TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 31/31 pp456–478
DOI: 10.26599/TST.2024.9010122
Volume 30, Number 1, February 2025

Quantum-Inspired Sensitive Data Measurement and Secure Transmission in 5G-Enabled Healthcare Systems

Xiaohong Lv, Shalli Rani, Shanmuganathan Manimurugan, Adam Slowik, and Yanhong Feng*

Abstract: The exponential advancement witnessed in 5G communication and quantum computing has presented unparalleled prospects for safeguarding sensitive data within healthcare infrastructures. This study proposes a novel framework for healthcare applications that integrates 5G communication, quantum computing, and sensitive data measurement to address the challenges of measuring and securely transmitting sensitive medical data. The framework includes a quantum-inspired method for quantifying data sensitivity based on quantum superposition and entanglement principles and a delegated quantum computing protocol for secure data transmission in 5G-enabled healthcare systems, ensuring user anonymity and data confidentiality. The framework is applied to innovative healthcare scenarios, such as secure 5G voice communication, data transmission, and short message services. Experimental results demonstrate the framework's high accuracy in sensitive data measurement and enhanced security for data transmission in 5G healthcare systems, surpassing existing approaches.

Key words: quantum computing; 5G; sensitive data measurement; healthcare

1 Introduction

A paradigm change in the healthcare industry has emerged with the arrival of 5G communication technology, making it possible to construct previously unthinkable novel applications and services. The high-speed, low-latency, and massive connectivity offered by 5G networks have opened up new possibilities for remote healthcare delivery, real-time patient monitoring, and personalized treatment planning[1–3]. 5G-enabled telemedicine platforms, for example, provide virtual consultations between patients and medical experts, decreasing the need for in-person visits and enhancing access to healthcare services in underprivileged regions. Additionally, 5G networks facilitate the deployment of wearable sensors and Internet of Things (IoT) devices that may continually monitor patients' vital signs, activity levels, and medication adherence. This data is essential for proactive treatments and the early diagnosis of health issues[4, 5]. That being said, it gets more and harder to guarantee the security and privacy of this sensitive data as more and more medical data is gathered and sent across 5G networks. Breach of medical data can result in serious repercussions, such as monetary losses, harm to one's reputation, and jeopardized patient safety[6, 7]. Thus, creating strong security protocols and privacy-maintaining strategies is essential to establishing confidence and encouraging using 5G-enabled healthcare applications.

The potential for quantum computing to tackle issues

• Xiaohong Lv and Yanhong Feng are with The First Affiliated Hospital of Jinzhou Medical University, Jinzhou 121000, China. E-mail: lvxh@jzmu.edu.cn; fengyh@jzmu.edu.cn.
• Shalli Rani is with Institute of Engineering and Technology, Chitkara University, Punjab 140401, India. E-mail: shalli.rani@chitkara.edu.in.
• Shanmuganathan Manimurugan is with Faculty of Computers and Information Technology, University of Tabuk, Tabuk 47512, Saudi Arabia. E-mail: mmurugan@ut.edu.sa.
• Adam Slowik is with Koszalin University of Technology, Koszalin 75453, Poland. E-mail: adam.slowik@tu.koszalin.pl.
* To whom correspondence should be addressed.
Manuscript received: 2024-04-20; revised: 2024-06-24; accepted: 2024-06-29

beyond the capability of traditional computers signifies a major shift in computing capabilities. Quantum computing can do some computations tenfold quicker than conventional computers by utilizing quantum mechanical concepts like superposition and entanglement[8–10], which has important ramifications for machine learning, cryptography, and optimization, among other fields. In the context of 5G communication and healthcare systems, quantum computing can provide enhanced security features using quantum key distribution (QKD) protocols. QKD enables the secure exchange of cryptographic keys between parties, guaranteeing the confidentiality and integrity of transmitted data. By leveraging quantum states' inherent randomness and unclonability, QKD offers unconditional security against eavesdropping and tampering, making it an attractive solution for protecting sensitive medical information in 5G networks[11, 12]. Moreover, quantum computing can be applied to solve complex optimization problems in healthcare, such as drug discovery, personalized medicine, and resource allocation. Improved patient outcomes and lower healthcare expenses can result from the capacity to investigate large solution spaces and choose the best course of action[13–17]. Consequently, much research is already being done on combining quantum computing with 5G connectivity and healthcare systems, which might completely change how healthcare is provided and improve patient care.

