IET Wireless Sensor Systems

WILEY

The Institution of Engineering and Technology

ORIGINAL RESEARCH OPEN ACCESS

Quantum-Resistant Security in Digital Twin Healthcare Systems

Ahmed K. Jameil[1,2] | Hamed Al-Raweshidy[1]

[1]College of Engineering, Design and Physical Sciences, Brunel University of London, London, UK | [2]Department of Computer Engineering, University of Diyala, Baqubah, Iraq

Correspondence: Hamed Al-Raweshidy (hamed.al-raweshidy@brunel.ac.uk)

Received: 4 May 2025 | **Revised:** 26 January 2026 | **Accepted:** 2 February 2026

Keywords: remote sensing | security of data | sensors | telecommunication security | wireless sensor networks

ABSTRACT

The development of digital twin (DT) systems for healthcare presents several challenges, particularly in ensuring data protection and communication security in real-time environments. The protection of patient information in the case of future quantum-powered attacks is one of the key issues, with traditional public-key cryptography tools being likely to be weakened in the context of the huge quantum computers. The objective of this research was to come up with a quantum-resistant security system to DT-based remote healthcare monitoring. With quantum-safe session key establishment with QKD or lattice-based postquantum interactions, along with symmetric authenticated encryption, secure far-edge, near-edge and cloud data transfer and processing was guaranteed. The results revealed a 40% reduction in latency, a 30% improvement in throughput and a 15% increase in system efficiency, demonstrating substantial enhancements in performance. The integration of quantum-resistant protocols provided robust protection without compromising system operation, achieving a 25.77% improvement in computational efficiency. The proposed framework significantly enhances the security, scalability and performance of remote healthcare systems, offering a future-proof solution against quantum computing threats.

1 | Introduction

The concept of digital twin (DT) technology has emerged as a transformative approach in various industries, that is, engineering and manufacturing, where it functions as a dynamic digital replica of physical entities. DT technology allows for optimised processes, predictive maintenance and overall improved system performance [1–5]. More recently, its potential has begun to be explored in healthcare applications, for example, for managing chronic diseases such as diabetes mellitus (DM), by creating virtual counterparts of patients' physiological states [6, 7]. These advancements enable real-time monitoring, diagnostics and personalised treatment planning, offering new possibilities in patient care [8, 9].

Nevertheless, in spite of this possibility, there are profound issues of data security and real-time communication of DT applications in healthcare, especially when working with sensitive healthcare data. With the trend where healthcare systems are becoming more interconnected and data-driven as a result of implementing Internet of Things (IoT) technologies, patient data protection is even more of a concern. Since the development of quantum computing, conventional public-key, such as RSA and ECC, encryption schemes will be susceptible to large-scale quantum computers with the Shor algorithm, but symmetric encryption schemes, such as AES, will remain unaffected as long as sufficiently large key sizes are used to overcome the impacts of the Grover algorithm. Therefore, the healthcare systems need to implement quantum-resistant security

measures that will help protect the healthcare data of the patients against these emerging threats [10–12].

In this context, quantum key distribution (QKD) and postquantum cryptography are viewed as essential components of next-generation healthcare systems. These technologies can ensure the integrity and privacy of patient data in a future where quantum computing poses a significant threat. However, integrating these quantum security mechanisms into healthcare's digital twin frameworks introduces new challenges in terms of performance, scalability and system complexity [13–15].

This paper addresses the growing concern for healthcare data security in DT systems by proposing a novel framework that incorporates quantum-resistant cryptographic techniques. Key innovations of this research include:

1. A quantum-secure DT framework for healthcare that integrates QKD to safeguard patient data during transmission, ensuring resistance to both classical and quantum computing threats.
2. The development of the quantum digital twin healthcare security (DTHQ) protocol, which combines quantum-resistant cryptography and secure communication mechanisms to enhance data integrity and confidentiality in healthcare environments.
3. An optimised cloud-edge architecture that supports secure data transmission and storage whilst maintaining real-time performance and scalability in healthcare systems.

This paper is structured as follows: Section 2 reviews related work on DTs and quantum security in healthcare. Section 3 describes the proposed DT system architecture with a focus on quantum-resistant security. Section 4 explains the DTHQ(A,B,Q) protocol. Section 5 presents the security evaluation and verification. Section 6 covers performance metrics and analysis. Section 7 discusses the results and Section 8 concludes the paper.

2 | Related Work

The evolution of Industry 4.0 has introduced transformative changes across multiple sectors, including healthcare, leading to the development of Healthcare 4.0. This new paradigm employs emerging technologies, such as automation, digitisation and intelligent systems, to enhance the quality of care as well as reduce costs [16–20]. A big driving force in this transition is DT technology, which works efficiently with the Internet of things (IoT) to maintain real-time monitoring of healthcare and data processing [21–23].

2.1 | Quantum Security in Healthcare Digital Twin Systems

As DT systems become more widely implemented in healthcare, ensuring the security of sensitive patient data is a primary concern. The emergence of quantum computing threatened classical public-key cryptography (RSA/ECC) via Shor's algorithm and reduced the effective security margin of symmetric primitives under Grover's algorithm unless larger key sizes were adopted. These security mechanisms are critical for protecting healthcare data, particularly in the context of real-time monitoring, where data breaches could lead to severe consequences [24–26].

Eliminating healthcare systems from the quantum paradigm, aside from postquantum cryptography and biometrics for postquantum authentication, other possible aspects have been proposed to include quantum zero-knowledge proof protocols. For example, Ahmadian et al. introduced the DARIUS framework to improve the performance of QKD systems that are used for secure data delivery within healthcare applications. QKD has been used to secure data in healthcare; it provides encryption keys that are impossible to intercept or hack, with neither classical nor quantum attack methods working [27, 28].

Apart from QKD, postquantum cryptographic algorithms, such as lattice-based cryptography and hash-based digital signatures, are studied to enhance data security towards DT frameworks. These algorithms target the requirements of PHI, ensuring that medical data are never transmitted unencrypted, whilst also securing storage and processing. Studies have shown that quantum-resistant security protocols can be integrated into cloud and edge computing environments, which are critical to modern healthcare systems [29–31]. Surveys that have been conducted recently have discussed quantum-secure authentication and key agreement protocols in IoT usage, pointing to the problem of scalability, computation costs and real-life implementation. These findings are consistent with the necessity of lightweight and hybrid quantum-safe models of edge centric healthcare digital twin systems [32, 33]. Mobile edge computing environments have also suggested lightweight authenticated key agreement mechanisms to reduce the amount of computation and communication overhead whilst maintaining high security assurances. Such resource-efficient designs highlight the importance of scalable and edge-friendly authentication schemes, which directly informed the security and performance trade-offs adopted in the proposed DTHQ protocol [34, 35].

2.2 | Challenges in Implementing Quantum Security for Healthcare Systems

Quantum-resistant cryptography may still be emerging, but what will it mean for systems being built with digital twins in healthcare? Kocabas et al. focused on major challenges related to data privacy, communication latency and computational overhead that may arise during the integration of quantum security mechanisms into real-time healthcare subsystems [29]. When QKD and postquantum cryptography are integrated into DT frameworks, they often consume too many resources, leading to compromised system performance or scalability issues. Hybrid quantum-safe authentication protocols with adaptive defences have been proposed to enhance resilience against advanced adversaries; however, their added complexity can limit suitability for latency-sensitive healthcare digital twin systems [36]. Related work has also investigated blockchain-

enabled secure communication protocols for large-scale IoT systems, such as the BSCP-SG framework, proposed for smart grid environments. Although blockchain-based approaches improve data integrity and trust management, they typically introduce additional computational and communication overhead, which can limit their suitability for latency-sensitive and resource-constrained healthcare digital twin systems [37].

Moreover, real-time monitoring systems need data to be communicated as quickly and securely as possible along a field–facility–cloud path due to the constant emanating of patient data from far-edge devices at an unsurprisingly frequent rate [22, 38]. Addressing these challenges requires a comprehensive approach that balances security with system performance. The development of lightweight quantum-resistant protocols, such as the DTHQ (A,B,Q) protocol proposed in this study, aims to overcome these limitations by optimising encryption processes whilst maintaining robust security standards.

2.3 | Identified Gaps and Research Directions

Existing research has laid the groundwork for integrating quantum security into healthcare's DT systems, but several gaps remain. First, most studies focus on either real-time data processing or security, but not both. This leaves room for exploring solutions that offer a balance between strong security measures and real-time operational efficiency. Second, there is limited research on how quantum security mechanisms impact the scalability of DT systems in large-scale healthcare applications. Finally, the application of quantum-resistant cryptography to specific healthcare use cases, such as chronic disease monitoring, has not been thoroughly investigated as shown in the Table 1.

