**Discover** Applied Sciences

Research

# Quantum-enhanced digital twin IoT for efficient healthcare task offloading

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

Received: 18 November 2024 / Accepted: 7 May 2025
Published online: 23 May 2025


**Abstract**
Task offloading frameworks play a crucial role in modern healthcare by optimizing resource utilization, reducing computational burdens, and enabling real-time medical decision-making. However, existing Digital Twin (DT)-based healthcare models suffer from high latency, inefficient resource allocation, cybersecurity vulnerabilities, and computational limitations when processing large-scale patient data. These constraints pose significant risks in time-sensitive applications such as ICU monitoring, robotic-assisted surgeries, and telemedicine. To address these limitations, this paper introduces a Quantum-Enhanced DT-IoT framework, integrating Artificial Intelligence (AI), Quantum Computing (QC), DT, and the Internet of Things (IoT) for real-time, secure, and efficient healthcare task offloading. The proposed system introduces two key optimization algorithms: (1) DTH-ATB-MAPPO, which dynamically adjusts task scheduling and resource distribution, and (2) AQDT-IoT, which enhances computational efficiency and cybersecurity compliance in 6 G-enabled IoT networks. By leveraging Approximate Amplitude Encoding (AAE) and Grover's search, the framework enhances task offloading efficiency, enabling faster decision-making and optimized resource distribution across 6 G-enabled IoT networks. Empirical evaluations show that quantum preprocessing improved Task Offloading Success Rate (TOSR) by 32% and reduced the Error Rate (ER) by 80%, significantly outperforming traditional DT-based healthcare models. These enhancements enable. Additionally, theoretical analysis demonstrates computational speed enhancements, adaptive cybersecurity mechanisms, and improved system scalability, positioning this framework as a viable candidate for future cloud-based quantum healthcare infrastructures, even in resource-constrained hospital environments.

## Article Highlights

- The integration of quantum computing in healthcare accelerates operational tasks, allowing for smoother task delegation and a reduction in computational faults.
- Advanced quantum models optimize resource allocation, decrease expenses, and prolong the operational lifespan of wearable medical technologies.
- A robust and scalable quantum architecture fortifies AI-enhanced healthcare, guaranteeing instantaneous diagnostics and remote patient care.

**Keywords** AQDT-IoT algorithm · Quantum computing · Task offloading success rates (TOSR) · IoT-6 G networks

✉ Hamed Al-Raweshidy, hamed.al-raweshidy@brunel.ac.uk; Ahmed K. Jameil, 2006957@brunel.ac.uk | [1]College of Engineering, Design and Physical Sciences, Brunel University of London, Uxbridge, Middlesex, London UB8 3PH, UK. [2]Department of Computer Engineering, College of Engineering, University of Diyala, New Baqubah, 32001 Baqubah, Diyala, Iraq.

## 1 Introduction

The integration of Digital Twins (DTs), 6 G networks, and Quantum Computing (QC) presents transformative opportunities for modern healthcare systems. DTs, as virtual representations of physical systems, enable real-time monitoring, predictive analytics, and personalized healthcare solutions [1]. These capabilities are particularly crucial in chronic disease management, intensive care monitoring, and real-time medical interventions, where efficient data processing and decision-making are essential. Recent progressions have elucidated the efficacy of DT across multifarious sectors, encompassing healthcare, intelligent edifices, and manufacturing, thereby illustrating how data-centric modeling, surveillance, and optimization augment system efficacy and decision-making mechanisms [2]. Furthermore, DTs have been progressively amalgamated with artificial intelligence-driven predictive analytics, facilitating real-time healthcare surveillance and secure management of patient data [3].

However, numerous pivotal obstacles impede the extensive implementation of DT-IoT healthcare systems, particularly within the domain of real-time applications. The escalating influx of real-time healthcare data, when juxtaposed with the constrained computational capabilities of edge devices, engenders substantial limitations in the efficiency of task offloading and the allocation of resources. Conventional artificial intelligence-based task scheduling paradigms frequently encounter challenges related to elevated latency, fluctuating network conditions, and computational bottlenecks, resulting in delays concerning emergency diagnostics and the optimization of treatment protocols [4–6].

DT offloading frameworks from traditional computing are generally inadequate for managing time-sensitive medical data streams and predictive analytics. On the other hand, QC provides remarkable advancements in parallel processing and optimization which makes it exceptional for speeding up task allocation, reducing error rates, and bolstering cybersecurity measures in healthcare systems [7].

Furthermore, the reliance on interconnected IoT and DT systems introduces significant cybersecurity threats, potentially compromising patient data through cyberattacks and breaches [8]. While many studies have assessed cloud and edge computing models for healthcare systems, emerging hybrid AI-quantum computing approaches offer promising insights into addressing security and computational challenges [9]. Researchers have explored the role of quantum computing in IoT, uncovering notable enhancements in network efficiency, security, and computational speed [10].

Addressing these challenges requires an advanced computational framework that enhances task execution efficiency, ensures system scalability, and strengthens security compliance within healthcare networks. Recent research has underscored the importance of hybrid cloud-edge AI frameworks in DT-based healthcare systems, advocating for real-time predictive analytics and secure data transmission [11, 12]. However, existing cloud-edge architectures still face latency issues, particularly in high-density IoT environments, requiring further optimization in scheduling and resource allocation [13].

To address these pressing challenges, this study proposes the AQDT-IoT framework, a Quantum-Enhanced AI-Digital Twin-IoT system designed to optimize task offloading, enhance security, and improve computational efficiency in healthcare applications. The proposed framework utilizes IBM Quantum, thereby obviating the necessity for local quantum computing infrastructure and facilitating viable and scalable computational solutions in healthcare.

### 1.1 Key contributions

This research builds upon DTH-ATB-MAPPO [14] by adding quantum preprocessing to improve offloading efficiency and cyber security mechanisms. Furthermore, it adds a hybrid security method that involves RSA and AES-256 to provide protection for key and encrypted data transmission in accordance with [15]. This study makes the following important contributions:

1. **Advancing DTH-ATB-MAPPO with Quantum Computing:**
   - Quantum preprocessing is integrated into reinforcement learning-based task scheduling, leading to improvements in Task Offloading Success Rate (TOSR) and Error Rate (ER).
2. **Proposing AQDT-IoT for AI-Quantum Integration:**
   - A novel AI-Quantum-Digital Twin-IoT (AQDT-IoT) framework is introduced for optimized healthcare task execution.
   - Approximate Amplitude Encoding (AAE) and Grover's search are leveraged to enhance real-time decision-making in quantum-assisted task offloading.

3. **Enhancing Cybersecurity with ACTO**:

   - Quantum-enhanced encryption and real-time threat mitigation mechanisms are implemented to secure patient-sensitive data against cyber threats.
   - Compliance with HIPAA and GDPR is ensured to safeguard healthcare data privacy.

4. **Validating Cloud-Based Quantum Feasibility with IBM Quantum:**

   - The scalability and cost-effectiveness of IBM Quantum's cloud-based quantum computing are demonstrated for healthcare applications.
   - Quantum-powered healthcare solutions are validated for deployment without requiring on-premises quantum infrastructure, making them viable for resource-limited hospitals.

By addressing these challenges, the proposed Quantum-Enhanced DT-IoT framework establishes an adaptive, secure, and scalable approach for next-generation healthcare systems, ensuring efficiency in real-time medical decision-making and cybersecurity compliance.

### 1.2 Paper organization

The remainder of this paper is structured as follows: Sect. 2 presents related work, outlining key challenges and existing research. The proposed system model is described in Sect. 3, with a focus on integrating DTs, AI, and quantum computing for healthcare task offloading. Section 4 details the algorithm design, emphasizing task scheduling and cybersecurity. Implementation and evaluation, including deployment and security validation, are discussed in Sect. 5. Section 6 presents practical simulations, demonstrating real-world feasibility. Insights, scalability, and limitations are analyzed in Sect. 7, while Sect. 8 concludes the study by summarizing key findings and future directions.

Table 1 includes the key symbols used in the mathematical equations throughout this paper.

## 2 Related work

Healthcare has been transformed by the convergence of QC, DT, and 6 G network integration, each analyzed for its individual and combined potential in revolutionizing healthcare delivery. QC advancements are expected to accelerate drug development and reduce treatment costs, particularly in medical imaging, where Rossman's quantum-enhanced ISM reconstruction algorithm demonstrated reduced scan times and improved clinical efficiency [16–18]. Quantum Machine Learning (QML) has further been explored in diagnostics and personalized therapies, enhancing predictive healthcare applications [19]. Additionally, quantum-enabled resource allocation in DT-empowered quantum networks has been proposed as a method for real-time healthcare optimization, ensuring efficient computational resource distribution [20].

Emerging technologies such as 6 G connectivity, quantum computing, and generative AI offer promising solutions for enhancing real-time data processing, predictive analytics, and immersive healthcare environments [21]. However, challenges remain in integrating QC into healthcare systems, particularly in areas of cost, system complexity, and regulatory adaptation [22]. These advancements lay the foundation for further research into the roles of AI, QC, and 6 G in shaping future healthcare models [23].

Health information surveillance has increasingly focused on disease-specific data collection, with multisensor data aggregation providing a more comprehensive view of patient status [24]. Traditionally, such data collection was fragmented across healthcare sectors [25], limiting the potential for real-time, cross-institutional health monitoring. However, recent advancements have emphasized the integration of multisensor technologies to enhance continuous patient monitoring and predictive diagnostics [26–28].

DT technology, initially adopted in manufacturing, smart cities, and industrial automation, has now gained prominence in healthcare due to its ability to create real-time virtual representations of patient physiology and healthcare systems. Recent studies have explored AI-generated digital twins, leveraging real-time data and multiomics analysis to enable personalized medicine, disease prediction, and treatment optimization [29]. In one study, Marksteiner et al. demonstrated the feasibility of cyber-digital twins (CDTs) for healthcare, showing how these virtual patient models can improve diagnostics and therapeutic outcomes by simulating treatment responses before actual implementation

**Table 1** Nomenclature Table

| Symbol | Definition | Symbol | Definition |
|---|---|---|---|
| $N_i$ | Necessity of offloading task *i* | $C_i$ | Computational requirement (CPU/GPU cycles) |
| $D_i$ | Data size for execution | $E_d$ | Residual energy of device *d* |
| $\alpha, \beta, \gamma$ | Weighting factors for computation, data, and energy | $\tau_{net}$ | Network latency |
| $R_i$ | Security risk factor | $\delta, \lambda$ | Weighting factors for latency and security risks |
| $O_i^{dec}$ | Offloading decision for task *i* | $S_{net}$ | Network condition |
| $\theta$ | Offloading threshold | $R_{th}$ | Maximum acceptable security risk |
| $P_i$ | Probability of offloading task *i* | $N_{max}$ | Maximum necessity score |
| $\eta_{qc}$ | Quantum speedup coefficient | $A_{dt}$ | Digital Twin accuracy |
| $S_f$ | Social factors (e.g., patient demographics) | $T_{qc}$ | Quantum task execution time |
| $\eta$ | Quantum processing weight | $\mathcal{C}$ | Computational complexity of quantum task offloading |
| $q_i$ | Qubit contribution | $\gamma_d$ | Quantum decoherence coefficient |
| $\frac{1}{\sqrt{2}}$ | Quantum efficiency factor | $O(N)$ | Classical computational complexity |
| $O(\sqrt{N})$ | Grover's Search | $X$ | Healthcare dataset |
| $\|\psi\rangle$ | Quantum state representation | $c_i$ | Amplitude coefficients in quantum encoding |
| $\theta_i$ | Rotation angle in Approximate Amplitude Encoding | $O_i^{opt}$ | Optimized offloading decision |
| *ER* | Error Rate | $E_c$ | Computational errors |
| $E_s$ | Security-based errors (cyberattacks, data breaches) | $\rho_c$ | Computational error weight |
| $\rho_s$ | Security error weight | $ACTO_{sec}$ | Adaptive security response |
| *IDS* | Intrusion Detection System | $\mathcal{R}$ | Risk evaluation score |
| $S_{threat}$ | Threat severity level | DTH-ATB-MAPPO | Digital Twin Healthcare-Enhanced Asynchronous Team-Based Multi-Agent Proximal Policy Optimization |
| AQDT-IoT | AI-Quantum-Digital Twin-IoT Framework | AAE | Approximate Amplitude Encoding |
| QSVT | Quantum Singular Value Transformation | SHD | Secure Healthcare Data |

[30]. These advancements reinforce the growing role of DTs in predictive healthcare, enabling data-driven clinical decision-making while addressing traditional inefficiencies in patient monitoring and personalized treatment.