One of the main obstacles to guarantee healthcare data safety and compliance with privacy requirements is measuring and evaluating its sensitivity[18]. Medical data comprises many types of information with different sensitivity levels, such as genetic data, biometric data, medical imaging, and electronic health records (EHRs)[19]. For example, a patient's HIV status or mental health history may be considered highly sensitive, requiring stringent access controls and encryption measures, while general demographic information may be less sensitive. However, given that it relies on many variables, including the context of usage, the possibility of harm, and the data subject's preferences, figuring out the right amount of sensitivity for each data element is difficult.

Traditional approaches to data sensitivity measurement, such as manual classification by experts or rule-based systems, have several limitations. Manual classification is time-consuming, costly, and prone to inconsistent results from human error, particularly when handling large amounts of data. Conversely, rule-based systems depend on pre-established standards and limitations, which could miss the subtleties and situational elements that affect data sensitivity. Moreover, these approaches often need more flexibility to adapt to evolving privacy requirements and changing data landscapes. Therefore, there is a pressing need for the development of efficient, accurate, and automated methods for measuring and quantifying the sensitivity of healthcare data, enabling the implementation of appropriate security measures and access controls in 5G-enabled healthcare systems.

Secure transmission of sensitive medical data is a critical requirement in 5G-enabled healthcare systems, as the increased connectivity and data sharing among various healthcare entities expose the data to a wide range of security threats[20–23]. These threats include unauthorized access, eavesdropping, tampering, and data breaches, which can compromise patient privacy and lead to serious consequences, such as identity theft, financial fraud, and social stigma. Traditional security mechanisms, such as encryption and access control, have been widely used to protect data confidentiality and integrity during transmission. However, these mechanisms face several limitations in 5G-enabled healthcare systems[24, 25]. First, the high volume and velocity of medical data generated by IoT devices and wearable sensors require computationally efficient encryption algorithms that can operate on resource-constrained devices. Second, the increasing sophistication of cyberattacks and the advent of quantum computing pose significant challenges to the security of classical encryption schemes. Therefore, there is a need for novel secure data transmission protocols that can leverage the advantages of quantum computing and 5G communication to provide enhanced security and privacy guarantees. Quantum-based security mechanisms, such as QKD and quantum encryption, offer the potential for unconditional security against eavesdropping and tampering. Moreover, integrating these mechanisms with 5G networks can enable secure and efficient data transmission across various healthcare entities, supporting real-time collaboration and data sharing for improved patient care.

Integrating quantum computing, 5G communication, and sensitive data measurement techniques in healthcare applications poses several challenges and

limitations. One of the main challenges is the scalability and reliability of quantum hardware and software systems, which are still in their early stages of development and may need to be ready for large-scale deployment in healthcare settings. Another challenge is the interoperability and standardization of quantum communication protocols and data formats, which may hinder the seamless integration of quantum technologies with existing healthcare systems.

To address these challenges, we propose a novel framework integrating quantum computing, 5G communication, and sensitive data measurement for healthcare applications. Our main contributions are as follows:

• We develop a quantum-inspired sensitive data measurement method to quantify the sensitivity of medical data based on quantum superposition and entanglement principles. The sensitivity of many kinds of medical data, including biometric data, medical pictures, and EHRs, may be effectively and precisely measured using the proposed framework.

• We design a delegated quantum computing protocol for secure data transmission in 5G-enabled healthcare systems. The protocol leverages QKD and quantum homomorphic encryption (QHE) to ensure the confidentiality and integrity of transmitted data. It also incorporates a quantum-based user authentication scheme to preserve user anonymity during transmission.

• We present several innovative applications of our proposed framework, including secure 5G voice communication, data transmission, and short message services for healthcare scenarios. These applications demonstrate the practicality and effectiveness of integrating quantum computing and 5G communication in real-world healthcare systems.

The rest of this paper is organized as follows. Section 2 reviews the related work on quantum computing, 5G communication, and sensitive data measurement in healthcare. Section 3 presents the proposed quantum-inspired sensitive data measurement method, describes the delegated quantum computing protocol for secure data transmission in 5G-enabled healthcare systems, and showcases several innovative applications of our proposed framework. The analysis and results of the experiment are reported in Section 4. Section 5 wraps up the work and addresses potential avenues for further research.

