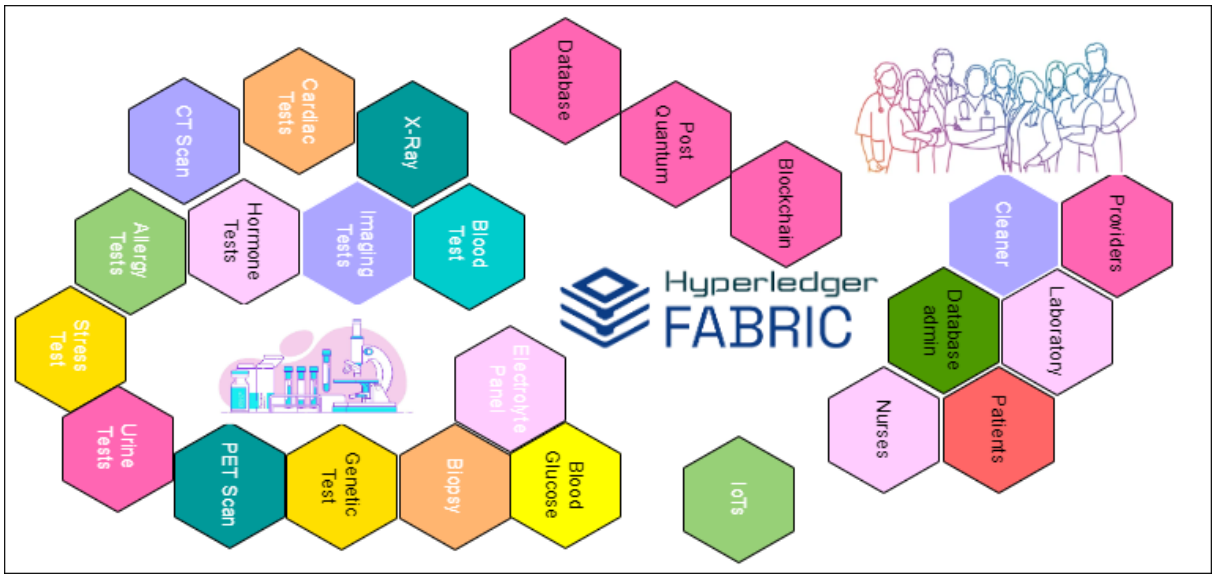

FIGURE 1. Hospital staff managing different diseases with the help of quantum computing and blockchain.

blockchain with IoT medical equipment [7]. Additionally, an algorithm that integrates federated learning (FL) and blockchain (BC) technologies has been suggested to tackle privacy and security issues in IoT-enabled healthcare scenarios [8]. Blockchain platforms also address data protection concerns by leveraging patient health information from other applications to deliver smart health services in smart city settings [9]. Moreover, in [10], the authors proposed a hospital system with several branches across the nation, enabling effective communication between patients and physicians while allowing data access at any time through a cloud-based paradigm. Considering quantum as an alternate solution, Routary et al. in [11] proposed a solution for quantum-based cryptography for IoTs using physical layer security detection. In parallel, [12] analyzed various research gaps and their solutions, focusing on the latest trends in quantum computing. Advancements such as a deep reinforcement learning (DRL)-based Lyapunov approach for computation offloading and latency minimization have also been introduced [13]. Blockchain has further been leveraged for early detection of diseases, as demonstrated by [14], who used machine learning algorithms for diabetes detection. A novel architecture combining decentralized Ethereum and centralized Hyperledger Fabric (Eth-Fab) with SQLite has been proposed to secure patient healthcare data by integrating Ethereum smart contracts with Hyperledger's permission model [15].

To further advance these developments discussed above and in Table. 1, this contribution introduces a novel framework for securing hospital data by using a post-quantum hash-based algorithm, ensuring robust encryption that is resistant to quantum computing attacks. The proposed system integrates PQC with a blockchain-based hospital database, combining advanced cryptographic techniques with the scalability and efficiency of blockchain technology. The framework is designed to enhance healthcare data security, storage, and accessibility while addressing the limitations of existing solutions.

Key contributions of this work include the implementation of a hybrid blockchain architecture that combines PQC with the Hyperledger Fabric platform for secure and efficient medical records management. The system's performance and scalability are validated using Discrete Event Simulation (DES), which models the interactions and dynamic behavior of system components over time. Additionally, comprehensive security and performance assessments demonstrate significant improvements in data protection without compromising the blockchain network's efficiency. This framework represents a significant advancement in ensuring secure and scalable healthcare data management in the face of emerging quantum computing threats.

Our primary contributions are as follows:

- **Integration of Post-Quantum Cryptography (PQC):** To enhance security against potential attackers, we utilized a post-quantum hash-based encryption technique for hospital data. This ensures that personal health information remains secure even in the presence of quantum computing threats.
- **Hyperledger Fabric Implementation:** The encrypted data is integrated into the Hyperledger Fabric blockchain platform. Hyperledger Fabric's permissioned and modular architecture ensures secure and efficient management of medical records within a blockchain framework. This approach guarantees data accessibility, confidentiality, and integrity within a managed provider network.
- **Discrete Event Simulation (DES):** We employed Discrete Event Simulation (DES) to evaluate the effectiveness and feasibility of our proposed approach. DES allowed us to model various system components, including their interactions and dynamic behaviors

over time. Through this simulation, we validated the performance, scalability, and security of our approach.

- **Blockchain Framework:** Our method leverages a hybrid blockchain architecture that combines post-quantum cryptographic (PQC) techniques with the capabilities of Hyperledger Fabric. This hybrid design addresses critical requirements in the healthcare industry, such as scalability, interoperability, and data security.
- **Enhanced Security and Performance Metrics:** To evaluate the security and functionality of our system, we conducted comprehensive assessments. The results demonstrate that our post-quantum encryption technique significantly enhances data security without compromising the efficiency of the blockchain network. Additionally, discrete event simulations further validate the stability and applicability of our proposed solution.

II. ORGANIZATION

In this paper, we discuss the use of quantum computing in healthcare in Section III. System architecture in Section IV, followed by the mathematical formulation in Section 1. The proposed model methodology and experimental results and analysis are presented in Section VI, and then we presented discussion on the proposed model with future research direction in Section VII with conclusion in Section VIII.