TABLE 1 | Performance comparison of quantum-resistant cryptographic protocols in DT systems.

Ref.	C1	C2	C3	C4	C5	C6	C7	C8	C9
[39] 2024	✓	✓	✓	—	✓	✓	—	✓	—
[40] 2024	✓	✓	✓	—	✓	✓	✓	✓	✓
[41] 2023	✓	✓	✓	—	✓	✓	—	✓	—
[42] 2024	✓	✓	✓	—	✓	✓	✓	✓	✓
[43] 2023	✓	✓	✓	—	✓	✓	✓	✓	—
[44] 2024	✓	✓	✓	—	✓	✓	✓	✓	—
[27] 2024	✓	✓	✓	✓	✓	—	—	✓	✓
[45] 2024	✓	✓	✓	✓	✓	—	—	✓	✓
[46] 2023	✓	✓	✓	—	✓	✓	✓	✓	✓
[15] 2024	✓	✓	✓	✓	✓	✓	✓	✓	✓
[13] 2024	✓	✓	✓	✓	✓	✓	✓	✓	✓
[47] 2024	✓	✓	✓	—	✓	✓	✓	✓	✓
Proposed	✓	✓	✓	✓	✓	✓	✓	✓	✓

Abbreviations: C, criteria; C1, quantum security; C2, data integrity; C3, scalability; C4, real-time processing; C5, postquantum cryptography; C6, IoT integration; C7, healthcare application; C8, resource Optimisation and C9, communication reliability.

In this paper, the gaps are bridged by outlining a detailed framework that incorporates quantum-resistant cryptographic methods in digital twin healthcare systems. The framework is aimed at providing secure data transmission and storage and ensuring scalability and effectiveness needed in real-time patient monitoring. The proposed system will be effective in protecting healthcare data against future quantum attacks through the combination of QKD and postquantum cryptography.

3 | Proposed DT Model Architecture

3.1 | Problem Formulation

The integration of modern technologies, that is, DT, IoT and cloud computing has great potential to revolutionise healthcare in terms of patient monitoring and fostering real-time interventions. Nevertheless, there are some critical challenges to consider, especially on the issue of security, scalability and integrity of data to make certain that these systems are robust and reliable when faced with the threats of emerging quantum computing. The main challenges include:

1. Scalability of Healthcare Monitoring Systems: The traditional healthcare systems may have problems in scaling to handle high volumes of real-time data of many patients. It needs a scalable architecture that will effectively manage large volumes of data without compromising system performance by providing continuous and reliable monitoring.
2. Data Integrity and Quantum Security: Healthcare data were highly sensitive, and large-scale quantum computers were expected to threaten classical public-key cryptography (RSA/ECC) via Shor's algorithm. Symmetric encryption remained viable, although larger key sizes were required to preserve security margins under Grover's algorithm. Therefore, quantum-safe key establishment and robust authenticated encryption were required to protect healthcare data during transmission and storage against both classical and quantum-enabled adversaries.
3. Fast Data Processing: Timely medical decision-making means that data need to be processed fast and transferred with low latency. This forces the architecture and security measures to perform real-time patient data processing as patient data are highly sensitive and must remain confidential between specific parties.
4. Interoperability and Integration: Existing healthcare infrastructures, such as electronic health records (EHRs) and hospital information systems (HIS), must seamlessly integrate with the proposed DT and IoT-based architecture. The system should comply with industry standards, for example, FHIR and HL7, to ensure smooth data exchange and system interoperability.
5. Resource Utilisation: Processing the data in real-time costs a lot of computational power and space, especially in the cloud and at the edge. The effective resource allocation mechanisms must be introduced to help in the evolution of healthcare workloads to allow them to perform in a cost-efficient manner without affecting the scalability and reliability of the system.

In our research, we have aimed to propose a secure, scalable and efficient data-driven healthcare monitoring architecture that integrates quantum-resistant cryptography for the protection of sensitive patient information.

3.2 | System Overview

The proposed architecture for the DT healthcare system, as shown in Figure 1, was designed to enable scalability and real-time processing with a high level of security. Far-edge devices collected data, the near-edge layer validated these data before transmitting them to the cloud. Dataflow security was realised using quantum-safe key establishment and authenticated encryption. Storage, processing and DT updates were managed by the cloud infrastructure, whereas real-time monitoring and decision-making were supported by IoT devices, edge servers and communication hubs. Key components of the system included:

1. Data acquisition devices deployed as IoT, enabling real-time health monitoring.
2. Quantum-safe key establishment and authenticated encryption for secure data transmission.
3. Secure storage and management of health data with low latency and high throughput in cloud infrastructure.

The real-time data flow between IoT devices, cloud services and the DT model was expressed as follows:

$$D_C(t) = f(S_r(t)) \rightarrow B_{\text{IoT}}(t), \tag{1}$$

where $D_C(t)$ is the data collected at time t, $S_r(t)$ denotes sensor readings and $B_{\text{IoT}}(t)$ represents the IoT data buffer.

3.3 | IoT Devices and Data Acquisition

The platform uses a suite of IoT devices that are installed with precision sensors to record key health parameters, enabling secure real-time monitoring. The devices used include:

- MAX30102: For heart rate (HR) and SpO2 readings.
- MLX90614: Measures body temperature (BT) with infrared sensing.

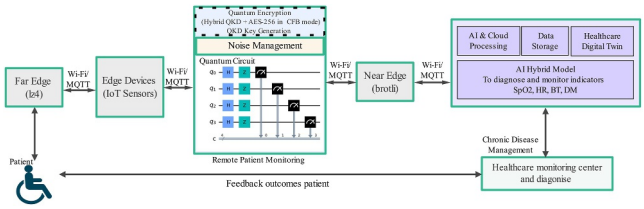

FIGURE 1 | Quantum-safe architecture for secure healthcare data transmission integrating QKD, edge devices, and cloud-based digital twin analytics.

- NodeMCU (Microcontroller): It acts as the unit receiving and reading data from sensors, and sends it to both the broker and end-user for communication.

All IoT devices collected physiological data and forwarded the information to the cloud using the MQTT protocol over a secured communication channel. To ensure quantum-resistant security, cryptographic key establishment was decoupled from payload encryption. A symmetric session key was first established using QKD when quantum communication infrastructure was available or alternatively via a lattice-based postquantum key encapsulation mechanism in classical deployments.

$$K_{\text{sess}}(t) \leftarrow \begin{cases} \text{QKD}(\cdot), & \text{if a quantum channel was available,} \\ \text{ML - KEM}(\cdot), & \text{otherwise.} \end{cases} \tag{2}$$

Once the session key was established, healthcare telemetry data were encrypted using symmetric authenticated encryption to guarantee confidentiality, integrity and authenticity during transmission.

$$C_{\text{data}}(t) = \text{AEAD - Enc}(K_{\text{sess}}(t),\ P_{\text{data}}(t),\ \text{AAD}(t)), \tag{3}$$

here, $P_{\text{data}}(t)$ denoted the plaintext sensor data at time t, $C_{\text{data}}(t)$ denoted the encrypted payload, $K_{\text{sess}}(t)$ denoted the established session key and $\text{AAD}(t)$ represented associated authenticated metadata, such as device identifiers and timestamps, which were integrity-protected but not encrypted.

3.4 | Cloud Computing Infrastructure

Ensured real-time communication between IoT devices and the cloud over Azure IoT Hub, a managed service in Microsoft Azure that routes device-generated data to other services, such as Time Series Insights and EventHubs, whilst enabling real-time processing. This infrastructure was designed for high-volume healthcare data transfer, whereas payload confidentiality and integrity were ensured using symmetric authenticated encryption with quantum-safe session key establishment as defined in Equations (2) and (3). The efficiency of data transmission is modelled as follows:

$$\mathcal{R}_{DT} = \frac{\mathcal{D}_T}{\Theta_{trans}}, \tag{4}$$

where $\mathcal{R}_{DT}$ represents the data transmission rate, $\mathcal{D}_T$ denotes the total data volume being transmitted and Θ_{trans} corresponds to the transmission time.

Symmetric authenticated encryption with quantum safe session key-establishment to secure all transmitted and stored data was also done to ensure that sensitive patient information was not compromised. This infrastructure guarantees privacy, integrity and confidentiality, especially with the new quantum challenges and low latency in real-time healthcare monitoring.

3.5 | Prediction and Analysis Module

The prediction and analysis module took real-time data streams, which were generated by IoT devices, and guaranteed the confidentiality and integrity of sensitive healthcare information throughout transit and computation. Cryptographic key establishment was decoupled with data encryption in order to attain quantum-resistant security. When quantum communication infrastructure was available, quantum keys were set up with QKD, whereas where only classical environments were required, key establishment was done with lattice based post-quantum key establishment mechanisms.