Digital twin integration has significantly enhanced personalized healthcare and hospital management. Sai et al. demonstrated its effectiveness in diabetes management by improving glycemic control compared to standard care models [31]. At the hospital level, Benedictis et al. optimized resource allocation, reducing patient waiting times by 15% [32]. Additionally, AI-generated DTs have been proposed for personalized treatment and predictive healthcare, addressing logistical inefficiencies and improving decision-making [33].

The emergence of 6 G technology is expected to enable ultra-reliable, low-latency communication, essential for telesurgery and real-time remote diagnostics. Research suggests that 6 G will facilitate seamless integration of communication and data, enhancing health monitoring devices and AI-driven analytical tools in medicine [34]. A comprehensive survey by Abdul et al. highlighted its transformative impact on telehealth, intelligent health systems, and real-time care through ultralow latency and high reliability [35]. Moreover, Zhou et al. [36] proposed cooperative DTs within dynamic and distributed ecosystems, demonstrating adaptive resource allocation and real-time data synchronization, further strengthening the role of 6 G in healthcare.

This study addresses the need for an efficient and reliable task offloading framework in healthcare by integrating AI, QC, DT, and IoT. Existing approaches lack this comprehensive combination, leading to inefficient resource utilization, high latency, and increased task execution errors. To bridge this gap, the AQDT-IoT algorithm is proposed, incorporating quantum preprocessing and DT models to enhance task offloading decisions. This integration improves efficiency and reliability in future IoT-6 G networks. Table 2 presents a comparative analysis of current task offloading frameworks, highlighting the unique contributions and advantages of the proposed approach.

**Table 2** Comparison of Task Offloading Frameworks in Healthcare and IoT

| Metric | M1 | M2 | M3 | M4 | M5 | M6 | M7 | M8 | M9 |
|---|---|---|---|---|---|---|---|---|---|
| Our work | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| [37] 2024 | × | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × |
| [38] 2024 | ✓ | ✓ | ✓ | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| [39] 2024 | ✓ | ✓ | × | ✓ | × | ✓ | ✓ | ✓ | ✓ |
| [40] 2023 | ✓ | × | ✓ | ✓ | × | × | × | ✓ | ✓ |
| [41] 2025 | × | ✓ | ✓ | ✓ | ✓ | ✓ | × | ✓ | ✓ |
| [42] 2024 | ✓ | ✓ | ✓ | ✓ | × | × | ✓ | ✓ | × |
| [43] 2024 | ✓ | ✓ | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ |
| [44] 2024 | ✓ | ✓ | ✓ | ✓ | ✓ | × | ✓ | × | ✓ |
| [45] 2024 | ✓ | ✓ | ✓ | ✓ | × | ✓ | × | ✓ | ✓ |

M1: TOSR; M2: ER; M3: Energy Efficiency; M4: Latency Reduction; M5: Security Protocol; M6: Confidentiality & Integrity; M7: Healthcare Application; M8: Network Adaptability; M9: Adaptability to Network Conditions

## 3 System model

A method for data security and integrity is proposed in the realm of DTH systems' edge computing. This study employs a multi-faceted approach to optimize task offloading in healthcare systems using advanced technologies such as DT, QC, AI, and IoT. The proposed framework integrates these technologies within a 6 G network environment to enhance the efficiency, security, and personalization of healthcare interventions as shown in Fig. 1.

### 3.1 Problem statement

Modern healthcare systems increasingly incorporate DT, QC, and IoT devices within 6 G networks to improve resource use, patient care, and data security. However, integrating these technologies poses challenges. Current frameworks often fail to maintain data integrity, reduce latency, and optimise real-time task offloading due to computational demands and the need for secure, adaptive systems.

Specific challenges are posed by task offloading, as data-intensive tasks must be dynamically distributed across edge, cloud, and IoT devices to ensure patient safety, privacy, and operational efficiency are upheld. Cybersecurity threats, e.g., Denial of Service (DoS) attacks and data breaches, further intensify the complexities of secure data management, necessitating the implementation of robust protective measures.

The AQDT-IoT algorithm is introduced in this research to manage task offloading through quantum-enhanced DT models combined with AI-driven scheduling. Adaptive task distribution, secure data management, and enhanced response times are enabled by this framework, effectively addressing critical gaps in healthcare task offloading and data security.

### 3.2 Framework design

The integration of partial and binary offloading techniques with DT, QC, and SHD technologies led to the formulation of a framework that provides a complete structure for the creation of personalized healthcare interventions. Two principal algorithms were central to this model: Digital Twin Healthcare-Enhanced Asynchronous Team-Based Multi-Agent Proximal Policy Optimization (DTH-ATB-MAPPO) and AI-Quantum-Digital Twin-Internet of Things (AQDT-IoT).

In addition, the devised framework incorporates quantum data preprocessing techniques, enhancing quantum data representation through approximate amplitude encoding (AAE). This approach optimizes input encoding, ensuring that quantum state formulation for healthcare-related tasks requires less computational effort. Such an improvement facilitates the seamless integration of quantum models into data-centric healthcare applications.

### 3.3 Task offloading strategy

1. **Dynamic Assessment of Offloading Necessity:** The DTH-ATB-MAPPO methodology was introduced to analyze offloading needs, considering a device's computational power and remaining energy. This necessity, $N_i$, was calculated as follows:

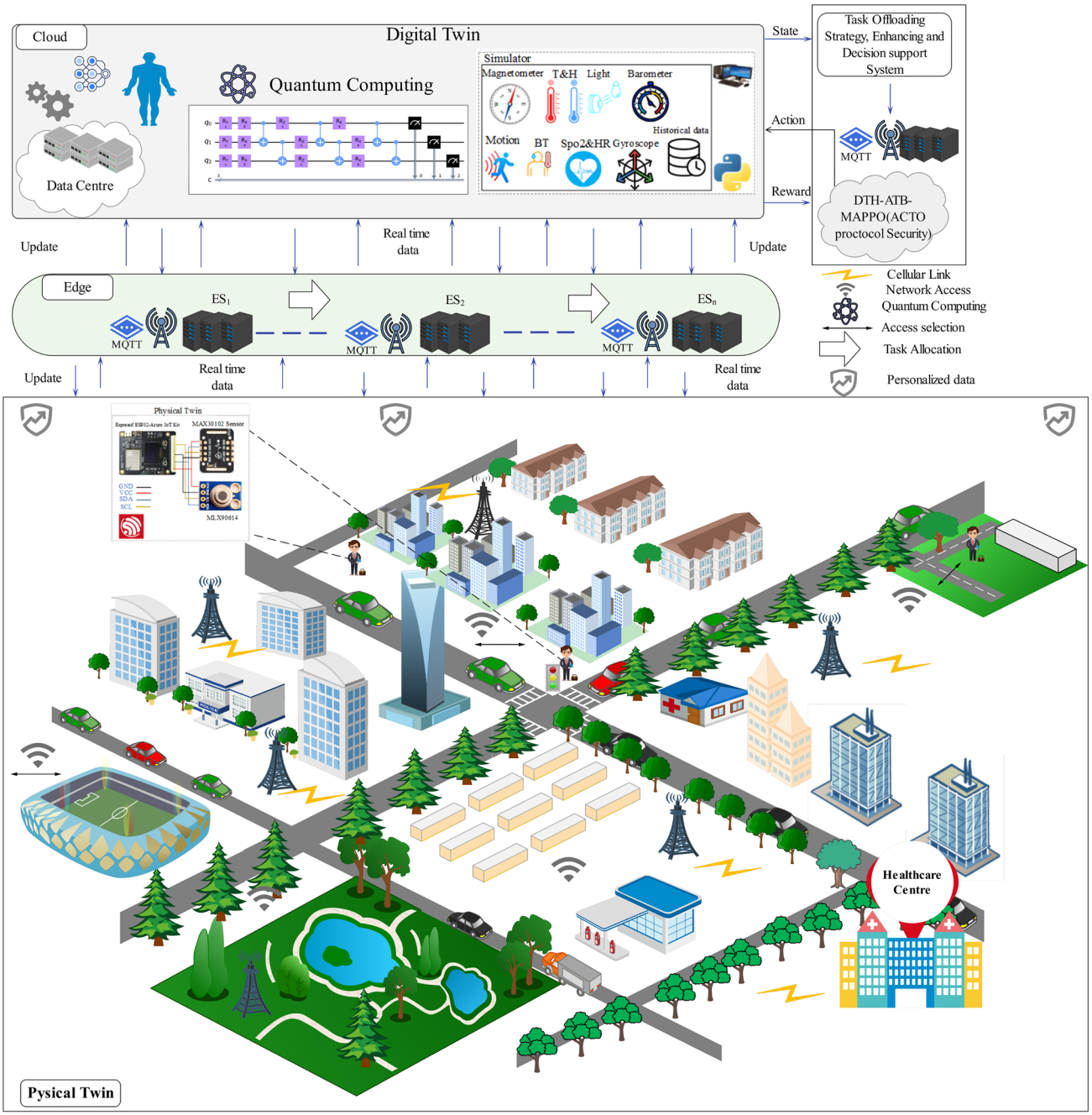


**Fig. 1** Framework of Task Offloading in Quantum AI DT-Enhanced 6 G Healthcare Networks

$$N_i = \alpha C_i + \beta D_i + \gamma E_d, \tag{1}$$

$C_i$ represents the computational requirements, quantified in CPU/GPU cycles, whereas $D_i$ signifies the quantity of data that necessitates transmission. $E_d$ pertains to the residual energy of device $d$. The weighting factors $\alpha, \beta, \gamma$ are utilized to assess the relative significance of each parameter in the decisions related to task offloading [14]. While this mathematical representation proficiently encapsulates the limitations related to resource availability, it fails to incorporate considerations of network latency and potential security vulnerabilities, which are indispensable in the context of real-time healthcare systems. Elevated latency can precipitate delays in medical diagnostics, and tasks allocated to compromised edge nodes may be susceptible to cyber threats. To integrate these supplementary variables, we refine Eq. (1) in the following manner:

$$N_i = \alpha C_i + \beta D_i + \gamma E_d + \delta \tau_{net} + \lambda R_i, \tag{2}$$

where $\tau_{net}$ denotes the latency associated with the network, quantified as the duration required for the transmission and processing of data throughout the communication infrastructure, and $R_i$ signifies the security risk variable, reflecting the probability of a task being susceptible to cyber threats, including unauthorized data breaches, malware infiltrations, or DoS attacks. The additional weighting factors $\delta$ and $\lambda$ quantify the impact of latency and security risks on the necessity of offloading.

The proposed enhancement ensures that tasks requiring substantial computational resources, involving large data transfers, operating with limited energy, experiencing high latency, or facing significant security threats are given priority for offloading, thereby improving real-time healthcare operations in 6 G networks. Furthermore, Quantum Singular Value Transformation (QSVT) is applied to enhance decision-making, leveraging quantum computing to dynamically adjust task allocation across computational nodes [46].

2. **Offloading Decision:** The decision to offload a task is determined by evaluating the necessity score $N_i$, the network condition $S_{net}$, and the security risk factor $R_i$. The original decision model considers only the necessity and network condition:

$$O_i^{dec} = \begin{cases} 1 \text{ if } N_i > \theta \text{ and } S_{net} \geq \sigma, \\ 0 \text{ otherwise.} \end{cases} \tag{3}$$

where $\theta$ represents the predefined offloading threshold and $S_{net}$ denotes the network condition, ensuring that offloading occurs only when the network has sufficient resources ($S_{net} \geq \sigma$). However, this model does not account for potential cybersecurity threats that may compromise the reliability of offloaded tasks. In real-time healthcare applications, where data integrity and security are paramount, offloading should be restricted if a computing node exhibits a high security risk. To address this limitation, the decision model is extended by introducing a security risk threshold $R_{th}$:

$$O_i^{dec} = \begin{cases} 1 \text{ if } N_i > \theta, S_{net} \geq \sigma, \text{ and } R_i \leq R_{th}, \\ 0 \text{ otherwise.} \end{cases} \tag{4}$$

where $R_i$ represents the security risk factor, quantifying the likelihood of a cyberattack or unauthorised access, while $R_{th}$ is the maximum acceptable risk level for a node to be considered safe for offloading.

From the derived Eq. (3) to (4), task offloading is designed to prioritize nodes that are not only computationally efficient and well-connected but also secure, effectively reducing the risks posed by malware infections, data breaches, and DoS attacks.