III. QUANTUM COMPUTING IN HEALTHCARE

This section highlights the current advancements and efforts in integrating quantum computing into healthcare research. Quantum computing, although compact in size compared to traditional computing systems, is about the size of a car due to the inclusion of superconductive processors and cooling systems. It uses qubits for complex computations, making it especially suitable for high-risk and sensitive fields like healthcare. As the healthcare industry evolves rapidly, medical professionals increasingly rely upon and utilize more complex frameworks to analyze patient clinical data, quickly and efficiently.

The integration of quantum computing into healthcare holds transformative potential, particularly for diagnostic processes involving vast amounts of data and complex analysis. The variety and complexity of diagnostic tests performed in hospitals depend on the patient's symptoms, medical history, and suspected condition. Quantum computing enhances the efficiency, accuracy, and speed of these tests, addressing the limitations of classical computing systems. This section provides an overview of common diagnostic tests in hospitals and explores how quantum computing can optimize these processes.

A. BLOOD TESTS

Blood tests are fundamental in diagnosing various conditions in patients. Key tests include:

1) COMPLETE BLOOD COUNT (CBC)

By increasing the speed of analyzing volumes of data in the CBC, quantum computing can help in matching cells to conditions like anemia or infections. Several demonstrative QML algorithms show that in comparison with the classical methods, certain blood disorders could be classified and predicted more quickly and effectively.

2) BLOOD GLUCOSE TEST

In diabetic treatment, quantum algorithms improve the modeling of blood sugar level changes during treatment, hence improving treatment planning. Quantum signal processing can also detect multiple correlations between multiple biomarkers that affect glucose levels, thereby giving a better understanding of diabetes.

3) LIVER AND KIDNEY FUNCTION TESTS

Advanced biochemical analysis with the application of quantum computing improves the assessment of liver and kidney function by processing high volumes of data. Quantum algorithms can simulate the molecular interactions in these organs and analyze their response to different diseases and treatments.

4) LIPID PROFILE

Quantum computing can improve lipid profile analysis by quickly capturing minor shifts in cholesterol and triglyceride levels that may point to cardiovascular diseases. As a result, it is possible to implement more individualized approaches to heart disease prevention.

5) THYROID FUNCTION TESTS

Quantum simulations can model hyperactive hormone functioning in the thyroid gland, gaining additional insights into thyroid disorders. It allows the prediction of models, and understanding of treatment-induced hormonal changes, and permits more tailored therapeutic approaches.

6) ELECTROLYTE PANEL

Increased precision in the measurement of electrolytes provides a better understanding of symptoms associated with hydration, kidney disorders, and overall heart health. New quantum algorithms are related to biochemical interactions that may affect the electrical properties of materials.

7) INFECTION MARKERS (CRP, ESR)

Quantum computing processes infection markers faster, allowing the assessment of inflammation or infection levels in a short time. Quantum algorithms can also combine these markers with other diagnoses for a single evaluation of the patient's inflammatory state.

B. IMAGING TESTS

Imaging tests are non-invasive and very essential in diagnosing various diseases due to their ability to show internal body parts.

TABLE 1. Comparison with the Existing Study.

Ref	Year	Main Contributions	Targeted Aspects								Quantum M L	Healthcare	Focus on IoT	Types of Cryptography							Techniques
		Contributions of the existing and our proposed research work		Scalability	Security	Data-set Used	Privacy	Algorithms	Interoperability	Challenges	Hashes				SKC	HASH	AKC	ECC	ZKP	Homomorphic	Others Techniques
[11]	2017	Quantum Cryptography for IoT	✗	✓	✗	✓	✗	✗	✓	✗	No	Yes	Yes	✗	✗	✗	✗	✗	✗	✗	QKD Protocol
[12]	2019	Quantum Computing in Machine Learning	✓	✓	✗	✓	✓	✗	✓	✓	Yes	No	Yes	✓	✓	✗	✗	✗	✗	✗	QML
[16]	2020	Quantum Computing-Inspired Network Optimization for IoT Applications	✗	✗	✓	✗	✗	✗	✗	✗	Yes	No	Yes	✗	✗	✗	✗	✗	✗	✗	DA, DTE
[17]	2022	Patient-Centric Token-Based Healthcare Blockchain using IOMTs	✓	✓	✓	✓	✓	✗	✗	✗	No	No	No	✗	✗	✗	✗	✗	✗	✗	deep learning models
[18]	2023	Improved Healthcare System with Quantum Computing	✗	✓	✓	✗	✓	✗	✗	✗	Yes	Yes	No	✗	✗	✗	✗	✗	✗	✗	Deep Learning Model
[19]	2023	Study on Quantum Computing	✗	✗	✗	✗	✗	✗	✗	✗	Yes	Yes	No	✗	✗	✗	✗	✗	✗	✗	Quantum Jumps
[20]	2023	Quantum Machine Learning in Healthcare: Developments and Challenges	✗	✗	✗	✓	✗	✗	✓	✓	Yes	Yes	Yes	✗	✗	✗	✗	✗	✗	✗	QML
[21]	2023	Quantum Machine Learning Algorithms in Noisy Channels	✗	✗	✓	✗	✓	✗	✗	✗	Yes	No	Yes	✗	✗	✗	✗	✗	✗	✗	Variational UU+ Method
[22]	2024	Quantum Blockchain-Envisioned Security Framework for IoT	✗	✓	✗	✓	✗	✓	✗	✓	Yes	No	Yes	✗	✗	✗	✗	✗	✗	✗	Threat Model
This Paper	**2024**	**Quantum Computing in Healthcare**	✓	✓	✗	✓	✓	✓	✗	✓	Yes	Yes	Yes	✓	✓	✓	✓	✓	✓	✓	**DES Algorithm**

1) X-RAY

Quantum computing saves several hours on X-ray image processing, improving the detection of fractures, infections, or abnormalities. Quantum image processing algorithms produce better images that help physicians enhance diagnostic results.

2) ULTRASOUND

Superposition of several limit conditions allows for higher picture detail and accurate noise elimination methods in ultrasound, improving diagnostic results for abdominal, pelvic, and cardiac scans. It also makes real-time 3D imaging possible, providing a better view of internal organs.