After the establishment of a secure session key, the encrypted prediction and analysis services in the clouds were used by encryption of the data obtained by IoT with the help of a symmetric-authenticated encryption algorithm. This strategy provided end-to-end security of healthcare information against classical and quantum powered attackers as well as maintained real-time processing speed.

The secure data processing and prediction workflow was modelled as follows:

$$\mathcal{P}(t) = f(\text{AEAD - Dec}\ (K_{\text{sess}}(t),\ \mathcal{C}_{IoT}(t),\ \text{AAD}(t)),\ \mathcal{H}(t-1)), \tag{5}$$

where $\mathcal{C}_{IoT}(t)$ denoted the encrypted IoT data received at time t, $K_{\text{sess}}(t)$ denoted the established session key derived via QKD or post-quantum key encapsulation, AAD(t) represented associated authenticated metadata and $\mathcal{H}(t-1)$ referred to historical patient data used for contextual analysis.

This architecture guaranteed both security of sensitive healthcare data during transmission and analytical processing, and, at the same time, offered safe and live digital twin updates in cloud-based healthcare environments.

3.6 | Security Mechanisms

The technology of hybrid quantum-safe security was implemented to secure communications and data storage in the digital twin healthcare architecture. The proposed design explicitly separated session key establishment from payload encryption in order to ensure technical correctness and deployment feasibility. Quantum key distribution (QKD) was employed exclusively for secure session key establishment between communicating entities when quantum infrastructure was available. Data confidentiality and integrity were subsequently ensured using symmetric authenticated encryption based on the established session keys.

Figure 1 illustrated the quantum-secure architecture of the proposed digital twin healthcare system. Far-edge IoT devices acquired physiological data, near-edge nodes performed data validation and preprocessing and cloud services maintained digital twin synchronisation, analytics and long-term storage. Compression algorithms were applied to reduce communication overhead, with LZ4 used at far-edge devices to prioritise low latency and Brotli used at near-edge nodes to optimise bandwidth utilisation.

In the absence of quantum infrastructure, a lattice-based post-quantum key encapsulation mechanism was considered as an alternative for session key establishment, ensuring resilience against quantum-enabled adversaries. Once a session key was established, healthcare telemetry data were encrypted using symmetric authenticated encryption before being transmitted over MQTT and cloud services. This design ensured confidentiality, integrity and authentication whilst maintaining real-time performance in resource-constrained IoT and edge environments.

The process for securing data transmission, processing and storage is summarised in Algorithm 1, which described the DTHQ protocol execution.

ALGORITHM 1 | DTHQ Protocol: Quantum-Safe Key Establishment and Secure Data Transmission

Input: ω_{conn}(ssid, password), Device Key
Output: Encrypted Telemetry Data, Secure API Payload and Updated Digital Twin State
procedure $\mathcal{I}_{\text{init}}$
  Establish authenticated network connection using device credentials
  Initialise secure communication parameters
end procedure
procedure $\mathcal{K}_{\text{establish}}$
  Establish symmetric session key K_{sess} using QKD
  or derive K_{sess} using postquantum key encapsulation
end procedure
procedure λ_{DT}
while system active **do**
  Acquire sensor data d
  Compress data based on edge type
  Encrypt data using authenticated encryption with K_{sess}
  Transmit encrypted payload to cloud services
  Update digital twin model with decrypted data
end while
end procedure

3.7 | Protocol Execution Flow

The DTHQ protocol was executed through the following ordered steps:

1. *Initialisation*: Edge devices and cloud services established authenticated communication channels using preregistered device identities and credentials.
2. *Quantum-Safe Key Establishment*: A symmetric session key was established using QKD over an authenticated quantum channel or, alternatively, through a lattice-based postquantum key encapsulation mechanism when quantum infrastructure was unavailable.
3. *Data Encryption and Transmission*: Healthcare telemetry data were compressed and encrypted using symmetric authenticated encryption with the established session key before transmission via MQTT and cloud services.

4. *Digital Twin Update*: The encrypted data were decrypted at the cloud layer and used to update the digital twin state in real time.
5. *Monitoring and Feedback*: Processed data and alerts were securely visualised on healthcare dashboards and utilised for decision support.

This gradual implementation guaranteed data confidentiality, integrity and authentication and maintained real-time performance in resource limited IoT and edge-based healthcare set-ups.

3.8 | Real-Time Processing and Secure Data Storage for Healthcare Monitoring

The engine of real-time data processing of the system provides the possibility of dynamic visualisation and notifications about this or that issue to healthcare professionals in case of the identification of critical indicators. Through the application of quantum-resistant encryption, any data transmission that is real time is safely processed so that patients remain private and their data does not violate the healthcare data laws. Such real time functions enable a continuous monitoring, which gives the healthcare professionals authority to make timely and informed decisions.

At the same time, the cloud-based storage system deals with secure storage of data on patients. This sensitive information is secured by encrypted storage means and the storage operation is given by:

$$\mathcal{S}_t = h(\mathcal{D}_B(t)), \tag{6}$$

where $\mathcal{S}_t$ represents secure storage at time t and $\mathcal{D}_B(t)$ refers to the data stored in the system.

To improve the data security in the process of archiving, the quantum-safe session key K_{sess} of Equation (2) was reused and periodic rekeying was introduced according to the storage policy. Records were stored in encrypted format through symmetric authenticated encryption as opposed to QKD being used as a primitive of payload encryption. The secure storage model was expressed as follows:

$$\mathcal{S}(t) = h(\text{AEAD - Enc}(K_{\text{sess}}(t),\ \mathcal{D}_B(t),\ \text{AAD}(t))), \tag{7}$$

where $\mathcal{D}_B(t)$ denoted the data being archived at time t and AAD(t) included integrity-protected metadata (e.g., patient identifiers, timestamps and access-policy tags).

Also, the storage system is important when updating the AI models using historical data so that the predictive abilities of the system are constantly being improved. The procedure of model update can be illustrated as follows:

$$F(t) : \mathcal{E}(t) \rightarrow \mathcal{M}_{DT}(t+1), \tag{8}$$

where $F(t)$ refers to the model update process that enhances the digital twin's predictive accuracy based on prior predictions.

This integrated architecture, which incorporates IoT devices, cloud computing, AI-driven predictive analytics and quantum-resistant encryption techniques, provides a scalable, secure and real-time solution for healthcare monitoring. The integration of quantum-safe key establishment, together with symmetric authenticated encryption, ensures that patient data remains protected against both classical and quantum-enabled threats.

4 | Quantum Security in Digital Twin Healthcare Systems

As DT frameworks became increasingly prevalent in healthcare for real-time patient monitoring, the security of sensitive patient data had to be prioritised. Classical public-key cryptography (RSA/ECC) was expected to become insecure under large-scale quantum computers due to Shor's algorithm, whereas symmetric cryptography remained viable provided that appropriate key sizes were adopted to mitigate Grover's algorithm. As pointed out above, the following vulnerabilities exposed the need for higher levels of security measures to safeguard health records from quantum invasions. The integration of quantum key distribution and quantum-resistant cryptographic techniques within the DT framework has been implemented to safeguard data against potential vulnerabilities posed by both classical and quantum adversaries. These quantum security protocols mean that healthcare data are protected and the best possible privacy and information integrity maintained, no matter the advances in quantum computing.

4.1 | Why Quantum Security?

Healthcare digital twin systems processed highly sensitive physiological data and therefore required long-term confidentiality, integrity and robust authentication. Under a quantum threat model, RSA and ECC were expected to become insecure due to Shor's algorithm, motivating quantum-safe key establishment. Symmetric cryptography (e.g., AES) remained viable, although larger key sizes were required to preserve security margins against Grover's algorithm. These observations motivated a hybrid design in which quantum-safe key establishment was combined with efficient symmetric authenticated encryption for real-time operation.

4.2 | Implementing Quantum Security in DT Healthcare

The safeguarding of digital healthcare frameworks is underpinned by an amalgamation of postquantum cryptographic techniques and QKD. The execution highlights several essential components as follows:

- *Quantum-safe key establishment*: QKD was employed to establish symmetric session keys when authenticated quantum infrastructure was available, whereas lattice-based ML-KEM was used as a deployable alternative in classical environments.

- *Payload protection*: Confidentiality, integrity and authenticity of healthcare telemetry were ensured using symmetric authenticated encryption (e.g., AES-GCM or ChaCha20-Poly1305) with the established session keys.
- *Authentication and access control*: Device and service authentication, together with access-policy enforcement, were applied to limit data exposure and mitigate insider and impersonation threats.

The principles establish security measures of patient information across the DT healthcare system. Table 2, important requirements for secure data transfer and computation were identified, namely, the strength of cryptographic protection, communication delay and resistance to quantum noise. They have also kept exploring and choosing each parameter with reference to the best security whilst enhancing the system's efficiency. This model maintains efficiency in the DT framework alongside an enhanced security against both classical and quantum threats.