3. **Offloading Execution:** The execution of offloading decisions follows a partial or binary approach, where the probability of offloading a task is determined based on its necessity score relative to the most critical task in the system. The original probability function is given by:

$$P_i = \min\left(\frac{N_i - \theta}{N_{max} - \theta}, 1\right), \tag{5}$$

where $N_{max}$ represents the maximum necessity score among all tasks. This equation ensures that tasks with higher necessity scores are prioritised for offloading, while those with lower necessity remain local or are partially offloaded. However, in quantum-enhanced task execution, quantum processing speedup must be considered, as quantum-enabled tasks are processed more efficiently. To integrate this enhancement, the necessity normalisation is modified to include the quantum efficiency factor $\eta_{qc}$:

$$P_i = \min\left(\frac{N_i - \theta}{\eta_{qc}(N_{max} - \theta)}, 1\right), \tag{6}$$

where $\eta_{qc}$ represents the quantum speedup coefficient, which accounts for the advantage provided by quantum computing in task execution.

From the derived Eqs. (5) to (6), the offloading probability is adjusted to reflect the efficiency gains from quantum-enabled processing, ensuring that critical tasks benefit from accelerated execution while optimising resource allocation across quantum and classical nodes.

4. **Integration with DT:** The framework is continuously updated with real-time task information and environmental changes, ensuring adaptability in task offloading decisions. The necessity of offloading a task is dynamically adjusted based on DT accuracy and social factors, leading to the refined necessity equation:

$$N_i' = N_i + \delta A_{dt} + \epsilon S_f, \tag{7}$$

$A_{dt}$ denotes the accuracy of a Digital Twin, signifying the extent to which the model replicates actual real-world scenarios. In a parallel manner, $S_f$ encompasses social determinants, which incorporate patient demographics, accessibility considerations, and external factors. The weighting coefficients, $\delta$ and $\epsilon$, modulate the impact of these variables on offloading determinations, thereby ensuring a balanced and flexible methodology.

While Eq. (7) accounts for task adaptation based on DT feedback and social determinants, it does not consider the quantum execution speed of offloaded tasks. Since quantum computing accelerates processing, the necessity of offloading should decrease for tasks that benefit from quantum speedup. To reflect this effect, we introduce a quantum execution time factor $T_{qc}$, leading to the modified equation:

$$N_i' = N_i + \delta A_{dt} + \epsilon S_f - \eta T_{qc}, \tag{8}$$

where $\eta$ serves as the quantum processing weight, regulating the influence of quantum speedup on the necessity estimation and ensuring that tasks benefiting from quantum acceleration are appropriately adjusted in the offloading decision process.

Through the transition from Eqs. (7) to (8), the necessity of offloading is dynamically adjusted to account for real-time DT updates, social determinants, and quantum acceleration effects, ensuring a more adaptive and efficient task allocation strategy.

5. **Quantum Computational Complexity:** QC plays a critical role in enhancing the performance of DT modelling and simulation, particularly in optimising resource-intensive healthcare tasks. The computational complexity $\mathcal{C}$ associated with quantum-based task offloading is subject to the influence of various determinants, which encompass the quantity of qubits, the computational overhead specific to the task, and the efficacy of quantum parallelism facilitated by phenomena such as superposition and entanglement.

(a) **General Formulation of Quantum Computational Complexity:** For a given quantum task, the total computational complexity can be represented as:

$$\mathcal{C} = \sum_{i=1}^{n} f(q_i), \tag{9}$$

where $f(q_i)$ denotes the computational contribution of each qubit $q_i$, and $n$ represents the total number of qubits involved in processing. The overall complexity is derived from two fundamental contributions: linear computational cost and quantum parallelism advantage.

(b) **Computational Contribution of Individual Qubits:**

(i) **Linear Contribution of Qubits:** The computational cost associatedwith processing a quantum task scales proportionally to the number ofqubits. This contribution can be expressed as:

$$C_1 = \sum_{i=1}^{n} \alpha_i \cdot q_i, \tag{10}$$

where $\alpha_i$ represents a complexity coefficient pertinent to a specific task,which is contingent upon the nature of the quantum computation beingexecuted.

(ii) **Quantum Parallelism Contribution:** Quantum algorithms leveragesuperposition and entanglement to enhance computational efficiency,reducing the effective complexity compared to classical methods. Acommonly used quantum efficiency factor, $\sqrt{12}$, models this improvement:

$$C_2 = \sum_{i=1}^{n} \beta_i \cdot \frac{q_i}{\sqrt{2}}. \tag{11}$$

where $\beta_i$ represents the scaling coefficient associated with quantumspeedup.

(iii) **Final Computational Complexity Expression:** By combining thelinear and quantum parallelism contributions from Eqs. 10 and 11, thetotal computational complexity of quantum task execution is given by:

$$C = \sum_{i=1}^{n} \left( \alpha_i \cdot q_i + \beta_i \cdot \frac{q_i}{\sqrt{2}} \right) \tag{12}$$

this equation reflects both classical-like computational scaling andquantum-enabled efficiency gains.

(c) **Impact of Quantum Decoherence on Computational Complexity:** While quantum computing offers significant speedup, real-world quantum processors suffer from quantum decoherence, which introduces computational errors and additional processing overhead. To account for this limitation, we introduce a decoherence factor $\gamma_d$, which models the impact of noise on quantum task execution:

$$\mathcal{C} = \sum_{i=1}^{n} \left( \alpha_i \cdot q_i + \beta_i \cdot \frac{q_i}{\sqrt{2}} - \gamma_d \cdot q_i^2 \right), \tag{13}$$

the term $\gamma_d \cdot q_i^2$ models the quadratic scaling of errors as the number of qubits increases, reflecting practical quantum hardware limitations.

(d) **Justification for the Quantum Efficiency Factor $\frac{1}{\sqrt{2}}$:** The inclusion of the $\frac{1}{\sqrt{2}}$ factor in Eq. 11 is justified based on the following quantum principles:

- Quantum Interference Effects: In quantum mechanics, probabilistic states collapse upon measurement. The probability amplitude of entangled states follows a $\frac{1}{\sqrt{2}}$ scaling, effectively reducing the number of computational steps.
- Quantum Speedup in Algorithms: Algorithms such as Grover's Search reduce computational complexity from $O(N)$ to $O(\sqrt{N})$, following a similar $\frac{1}{\sqrt{2}}$ scaling pattern. This is particularly beneficial for quantum-assisted task offloading in large-scale healthcare applications.

## 4 Algorithm design

### 4.1 Quantum-enhanced task offloading with AQDT-IoT

The AI-Quantum-Digital Twin-IoT (AQDT-IoT) algorithm integrates quantum computing, DTs, and AI-driven optimization to enhance task offloading efficiency in resource-constrained 6 G healthcare networks. The approach leverages Approximate Amplitude Encoding (AAE) to encode healthcare data into quantum states, facilitating more efficient task allocation and execution. Given a healthcare dataset:

$$X = \{x_1, x_2, \ldots, x_n\}, \quad x_i \in \mathbb{R} \tag{14}$$

where each $x_i$ represents a task feature, such as computational load, patient vitals, or network latency, the encoding process maps these features into quantum states using AAE. The quantum state representation is given by:

$$|\psi\rangle = \sum_{i=1}^{n} c_i |i\rangle, \tag{15}$$

$$\sum_{i=1}^{n} |c_i|^2 \approx 1, \tag{16}$$

where the coefficients $c_i$ are computed as:

$$c_i = \frac{x_i}{\sqrt{\sum_{j=1}^{n} x_j^2}} = \sin(\theta_i), \tag{17}$$

$$\theta_i = \arcsin\left(\frac{x_i}{\sqrt{\sum x_j^2}}\right). \tag{18}$$

This transformation normalisess task features, ensuring compatibility with quantum registers and reducing the classical-to-quantum computational overhead.

Quantum-Assisted Offloading Decision via Grover's Search Once task features are encoded into quantum states, quantum search algorithms enhance the decision-making process. The optimal offloading decision is formulated as:

$$O_i^{opt} = \arg\min_i \left(\alpha C_i + \beta D_i + \gamma E_d + \lambda \sum_{i=1}^{n} |c_i|^2\right), \tag{19}$$

where $\lambda$ acts as a quantum regularization parameter, ensuring encoding efficiency. Grover's algorithm is then applied to accelerate task selection, achieving a complexity reduction from $O(N)$ to $O(\sqrt{N})$, significantly improving decision-making for large-scale healthcare applications. Quantum-Enhanced AQDT-IoT Offloading Algorithm The following algorithm outlines the step-by-step execution of AQDT-IoT, incorporating quantum preprocessing, AI-based optimization, and MEC task offloading.

**Algorithm 1** Quantum-Enhanced AQDT-IoT Offloading Algorithm

```
procedure AQDT-IoT(tasks)
    for each task in tasks do
        Compute necessity N_i using Eq. 1 based on computational, data, and energy requirements.
        Encode healthcare task features using Approximate Amplitude Encoding (Eqs. 17 and 18).
        Evaluate the quantum-optimised offloading decision O_i^opt using Eq. 19.
        if O_i^opt == 1 then
            Offload task to MEC node.
        else
            Process task locally.
        end if
    end for
end procedure
```

A comprehensive overview of the quantum-enhanced task offloading process is illustrated in Fig. 2, depicting the end-to-end execution of AQDT-IoT.

#### 4.1.1 Performance evaluation

To assess the effectiveness of AQDT-IoT, two key performance metrics were evaluated: Task Offloading Success Rate (TOSR) and Error Rate (ER).

**The Task Offloading Success Rate (TOSR)** quantifies the efficiency of AQDT-IoT in successfully offloading tasks to MEC nodes:

$$TOSR = \frac{\text{Number of Successfully Offloaded Tasks}}{\text{Total Number of Tasks}} \tag{20}$$

Tasks were simulated with varying computational intensities and network conditions to evaluate the algorithm's performance. The offloading process was guided by AI-driven scheduling and quantum-enhanced preprocessing, which improved resource utilisation and latency reduction.

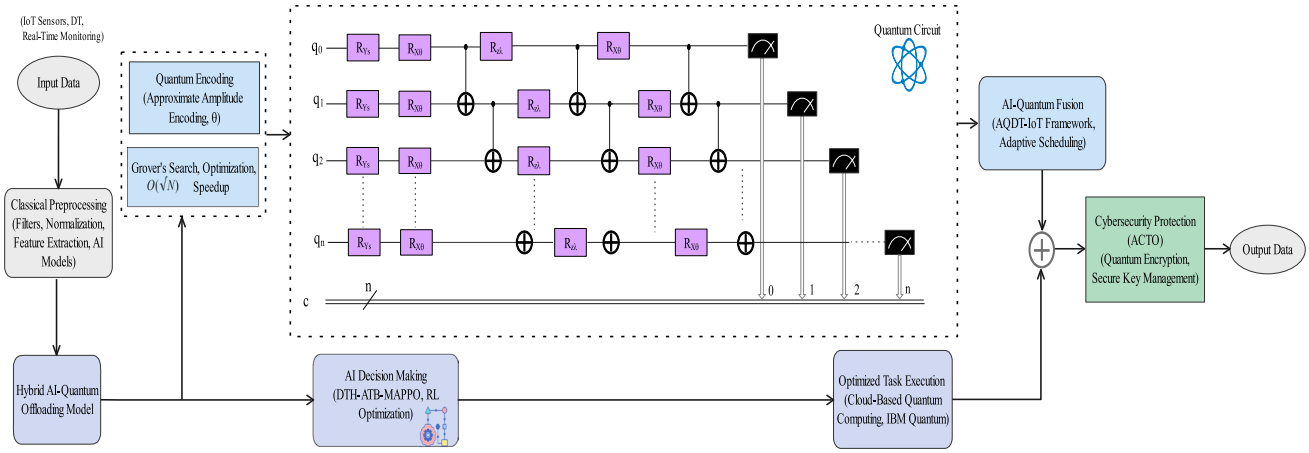


**Fig. 2** Hybrid AI-Quantum Offloading Architecture for Secure and Optimized Computing

In the realm of healthcare, ER in Task Offloading gauges execution blunders stemming from cyber perils or system breakdowns, which jeopardize diagnostic accuracy and patient well-being, computed as the fraction of errors to overall tasks, encompassing computational mishaps, data transfer glitches, and cybersecurity threats.

The ER formula is expressed as:

$$ER_c = \frac{\text{Number of Computational Errors}}{\text{Total Number of Tasks}} \tag{21}$$

The assessment procedure encompasses four distinct phases: task formulation, analysis, error detection, and conclusive computation. An elevated $ER_c$ indicates deficiencies within the system that necessitate enhanced security protocols.