2 Related Work

The rapid advancements in quantum computing, 5G communication, and sensitive data measurement technologies have paved the way for innovative applications in healthcare systems. We review the recent research efforts in these domains and their potential impact on revolutionizing healthcare delivery and improving patient outcomes.

Quantum computing has emerged as a promising paradigm for solving complex computational problems in healthcare. Almulihi et al.[26] analyzed the implications of healthcare data breaches through computational techniques, highlighting the importance of secure and privacy-preserving data management. Qian et al.[27] proposed a quantum-enhanced privacy-preserving data aggregation scheme for smart healthcare systems, leveraging the power of quantum cryptography to ensure data confidentiality.

The advent of 5G communication networks has opened up new opportunities for efficient and reliable data transmission in healthcare. Elhoseny and Shankar[28] presented a comprehensive review of 5G-enabled healthcare applications, discussing the potential of 5G networks in enabling real-time remote monitoring, telesurgery, and personalized medicine. Yang et al.[29] proposed a secure and efficient data transmission scheme for the 5G-enabled Internet of medical things, ensuring data integrity and privacy. Moreover, Bishoyi and Misra[30] investigated integrating 5G networks with edge computing for low-latency and high-reliability healthcare applications.

Sensitive data measurement techniques have gained significant attention in healthcare due to the increasing concerns over data privacy and security. The integration of quantum computing, 5G communication, and sensitive data measurement technologies has the potential to revolutionize healthcare delivery. Hossain and Muhammad[31] proposed a 5G-enabled quantum-enhanced healthcare framework for secure and efficient data transmission and analysis, leveraging the benefits of both technologies. Chen et al.[32] developed a quantum-secure smart healthcare system using 5G networks and QKD to ensure data confidentiality and integrity. Furthermore, Li et al.[33] explored the application of quantum-enhanced machine learning algorithms for sensitive data analysis in 5G-enabled healthcare systems.

Despite the promising advancements in these

domains, several challenges remain to be addressed for the widespread adoption of these technologies in healthcare. These challenges include the scalability and practicality of quantum computing systems, the security and privacy concerns associated with 5G networks, and the efficiency and robustness of sensitive data measurement techniques. The proposed framework builds upon these advancements, aiming to provide a comprehensive and integrated solution for secure, efficient, and intelligent healthcare delivery in the era of quantum computing and 5G communication.

3 Proposed Method

3.1 Quantum-inspired sensitive data measurement

In the era of 5G-enabled healthcare systems, the volume and complexity of medical data have grown exponentially, posing significant challenges for sensitive data measurement and protection. Traditional approaches, such as manual classification and rule-based methods, struggle to keep pace with medical data's increasing scale and diversity. To address these challenges, we propose a quantum-inspired sensitive data measurement approach that leverages the principles of quantum computing to efficiently and accurately quantify the sensitivity of medical data in 5G networks.

In order to make use of the special qualities of quantum systems, such as superposition and entanglement, we first encode medical data using quantum states. Let $|\psi_i\rangle$ denote the quantum state representation of a medical data item i, which can be expressed as a superposition of two basis states:

$$|\psi_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle \tag{1}$$

where $|0\rangle$ and $|1\rangle$ represent the non-sensitive and sensitive states of the data item, respectively. α_i and β_i are complex amplitudes satisfying $|\alpha_i|^2 + |\beta_i|^2 = 1$.

We first perform a distributed structural reorganization of the data to measure the sensitivity of medical data in a 5G-enabled distributed healthcare environment. This process involves partitioning the medical data into smaller, more manageable subsets and redistributing them across multiple 5G network nodes. By leveraging the high-speed, low-latency characteristics of 5G networks, we can efficiently perform this distributed reorganization while ensuring data integrity and consistency.

The collection of medical data items is denoted by $\mathcal{A} = a_1, a_2, \ldots, a_N$, where N is the total number of items. $\mathcal{A}$ is divided into K subsets, which are identified as $\mathcal{A}_1, \mathcal{A}_2, \ldots, \mathcal{A}_K$. This is done such that:

$$|\mathcal{A} = \bigcup_{k=1}^{K} \mathcal{A}_k \tag{2}$$

$$|\mathcal{A}_i \cap \mathcal{A}_j = \emptyset, \forall i \neq j \tag{3}$$

Each subset $\mathcal{A}_k$ is then assigned to a different 5G network node for further processing.