3) CT SCAN (COMPUTED TOMOGRAPHY)

Sophisticated signal processing algorithms implemented with a quantum computer accelerate CT image processing, decrease radiation doses, and increase the accuracy of identifying cancer, infections, and vascular diseases.

4) MRI (MAGNETIC RESONANCE IMAGING)

Quantum computing reduces the time needed to analyze MRI data and compute algorithms for image reconstruction. This leads to shorter scan times, better resolution, and improved visualization of soft tissues, the brain, spinal cord, and joints.

5) PET SCAN (POSITRON EMISSION TOMOGRAPHY)

Quantum machine learning models help diagnose cancer from PET scans and track treatment responses more effectively. This advanced analysis also aids in determining how a tumor will react to treatments like chemotherapy.

C. CARDIAC TESTS

Tissue diseases of the heart can be identified by cardiac tests, which also evaluate the general condition of the organ

1) ELECTROCARDIOGRAM (ECG/EKG)

Quantum computing benefits ECG signal processing by simplifying the identification of arrhythmias and other heart problems. Quantum algorithms can also integrate

ECG information with other diagnostic results for enhanced evaluation of cardiovascular functions.

2) ECHOCARDIOGRAM

This is proved by the enhanced ultrasound imaging which could create better images and a detailed analysis of the structure and functioning of the heart as well as that of the entire echocardiogram. This may be useful in determining heart valve disorders and cardiomyopathy.

3) STRESS TEST

Quantum models can predict the working of the heart under stress in greater detail and even give a better picture of likely cardiac incidents. This simulation capability also means that we can have a better estimate of risk in patient care for their cardiac diseases.

D. RESPIRATORY TESTS

Respiratory tests are essential for assessing lung function and diagnosing respiratory conditions.

1) PULMONARY FUNCTION TESTS (PFTS)

Pulmonary tests are vital in a variety of situations such as the determination of the degree of lung function impairment and the identification of respiratory disorders.

2) CHEST X-RAY OR CT SCAN

Quantum computing can improve the information processing of lung function data; the analysis of lung function will be more accurate and could provide more ways of measuring respiratory capacity. It is also worth mentioning that using quantum algorithms, one can predict the further development of lung illnesses with the help of individual information.

E. GASTROINTESTINAL TESTS

Gastrointestinal tests examine the functioning of the gastrointestinal tract, regularly employing imaging or visual inspection.

1) ENDOSCOPY/COLONOSCOPY

Quantum technology in image processing for endoscopy and colonoscopy improves the accuracy of detecting digestive tract pathologies, aiding in the early diagnosis of diseases like colorectal cancer.

2) STOOL TEST

Quantum methods analyze stool sample data more precisely, diagnosing infections, bleeding, or irregularities in the gastrointestinal tract more efficiently.

3) ABDOMINAL ULTRASOUND OR CT SCAN

Through its application in abdominal imaging, quantum computing also adds to the aspirations of imaging various organs in the tummy such as the liver, gallbladder, pancreas, and intestines in the identification of various ailments.

F. URINE TESTS

Laboratory findings that include chemical, hematology and urinalysis are vital owing to the fact that they give an indication of the state of the kidneys, and infections among others.

1) URINALYSIS

The applications of quantum data analysis allow for a more rapid determination of such inflection points or signs of infection or other abnormalities that may appear in the urinalysis and therefore improving the accuracy and timeliness of its diagnosis.

2) URINE CULTURE

In this case, quantum algorithms can diagnose the general presence of the bacteria in infections associated with the urinary tracts more efficiently than conventional culture tests thus helping enhance the efficiency of treatment decisions.

G. NEUROLOGICAL TESTS

Neurological tests are clinical procedures involving brain and nerve function diagnosis that is inevitable in neurological diseases.

1) EEG (ELECTROENCEPHALOGRAM)

Quantum computing can enhance EEG data analysis, giving doctors and scientists a better understanding of the signals that correspond with diseases such as epilepsy or other neurological disorders.

2) NERVE CONDUCTION STUDIES (NCS)

High speed and high accuracy in data processing can be offered by quantum techniques that will help in the diagnosis of diseases in the peripheral nervous system by assessing the degree/Nerve damage or dysfunction.

H. GENETIC AND MOLECULAR TESTS

Molecular diagnostic tests establish the presence of a health condition genetically or in terms of an infection's molecular structure.

1) GENETIC TESTING

Quantum algorithms can process large genomic datasets more efficiently, enabling faster identification of genetic disorders or predispositions, and paving the way for more personalized medicine.

2) PCR (POLYMERASE CHAIN REACTION)

Quantum computing makes use of genomics in PCR to fasten the three main processes hence minimizing the time taken to diagnose infections.

I. BIOPSY

Tissue examination through biopsy is very crucial in diagnosing cancers and other illnesses.

1) BIOPSY ANALYSIS

In exceptional cases, quantum image processing may help to showcase some of the irregularities on the body tissue samples, thus enabling accurate diagnosis of cancerous cells and subsequent treatment.

J. SPECIALIZED TESTS

Serological tests are those done on body fluids like vaccines or detect a certain disease or evaluate a certain organ system.

1) ALLERGY TESTS

It can also give prompt medical diagnoses in allergy tests since it increases the speed of immune response recognition, towards creating effective treatments.

2) HORMONE TESTS

Quantum data processing may improve the hormone level 'diagnosis,' giving better feedback about the endocrine system and better treatment strategies.

IV. SYSTEM ARCHITECTURE

In order to address data security and privacy issues, we proposed the Hyperledger Fabric-Based PQC Healthcare Application. Fig. 2 demonstrates that the hospital uses post-quantum hash-based cryptography to encrypt its database. Hash-based cryptography appears to be resistant to quantum computing because hash functions are thought to be secure from quantum computers. When given an input (or message), a hash function outputs a fixed-length string of bytes. Every unique input has a unique output, also referred to as a digest or hash value. All the data is sent to Hyperledger Fabric Blockchain.

- **Hospital Database:**In order to prevent unwanted access and guarantee patient privacy, this data contains sensitive information that needs to be protected with strong security measures.
- **Cryptographic Hash Functions:** We used One-Time Signatures (OTS). A pair of public and private keys is generated for each bit of the message to be signed. Each key pair is used only once.
- **Integration of Blockchain:**The Hyperledger Fabric blockchain platform receives the hashed data. Hyperledger Fabric, which has a modular design stores the data and makes sure it is unchangeable and impervious to tampering.
- **Validation and Consensus:** With the use of a consensus process, the network nodes validate the transactions, guaranteeing that only authentic and validated data is added to the blockchain.