To account for security-based errors, the formula is refined as:

$$ER = \frac{\sum(\rho_c E_c + \rho_s E_s)}{\text{Total Number of Tasks}}. \tag{22}$$

$E_c$ represents computational inaccuracies arising from the limitations of devices, whereas $E_s$ encompasses security vulnerabilities such as data breaches and Denial of Service (DoS) attacks. The scaling factors $\rho_c$ and $\rho_s$ modulate their influence on the calculations of error rates, thereby enhancing the model for precise oversight in 6 G healthcare networks.

### 4.2 ACTO's dynamic security adaptation

The ACTO framework dynamically adjusts security measures in response to continuous network monitoring, employing a three-layered approach:

1. **Real-time Monitoring and Intrusion Detection:** ACTO continuously monitors network activity using advanced Intrusion Detection Systems (IDS) and anomaly-based behavior detection. Any deviation from standard network behavior triggers an immediate security assessment and initiates adaptive countermeasures.
2. **Risk-Based Adaptive Response Mechanisms:** Upon detecting a security threat, ACTO evaluates the risk level $\mathcal{R}$ based on anomaly confidence scores and threat severity. Security responses are dynamically adjusted according to the evaluated risk and real-time network conditions. For instance:
   - In the event of a DoS attack, critical healthcare data is rerouted to stable and secure nodes, effectively isolating compromised areas.
   - If ransomware or data breaches are detected, ACTO automatically encrypts data transmissions and triggers secure backup protocols.
3. **Threat Categorization and Security Adjustments:** ACTO classifies threats into four severity levels (*low, medium, high, and critical*), each triggering a specific security response. Minor threats activate enhanced encryption, while

major incidents, such as ransomware attacks, lead to comprehensive task rerouting and encrypted data replication across secure nodes.

To mathematically model ACTO's cybersecurity adaptation, the security response function is defined as:

$$ACTO_{sec} = f(IDS, \mathcal{R}, S_{threat}) \tag{23}$$

where:

- $ACTO_{sec}$ represents the adaptive cybersecurity response.
- $f(\cdot)$ is the function dynamically adjusting security measures.
- $IDS$ denotes the Intrusion Detection System output, identifying anomalies.
- $\mathcal{R}$ represents the risk evaluation score, incorporating anomaly confidence and attack probability.
- The severity level of $S_{threat}$ serves as a determinant for the corresponding security measures that should be enacted.

**Case Study:** A ransomware attack targeting a hospital's patient management system. When encryption anomalies are detected, ACTO initiates an adaptive response, dynamically rerouting critical operations such as real-time patient monitoring and emergency response to unaffected nodes. Simultaneously, sensitive patient data is encrypted using ACTO's secure transmission methods to prevent unauthorized access.

## 5 Implementation and evaluation

The proposed framework was rigorously assessed employing critical metrics to evaluate its efficacy within the domain of healthcare applications.

### 5.1 Simulation setup

The simulation setup included both hardware and software components designed to replicate real-world healthcare environments:

- Hardware: Simulations ran on an MSI GF63 Thin 11SC laptop with an Intel Core i7 Processor, 16 GB RAM, and a 512 GB SSD for efficient multi-task handling.
- MEC Nodes: ESP32-WROVER-B devices, with 4MB RAM, Wi-Fi, and Bluetooth, served as MEC nodes, processing offloaded tasks from healthcare devices.
- Sensors: Various sensors simulated diverse healthcare scenarios:

    1. InvenSense MPU6050 for motion sensing.
    2. NXP MAG3110 for magnetic field measurements.
    3. FBM320 for atmospheric pressure.
    4. STMicro HTS221 for humidity and temperature.
    5. ROHM BH1750FVI for ambient light.
    6. MAX30102 for pulse and oxygen saturation.
    7. MLX90614 for non-contact temperature.

- Cloud Computing: IBM Quantum supported data processing, storage, and scalability for quantum task processing. The adoption of cloud-based quantum services eliminates the need for dedicated quantum hardware within healthcare facilities while allowing seamless integration of quantum-enhanced task offloading.

    To ensure real-world applicability, the cloud-based framework was designed to interact with IoT healthcare sensors in a hospital-like setting. Anonymized records from the MIMIC-III dataset were used to support evaluation under realistic healthcare conditions [47]. The cloud-based quantum workflow follows these steps:

1. **Data Collection:** IoT sensors continuously monitor patient vitals (e.g., heart rate (HR), oxygen levels (SpO2), body temperature (BT)) and transmit data to the DT system.
2. **Digital Twin Analysis:** The DT framework simulates patient conditions and determines necessary healthcare computations.
3. **Quantum Processing (Cloud-Based):**
   - Quantum AAE encodes healthcare tasks for efficient preprocessing.
   - Grover's search optimizes task allocation, ensuring rapid offloading decisions.
4. **Task Execution:** Optimised offloading tasks are dispatched to MEC nodes, reducing latency and energy consumption.
5. **Decision Refinement:** The DT model updates continuously, ensuring adaptive and self-improving task scheduling.

This integration with IBM Quantum ensures that hospitals can utilize quantum computing without requiring dedicated on-premise quantum infrastructure, enabling cost-effective and scalable healthcare solutions.

- Quantum Computing: Quantum preprocessing simulations employed Qiskit 0.24.1, implementing algorithms like Grover's for optimised task offloading. IBM Quantum utilised to facilitate quantum-enhanced decision-making, with quantum algorithms deployed in cloud environments. The flexibility of cloud quantum services ensures that healthcare institutions can scale their quantum computing capabilities without major infrastructure investments, making it a viable real-world solution.
- Communication Protocols: MQTT was used within the IoT network for low-bandwidth, high-latency conditions, with HTTP and HTTPS for secure data exchange.

The system adhered to the Ultra-Reliable Low Latency Communications (URLLC) standard, ensuring data transmission with $\leq$1 ms latency and up to 2 Gbps quantum-enhanced data rate, suitable for remote diagnostics and surgical assistance. Simulation parameters, including bandwidth, latency, and qubit usage, are detailed in Table 3.

### 5.2 Analysis of task offloading performance

The cumulative ER was plotted over time against the number of tasks, comparing QC and non-QC performance, as shown in Fig. 3. The blue line represents ER with QC, while the orange line shows ER without QC. Quantum preprocessing stabilized the cumulative error at an average of 0.1, regardless of task load, highlighting its efficacy in minimizing errors and ensuring precise task processing.

A comparative execution time analysis between classical and quantum offloading is presented in Fig. 4. The results indicate that quantum task offloading significantly reduces execution time, achieving a speedup factor of approximately 14.6× over classical methods. This improvement is attributed to Grover's algorithm and Approximate Amplitude Encoding, which optimize task scheduling and minimize processing delays.

Figure 5 illustrates Task Offloading Success Rates (TOSR) with and without QC. Higher median success rates (approx. 0.8) were observed on the left side of the box plot, with a narrow interquartile range indicating consistent success.

**Table 3** Parameters for Simulation Scenarios in Quantum-Enhanced 6 G Healthcare Networks

| Parameters | Description | Value |
|---|---|---|
| Network Type | Classification of 6G network utilized | URLLC |
| Quantum Data Rate | Data transfer speed enhanced by QC | Up to 2 Gbps |
| Network Latency | Expected latency in a 6G network enhanced with QC | $\leq$ 1 ms |
| Health Data Update Interval | Frequency of updates to the digital twin's patient data | Every 10 seconds |
| Simulation Duration | Total duration for each simulation scenario | 3 hours |
| $\alpha$ | Coefficients for quantum complexity calculation | [0.5, 0.8, 0.6] |
| $\beta$ | for quantum complexity calculation | [0.2, 0.3, 0.4] |
| qubits | Number of qubits used for quantum processing | [5, 10, 15] |

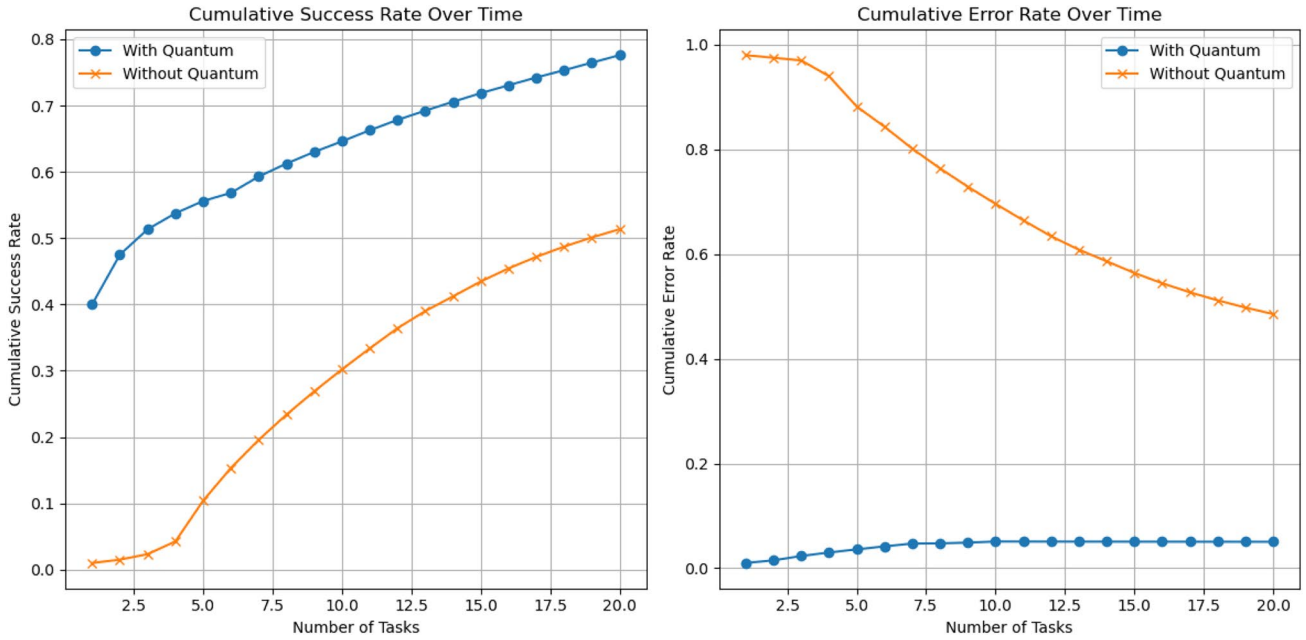


**Fig. 3** Performance Comparison of Task Offloading with and without Quantum Computing

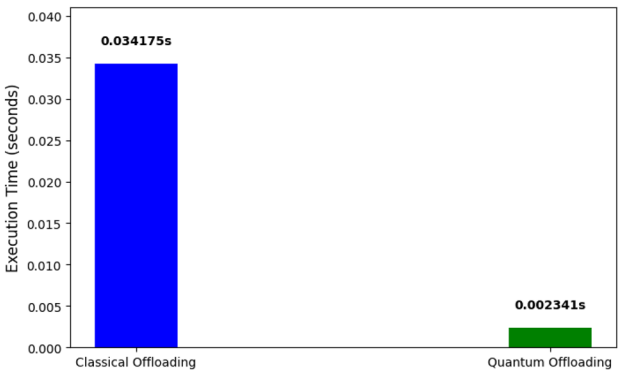


**Fig. 4** Comparison of Execution Time for Classical vs. Quantum Task Offloading

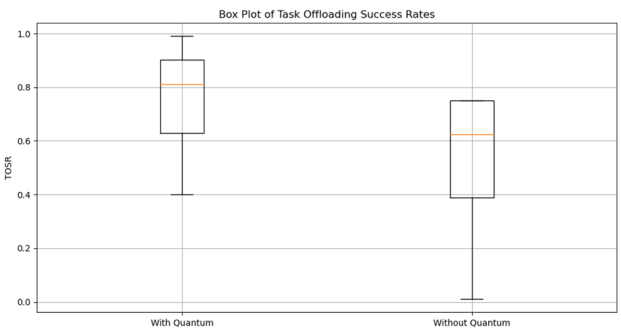


**Fig. 5** Box Plot of Task Offloading Success Rates

The upper quartile was found to reach near-optimal levels, while the lower quartile remained above 0.4, suggesting that a relatively high success rate was maintained even under challenging conditions.

The scatter plot in Fig. 6 compares TOSR and ER with and without QC. Consistently low error rates were maintained with QC, clustering around optimal performance at high success rates. In contrast, the non-QC setup exhibited greater variability in error rates, even at moderate success rates, demonstrating the efficiency gained through QC in high-performance settings.