4.3 | Justification of Quantum-Resistant Cryptographic Choices

Quantum-resistant security in the proposed digital twin healthcare system was achieved by separating key establishment from payload encryption. Quantum key distribution (QKD) was employed exclusively for secure session key distribution under the assumption of an authenticated quantum channel, whereas data confidentiality and integrity were ensured using symmetric authenticated encryption.

For scenarios where QKD infrastructure is unavailable or impractical, postquantum cryptographic algorithms were considered as drop-in alternatives for key establishment. Among the candidates proposed by the NIST postquantum cryptography standardisation process, lattice-based key encapsulation mechanisms, particularly ML-KEM (formerly Kyber), were identified as the most suitable for IoT and edge environments. This choice was justified by their strong security foundation based on the hardness of the learning with errors (LWE) problem, moderate key and ciphertext sizes, and efficient polynomial arithmetic operations that can be implemented on resource-constrained devices.

In contrast, NTRU-based schemes, although efficient, exhibited larger parameter sets and more complex implementation trade-offs for constrained hardware platforms. Isogeny-based schemes, such as SIDH, were not adopted due to their significantly higher computational cost and the disclosure of practical cryptanalytic attacks, which rendered them unsuitable for latency-sensitive healthcare monitoring systems.

Consequently, the proposed framework prioritised lattice-based postquantum key establishment for classical communication channels and QKD for quantum-enabled links, thereby achieving a balanced trade-off between security, efficiency and deployability in real-time IoT and edge-based healthcare environments.

TABLE 2 | Parameter definitions for digital twin, AI, and quantum security in healthcare.

Parameter name	Symbol	Type	Value range	Description
Data volume	ΔV	Integer	1 MB–10 GB	Size of data processed or transmitted by the system varies by application.
Data block size	—	Integer	1 KB, 4 KB, 16 KB	Size of data blocks for encryption affects processing and transmission speed.
System demand	ΔD	Integer	0%–100%	Current load on the system as a percentage of total capacity.
Processing adjustment	ϵ	Float	0.1–1.0	Adjustment step for scaling resources based on demand.
Energy consumption	$\mathcal{E}_C$	Float	10–500 W	Energy consumed during real-time processing and data transmission measured in watts.
Real-time processing latency	$\mathcal{L}_{RT}$	Integer/float	100–500 ms	Latency in processing real-time data and delivering results measured in milliseconds.
Threshold for scaling (high)	Υ_{high}	Integer/float	70%–90%	Upper system load threshold for scaling resources.
Threshold for scaling (low)	Υ_{low}	Integer/float	10%–30%	Lower system load threshold for reducing resources.
Quantum key length	—	Integer	128, 256, 512 bits	Length of the quantum encryption key for data protection.
Quantum noise tolerance	—	Float	1%–5%	Tolerance level for noise in the quantum communication channel.
Encryption efficiency	$\mathcal{E}_{\text{enc}}$	Float	80%–99%	Efficiency of encryption methods, that is, quantum-resistant algorithms in securing data.
Redundancy and fault tolerance	Σ_{RFT}	Integer/float	1–5	Degree of system redundancy and fault tolerance.
Backup service status	Ψ	Boolean	True/false	Whether the backup service is active for fault tolerance.

5 | Security Evaluation and Verification

The security of the DTHQ (A,B,Q) protocol has been informally and formally tested. To identify the important security properties informal appraisals were used, whereas formal verification was done using the Scyther verification tool to verify strength to face known attack vectors.

5.1 | Informal Security Evaluation

DTHQ (A,B,Q) scheme enabled to generate a quantum-derived session key K_{sess} that ensured confidentiality and message authenticity through the use of both conventional and post-quantum cryptography. The important security measures were as follows:

- *Confidentiality*: Sensitive healthcare data were protected using symmetric authenticated encryption with a session key K_{sess} established via quantum-safe mechanisms. Without access to K_{sess}, adversaries could not recover plaintext data.
- *Authentication*: Mutual authentication between communicating entities was achieved through nonce-based challenge–response exchanges and authenticated key establishment, ensuring that only legitimate parties participated in protocol execution.
- *Quantum-Safe Key Establishment*: Session keys were established either via quantum key distribution over an authenticated quantum channel or via lattice-based post-quantum key encapsulation. Raw quantum-derived session keys were not transmitted as payload data.
- *Replay Protection*: Fresh nonces ensured message freshness and prevented replay attacks as previously captured messages could not be reused to impersonate legitimate entities.

5.2 | Formal Security Verification

Using the Scyther verification tool, the DTHQ (A,B,Q) protocol was put through a formal verification. This automated tool affirmed the secret, authenticity and message interop of the protocol and affirmed its immunity to the mentioned types of attacks.

Although the basic objective of the verification process was to discover possible weak links and to be better prepared for threats, which were by then known, Scyther results are presented in Figure 2.

- Secrecy Claims: Scyther confirmed that secret values, that is, nonces (nA and nB) and Kq, remained confidential and were not accessible to unauthorised entities.
- Alive Claims: Both entities A and B confirmed each other's engagement, thus guaranteeing the protocols' compliance with the communication process.

Scyther results : autoverify

Claim				Status		Comment
DTHQ	A	DTHQ,A2	Secret secKeyA	Ok	Verified	No attacks.
		DTHQ,A3	Secret nB	Ok	Verified	No attacks.
		DTHQ,A4	Secret nA	Ok	Verified	No attacks.
		DTHQ,A5	Secret reqKey	Ok	Verified	No attacks.
		DTHQ,A6	Secret Kq	Ok	Verified	No attacks.
		DTHQ,A7	Alive	Ok	Verified	No attacks.
		DTHQ,A8	Weakagree	Ok	Verified	No attacks.
		DTHQ,A9	Niagree	Ok	Verified	No attacks.
		DTHQ,A10	Nisynch	Ok	Verified	No attacks.
	B	DTHQ,B2	Secret nB	Ok	Verified	No attacks.
		DTHQ,B3	Secret Kq	Ok	Verified	No attacks.
		DTHQ,B4	Secret nA	Ok	Verified	No attacks.
		DTHQ,B5	Alive	Ok	Verified	No attacks.
		DTHQ,B6	Weakagree	Ok	Verified	No attacks.
		DTHQ,B7	Niagree	Ok	Verified	No attacks.
		DTHQ,B8	Nisynch	Ok	Verified	No attacks.
	Q	DTHQ,Q2	Secret secKeyA	Ok	Verified	No attacks.
		DTHQ,Q3	Secret Kq	Ok	Verified	No attacks.
		DTHQ,Q4	Secret nA	Ok	Verified	No attacks.
		DTHQ,Q5	Secret reqKey	Ok	Verified	No attacks.
		DTHQ,Q6	Alive	Ok	Verified	No attacks.
		DTHQ,Q7	Weakagree	Ok	Verified	No attacks.
		DTHQ,Q8	Niagree	Ok	Verified	No attacks.
		DTHQ,Q9	Nisynch	Ok	Verified	No attacks.

Done.

FIGURE 2 | Formal verification of DTHQ protocol using Scyther tool.

- Message Integrity: Data integrity checks were performed and the results were positive which indicated there was no interference on the communicated data.

As illustrated in Figure 2, all security claims were successfully validated, with no vulnerabilities such as man-in-the-middle, replay or impersonation attacks identified.

5.3 | Adversary Model and Security Assumptions

The security analysis of the proposed digital twin healthcare system was conducted under a well-defined adversary model that captured both classical and quantum-enabled threats. The considered adversaries were categorised as follows:

Classical Network Adversary: A probabilistic polynomial-time attacker with full control over the communication channel, capable of eavesdropping, intercepting, modifying, replaying and injecting messages in accordance with the Dolev–Yao threat model. This adversary was assumed to have no access to long-term secret keys stored within trusted devices.

Quantum-Enabled Adversary: An extension of the classical adversary equipped with quantum computational capabilities, enabling the execution of algorithms such as Shor's and Grover's algorithms. This adversary was assumed to compromise classical public-key cryptosystems but remained unable to break

information-theoretic secure key distribution provided by QKD or the hardness assumptions underlying lattice-based post-quantum cryptographic schemes.

Insider Adversary: A partially trusted entity with authorised system access, such as a compromised healthcare operator or edge node, capable of observing or manipulating data but without access to quantum-derived session keys or secure hardware-protected cryptographic material.

The following assumptions were made throughout the analysis: (i) edge devices and cloud servers were equipped with tamper-resistant hardware for storing long-term secrets; (ii) initial device registration and authentication were performed securely; (iii) the quantum channel used for QKD was authenticated and (iv) cryptographic primitives were implemented correctly and followed standard parameter recommendations.