A. POST-QUANTUM HASH-BASED CRYPTOGRAPHY

The goal of PQC is to create cryptographic algorithms resistant to attacks from quantum computing systems. Since the security of hash-based cryptography relies on hash function properties. Properties that are difficult for quantum

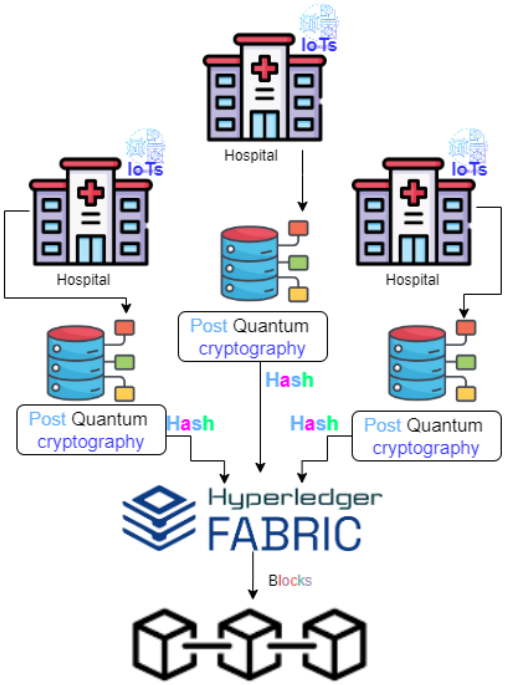

FIGURE 2. Integration of Post-Quantum Cryptography with Hyperledger Fabric Blockchain for Securing Hospital Data.

algorithms to breach. These techniques are seen as excellent candidates for post-quantum security. Types of Hash-Based PQC are:

- Lamport Signatures: One of the earliest forms of digital signatures using hash functions. Although secure, they require large key sizes.
- Merkle Signatures: Use Merkle trees to reduce the key size and allow for multiple signatures.
- SPHINCS: A stateless hash-based signature scheme that provides strong security and efficiency.

1) LAMPORT SIGNATURES

1) Overview: Lamport Signatures are one of the earliest and simplest forms of hash-based digital signatures. They are secure against quantum attacks but suffer from large key and signature sizes, making them less practical for many applications.
2) Mathematical Basis: Lamport signatures work by creating one-time keys for each bit of the message hash.
   a) **Key Generation:**
      - For a message of length n bits, two random values are generated for each bit position, resulting in a private key $SK = (sk_{0,1}, sk_{0,2}, \ldots, sk_{n,1}, sk_{n,2})$.
      - The public key PK is generated by hashing each private key value:

$$PK = (H(sk_{0,1}), H(sk_{0,2}), \ldots, H(sk_{n,1}), H(sk_{n,2})).$$

b) **Signing:**
- The message m is hashed to create a digest h.
- For each bit h_i in the hash:
- If $h_i = 0$, include $sk_{i,1}$ in the signature.
- If $h_i = 1$, include $sk_{i,2}$ in the signature.

c) **Verification:**
- Hash the corresponding private key components in the signature and compare them to the public key.
- If all match correctly, the signature is valid.

3) Mathematical Derivation: The security relies on the one-way property of the hash function H. If an adversary tries to forge a signature, they would need to invert the hash function, which is computationally infeasible.
- Key Size: The public key size and signature size is proportional to the length of the hash function output multiplied by the number of bits in the message digest.

B. MERKLE SIGNATURES

1) Overview: Merkle Signatures use a tree structure to efficiently manage multiple Lamport or other hash-based signatures, allowing for the reuse of a single public key across multiple signatures.
2) Mathematical Basis:

a) **Key Generation:**
- A large number of one-time keys (e.g., Lamport keys) are generated.
- Each key is signed with its corresponding public key.

b) **Merkle Tree Construction:**
- The public keys are used as the leaves of a binary Merkle tree.
- Internal nodes of the tree are created by hashing pairs of child nodes.
- The root node of the tree becomes the overall public key.

c) **Signing:**
- For each message, a one-time key pair is used to create a signature.
- A path from the corresponding leaf to the root is provided, showing that the leaf is part of the tree.

d) **Verification:**
- The signature is verified using the one-time public key.
- The path is checked to ensure the one-time public key was part of the Merkle tree.

3) Mathematical Derivation: The security of the Merkle signature scheme relies on the collision resistance of the hash function used in the Merkle tree. The Merkle tree reduces the overall public key size, allowing for multiple secure signatures with a single root key.
- Key Size: Significantly reduced compared to individual hash-based signatures since a single root key is used for verification.

C. SPHINCS (STATELESS PRACTICAL HASH-BASED INCREDIBLY NICE CRYPTOGRAPHIC SIGNATURE)

1) Overview: SPHINCS is a stateless, hash-based signature scheme that combines Merkle trees and other cryptographic techniques to provide efficient and secure digital signatures without the need for state tracking.
2) Mathematical Basis:

a) **Hybrid Structure:**
- SPHINCS combines multiple layers of hash-based signature schemes (e.g., WOTS - Winternitz One-Time Signature) and a hyper-tree structure.
- It uses Merkle trees, hash chains, and a few-time signature schemes to manage key reuse and provide security.

b) **Key Generation:**
- A large number of keys are generated using a tree structure.
- A main Merkle tree connects lower-level trees, creating a hierarchy.

c) **Signing:**
- The signing process involves creating signatures with several layers of Merkle trees, with each layer reducing the key management overhead.

d) **Verification:**
- Similar to Merkle signatures, verification involves checking signatures against public keys and validating paths in the Merkle tree hierarchy.

3) Mathematical Derivation: SPHINCS provides tight security bounds by combining various forms of hash-based signatures into a single scheme. The security derives from the properties of the underlying hash functions and the hierarchical structure.
- Key Size: SPHINCS significantly reduces key and signature sizes compared to earlier hash-based schemes, balancing efficiency and security.