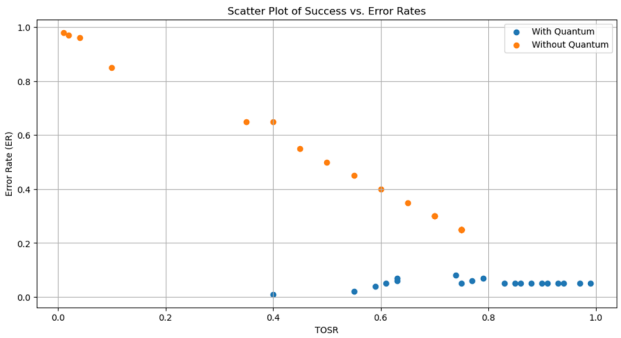


**Fig. 6** Scatter Plot of Task Offloading Success Rates vs. Error Rates

## 5.3 Protocol verification and security analysis

The ACTO (ADTHO) protocol was verified using the Scyther security verification tool, which analyzed key security properties such as secrecy, authenticity, and agreement among the Initiator (I), Responder (R), and a central server (Q). As shown in Fig. 7, all security claims-Secret secKeyI, Secret nI, Secret reqNonce, Alive, and Niagree-were validated without detected vulnerabilities, confirming the protocol's robustness against cyber threats.

Beyond formal verification, ACTO's adaptive cybersecurity responses are designed to minimize system performance degradation by distributing tasks across secure nodes.

### 5.3.1 Deployment and validation through API integration and testing

To evaluate ACTO's real-world security performance, a Flask-based API was implemented for healthcare task processing, and Postman was used to simulate various cyber threats.

**Implementation Workflow:**

**Fig. 7** Scyther Verification Results for ACTO Protocol

Scyther results : autoverify

| Claim | | | | Status | | Comment |
|---|---|---|---|---|---|---|
| ADTHO | I | ADTHO,I2 | Secret secKeyI | Ok | Verified | No attacks. |
| | | ADTHO,I3 | Secret nI | Ok | Verified | No attacks. |
| | | ADTHO,I4 | Secret reqNonce | Ok | Verified | No attacks. |
| | | ADTHO,I5 | Secret nR | Ok | Verified | No attacks. |
| | | ADTHO,I6 | Secret taskKey | Ok | Verified | No attacks. |
| | | ADTHO,I7 | Alive | Ok | Verified | No attacks. |
| | | ADTHO,I8 | Weakagree | Ok | Verified | No attacks. |
| | | ADTHO,I9 | Niagree | Ok | Verified | No attacks. |
| | | ADTHO,I10 | Nisynch | Ok | Verified | No attacks. |
| | R | ADTHO,R2 | Secret nR | Ok | Verified | No attacks. |
| | | ADTHO,R3 | Secret taskKey | Ok | Verified | No attacks. |
| | | ADTHO,R4 | Secret nI | Ok | Verified | No attacks. |
| | | ADTHO,R5 | Alive | Ok | Verified | No attacks. |
| | | ADTHO,R6 | Weakagree | Ok | Verified | No attacks. |
| | | ADTHO,R7 | Niagree | Ok | Verified | No attacks. |
| | | ADTHO,R8 | Nisynch | Ok | Verified | No attacks. |
| | Q | ADTHO,Q2 | Secret secKeyI | Ok | Verified | No attacks. |
| | | ADTHO,Q3 | Secret taskKey | Ok | Verified | No attacks. |
| | | ADTHO,Q4 | Secret nI | Ok | Verified | No attacks. |
| | | ADTHO,Q5 | Secret reqNonce | Ok | Verified | No attacks. |
| | | ADTHO,Q6 | Alive | Ok | Verified | No attacks. |
| | | ADTHO,Q7 | Weakagree | Ok | Verified | No attacks. |
| | | ADTHO,Q8 | Niagree | Ok | Verified | No attacks. |
| | | ADTHO,Q9 | Nisynch | Ok | Verified | No attacks. |

Done.

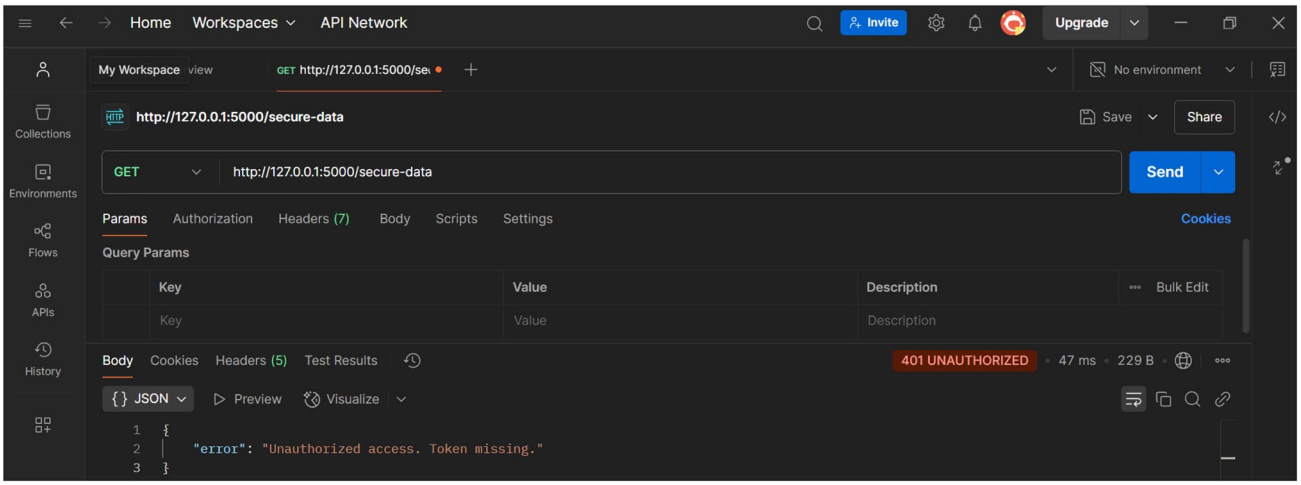


**Fig. 8** Unauthorized access attempt detected via Postman API testing

**Fig. 9** Flask logs capturing and mitigating a DoS attack using rate-limiting

```
2025-02-12 11:32:04,653 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 200 -
2025-02-12 11:32:04,653 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 200 -
2025-02-12 11:32:04,654 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 200 -
2025-02-12 11:32:04,654 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 200 -
2025-02-12 11:32:04,661 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,661 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
2025-02-12 11:32:04,665 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,666 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
2025-02-12 11:32:04,666 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,667 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
2025-02-12 11:32:04,668 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,668 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,669 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
2025-02-12 11:32:04,669 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
2025-02-12 11:32:04,672 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,672 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
2025-02-12 11:32:04,678 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,679 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
2025-02-12 11:32:04,679 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,680 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
2025-02-12 11:32:04,681 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,681 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
2025-02-12 11:32:04,681 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,682 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
2025-02-12 11:32:04,684 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,684 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
2025-02-12 11:32:04,690 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,691 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
2025-02-12 11:32:04,692 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,693 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,693 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
2025-02-12 11:32:04,693 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
2025-02-12 11:32:04,694 - ratelimit 5 per 1 minute (127.0.0.1) exceeded at endpoint: test
2025-02-12 11:32:04,695 - 127.0.0.1 - - [12/Feb/2025 11:32:04] "GET /test HTTP/1.0" 429 -
```

1. **Flask API Deployment:** A lightweight REST API was developed to handle patient data transactions and secure task offloading.
2. **Simulating Cyber Threats:** Using Postman, the following attack scenarios were tested:
   - **Unauthorised Access Attempts:** Simulated repeated login failures tested the effectiveness of RSA-based authentication. As shown in Fig. 8, unauthorised attempts were detected and logged via Postman API testing.
   - **Denial of Service (DoS) Attack:** High-volume request flooding was initiated to test MEC node overload resilience. ACTO successfully mitigated excessive API requests using rate-limiting mechanisms, as demonstrated in Fig. 9.
   - **Data Tampering Attack (MitM):** Malicious modifications of encrypted patient records were attempted to assess the integrity of AES-256 encryption. As seen in Fig. 10, ACTO ensured that data remained encrypted and secure,

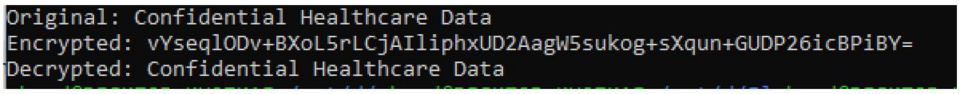


**Fig. 10** Secure data integrity maintained under a simulated Man-in-the-Middle attack using AES-256 and RSA encryption

effectively preventing MitM attacks. Also, detected unauthorized access attempts using intrusion detection and anomaly-based analysis (Fig. 11).

#### 5.3.2 Ethical considerations in quantum-enhanced healthcare

Ensuring equity in artificial intelligence and quantum-enhanced healthcare decision-making is imperative to mitigate biases in medical forecasts. The AQDT-IoT framework is specifically constructed to integrate a variety of diverse and impartial datasets, thereby reducing the likelihood of prejudicial outcomes. Furthermore, transparency and explicability constitute fundamental elements, enabling healthcare practitioners to comprehend quantum-augmented recommendations prior to their implementation, thus cultivating trust in the decision-making process. Moreover, as regulatory frameworks such as HIPAA and GDPR progress, the ACTO security model is engineered to adaptively revise its protocols, thereby guaranteeing ongoing adherence to emerging data protection regulations. This flexibility ensures that patient information remains safeguarded while upholding the integrity and ethical standards necessitated by contemporary healthcare systems.

## 6 Practical simulations for healthcare applications

The AQDT-IoT framework integrates IBM Quantum for cloud-based execution of computationally intensive tasks, eliminating the need for on-premises quantum infrastructure while ensuring scalability and efficiency.

### 6.1 IBM quantum hardware for real-time offloading

IBM Quantum provides a set of cloud-accessible quantum backends that facilitate secure and scalable task offloading. Figure 12 presents the IBM Quantum backends utilised in this study, including 'ibm_brisbane', 'ibm_kyiv', and 'ibm_sherbrooke'. These quantum processors execute task scheduling algorithms, leveraging AAE and Grover's search for optimal decision-making in resource allocation.

To ensure high reliability in quantum-assisted task execution, IBM Quantum provides hardware calibration metrics that help assess performance constraints. Figures 13, 14, 15, 1617 present key qubit metrics, including anharmonicity, frequency, readout assignment errors, and coherence times ($T_1$, $T_2$), which influence the efficiency and stability of quantum-based healthcare computations.