Based on this adversary model, the security analysis considered the following attacks: man-in-the-middle attacks, replay attacks, impersonation attacks, key compromise impersonation, data tampering and passive eavesdropping. Mutual authentication, isolation of session keys and encrypted storage were used to prevent insider threats. The symbolic model proved resistance to such attacks by verifying it formally by the Scyther tool.

6 | Performance Metrics and Analysis

6.1 | Simulation Setting

The environment used in the simulation was to provide high performance and fairly assessment of the algorithms proposed. The system operates on the ESP-IDF framework, built on FreeRTOS, which enables real-time patient monitoring using digital twin technology on a cloud platform. Simulations were performed on a custom-built machine with an Intel Core i7-9700 K CPU (8 cores, 3.6 GHz) and an NVIDIA GTX 1080 Ti GPU, providing the necessary computational capacity for executing algorithms and managing simulation workloads.

Data were acquired via IoT devices, which transmitted information to the cloud through a NodeMCU8266 gateway. Communication utilised the MQTT protocol over a 2.4 GHz Wi-Fi network (i.e., IEEE 802.11n). Azure IoT Hub served as the secure gateway for transmitting data, whereas cloud services (e.g., API Management and IoT Hub) were used for processing and storage.

The system operates within the Windows OS environment, with simulation algorithms implemented using Python 3.10.9. In the same way, the security of the protocol was checked using Scyther on Ubuntu 22.04 running via WSL2 on Windows. The selected hardware and software configuration provided a stable and efficient simulation environment for evaluating security and performance.

The critical parameters that guide system functionality, which involve data processing, resource scaling and fault management, are detailed in Table 2.

6.2 | Healthcare Infrastructure Integration

The DT framework has been intricately developed to cohesively connect with standard healthcare infrastructures, promoting secure and efficient data interchange between systems such as electronic health records (EHR) and hospital information systems (HIS). The proposed integration guarantees alignment with established standards, such as FHIR and HL7, in the administration of healthcare data. The security framework is fortified by employing QKD, which safeguards confidential patient data during transmission and provides resilience against possible quantum computing threats. Patient information exchange and management require secure handling and transfers and are enhanced by the QHIM Algorithm 2.

ALGORITHM 2 | QHIM Algorithm: Quantum-Safe Healthcare Information Management

Input: P_{data}, P_{policy} P_{id}
Output: R_{EHR}, R_{HIS} S_{policy}
procedure KEY_ESTABLISHMENT
    Establish symmetric session key K_{sess}
    $K_{sess} \leftarrow$ QKD($\cdot$) **or** ML - KEM($\cdot$)
end procedure
procedure ESTABLISH_SHARED_ACCESS_POLICY
    $S_{policy} \leftarrow$ NewPolicy(P_{policy})
    SetPermissions(S_{policy}, Permissions)
end procedure
procedure SECURE_DATA_TRANSMISSION_TO_EHR
    $E_{endpoint} \leftarrow$ GetEndpoint(P_{id})
    $C_{data} \leftarrow$ AEAD - Enc(K_{sess}, P_{data}, AAD)
    $R_{EHR} \leftarrow$ SendData($E_{endpoint}$, C_{data})
end procedure
procedure INTEGRATE_DATA_WITH_HIS
    $H_{data} \leftarrow$ FormatForHIS(P_{data})
    $C_H \leftarrow$ AEAD - Enc(K_{sess}, H_{data}, AAD)
    $R_{HIS} \leftarrow$ TransferToHIS(C_H)
end procedure
procedure SYNCHRONISE_DATA_BETWEEN_SYSTEMS
    SyncData(R_{EHR}, R_{HIS})
end procedure
return R_{EHR}, R_{HIS}, S_{policy}

6.2.1 | FHIR/HL7 Interoperability and Data Mapping

The data abstraction layer was standards based to match HL7 FHIR specifications and provided interoperability with already existing healthcare information systems. The proposed digital twin model, instead of using direct modifications of EHR or HIS platforms, adopted a gateway-based integration model where encrypted IoT telemetry was converted into FHIR-compliant resources before being stored or exchanged.

Specifically, physiological data collected from far-edge IoT devices were mapped to standard FHIR resources as follows: patient metadata were represented using the patient resource, device identifiers and capabilities were encoded using the device resource and real-time sensor readings were encapsulated using

the observation resource. This mapping enabled compatibility with modern RESTful EHR systems that support FHIR-based interfaces.

Edge devices sent MQTT payloads in a lightweight form of JSON and these were then converted into FHIR-compliant JSON objects by the integration layer. An example is that a measurement of the heart-rate received through MQTT was coded as a FHIR Observation resource with timestamps, patient references and correct coding. The ensuing FHIR message was authentically relayed to EHR or HIS endpoints via authenticated RESTful APIs.

This mechanism of interoperability was applied as a proof of concept logical integration layer, prove standards conformity without the need to adjust the old healthcare systems. Through the compliance with the FHIR and HL7 data models, the proposed framework provided harmony with heterogeneous healthcare infrastructures without compromising on the security, scalability as well as real-time performance.

6.3 | Scalability and Fault Tolerance

The configuration was established to self-regulate cloud assets in line with real-time workload expectations, consequently maintaining operational work performance and steadiness throughout periods of elevated demand. Resource scaling was managed through predefined control policies that regulated resource utilisation to achieve performance objectives with minimal overhead. To safeguard data reliability and accessibility through system issues or data corruption, measures for business continuity and recovery from disasters were established. To facilitate uninterrupted performance although minimising resource fragmentation, the QHIM algorithm (Algorithm 2) featured components including load balancing, adjustments to cloud density and trustworthy failover systems. Backup and recovery strategies were employed to minimise service downtime and enable rapid restoration of system functionality.

The proposed digital twin healthcare framework had been scaled to support growing counts of IoT and edge devices either by means of cloud-based auto-scaling or decentralised edge processing in large-scale deployment situations. With more connected devices, the distribution of workload among the nodes on near-edges reduced the congestion and minimised performance degradation in that case, latency and throughput were able to increase in proportion to the computational resources at their disposal. This design allowed the system to serve such large healthcare settings as hospital or a region-wide monitoring platform without adding a single failure point.

Regarding the practical implementation, a number of challenges related to QKD and postquantum cryptography were discovered. QKD deployment required specialised quantum communication infrastructure and trusted node configurations, which limited its immediate applicability to backbone or data-centre-level links. For resource-constrained or geographically distributed environments, lattice-based post-quantum cryptographic mechanisms provided more deployable alternative with acceptable computational overhead. Other challenges were session key scaling, the need to integrate with the current healthcare network protocols and the need to be compatible with legacy systems. These implications suggested that there was the need to have hybrid deployment models integrating QKD, PQC and classical cloud-edge security solutions to achieve scalability, feasibility and cost-effective implementation in the real healthcare systems.

6.4 | Security-Related Performance

The DTHQ (A,B,Q) protocol was evaluated using the proposed metrics of latency, communication cost, computational cost and throughput. The testing of the long edge and near edge environment was completed and key lengths 128, 256 and 512 bits were tried. Simulation of data of different sizes was done using compression algorithms, that is, LZ4 and Brotli, providing information about the effectiveness of the protocol in the radio network.

To conduct quantitative benchmarking, the proposed DTHQ protocol was benchmarked against the representative classical security schemes, such as RSA-based key exchange, ECC-based key exchange and standard TLS communication using AES-GCM. All schemes were evaluated under identical hardware, network and data size configurations. The comparison focused on processing latency, throughput and computational overhead in both far-edge and near-edge environments.

Measurement protocol: All baseline schemes were implemented using the same message format and payload size under the same near-edge execution environment. RSA-2048 and ECC-256 were used for session key establishment, followed by AES-GCM for payload protection. TLS (AES-GCM) values were reported as an application-layer baseline using a standard TLS configuration and were not claimed as protocol-level measurements. For each scheme, latency was measured as the end-to-end time required to establish a session key (amortised per session) and to encrypt and transmit a fixed-size telemetry message. Throughput was measured as the number of protected telemetry messages processed per second after session establishment. Computational overhead reflected cryptographic processing time only (key establishment and AEAD), excluding compression and network delay. Each measurement was averaged over N trials (e.g., $N = 1000$) using Python perf_counter() on the specified hardware as shown in Table 3. All implementations and scripts used for benchmarking are available upon reasonable request.

Detailed performance results of the proposed DTHQ protocol across edge environments are reported in Table 4.

Quantum-safe cryptographic mechanisms were incorporated into the proposed protocol to ensure resistance against both classical and quantum-enabled adversaries. LZ4 was chosen in far-edge deployment in favour of low latency whereas Brotli was used in near-edge deployment to maximise bandwidth usage. Latency was determined in terms of most time taken to compress, encrypt and transfer data, through the `perf_counter()` function available in Python. The measure of communication cost was the

TABLE 3 | Quantitative comparison with classical security schemes.