V. MATHEMATICAL FORMULATION OF BLOCKCHAIN FOR HEALTHCARE SECURITY

Since people are frequently reluctant to share their health details, data security and privacy are vital in the healthcare industry. With a focus on Consensus Algorithm (CA), Transaction Consistency (TC), and Block Attachment (BA), this section presents blockchain in the context of healthcare security. These elements are required to maintain the privacy

and security of blockchain technology used in healthcare.

$$BA = \frac{CA}{TC} \tag{1}$$

The eq. 1 illustrates the collaborative connection between the consensus algorithm and transaction consistency, enabling the secure incorporation of new blocks into the blockchain.

A. TRANSACTION CONSISTENCY

All healthcare blockchain transactions undergo verification and synchronization with every other transaction to ensure transaction consistency, which is essential for block attachment and is maintained through the consensus mechanism.

$$BA = 1 - TC \times 1 - CA. \tag{2}$$

Eq. 2 demonstrates the preservation of the immutability and integrity of the blockchain through the transaction consistency and consensus process.

$$TC = \{t1, t2, \ldots, tn\} \tag{3}$$
$$CA = \{c1, c2, \ldots, cm\} \tag{4}$$
$$BA = \{b1, b2, \ldots, bk\} \tag{5}$$
$$(t1, t2, \ldots, tn) \times (c1, c2, \ldots, cm) \rightarrow (b1, b2, \ldots, bk) \tag{6}$$

Eq.6 depict the preservation of integrity in the Hyperledger Fabric blockchain through the use of transaction consistency and consensus techniques, providing a secure foundation for the exchange and storage of medical data.

B. TRANSACTIONAL INTEGRITY

Blockchain employs a hash-based storing method to safeguard medical data from manipulation and interference.

$$M_{di} = \sum_{H}^{MR_i} \oplus (H(MR_{i-1})) + V \tag{7}$$

Eq. 7 guarantees the confidentiality and authenticity M_{di} of medical data by using XOR operations and hash algorithms.

C. TRANSACTIONAL AUTHENTICITY

The authenticity of medical data is ensured through the use of digital signatures, which involve verifying the identity of the data owner and preventing fraud.

$$M = V(D + S + H(M_R)) \tag{8}$$
$$V(D + S + H(MR)) = H(M_R) == D^S \tag{9}$$

Eq 8 and 9 make use of digital signatures and validation features to guarantee the authenticity of medical data.

D. SYSTEM AND TRANSACTION ACCESSIBILITY

System availability ensures that users can access transaction data at any time, even during large-scale network attacks.

$$\alpha = P(1 - F)\frac{(1 - F + F \times n)}{B^n} \tag{10}$$

Eq 10 shows system-level availability depending on the probability of continued operation during network assaults.

Transaction availability ensures transactions are broadcasted, processed, and stored reliably.

$$\text{Prob}(\gamma = 1 - ((1 - \gamma_c) \times (1 - \gamma_s) \times (1 - \gamma_t))) \tag{11}$$
$$\text{Prob}(\gamma_c = P_{bc} \times P_{ne}) \tag{12}$$
$$\text{Prob}(\gamma_s = P_{vp} \times P_{co}) \tag{13}$$
$$\text{Prob}(\gamma_t = P_{rs} \times P_{ae}) \tag{14}$$

Eq 11, 12, 13, and 14 outline the factors influencing transaction-level availability.

E. ANONYMOUS USERS

Anonymity in medical data transactions is essential to prevent linking medical data to user identities.

$$Prob(P_a = 1 - (P_c \times P_i)) \tag{15}$$
$$Prob(P_c = P_{bc} \times P_{vp} \times P_{co}) \tag{16}$$
$$Prob(P_i = P_{id} \times P_{md}) \tag{17}$$

Equations 15, 16, and 17 show the probability of maintaining user anonymity and preventing identity linkage to medical data.

VI. METHODOLOGY

Privacy for the healthcare sector is essential therefore this study looks into the effectiveness of PQC and blockchain using Discrete event simulation. A useful technique for simulating complex systems is discrete event simulation (DES), especially in blockchain-based healthcare scenarios where events happen at discrete times. We have a hospital that stores data in a database server, where the data is encrypted using PQC techniques based on hash functions. The encrypted data is then sent to a Hyperledger Fabric blockchain.

A. EVENTS

- Patient Data Request (PDR).
- Data Encryption (DE).
- Blockchain Transaction Processing (BTP).

B. KEY PARAMETERS

λ: Rate of patient data requests (requests per unit time).

μ: Rate of data encryption completion (encryptions per unit time).

γ: Rate of blockchain transaction processing (transactions per unit time).

t: Time variable.

N(t): Number of patient data requests at time t.

E(t): Number of data encryptions at time t.

B(t): Number of blockchain transactions at time t.

Algorithm 1 Hospital Data Management Using PQC and Hyperledger Fabric Blockchain

Initialize:
Set $t = 0$
Initialize empty database *DB*
Initialize Hyperledger Fabric blockchain *BC*
procedure StoreAndEncryptData(*patient_data*)
    $t_{request} \leftarrow$ current time
    Step 1: Store Data
    Store *patient_data* in *DB*
    $N(t + \Delta t) \leftarrow N(t) + 1$
    Step 2: Encrypt Data
    encrypted_data $\leftarrow$ HashBasedPQC(*patient_data*)
    $E(t + \Delta t) \leftarrow E(t) + 1$
    Step 3: Send Encrypted Data to Blockchain
    Send *encrypted_data* to *BC*
    $B(t + \Delta t) \leftarrow B(t) + 1$
end procedure
function HashBasedPQC(*data*)
    Input: *data*
    Output: *encrypted_data*
    Apply hash-based PQC technique on *data*
    return *encrypted_data*
end function
Generate Next Events:
Generate next patient data request time t_{PDR} using rate λ
Generate next data encryption time t_{DE} using rate μ
Generate next blockchain transaction processing time t_{BTP} using rate δ
Event Occurrence:
if t_{PDR} is the smallest **then**
    $N(t) \leftarrow N(t) + 1$
    $t \leftarrow t_{PDR}$
end if
if t_{DE} is the smallest **then**
    $E(t) \leftarrow E(t) + 1$
    $t \leftarrow t_{DE}$
end if
if t_{BTP} is the smallest **then**
    $B(t) \leftarrow B(t) + 1$
    $t \leftarrow t_{BTP}$
end if
Repeat: Continue the process until a specified simulation end time is reached.