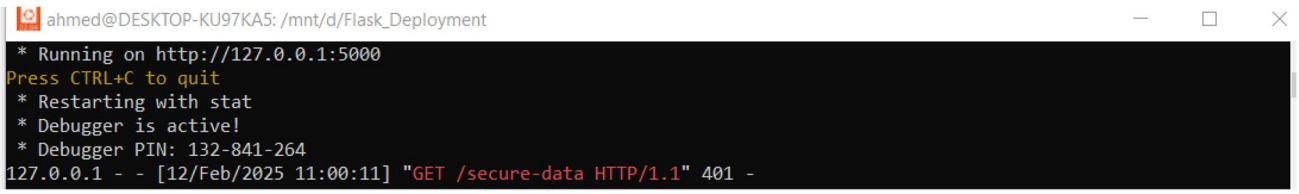


**Fig. 11** Flask server logs showing unauthorized access rejection due to missing authentication credentials

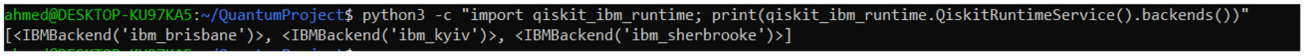


**Fig. 12** IBM Quantum backends used for task offloading, showcasing real hardware access for quantum execution

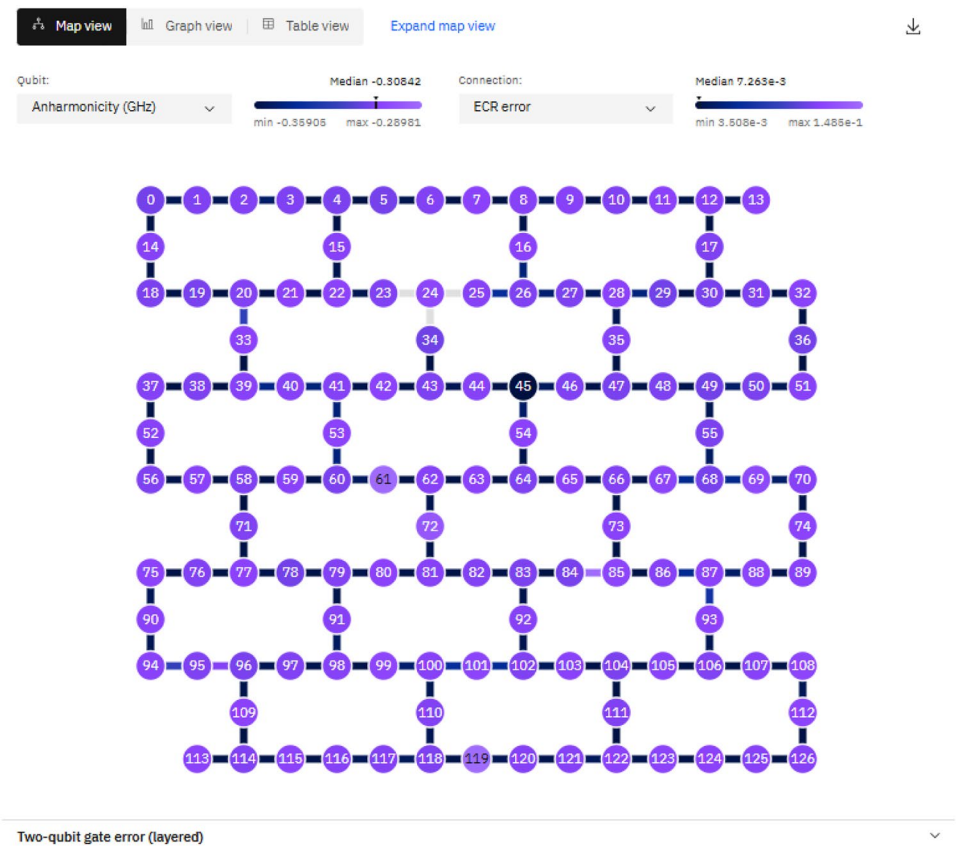


**Fig. 13** IBM Quantum hardware calibration data: Qubit anharmonicity (GHz) distribution

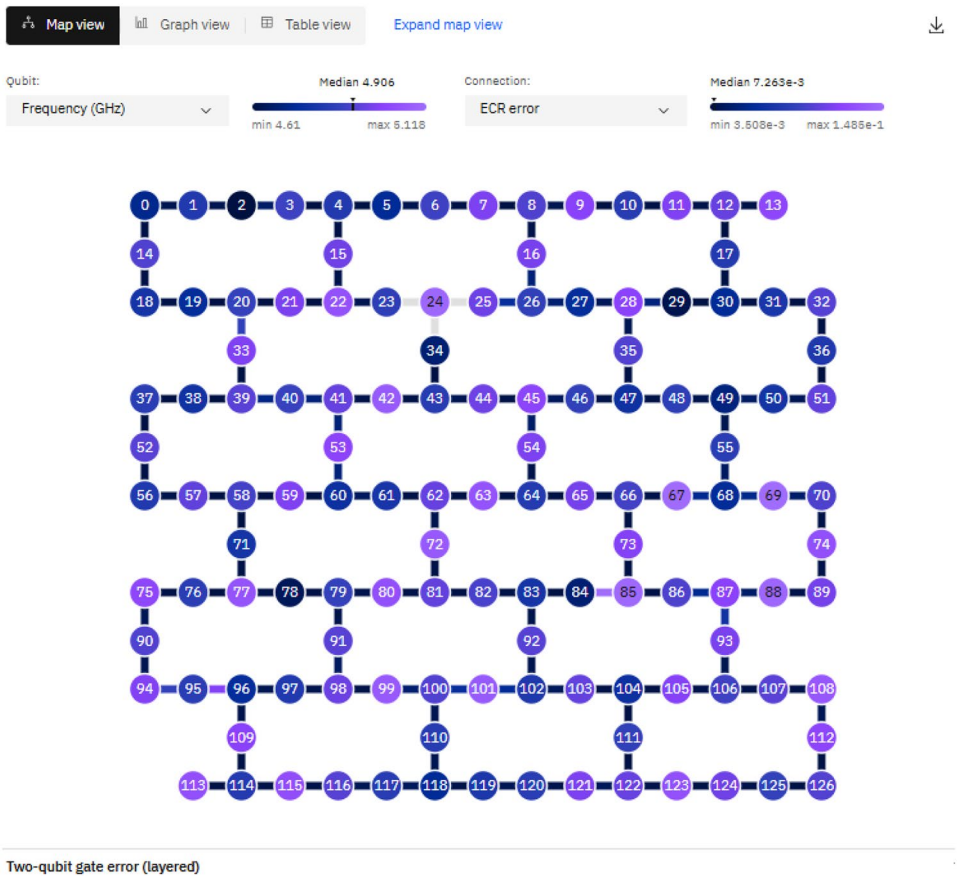


**Fig. 14** IBM Quantum hardware calibration data: Qubit frequency (GHz) variation across devices

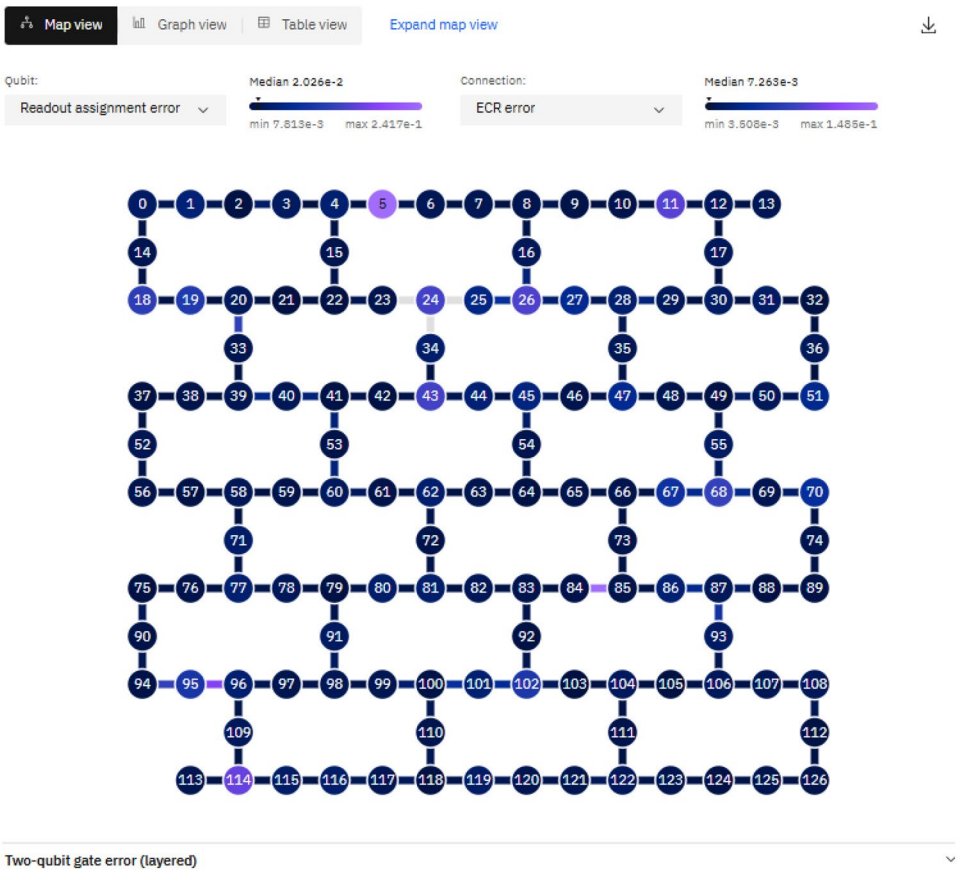


**Fig. 15** IBM Quantum hardware calibration data: Readout assignment error analysis

IBM Quantum processors operate at microwave frequencies, and their performance depends on qubit anharmonicity and resonance frequencies. Figure 13 illustrates the qubit anharmonicity distribution (GHz) across the IBM Quantum hardware used in this study. This metric impacts gate fidelities and the feasibility of executing multi-qubit operations essential for complex healthcare diagnostics.

Similarly, Fig. 14 depicts the qubit frequency range (GHz) across the IBM Quantum devices. Higher frequency stability correlates with reduced qubit dephasing, ensuring accurate quantum computations in patient monitoring and AI-assisted healthcare diagnostics.

Quantum computations are susceptible to readout errors, which impact the accuracy of healthcare task offloading. Figure 15 presents the readout assignment error distribution across IBM Quantum hardware, providing insights into the reliability of measurement outcomes during quantum-enhanced medical computations.

Since quantum healthcare applications rely on multi-qubit operations, the system's stability depends on the two-qubit gate error rate. Figures 16 and 17 illustrate the coherence properties of IBM Quantum processors, specifically the $T_1$ (decoherence time) and $T_2$ (relaxation time). Longer coherence times ensure higher computational accuracy, making quantum-assisted healthcare task scheduling more efficient.

#### 6.1.1 Impact of IBM quantum in healthcare task offloading

The integration of IBM Quantum hardware with AQDT-IoT enables:

- Task Execution Reliability: Calibration data helps optimise task selection strategies based on qubit performance.
- Optimised Decision-Making: Quantum-assisted Grover's search prioritises high-complexity medical tasks, ensuring rapid execution.
- Energy Efficiency: Offloading computationally demanding AI tasks to quantum processors reduces power consumption in hospital IT infrastructures.

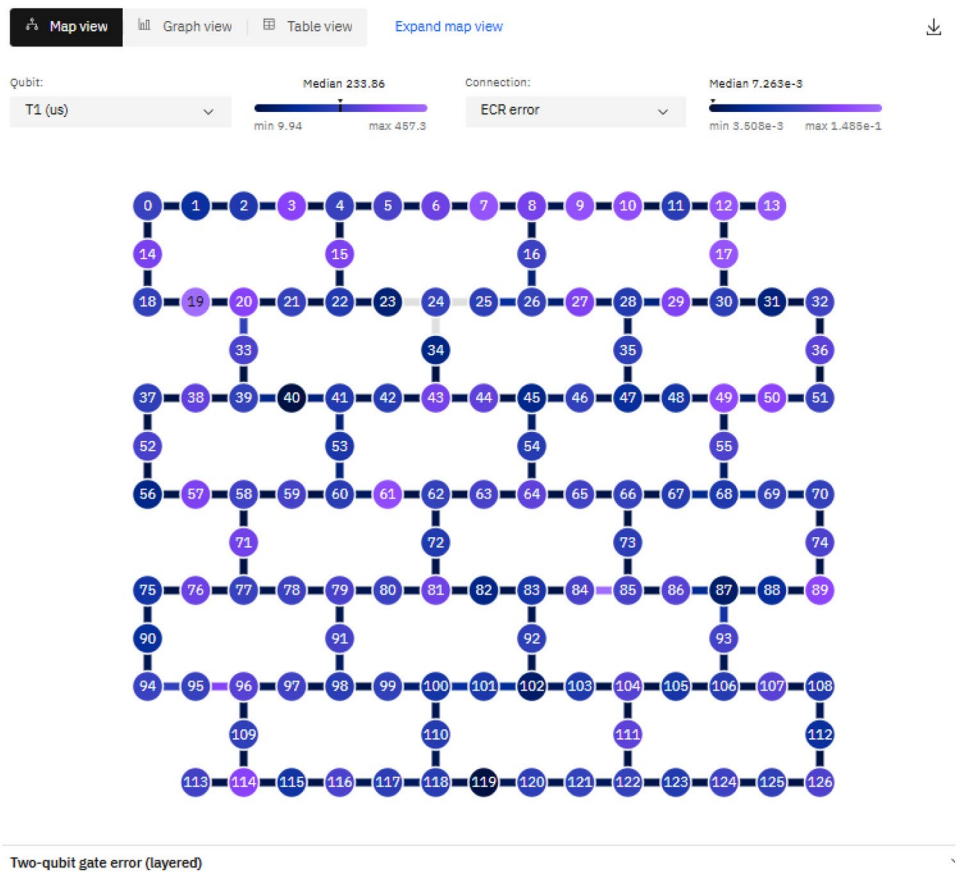


**Fig. 16** IBM Quantum hardware calibration data: $T_1$ (us) - Qubit decoherence time

– Security Compliance: IBM Quantum's cloud-based encryption ensures secure patient data transmission, mitigating cybersecurity risks in healthcare networks.