Scheme	Latency (ms)	Throughput (msg/s)	Comp. overhead (ms)
RSA-2048	18.7	120	22.4
ECC-256	6.9	480	8.1
TLS (AES-GCM)	4.8	950	5.3
Proposed DTHQ	1.2	3880	4.1

TABLE 4 | Performance metrics of DTHQ protocol across edge environments.

KL	ET	Data size	CA	AL (ms)	CC (ms)	Thrpt (msgs/s)
128	Far edge	Small	LZ4	1.2	12	67.737
128	Near edge	Small	Brotli	4.2	45	3880.330
256	Far edge	Medium	LZ4	1.3	15	682.756
256	Near edge	Medium	Brotli	5.1	47	2039.359
512	Far edge	Large	LZ4	2.5	21	1597.010
512	Near edge	Large	Brotli	8.4	52	847.314

Abbreviations: AL, average latency; CA, compression algorithm; CC, computational cost; ET, edge type; KL, key length and Thrpt, throughput.

amount of bits transmitted following compression and the measure of computational cost was the time taken to execute cryptographic operations.

The classical RSA and ECC based key exchange mechanisms were taken only as references points of comparison. By contrast, the suggested DTHQ protocol was based on quantum-safe protocols of key establishment with symmetric authenticated encryption.

The computational cost of cryptographic processing was modelled as follows:

$$\text{Computational Cost} = 2T_{ECC} + 3T_H + T_E + T_D \tag{9}$$

where T_{ECC} is the time of multiplication of elliptic curve point, T_H is the time of hashing, T_E is the time of symmetric encryption and T_D is the time of symmetric decryption.

Comparative protocols that have been described in the literature were based on more resource intensive operations, such as modular exponentiation, and hence had increased computational overhead. The trends of Figure 3 showed that near-edge deployments had better performance in terms of throughput, whereas far-edge deployments had greater latency in the conditions of limited resources.

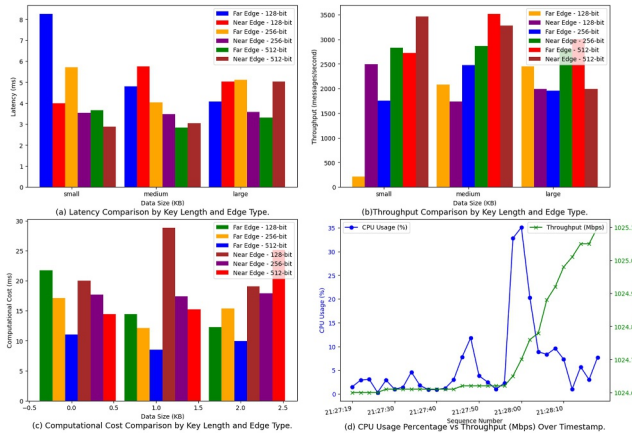

FIGURE 3 | Performance analysis of edge computing based on key length, edge type and data size.

7 | Results and Discussions

7.1 | System Impact of Digital Twin

A comparative study was performed to compare performance of the system with and without integration of DT, when data size varied (1 KB to 100 MB). It was found that the system with DT exhibited significant efficiency, throughput and latencies enhancements because of advanced latency reduction and data management tricks.

7.1.1 | Latency Reduction

Figure 4a demonstrated 40% latency reduction in the DT-integrated system. The resilient and scalable digital twin healthcare (DTH) system optimisation strategy (Algorithm 2) enabled this reduction by dynamically adjusting resources and processing power based on system load.

7.1.2 | Throughput Improvement

As illustrated in Figure 4b, the DT system increased throughput by 30%, facilitated by the unified patient data management

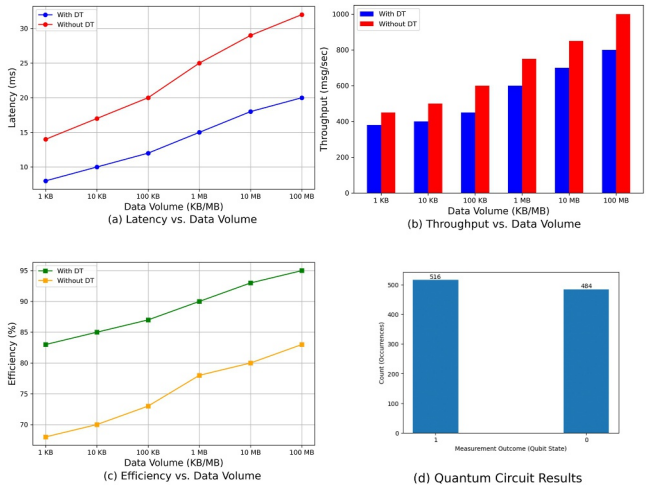

FIGURE 4 | System performance metrics with and without digital twin integration and quantum circuit measurement results.

strategy (Algorithm 2). This improvement ensured faster data availability and efficient processing.

7.1.3 | Efficiency Enhancement

Figure 4c indicates that the DT enabled system improved by 15% over the non-DT system. This has been realised by the mechanism of data transfer and acquisition (Algorithm 2) which streamlined the transmission of data between the IoT devices and the cloud which reduced overhead and minimised data usage.

In total, the adoption of DT technology improved the performance of the system greatly in terms of efficiency, throughput and latency. These gains were made possible by the underlying algorithms of data transfer, patient data management and system optimisation and point to the potential of DT in healthcare applications.

7.2 | Cross-Domain Protocol Comparison

A number of protocols were compared, and DTHQ (A,B,Q) protocol proved to work the best in terms of computational and communication costs. These performance metrics are detailed in Tables 5 and 6. The quantum resistant nature of DTHQ and its low computational cost can be highlighted as features that make it suitable in any edge setting. Other protocols, such as refs. [48, 49], are device-specific protocols, such as wearable sensors, but do not offer the whole gamut of quantum security of DTHQ. Even though blockchain-based protocols, such as VANET [50] and LA-IMDCN [51], are highly secured, they are more costly in terms of computation and therefore cannot be used in real-time.

The enhanced performance of DTHQ in far and near-edge deployments was because it has an optimised cryptography structure, which uses elliptic curve cryptography (ECC) and quantum-safe encryption. DTHQ is highly applicable to real-time IoT system considering that it reduces the computing requirements without lowering the security level compared to protocols that rely on blockchain.

7.3 | Quantum Computing Integration in Classical PC Systems: Challenges and Adaptations

Quantum technology integration into classical computing systems posed viable issues, since quantum and classical systems differ in fundamental aspects. Classical systems used binary logic to process information, unlike quantum computing, which used qubit-based operations, which needed specific hardware and communication infrastructure. As a result, quantum algorithms and protocols could not be executed directly on conventional pCs without abstraction layers or simulation frameworks.

Within the framework of this study, quantum-related functionality was assessed with the help of software-based simulators, including the Qiskit and the Quantum Development Kit offered by Microsoft, which allowed operating quantum workflows on classical hardware and validating their functionality. These devices, even though they do not fully imitate the efficacy of physical quantum systems, supplied a practical framework to scrutinise protocol logic, key management processes and system interoperability during the early developmental phases.

From a deployment perspective, the integration of quantum-safe security mechanisms introduced additional considerations. QKD required dedicated quantum communication channels and trusted node configurations, which limited its applicability to selected backbone or data-centre links in current healthcare infrastructures. For edge and large-scale deployments, post-quantum cryptographic mechanisms offered a more immediately deployable solution as they operated entirely on classical hardware whilst providing resistance to quantum-enabled adversaries. These findings have shown the necessity of hybrid deployment schemes that implemented classical cloud-edge systems where possible, and PQC-based security measures in other parts so that quantum-safe technologies could be introduced gradually and with low costs in actual healthcare settings.

8 | Conclusion

A hybrid cloud-edge quantum computing system has been presented in this study, designed to facilitate real-time healthcare monitoring. The system integrates DT technology, quantum security and IoT sensors.

The DTHQ (A,B,Q) protocol underwent rigorous security verification through the Scyther tool, confirming its resilience against various attack vectors. Quantum-resistant security measures were successfully applied to safeguard sensitive healthcare data, ensuring both privacy and integrity in anticipation of future quantum threats.

The system achieved a 40% reduction in latency compared to traditional non-DT systems, enhancing real-time responsiveness. Furthermore, throughput was increased by 30%, and

TABLE 5 | Computational costs of various protocols (ms).