C. INTERARRIVAL TIME DISTRIBUTION

The interarrival time between patient data requests follows an exponential distribution with rate λ.

$$P(\text{Interarrival time} \leq t) = 1 - e^{-\lambda t} \tag{18}$$

Algorithm 2 Hash-Based Digital Signature Scheme

Initialization:
Choose a secure hash function H
Generate a private key SK consisting of n random bit strings: $SK = (sk_1, sk_2, \ldots, sk_n)$
Compute the public key PK by hashing each bit string in SK: $PK = (H(sk_1), H(sk_2), \ldots, H(sk_n))$
procedure Sign(*message*, *SK*)
    Input: A message *message* and private key *SK*
    Output: A digital signature *signature*
    Compute the hash of the message: $h = H(message)$
    Initialize an empty signature *signature*
    for each bit h_i in h **do**
        if $h_i = 0$ **then**
            Append sk_i to *signature*
        else
            Append an empty string to *signature*
        end if
    end for
    return *signature*
end procedure
procedure Verify(*message*, *signature*, *PK*)
    Input: A message *message*, a digital signature *signature*, and public key *PK*
    Output: Boolean value indicating the validity of the signature
    Compute the hash of the message: $h = H(message)$
    for each bit h_i in h **do**
        if $h_i = 0$ **then**
            if $H(signature_i) \neq PK_i$ **then**
                return false
            end if
        end if
    end for
    return true
end procedure

D. SERVICE TIME DISTRIBUTION FOR DATA ENCRYPTION

The service time for data encryption follows an exponential distribution with rate μ

$$P(\text{Service time} \leq t) = 1 - e^{-\mu t} \tag{19}$$

E. SERVICE TIME DISTRIBUTION FOR BLOCKCHAIN TRANSACTION PROCESSING

The service time for blockchain transaction processing follows an exponential distribution with rate δ:

$$P(\text{Service time} \leq t) = 1 - e^{-\delta t} \tag{20}$$

F. STATE TRANSITIONS

When a patient data request occurs, the state changes as:

$$N(t + \Delta t) = N(t) + 1 \tag{21}$$

Algorithm 3 Event Handling Algorithm

```
Initialize: t = 0, N(0) = 0, E(0) = 0, B(0) = 0
while simulation end time not reached do
    Generate next patient data request time t_PDR using λ
    Generate next data encryption time t_DE using μ
    Generate next blockchain transaction processing time t_BTP using δ
    if t_PDR is the smallest then
        Update N(t)
        Set t = t_PDR
    else if t_DE is the smallest then
        Update E(t)
        Set t = t_DE
    else
        Update B(t)
        Set t = t_BTP
    end if
end while
```

When data encryption is completed, the state changes as:

$$E(t + \Delta t) = E(t) + 1 \tag{22}$$

When a blockchain transaction is processed, the state changes as:

$$B(t + \Delta t) = B(t) + 1 \tag{23}$$

G. PATIENTS DATA REQUEST OVER TIME

Fig. 3 illustrates the cumulative pattern of patient data requests over a 10-hour simulation period. The x-axis represents the simulation time (in hours), while the y-axis shows the cumulative number of requests made during this period. The figure provides a clear graphical representation of how requests accumulate over time in a simulated healthcare environment. Particularly, the stepwise nature of the plot indicates that requests arrive at irregular intervals, consistent with an exponential distribution. Each upward step in the graph represents the arrival of a new patient data request. The varying size of intervals between steps highlights the randomness in the timing of requests. As the simulation progresses, the increasing height of the cumulative line reflects the total number of requests received up to that point in time.

The rate parameter (λ) of the exponential distribution governs the average frequency of these requests. A higher λ value would correspond to a higher rate of incoming requests, while a lower value would indicate more sporadic request arrivals. Fig. 3 is significant as it demonstrates the dynamic and varied nature of patient data requests in a healthcare setting. It captures the intermittent nature of healthcare data demands, reflecting real-world scenarios where such requests occur unpredictably, often depending on patient care needs, emergencies, or routine data checks. The insight gained from this simulation can be used to optimize system design, such as load balancing or resource allocation, ensuring the infrastructure can handle variable data loads efficiently.

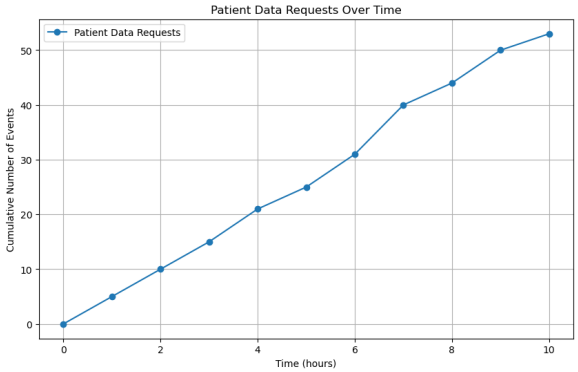

FIGURE 3. The timing and frequency of patient data requests in the simulated healthcare environment.

H. DATA ENCRYPTION OVER TIME

Fig. 4 represents the cumulative progression of data encryption tasks completed during a 10-hour simulation. The x-axis represents the simulation time (in hours), while the y-axis shows the cumulative number of encryption processes completed up to a given time. To be more precise, Fig 4 depicts the timing and frequency of encryption tasks in the simulated healthcare system. Each step in Fig. 4 signifies the completion of an individual data encryption task, reflecting the system's capability to process encryption requests and maintain data security. The intervals between steps are determined by an exponential distribution with a specified rate (μ), which governs the average frequency of encryption processes. A higher rate indicates faster encryption completion, whereas a lower rate suggests a more staggered process. This provides insights into the efficiency and performance of the encryption protocols. The steadily increasing curve highlights the system's capacity to handle encryption requests continuously over time, ensuring that sensitive patient data is securely processed.

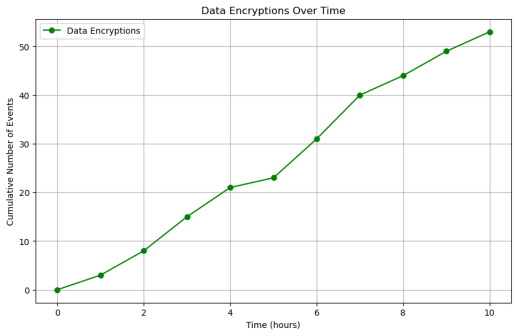

FIGURE 4. The completion times of data encryption processes within the simulated healthcare system.