### 6.1.2 Quantum-enhanced use cases in healthcare

***Example 1: Wearables and Real-Time Patient Monitoring:*** Within a hospital network, wearable IoT health sensors continuously monitor vital parameters such as heart rate, oxygen saturation, and body temperature. These devices generate large volumes of real-time health data, which, if processed locally, could overload on-site computing infrastructure and delay critical decision-making.

To mitigate this, the AQDT-IoT algorithm applies quantum preprocessing via IBM Quantum APIs, utilising techniques such as:

- Approximate Amplitude Encoding (AAE) for efficient quantum feature mapping.
- Grover's search algorithm for rapid task offloading decisions.
- Quantum-enhanced DT updates to optimise patient monitoring and predictive diagnostics.

By offloading computationally intensive tasks to cloud-based quantum services, the system ensures that healthcare professionals receive instant alerts on critical patient conditions, reducing response times and improving patient safety.

***Example 2: Remote Telemedicine Consultations:*** In remote healthcare scenarios, telemedicine consultations rely on real-time patient data sharing through secure digital twin models. IBM Quantum enhances telemedicine applications by enabling:

- Efficient task scheduling for real-time patient data processing.
- Secure transmission of encrypted patient vitals between DTs and cloud-based quantum services.

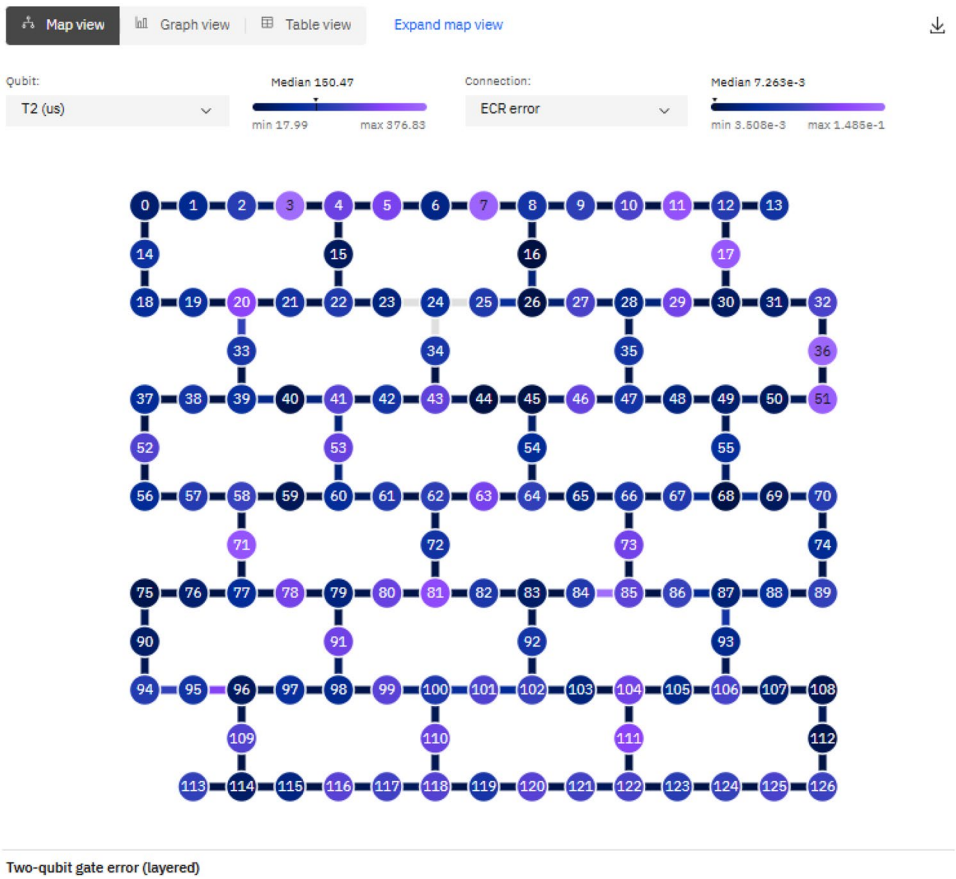


**Fig. 17** IBM Quantum hardware calibration data: $T_2$ (us) - Qubit relaxation time

- Optimised resource allocation for bandwidth-intensive operations (e.g., live video consultations with AI-assisted diagnostics).

For example, during a virtual consultation, patient oxygen levels, environmental humidity, and heart rate variability are streamed in real time. Quantum-enhanced DT models use Grover's search and AI-driven predictions to assess potential respiratory distress and optimise remote interventions. This cloud-based approach ensures scalability and reliability, even in bandwidth-constrained environments.

### 6.2 Scalability of AQDT-IoT in real-time healthcare networks

In addition to scalability, the efficiency of data transmission was evaluated using the compression ratio (Ccomm) as a metric for communication cost:

$$C_{\text{comm}} = \frac{\text{Original Size}}{\text{Compressed Size}}. \tag{24}$$

The AQDT-IoT framework was tested under increasing IoT device densities and MEC node workloads, demonstrating its ability to maintain low latency, high efficiency, and reliable task scheduling (Fig. 18).

- **Latency:** As shown in Fig. 18, average latency remains below 1 ms, even with a substantial increase in active IoT devices, due to the quantum preprocessing framework, which reduces decision-making complexity from $O(N)$ to $O(\sqrt{N})$. This low-latency operation is critical for applications like remote surgeries and real-time diagnostics, where rapid response times are vital.
- **Energy Efficiency:** Quantum-enhanced task scheduling reduced overall power consumption. Figure 18 shows that, as the number of devices increased, power consumption remained consistent, with up to a 20% reduction compared

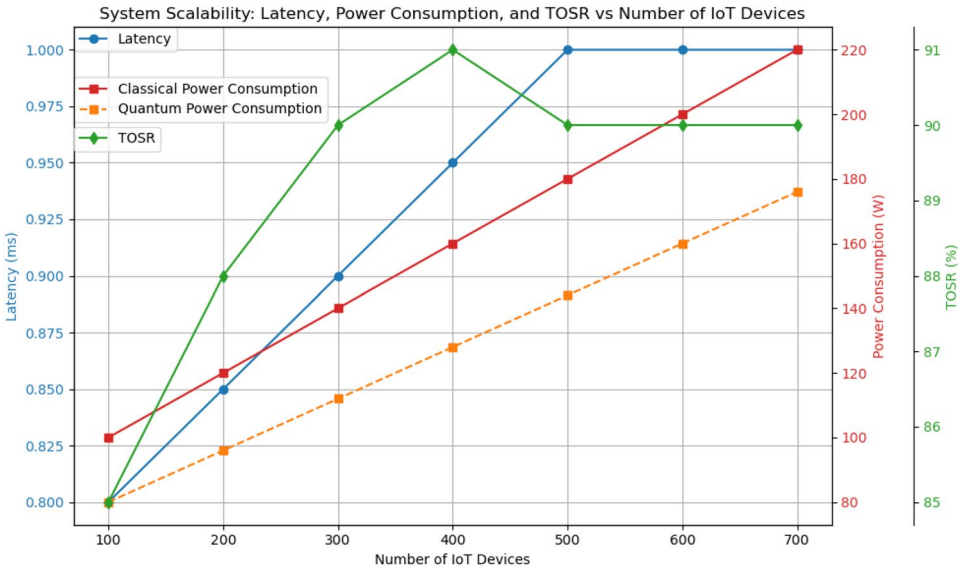


**Fig. 18** System Scalability: Latency, Power Consumption, and TOSR vs. Number of IoT Devices

to classical offloading systems. This energy efficiency is particularly beneficial for battery-operated wearable devices in continuous operation.

- **Computational Load Balance:** As the number of tasks and sensors increased, the system effectively managed the load, maintaining TOSR of approximately 90%. This ensured that even in high-demand healthcare environments (e.g., during mass patient monitoring or diagnostic imaging), critical operations like real-time sensor data analysis were handled reliably without interruption.

## 7 Insights and implications

### 7.1 Strategic insights on quantum computing in healthcare

As quantum computing advances, its feasibility and cost-effectiveness for healthcare applications continue to improve. Cloud-based quantum resources, particularly IBM Quantum, eliminate infrastructure costs while enhancing computational scalability for real-time patient monitoring, medical diagnostics, and secure data transmission. This flexibility ensures that healthcare organizations can scale computational resources efficiently without major upfront investments, aligning quantum processing capabilities with real-world patient care needs.

### 7.2 Cost-benefit analysis

To evaluate the practical impact of quantum computing in healthcare, a cost-benefit analysis was conducted, comparing traditional systems (C-S) to Quantum-Enhanced Systems (Q-ES). Table 4 summarises key performance improvements:

**Key Insights:** Task offloading success rate (TOSR) increased significantly, rising from 68% in traditional computing to 90% with quantum systems, marking a 32% improvement in efficiency. Similarly, the error rate (ER) dropped from 5% to

**Table 4** Comparison between Classical and Quantum-Enhanced Systems

| Metric | C-S | Q-ES | Improvement |
|---|---|---|---|
| TOSR | 68% | 90% | +32% |
| ER | 5% | 1% | 80% |
| Computational Speed | $\mathcal{O}(N)$ | $\mathcal{O}(\sqrt{N})$ | 2x faster |
| Energy Consumption | High | 20% lower | +20% savings |
| Cost of Infrastructure | Medium | Low (cloud-based) | Cost-effective |

Q-ES: Quantum-Enhanced System; TOSR: Task Offloading Success Rate; ER: Error Rate; C-S: Classical System

just 1%, demonstrating an 80% reduction due to quantum processing. Classical computing, constrained by $O(N)$ complexity, is surpassed by quantum-enhanced systems (Q-ES), which optimize processing to $O(\sqrt{N})$, effectively doubling computational speed. Moreover, conventional systems exhibit high energy consumption, whereas quantum scheduling reduces energy usage by 20%, promoting efficiency in resource utilization. Infrastructure costs in traditional systems range from moderate to high, but quantum cloud solutions present a scalable and cost-effective alternative, making advanced computing more accessible to healthcare facilities.

## 8 Conclusion

This study demonstrated the effectiveness of integrating DT, QC, AI, and IoT within a 6 G-enabled healthcare framework. The proposed DTH-ATB-MAPPO and AQDT-IoT algorithms significantly improved task offloading and resource optimisation, enabling personalised and efficient healthcare interventions.

Empirical evaluations demonstrated that quantum preprocessing improved Task Offloading Success Rate (TOSR) by 32% while reducing ER by 80%. These improvements translated to faster and more reliable decision-making, which is critical for real-time patient monitoring and emergency response scenarios.

Simulations confirmed that quantum-enhanced task scheduling significantly outperformed conventional offloading models, achieving higher success rates and lower error margins. Statistical analyses-including box plots and scatter plots-demonstrated that QC improved prediction accuracy and system reliability, reinforcing its role in optimising task execution, workload distribution, and cybersecurity resilience.

Future research should focus on enhancing offloading strategies through adaptive AI-driven models, reinforcement learning, and hybrid quantum-classical scheduling techniques. Further investigations into quantum noise mitigation and error correction mechanisms will be crucial to improving scalability and real-world deployment feasibility.

Despite its promise, the integration of QC into real-world healthcare infrastructures presents technical, financial, and operational challenges. Issues such as hardware limitations, high latency in cloud-based quantum services, and interoperability with classical computing frameworks must be addressed. Additionally, cybersecurity risks, including quantum-based threats and data encryption vulnerabilities, necessitate ongoing advancements in post-quantum cryptography and secure authentication models.

A major challenge in adopting cloud-based quantum computing-such as IBM Quantum-is cost scalability. While cloud access eliminates infrastructure costs, quantum processing time remains expensive, especially for real-time, high-frequency medical computations. Future optimisations should explore cost-efficient hybrid quantum-classical computing models to maximise computational performance while reducing financial burdens on healthcare providers.

By continuing to refine quantum-enhanced healthcare frameworks, the potential for faster, more secure, and energy-efficient medical data processing can be fully realised, shaping the future of intelligent, data-driven patient care.

**Author contributions** Ahmed K. Jameil contributed to the conceptualisation, design, data acquisition, analysis, and interpretation. He developed the methodology, provided resources, validated results, and drafted the manuscript. Hamed Al Raweshidy oversaw funding acquisition, investigation, project management, and supervision. He provided resources and critically revised the manuscript. Both authors are accountable for the accuracy and integrity of the work.