Protocol	Computational cost (equation)	Computational cost (ms)
2024 [48]	$9TM + 13TH + TB$	13.476
2021 [49]	$10TM + 9TH$	0.88–51.51
2024 [50]	$2TECM + (3n + 1)TECA$	38.6 + 13.2n
2024 [51]	Device: $2Tsm + 4TH + Ten$	N/A
2024 [52]	N/A	N/A
2024 [53]	$2THMac + TE + TD$	20
Proposed DTHQ	$2TECC + 3TH + TE + TD$	7–10

TABLE 6 | Latency, throughput and edge deployment capabilities.

Protocol	Latency (ms)	Throughput (msg/sec)	Edge deployment
2024 [48]	10–15	Medium	Both far and near edge
2021 [49]	0.88–51.51	High	Near edge optimised
2024 [50]	High	Medium	Near edge (batch)
2024 [51]	74	Medium	Near edge
2024 [52]	N/A	N/A	Both far and near edge
2024 [53]	N/A	High	Both far and near edge
Proposed DTHQ	1–10	Very high	Both far and near edge

efficiency improved by 15%, demonstrating the substantial performance benefits of integrating digital twin technology.

From a computational standpoint, the system demonstrated a 25.77% improvement over prior work, whereas latency metrics reached the order of a few milliseconds, ensuring responsive real-time operation in healthcare monitoring environments.

Future research will aim to enhance system robustness by integrating more advanced quantum cryptographic techniques, further improving both security and efficiency.

Author Contributions

Ahmed K. Jameil has made substantial contributions to the conceptualisation and design of the work, acquisition, analysis and interpretation of data, developed the methodology, provided essential resources and software tools, validated the results and methods used, visualised the data and played a primary role in writing the original draft of the manuscript. Hamed Al Raweshidy has contributed to the funding acquisition, overseeing and leading the investigation process, managed project administration and coordination, supplied necessary resources, ensured the accuracy and validity of the procedures and results, supervised the project and revised the manuscript critically for important intellectual content. Both authors agree to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Acknowledgements

The study was supported by Brunel University of London.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Data are available from the authors upon request.

References

1. M. Attaran and B. G. Celik, "Digital Twin: Benefits, Use Cases, Challenges, and Opportunities," *Decision Analytics Journal* 6 (2023): 100165, https://doi.org/10.1016/j.dajour.2023.100165.

2. Z. Lv and S. Xie, "Artificial Intelligence in the Digital Twins: State of the Art, Challenges, and Future Research Topics," *Digital Twin* 1 (2022): 12, https://doi.org/10.12688/digitaltwin.17524.2.

3. I. FernándezRuiz, "Computer Modelling to Personalize Bio-engineered Heart Valves," *Nature Reviews Cardiology* 15, no. 8 (2018): 440–441, https://doi.org/10.1038/s41569-018-0040-x.

4. M. Grieves, "Digital Twin: Manufacturing Excellence Through Virtual Factory Replication—a Whitepaper by Dr. Michael Grieves'," *White Paper* (2014): 1–7.

5. A. K. Jameil and H. Al.Raweshidy, "A Digital Twin Framework for Real-Time Healthcare Monitoring: Leveraging Ai and Secure Systems for Enhanced Patient Outcomes," *Discover Internet of Things* 5, no. 1 (2025): 37, https://doi.org/10.1007/s43926-025-00135-3.

6. Y. Chu, S. Li, J. Tang, and H. Wu, "The Potential of the Medical Digital Twin in Diabetes Management: A Review," *Frontiers of Medicine* 10 (2023): 1178912, https://doi.org/10.3389/fmed.2023.1178912.

7. A. K. Jameil and H. Al-Raweshidy, "Implementation and Evaluation of Digital Twin Framework for Internet of Things Based Healthcare Systems," *IET Wireless Sensor Systems* 14, no. 6 (2024): 507–527, https://doi.org/10.1049/wss2.12101.

8. N. Mohamed, J. Al.Jaroodi, I. Jawhar, and N. Kesserwan, "Leveraging Digital Twins for Healthcare Systems Engineering," *IEEE Access* 11 (2023): 69841–69853, https://doi.org/10.1109/access.2023.3292119.

9. M. Singh, E. Fuenmayor, E. P. Hinchy, Y. Qiao, N. Murray, and D. Devine, "Digital Twin: Origin to Future," *Applied System Innovation* 4, no. 2 (2021): 36, https://doi.org/10.3390/asi4020036.

10. G. Cappon, M. Vettoretti, G. Sparacino, S. D. Favero, and A. Facchinetti, "Replaybg: A Digital Twin-Based Methodology to Identify a Personalized Model From Type 1 Diabetes Data and Simulate Glucose Concentrations to Assess Alternative Therapies," *IEEE Transactions on Biomedical Engineering* 70, no. 11 (2023): 1–12, https://doi.org/10.1109/tbme.2023.3286856.

11. A. Ajith and T. G. Venkatesh, "Delayed Mobile Data Offloading Scheme for Quality of Service Traffic: Design and Analysis," *IET Networks* 10, no. 5 (2021): 217–229, https://doi.org/10.1049/ntw2.12012.

12. A. K. Jameil and H. Al-Raweshidy, "Enhancing Offloading With Cybersecurity in Edge Computing for Digital Twin-Driven Patient Monitoring," *IET Wireless Sensor Systems* 14, no. 6 (2024): 363–380, https://doi.org/10.1049/wss2.12086.

13. A. Manocha, S. K. Sood, and M. Bhatia, "Digital-Twin-Assisted Academic Environment Monitoring for Anxiety Disorder," *IEEE Internet of Things Journal* 11, no. 8 (2024): 13563–13570, https://doi.org/10.1109/jiot.2023.3337846.

14. B. Wang, H. Zhou, X. Li, et al., "Human Digital Twin in the Context of Industry 5.0," *Robotics and Computer-Integrated Manufacturing* 85 (2024): 102626, https://doi.org/10.1016/j.rcim.2023.102626.

15. R. Girau, M. Anedda, R. Presta, et al., "Definition and Implementation of the Cloud Infrastructure for the Integration of the Human Digital Twin in the Social Internet of Things," *Computer Networks* 251 (2024): 110632, https://doi.org/10.1016/j.comnet.2024.110632.

16. A. K. Jameil and H. Al.Raweshidy, "Efficient Cnn Architecture on Fpga Using High Level Module for Healthcare Devices," *IEEE Access* 10 (2022): 60486–60495, https://doi.org/10.1109/access.2022.3180829.

17. G. Aceto, V. Persico, and A. Pescapé, "Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0," *Journal of Industrial Information Integration* 18 (2020): 100129, https://doi.org/10.1016/j.jii.2020.100129.

18. N. Dey, A. S. Ashour, F. Shi, S. J. Fong, and J. M. R. Tavares, "Medical Cyber-Physical Systems: A Survey," *Journal of Medical Systems* 42, no. 4 (2018): 1–13, https://doi.org/10.1007/s10916-018-0921-x.

19. Y. Feng, J. Zhao, X. Chen, and J. Lin, "An in Silico Subject-Variability Study of Upper Airway Morphological Influence on the Airflow Regime in a Tracheobronchial Tree," *Bioengineering* 4, no. 4 (2017): 90, https://doi.org/10.3390/bioengineering4040090.

20. A. K. Jameil, *High-Performance Hybrid AI Systems with Quantum-Secure Protocols for Cyber-Physical Remote Healthcare Applications' [Ph.D. dissertation]* (Brunel University of London, 2025).

21. S. M. S. Hussain, "Public Key-Based Quantum-Resistant Security Scheme for IEEE c37.118.2 Pmu Communication," *Electric Power Systems Research* 252 (2026): 112378, https://doi.org/10.1016/j.epsr.2025.112378.

22. H. Elayan, M. Aloqaily, and M. Guizani, "Digital Twin for Intelligent Context-Aware Iot Healthcare Systems," *IEEE Internet of Things Journal* 8, no. 23 (2021): 16749–16757, https://doi.org/10.1109/jiot.2021.3051158.

23. A. K. Jameil and H. Al.Raweshidy, "Ai-Enabled Healthcare and Enhanced Computational Resource Management With Digital Twins Into Task Offloading Strategies," *IEEE Access* 12 (2024): 90353–90370, https://doi.org/10.1109/access.2024.3420741.

24. A. CanoAguilera, *Accelerating Quantum-Secure Communications via DPU-Based Network Offloads' [Ph.D. Thesis]* (Eindhoven University of Technology, 2026): Accepted/In press.

25. S. C. S. Pirbhulal and H. Abie, "Improving Security and Privacy of Cognitive Digital Twins Through Dynamic Consent," in *HCI International 2025–Late Breaking Papers: 27Th International Conference on Human-Computer Interaction, HCII 2025* (Springer Nature, 2026).