Next, we apply a quantum-inspired statistical analysis model to each data subset $\mathcal{A}_k$. This model leverages the concepts of quantum superposition and interference to efficiently compute statistical properties of the data, such as mean, variance, and sensitivity scores. The quantum-inspired statistical analysis model is defined as follows:

$$|\mu_k\rangle = \frac{1}{\sqrt{|\mathcal{A}_k|}} \sum_{i \in \mathcal{A}_k} |\psi_i\rangle \tag{4}$$

where $|\mathcal{A}_k|$ indicates the cardinality of $\mathcal{A}_k$ and $|\mu_k\rangle$ is the quantum state storing the statistical features of the data subset $\mathcal{A}_k$.

We perform a quantum measurement operation to extract the sensitivity information from the quantum state $|\mu_k\rangle$. Let M_k denote the measurement operator corresponding to the sensitivity measurement of the data subset $\mathcal{A}_k$. The sensitivity score S_k of $\mathcal{A}_k$ is given by:

$$|S_k = \langle\mu_k|M_k|\mu_k\rangle \tag{5}$$

where $\langle\mu_k|$ represents the conjugate transpose of $|\mu_k\rangle$.

The measurement operator M_k is designed to capture the sensitivity information based on the quantum states of the individual data items in $\mathcal{A}_k$. One possible way to construct M_k is using a weighted sum of the projectors onto the sensitive basis state $\langle 1|$:

$$|M_k = \sum_{i \in \mathcal{D}_k} w_i|1\rangle\langle 1| \tag{6}$$

where w_i represents the weight assigned to the sensitive basis state of the data item i, the weights w_i can be determined based on various factors, such as the type of medical data, the context of use, and the potential impact of a breach.

We further employ a fuzzy fusion and clustering method inspired by quantum mechanics to improve the precision and effectiveness of the sensitivity measuring process. This technique allows us to group similar medical data items and compute their collective

sensitivity scores, reducing the computational overhead and improving the robustness of the measurement results.

The set of clusters is denoted by $C = c_1, c_2, \ldots, c_L$, where each cluster c_l represents a collection of related medical data items. The fuzzy membership degree of a data item i to a cluster c_l is given by

$$|\mu_{il} = \frac{1}{\sum_{j=1}^{L}\left(\frac{d(i,c_l)}{d(i,c_j)}\right)^{\frac{2}{m-1}}} \tag{7}$$

where $d(i,c_l)$ represents the distance between the data item i and the cluster center of c_l, and m is a fuzzy parameter that controls the degree of fuzziness.

The fuzzy fusion and clustering process is performed iteratively, updating the cluster centers and membership degrees until convergence. The updated cluster centers are computed using the quantum-inspired centroid calculation:

$$|c_l\rangle = \frac{\sum_{i=1}^{N}(\mu_{il})^m|\psi_i\rangle}{\sum_{i=1}^{N}(\mu_{il})^m} \tag{8}$$

where $|c_l\rangle$ represents the quantum state of the cluster center of c_l.

After the fuzzy fusion and clustering process, the sensitivity score of each cluster c_l is computed using the quantum measurement operation:

$$|S_{c_l} = \langle c_l|M_{c_l}|c_l\rangle \tag{9}$$

where M_{c_l} is the measurement operator corresponding to the sensitivity measurement of the cluster c_l.

The overall sensitivity score of the medical data set $\mathcal{A}$ is then obtained by aggregating the sensitivity scores of the individual clusters:

$$|S = \sum_{l=1}^{L} w_{c_l} S_{c_l} \tag{10}$$

where w_{c_l} represents the weight assigned to the sensitivity score of the cluster c_l, which can be determined based on the size and importance of the cluster.

We employ quantum-based encryption and decryption techniques to ensure the security and privacy of sensitive data during the measurement process. Medical data elements undergo encryption utilizing QHE techniques, facilitating computations to be executed directly on encrypted data sans the necessity of decryption[34].

$$|\psi_i^{\text{enc}}\rangle = E(|\psi_i\rangle) \tag{11}$$

The encrypted quantum states are then used in the quantum-inspired statistical analysis and fuzzy fusion and clustering processes, ensuring that the sensitive information remains protected throughout the measurement pipeline.