The analysis shown in Fig. 4 is crucial for evaluating the robustness of encryption protocols within the healthcare simulation. By tracking the timing and rate of encryptions, this graph aids in assessing the impact of these protocols on overall data integrity, confidentiality, and system performance. Such insights are instrumental in optimizing encryption strategies to enhance patient data security in real-world healthcare environments.

I. BLOCKCHAIN TRANSACTION OVER TIME

The interarrival times between patient data requests are exponentially distributed with a mean interarrival time of $\frac{1}{\lambda}$. Similarly, the processes for data encryption and blockchain transactions follow exponential distributions with mean interarrival times of $\frac{1}{\mu}$ and $\frac{1}{\gamma}$, respectively.

Fig. 5 illustrates the cumulative progression of blockchain transactions processed during the simulation. The x-axis represents the simulation time (in hours), while the y-axis denotes the cumulative number of blockchain transactions completed. Each upward step in the figure corresponds to the completion of an individual blockchain transaction, with intervals between steps determined by an exponential distribution governed by the rate parameter γ.

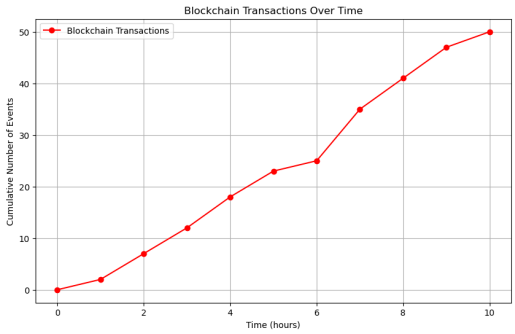

FIGURE 5. The processing times of blockchain transactions in the simulated healthcare context.

Additionally, Fig. 5 also provides insights into the timing and throughput of blockchain transaction processing in the simulated healthcare environment. The stepwise increase highlights the capability of the system to handle transactions at varying intervals, reflecting the randomness and dynamic nature of healthcare data operations. The steadily increasing cumulative curve demonstrates the reliability and scalability of the blockchain infrastructure over the simulation period.

The analysis in Fig. 5 emphasizes the system's efficiency in securely recording and managing healthcare data. By understanding the completion times and throughput of blockchain transactions, this visualization supports the evaluation of blockchain technology's role in healthcare applications, particularly in enhancing data security, transparency, and operational efficiency. Such insights are critical for optimizing blockchain-based solutions in real-world healthcare scenarios.

VII. DISCUSSION AND FUTURE DIRECTION

Our framework uniquely integrates PQC techniques with hospital databases and Hyperledger Fabric, addressing critical gaps in existing blockchain-based healthcare systems. By incorporating PQC, our solution ensures resilience against future quantum computing threats, a significant advancement over traditional cryptographic methods used in systems like MediBloc and Medicalchain. The simulation results confirm the efficiency and reliability of the framework, with patient data requests, encryption processes, and blockchain transactions demonstrating the system's ability to handle dynamic healthcare data workflows effectively.

The modular and permissioned architecture of Hyperledger Fabric adds further value by enabling lower latency, higher transaction throughput, and scalability, all of which are important for real-time healthcare applications such as EHR management. Additionally, the dual-layer security mechanism combining DES-based encryption and PQC ensures data integrity, privacy, and non-repudiation, addressing critical requirements for healthcare data management. These features collectively highlight the robustness and scalability of the proposed framework.

While our framework demonstrates the possible solutions, however, it is important to consider the limitations which are important for future research. For instance, scalability under extremely large-scale deployments, particularly in environments with high volumes of patient data requests and transactions, requires further investigation. Resource optimization for PQC algorithms, especially for resource-constrained devices in the IoMT, real-world deployment considering Cross-Platform Compatibility and Integration with Healthcare Standards, remains an important area for future exploration. Addressing these challenges will be key to ensuring the framework's adaptability in real-world healthcare environments.

VIII. CONCLUSION

In this paper, we investigated the integration of PQC with hospital databases and the transmission of data to the Hyperledger Fabric blockchain. We conducted extensive simulations utilizing Discrete Event Simulation (DES) to explore the integration of blockchain technology in healthcare data management. The graphs of blockchain transactions, data encryptions, and patient data requests provided valuable insights into the dynamics of healthcare data flow and security. The simulation highlighted the sporadic nature of patient data requests, the efficiency of data encryption processes, and the reliability of blockchain transactions. These results underscore the potential of blockchain technology to enhance data security, streamline workflows, and improve patient outcomes within healthcare environments. Additionally, the analysis demonstrates the robustness and scalability of the proposed framework, reinforcing its applicability in real-world healthcare scenarios to address data integrity, confidentiality, and operational efficiency.

REFERENCES

[1] A. Bansal, Arju, Esha, and P. S. Mehra, "A post-quantum consortium blockchain based secure EHR framework," in *Proc. Int. Conf. IoT, Commun. Autom. Technol. (ICICAT)*, Jun. 2023, pp. 1–6.

[2] J. L. Fernández-Alemán, I. C. Señor, P. Á. O. Lozoya, and A. Toval, "Security and privacy in electronic health records: A systematic literature review," *J. Biomed. Informat.*, vol. 46, no. 3, pp. 541–562, Jun. 2013.

[3] S. Barman, S. Chattopadhyay, D. Samanta, and S. Barman, "A blockchain-based approach to secure electronic health records using fuzzy commitment scheme," *Secur. Privacy*, vol. 5, no. 4, p. 231, Jul. 2022.

[4] N. Dey, M. Ghosh, and A. Chakrabarti, "Quantum solutions to possible challenges of blockchain technology," in *Quantum and Blockchain for Modern Computing Systems: Vision and Advancements: Quantum and Blockchain Technologies: Current Trends and Challenges*. Cham, Switzerland: Springer, 2022, pp. 249–282.