**Funding** This research was supported by Brunel University of London.

**Data availability** The datasets generated during and/or analyzed during the current study are available from the corresponding author, Hamed Al-Raweshidy, upon reasonable request. Data collected from IoT healthcare sensors (e.g., SpO2, heart rate, body temperature) were simulated for the purpose of this research. Quantum computing experiments were conducted via IBM Quantum cloud services, and corresponding simulation logs are available upon request. Additionally, publicly available anonymized data from the MIMIC-III database were used and can be accessed at https://physionet.org/content/mimiciii/1.4/.

## Declarations

**Ethics approval and consent to participate** Not applicable.

**Consent for publication** Not applicable.

**Competing interests** The authors declare no competing interests.

## References

1. Maïzi Y, Arcand A, Bendavid Y. Digital twin in healthcare: classification and typology of models based on hierarchy, application, and maturity. Internet of Things. 2024;28: 101379. https://doi.org/10.1016/j.iot.2024.101379.
2. Nele L, Mattera G, Yap EW, Vozza M, Vespoli S. Towards the application of machine learning in digital twin technology: a multi-scale review. Discover Appl Sci. 2024. https://doi.org/10.1007/s42452-024-06206-4.
3. Jameil AK, Al-Raweshidy H. Implementation and evaluation of digital twin framework for internet of things based healthcare systems. IET Wirel Sensor Syst. 2024;14(6):507–27. https://doi.org/10.1049/wss2.12101.
4. Mohamed N, Al-Jaroodi J, Jawhar I, Kesserwan N. How healthcare systems engineering can benefit from digital twins? 2023 IEEE International Systems Conference (SysCon), 2023;1–6.
5. Al-Sadoon ME, Jedidi A, Al-Raweshidy H. Dual-tier cluster-based routing in mobile wireless sensor network for iot application. IEEE Access. 2023;11:4079–94. https://doi.org/10.1109/ACCESS.2023.3235200.
6. Zhao L, Wang S, Ding X. Optimization method of task uninstallation in mobile edge computing environment combining improved deep q-learning and transmission learning. Discover Appl Sci. 2024. https://doi.org/10.1007/s42452-024-06396-x.
7. Adeli M, Bagheri N, Maimani HR, Kumari S, Rodrigues JJPC. A post-quantum compliant authentication scheme for iot healthcare systems. IEEE Internet of Things J. 2023. https://doi.org/10.1109/JIOT.2023.3309931.
8. Alturki B, Abu Al-Haija Q, Alsemmeari RA, Alsulami AA, Alqahtani A, Alghamdi BM, Bakhsh ST, Shaikh RA. Iomt landscape: navigating current challenges and pioneering future research trends. Discover Appl Sci. 2024;7(1):26. https://doi.org/10.1007/s42452-024-06351-w.
9. Rishiwal V, Agarwal U, Yadav M, Tanwar S, Garg D, Guizani M. A new alliance of machine learning and quantum computing: concepts, attacks, and challenges in iot networks. IEEE Internet of Things J. 2025. https://doi.org/10.1109/JIOT.2025.3535414.
10. Peelam MS, Rout AA, Chamola V. Quantum computing applications for internet of things. IET Quantum Commun. 2024;5(2):103–12. https://doi.org/10.1049/qtc2.12079.
11. Jameil AK, Al-Raweshidy H. A digital twin framework for real-time healthcare monitoring: leveraging ai and secure systems for enhanced patient outcomes. Discover Internet of Things. 2025;5(1):37. https://doi.org/10.1007/s43926-025-00135-3.
12. Jameil AK, Al-Raweshidy H. Hybrid cloud-edge AI framework for real-time predictive analytics in digital twin healthcare systems. Res Sq. 2024. https://doi.org/10.2120/rs.3.rs-5412158/v1.
13. Al-Janabi TA, Al-Raweshidy HS. An energy efficient hybrid mac protocol with dynamic sleep-based scheduling for high density iot networks. IEEE Internet of Things J. 2019;6(2):2273–87. https://doi.org/10.1109/JIOT.2019.2905952.
14. Jameil AK, Al-Raweshidy H. Ai-enabled healthcare and enhanced computational resource management with digital twins into task offloading strategies. IEEE Access. 2024;12:90353–70. https://doi.org/10.1109/ACCESS.2024.3420741.
15. Jameil AK, Al-Raweshidy H. Enhancing offloading with cybersecurity in edge computing for digital twin-driven patient monitoring. IET Wirel Sensor Syst. 2024. https://doi.org/10.1049/wss2.12086.
16. Rossman U, Tenne R, Solomon O, Kaplan-Ashiri I, Dadosh T, Eldar YC, Oron D. Rapid quantum image scanning microscopy by joint sparse reconstruction. Optica. 2019;6(10):1290. https://doi.org/10.1364/OPTICA.6.001290.
17. Ahmadian M, Ruiz M, Comellas J, Velasco L. Darius: a digital twin to improve the performance of quantum key distribution. J Lightwave Technol. 2024;42(5):1356–67. https://doi.org/10.1109/JLT.2023.3321774.
18. Jameil AK, Al-Raweshidy H. Efficient cnn architecture on fpga using high level module for healthcare devices. IEEE Access. 2022;10:60486–95. https://doi.org/10.1109/ACCESS.2022.3180829.
19. Tunc HSD, Wang Y, Bassoli R, Fitzek FHP. Machine learning based attack detection for quantum key distribution. In: 2023 IEEE 9th World Forum on Internet of Things (WF-IoT), pp. 1–6. IEEE, Aveiro, Portugal. 2023. https://doi.org/10.1109/WF-IoT58464.2023.10539417. https://ieeexplore.ieee.org/document/10539417/.
20. Cao H, Garg S, Mumtaz S, Alrashoud M, Yang L, Kaddoum G. Softwarized resource allocation in digital twins-empowered networks for future quantum-enabled consumer applications. IEEE Trans Consumer Electron. 2024;70(1):800–10. https://doi.org/10.1109/TCE.2024.3370052.
21. Ebrahimi A, Afghah F. Intelligent task offloading: advanced mec task offloading and resource management in 5g networks. arXiv preprint. 2025. https://doi.org/10.4855/arXiv.2501.06242.
22. Pratama D. Securing social well-being in the quantum age: Legal roadmaps for pqc in banking to healthcare. Int J Soc Health. 2024. https://doi.org/10.1007/978-3-031-73350-5_7.
23. Giang V. Quantum computing and its applications in healthcare. ODU Digit Commons. 2023. https://doi.org/10.2577/46Q5-SJ29.
24. VanGeest JB, Fogarty KJ, Hervey WG, Hanson RA, Nair S, Akers TA. Quantum readiness in healthcare and public health: building a quantum literate workforce. arXiv preprint. 2024. https://doi.org/10.4855/arXiv.2403.00122.
25. Katsoulakis E, Wang Q, Wu H, Shahriyari L, Fletcher R, Liu J, Achenie L, Liu H, Jackson P, Xiao Y, Syeda-Mahmood T, Tuli R, Deng J. Digital twins for health: a scoping review. npj Digit Med. 2024;7(1):77. https://doi.org/10.1038/s41746-024-01073-0.
26. Sahal R, Alsamhi SH, Brown KN. Personal digital twin: a close look into the present and a step towards the future of personalised healthcare industry. Sensors. 2022;22(15):5918. https://doi.org/10.3390/s22155918.

27. Qu Z, Li Y, Liu B, Gupta D, Tiwari P. Dtqfl: a digital twin-assisted quantum federated learning algorithm for intelligent diagnosis in 5g mobile network. IEEE J Biomed Health Inform. 2024. https://doi.org/10.1109/JBHI.2023.3303401.
28. KhademHosseini V, Jameil AK, Ahmadi MT. Analysis of temperature limitation of graphene single electron transistor: communication. Diyala J Eng Sci (DJES). 2015;8(4):568–73.
29. Łukaniszyn M, Majka Grochowicz B, Mikołajewski D, Kawala-Sterniuk A. Digital twins generated by artificial intelligence in personalized healthcare. Appl Sci. 2024. https://doi.org/10.3390/app14209404.
30. Zhang J, Li L, Lin G, Fang D, Tai Y, Huang J. Cyber resilience in healthcare digital twin on lung cancer. IEEE Access. 2020;8:201900–13. https://doi.org/10.1109/ACCESS.2020.3034324.
31. Sai S, Gaur A, Hassija V, Chamola V. Artificial intelligence empowered digital twin and nft-based patient monitoring and assisting framework for chronic disease patients. IEEE Internet of Things Mag. 2024;7(2):101–6. https://doi.org/10.1109/IOTM.001.2300138.
32. De Benedictis A, Mazzocca N, Somma A, Strigaro C. Digital twins in healthcare: an architectural proposal and its application in a social distancing case study. IEEE J Biomed Health Inform. 2023;27(10):5143–54. https://doi.org/10.1109/JBHI.2022.3205506.
33. Srivastava R. Quantum computing in drug discovery. Inform Syst Smart City. 2023. https://doi.org/10.5940/issc.v1i1.294.
34. Sheraz M, Chuah TC, Lee YL, Alam MM, Al-Habashna A, Han Z. A comprehensive survey on revolutionizing connectivity through artificial intelligence-enabled digital twin network in 6g. IEEE Access. 2024. https://doi.org/10.1109/ACCESS.2024.3384272.
35. Sharma N, Prakash Verma J, Gautam S, Balas VE, Krishnan S. Green computing for sustainable smart cities: a data analytics applications perspective. 1st ed. Boca Raton: CRC Press; 2024.
36. Zhou L, Leng S, Wang Q, Quek TQS, Guizani M. Cooperative digital twins for uav-based scenarios. IEEE Commun Mag. 2024. https://doi.org/10.1109/MCOM.001.2400207.
37. Mondal A, Chatterjee PS, Ray NK. An optimal novel approach for dynamic energy-efficient task offloading in mobile edge-cloud computing networks. SN Comput Sci. 2024;5(5):655. https://doi.org/10.1007/s42979-024-02992-1.
38. Tatekalva S, Ravuri Y, Maddipatla SK, Macigi UR. Design of dynamic task offloading method in multi cloud mec environments using deep learning. J Auton Intell. 2024;7(5):1367. https://doi.org/10.32629/jai.v7i5.1367.
39. Zhang Q, Yang Y, Yi C, Okegbile SD, Cai J. Energy- and cost-aware offloading of dependent tasks with edge-cloud collaboration for human digital twin. IEEE Internet of Things J. 2024;11(17):29116–31. https://doi.org/10.1109/JIOT.2024.3406591.
40. Tan B, Ai L, Wang M, Wang J. Toward a task offloading framework based on cyber digital twins in mobile edge computing. IEEE Wirel Commun. 2023;30(3):157–62. https://doi.org/10.1109/MWC.020.2200533.
41. Wang J, Zhang M, Yin Q, Yin L, Peng Y. Multi-agent reinforcement learning for task offloading with hybrid decision space in multi-access edge computing. Ad Hoc Netw. 2025;166: 103671. https://doi.org/10.1016/j.adhoc.2024.103671.
42. Kulkarni C, Quraishi A, Raparthi M, Shabaz M, Khan MA, Varma RA, Keshta I, Soni M, Byeon H. Hybrid disease prediction approach leveraging digital twin and metaverse technologies for health consumer. BMC Med Inform Decis Making. 2024;24(1):92. https://doi.org/10.1186/s12911-024-02495-2.
43. Zheng X, Tahir M, Aurangzeb K, Anwar MS, Aamir M, Farzan A, Ullah R. Non-orthogonal multiple access-based mec for energy-efficient task offloading in e-commerce systems. J Cloud Comput. 2024;13(1):117. https://doi.org/10.1186/s13677-024-00680-2.
44. Liu C, Wang H, Zhao M, Liu J, Zhao X, Yuan P. Dependency-aware online task offloading based on deep reinforcement learning for iov. J Cloud Comput. 2024;13(1):136. https://doi.org/10.1186/s13677-024-00701-0.
45. Alqahtani A, Alsubai S, Bhatia M. Digital-twin-assisted healthcare framework for adult. IEEE Internet of Things J. 2024;11(8):14963–70. https://doi.org/10.1109/JIOT.2023.3345331.
46. Wei X, Gao X, Ye K, Xu C-Z, Wang Y. A quantum reinforcement learning approach for joint resource allocation and task offloading in mobile edge computing. IEEE Trans Mobile Comput. 2024. https://doi.org/10.1109/TMC.2024.3496918.
47. Das C, Mumu AA, Ali MF, Sarker SK, Muyeen SM, Das SK, et al. Toward iort collaborative digital twin technology enabled future surgical sector: technical innovations, opportunities and challenges. IEEE Access. 2022;10:129079–104. https://doi.org/10.1109/access.2022.3227644.