26. M. F. Anka, J. A. MoraRodríguez, D. F. Pinto, L. Q. Galvão, M. A. Dias, and A. B. Tacla, "An Introductory Review of the Theory of Continuous-Variable Quantum Key Distribution: Fundamentals, Protocols, and Security," *Brazilian Journal of Physics* 56, no. 2 (2026): 72, https://doi.org/10.1007/s13538-025-01975-8.

27. M. Ahmadian, M. Ruiz, J. Comellas, and L. Velasco, "Darius: A Digital Twin to Improve the Performance of Quantum Key Distribution," *Journal of Lightwave Technology* 42, no. 5 (2024): 1356–1367, https://doi.org/10.1109/jlt.2023.3321774.

28. N. Garigipati, S. Srithar, and V. KrishnaReddy, "An Efficient Poly-Quantum Integrity Key Generation Based Multi-User Access Control Encryption and Decryption Framework for Homogeneous and Heterogeneous Cloud Ehr Databases," *Information Security Journal: A Global Perspective* 35, no. 1 (2026): 168–188, https://doi.org/10.1080/19393555.2025.2479029.

29. O. Kocabas, T. Soyata, and M. K. Aktas, "Emerging Security Mechanisms for Medical Cyber Physical Systems," *IEEE/ACM Transactions on Computational Biology and Bioinformatics* 13, no. 3 (2016): 401–416, https://doi.org/10.1109/tcbb.2016.2520933.

30. Y. Lin, Z. Gao, W. Shi, et al., "A Novel Architecture Combining Oracle With Decentralized Learning for Iiot," *IEEE Internet of Things Journal* (2022).

31. A. Asghari and M. K. Sohrabi, "Server Placement in Mobile Cloud Computing: A Comprehensive Survey for Edge Computing, Fog Computing and Cloudlet," *Computer Science Review* 51 (2024): 100616, https://doi.org/10.1016/j.cosrev.2023.100616.

32. P. R. Babu, S. A. P. Kumar, A. G. Reddy, and A. K. Das, "Quantum Secure Authentication and Key Agreement Protocols for Iot-Enabled Applications: A Comprehensive Survey and Open Challenges," *Computer Science Review* 54 (2024): 100676, https://doi.org/10.1016/j.cosrev.2024.100676.

33. N. T. Priya and V. S. Kumari, "A Quantum-Resilient and Adaptive Privacy Framework With Anonymization Techniques for Secure Data Mining Operations," *Security and Privacy* 9, no. 1 (2026): e70129, https://onlinelibrary.wiley.com/doi/10.1002/spy2.70129.

34. M. Tanveer, A. G. Alharbi, and M. J. Akhtar, "A Secure and Resource-Efficient Authenticated Key Agreement Framework for Mobile Edge Computing," *Peer-to-Peer Networking and Applications* 18, no. 4 (2025): 200, https://doi.org/10.1007/s12083-025-02016-6.

35. P. V. Thawani, P. E. Ajmre, and S. Chaurasia, "Quantum Computing in Security and Cryptography: Challenges and Future Directions," in *From Bits to Qubits: The Quantum Transformation of Computing. Vol. 179 of Studies in Big Data*, eds. S. Sharma and A. Sharma (Springer, 2026), 221–236.

36. R. BabuPonnuru, B. Palaniswamy, M. Azab, P. Palmieri, and U. Roedig, "Protecting dnp3-sab (Sav6): A Quantum-Safe Hybrid Authentication Protocol With Moving Target Defense," *IEEE Transactions on Consumer Electronics* 71, no. 3 (2025): 8383–8395, https://doi.org/10.1109/tce.2025.3593848.

37. I. Alrashdi, M. Tanveer, S. A. Aldossari, M. Alshammeri, and A. Armghan, "Bscp-Sg: Blockchain-Enabled Secure Communication Protocols for Iot-Driven Smart Grid Systems," *Internet of Things* 32 (2025): 101626, https://doi.org/10.1016/j.iot.2025.101626.

38. M. C. Saxena, A. Tamrakar, B. Balusamy, S. A. Yadav, S. Ramesh, and M. VinothKumar, *Foundations of Quantum Computing: Overview, Foundation and Scope'* (Wiley, 2026), 21–50.

39. Y. Zhang, G. Qin, B. Aguilar, et al., "A Framework Towards Digital Twins for Type 2 Diabetes," *Frontiers in Digital Health* 6 (2024): 1336050, https://doi.org/10.3389/fdgth.2024.1336050.

40. R. Avanzato, F. Beritelli, A. Lombardo, and C. Ricci, "Lung-Dt: An Ai-Powered Digital Twin Framework for Thoracic Health Monitoring and Diagnosis," *Sensors* 24, no. 3 (2024): 958, https://doi.org/10.3390/s24030958.

41. Z. Lv, J. Guo, and H. Lv, "Deep Learning-Empowered Clinical Big Data Analytics in Healthcare Digital Twins," *IEEE/ACM Transactions on Computational Biology and Bioinformatics* 21, no. 4 (2023): 1–11, https://doi.org/10.1109/tcbb.2023.3252668.

42. Y. Wu, Y. Wu, R. Yang, M. Feng, and G. Pu, "Cyber-Physical Wireless Networks for Smart Health Monitoring for Elderly Persons," *Wireless Personal Communications* (2024), https://doi.org/10.1007/s11277-024-11191-3.

43. L. Abirami and J. Karthikeyan, "Digital Twin-Based Healthcare System (Dths) for Earlier Parkinson Disease Identification and Diagnosis Using Optimized Fuzzy Based k-Nearest Neighbor Classifier Model," *IEEE Access* 11 (2023): 96661–96672, https://doi.org/10.1109/access.2023.3312278.

44. A. Gorelova, S. Meliá, and D. Gadzhimusieva, "A Discrete Event Simulation of Patient Flow in an Assisted Reproduction Clinic With the Integration of a Smart Health Monitoring System," *IEEE Access* 12 (2024): 46304–46318, https://doi.org/10.1109/access.2024.3380021.

45. H. Cao, S. Garg, S. Mumtaz, M. Alrashoud, L. Yang, and G. Kaddoum, "Softwarized Resource Allocation in Digital Twins-Empowered Networks for Future Quantum-Enabled Consumer Applications," *IEEE Transactions on Consumer Electronics* 70, no. 1 (2024): 800–810, https://doi.org/10.1109/tce.2024.3370052.

46. V. F. Rodrigues, R. da Rosa Righi, C. A. Da Costa, et al., "Digital Health in Smart Cities: Rethinking the Remote Health Monitoring Architecture on Combining Edge, Fog, and Cloud," *Health and Technology* 13, no. 3 (2023): 449–472, https://doi.org/10.1007/s12553-023-00753-3.

47. F. Yu, C. Yu, Z. Tian, et al., "Intelligent Wearable System With Motion and Emotion Recognition Based on Digital Twin Technology," *IEEE Internet of Things Journal* 11, no. 15 (2024): 26314–26328, https://doi.org/10.1109/jiot.2024.3394244.

48. O. B. J. Rabie, S. Selvarajan, T. Hasanin, G. B. Mohammed, A. M. Alshareef, and M. Uddin, "A Full Privacy-Preserving Distributed Batch-Based Certificate-Less Aggregate Signature Authentication Scheme for Healthcare Wearable Wireless Medical Sensor Networks (Hwmsns)," *International Journal of Information Security* 23, no. 1 (2024): 51–80, https://doi.org/10.1007/s10207-023-00748-1.

49. H. Ryu and H. Kim, "Privacy-Preserving Authentication Protocol for Wireless Body Area Networks in Healthcare Applications," *Healthcare* 9, no. 9 (2021): 1114, https://doi.org/10.3390/healthcare9091114.

50. S. K. Dwivedi, R. Amin, S. Vollala, and A. K. Das, "Design of Blockchain and Ecc-Based Robust and Efficient Batch Authentication Protocol for Vehicular Ad-Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems* 25, no. 1 (2024): 275–288, https://doi.org/10.1109/tits.2023.3310514.

51. J. Kar, X. Liu, and F. Li, "La-imdcn: A Lightweight Authentication Scheme With Smart Contract in Implantable Medical Device Communication Networks," *IEEE Access* 12 (2024): 99694–99703, https://doi.org/10.1109/access.2024.3429137.

52. R. Venkatesh, "A Lightweight Quantum Blockchain-Based Framework to Protect Patients Private Medical Information," *IEEE Transactions on Network Science and Engineering* 11, no. 4 (2024): 3577–3584, https://doi.org/10.1109/tnse.2024.3378922.

53. S. Prajapat, P. Kumar, D. Kumar, A. K. Das, M. S. Hossain, and J. J. P. C. Rodrigues, "Quantum Secure Authentication Scheme for Internet of Medical Things Using Blockchain," *IEEE Internet of Things Journal* 11, no. 23 (2024): 1–38507, https://doi.org/10.1109/jiot.2024.3448212.