[5] M. Adeli, N. Bagheri, H. R. Maimani, S. Kumari, and J. J. P. C. Rodrigues, "A post-quantum compliant authentication scheme for IoT healthcare systems," *IEEE Internet Things J.*, vol. 11, no. 4, pp. 6111–6118, Feb. 2024.

[6] M. Ei-Hadedy, P. V. Ankunda, J. Ung, and W.-M. Hwu, "Securing the Internet of Medical things (IoMT) with K3S and hybrid cryptography: Integrating post-quantum approaches for enhanced embedded system security," in *Proc. IEEE 17th Dallas Circuits Syst. Conf. (DCAS)*, Apr. 2024, pp. 1–6.

[7] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019.

[8] N. Waheed, A. Ur Rehman, A. Nehra, M. Farooq, N. Tariq, M. A. Jan, F. Khan, A. Z. Alalmaie, and P. Nanda, "FedBlockHealth: A synergistic approach to privacy and security in IoT-enabled healthcare through federated learning and blockchain," in *Proc. IEEE Global Commun. Conf.*, Dec. 2023, pp. 3855–3860.

[9] S. Belludi and H. Kopácková, "Securing smart city health services using blockchain technology," in *Proc. Zooming Innov. Consum. Technol. Conf. (ZINC)*, May 2024, pp. 188–193.

[10] H. Arshad, A. Sheikh, A. Bibi, A. A. Kiani, M. Arshad, and F. Arif, "A blockchain-powered paradigm for cloud-based healthcare information sharing: Decentralized patient data exchange," in *Proc. Int. Conf. Eng. Comput. Technol. (ICECT)*, May 2024, pp. 1–7.

[11] S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, and S. Sarkar, "Quantum cryptography for IoT: APerspective," in *Proc. Int. Conf. IoT Appl. (ICIOT)*, May 2017, pp. 1–4.

[12] Shubham, P. Sajwan, and N. Jayapandian, "Challenges and opportunities: Quantum computing in machine learning," in *Proc. 3rd Int. Conf. I-SMAC (IoT Social, Mobile, Analytics Cloud) (I-SMAC)*, Dec. 2019, pp. 598–602.

[13] Z. Ye, Y. Gao, Y. Xiao, M. Xu, H. Yu, and D. Niyato, "Smart healthcare with hybrid mobile edge-quantum computing: Dynamic computation offloading for latency improvement," in *Proc. IEEE 98th Veh. Technol. Conf. (VTC-Fall)*, Oct. 2023, pp. 1–5.

[14] M. Chen, T. Malook, A. U. Rehman, Y. Muhammad, M. D. Alshehri, A. Akbar, M. Bilal, and M. A. Khan, "Blockchain-enabled healthcare system for detection of diabetes," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102771.

[15] A. U. Rehman, N. Tariq, M. A. Jan, F. Khan, H. Song, and M. Ibrahim, "A blockchain-based hybrid model for IoMT-enabled intelligent healthcare system," *IEEE Trans. Netw. Sci. Eng.*, vol. 11, no. 4, pp. 3512–3521, Jul. 2024.

[16] M. Bhatia and S. K. Sood, "Quantum computing-inspired network optimization for IoT applications," *IEEE Internet Things J.*, vol. 7, no. 6, pp. 5590–5598, Jun. 2020.

[17] N. K. Dewangan and P. Chandrakar, "Patient-centric token-based healthcare blockchain implementation using secure Internet of Medical things," *IEEE Trans. Computat. Social Syst.*, vol. 10, no. 6, pp. 1–11, Apr. 2022.

[18] S. Chandrasekaran, R. Agrawal, V. Dutt, and N. Vyas, "Improved healthcare system with quantum computing," in *Proc. Int. Conf. Artif. Intell. Smart Commun. (AISC)*, Jan. 2023, pp. 99–103.

[19] R. Ur Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, J. Qadir, and Z. Anwar, "Quantum computing for healthcare: A review," *Future Internet*, vol. 15, no. 3, p. 94, Feb. 2023.

[20] S. Rani, P. Kumar Pareek, J. Kaur, M. Chauhan, and P. Bhambri, "Quantum machine learning in healthcare: Developments and challenges," in *Proc. IEEE Int. Conf. Integr. Circuits Commun. Syst. (ICICACS)*, Feb. 2023, pp. 1–7.

[21] S. K. Satpathy, V. Vibhu, B. K. Behera, S. Al-Kuwari, S. Mumtaz, and A. Farouk, "Analysis of quantum machine learning algorithms in noisy channels for classification tasks in the IoT extreme environment," *IEEE Internet Things J.*, vol. 11, no. 3, pp. 3840–3852, Feb. 2024.

[22] M. Wazid, A. K. Das, and Y. Park, "Generic quantum blockchain-envisioned security framework for IoT environment: Architecture, security benefits and future research," *IEEE Open J. Comput. Soc.*, vol. 5, pp. 248–267, 2024.

TAMARA ZHUKABAYEVA (Member, IEEE) received the Ph.D. degree in computer science, computer engineering, and control' from Kazakh National Technical University. She is currently a Full Professor with the Department of Information Systems, L. N. Gumilyov Eurasian National University. She has published more than 110 scientific articles, books and monographs, has an innovative patent and copyright certificates for intellectual property rights. She has extensive experience as a Researcher and an Educator, contributing to various national and international projects. Her research interests include artificial intelligence (AI), information security, computer vision, and the Internet of Things (IoT). She has received numerous awards, including the Best University Teacher Award and the "Bolashak" International Scholarship.

ATEEQ UR REHMAN (Member, IEEE) received the Ph.D. degree from the University of Southampton, U.K., in 2017. He is currently a Lecturer with the Department of Computing, Staffordshire University, U.K. His research interests include cyber security, blockchain, and privacy-preserved machine learning, particularly in healthcare and smart cities.

NARGIS TARIQ (Member, IEEE) received the M.S. degree in computer science from The University of Haripur, Pakistan. Her research interests include privacy, blockchain, and deep learning.

ELHADJ BENKHELIFA (Senior Member, IEEE) is currently a Full Professor with Staffordshire University and the Director of the Smart Systems, AI, and Cybersecurity Research Centre. He is a member of the Board of Directors for the Knowledge Graph Alliance, and the Chair for IEEE region eight, area two for the computer society. His research interests include cloud/edge computing, IoT, cybersecurity, AI, and software engineering.