To decrypt the sensitivity scores and obtain the final results, a quantum homomorphic decryption operation D is applied:

$$|S = D(S^{\text{enc}}) \tag{12}$$

where S^{enc} represents the encrypted sensitivity score obtained from the measurement process.

The quantum-inspired sensitive data measurement method employs a combination of quantum algorithms and techniques to efficiently and accurately measure the sensitivity of healthcare data. One of the key algorithms used is the quantum amplitude estimation algorithm, which leverages the quantum phase estimation algorithm to estimate the amplitudes of quantum states encoding the sensitive information. This allows for the efficient computation of sensitivity scores based on the probability distributions of the data.

The QHE schemes are integrated with the delegated quantum computing protocol to enable secure outsourcing of quantum computations on sensitive healthcare data. The healthcare providers encrypt the data using QHE before transmitting it to the quantum computing servers, which can perform the required computations on the encrypted data without accessing the plaintext. The results of the computations are then returned to the healthcare providers in encrypted form, which can be decrypted using the corresponding QHE keys.

The proposed quantum-inspired sensitive data measurement approach offers several advantages over traditional methods. First, leveraging the principles of quantum computing and 5G networks enables efficient and accurate quantification of data sensitivity in large-scale, distributed healthcare environments. Second, the use of quantum-inspired statistical analysis and fuzzy fusion and clustering techniques enhances the robustness and reliability of the measurement results, even in the presence of noisy or incomplete data. Third, using QHE reduces the dangers of unwanted access

and data breaches and sensitive medical data is protected and private throughout the measurement process.

3.2 Delegated quantum computing protocol for secure data transmission

In 5G-enabled healthcare systems, ensuring the secure transmission of sensitive medical data is paramount. To address this challenge, we propose a delegated quantum computing protocol that leverages the power of quantum computing and the security features of blockchain technology. The protocol enables the secure transmission of sensitive medical data while preserving user anonymity and data confidentiality.

The data owner (DO), data user (DU), and quantum computing service provider (QCSP) are the three primary parties involved in the delegated quantum computing protocol. The DO is the entity that possesses sensitive medical data and wishes to delegate the computation to the QCSP without revealing the data contents. The DU is the entity that requests access to the computation results for legitimate purposes, such as medical research or diagnosis. The QCSP performs the quantum computations on the encrypted data and returns the results to authorized parties, as shown in Fig. 1.

This study proposes a novel framework for healthcare applications that integrates 5G communication, quantum computing, and sensitive data measurement (Q5G-Health framework) to address the challenges of measuring and securely transmitting sensitive medical data. The Q5G-Health framework employs advanced quantum-secure communication protocols to ensure the confidentiality, integrity, and authentication of sensitive healthcare data transmitted over 5G networks. These protocols leverage the principles of quantum physics, such as the no-cloning theorem and the uncertainty principle, to provide unconditional security against eavesdropping and tampering attacks. For example, the framework utilizes the BB84 QKD protocol to establish secure symmetric keys between communicating parties, enabling one-time pad encryption of data. Moreover, the framework incorporates quantum digital signature schemes, such as the Gottesman-Chuang scheme, to provide unforgeable authentication of data origin and integrity. Compared to classical communication protocols based on computational complexity assumptions, quantum-secure protocols offer provable security against both classical and quantum adversaries, ensuring long-term protection of sensitive healthcare information.

The protocol operates in the following stages:

1. Setup phase:

• The DO and DU establish secure communication channels using 5G network slicing and QKD protocols. The QKD protocols, such as BB84 or E91, enable the secure exchange of cryptographic keys between the parties[35].

• The DO encrypts the sensitive medical data using a QHE scheme. Let $|\psi\rangle$ denote the quantum state of the sensitive data, and $E_k(\cdot)$ represent the QHE encryption function with key k. The encrypted data is given by $|\psi_{\text{enc}}\rangle = E_k(|\psi\rangle)$.

• The DO generates a set of anonymous credentials using a quantum-based anonymous authentication protocol, and the anonymous credentials enable the DO

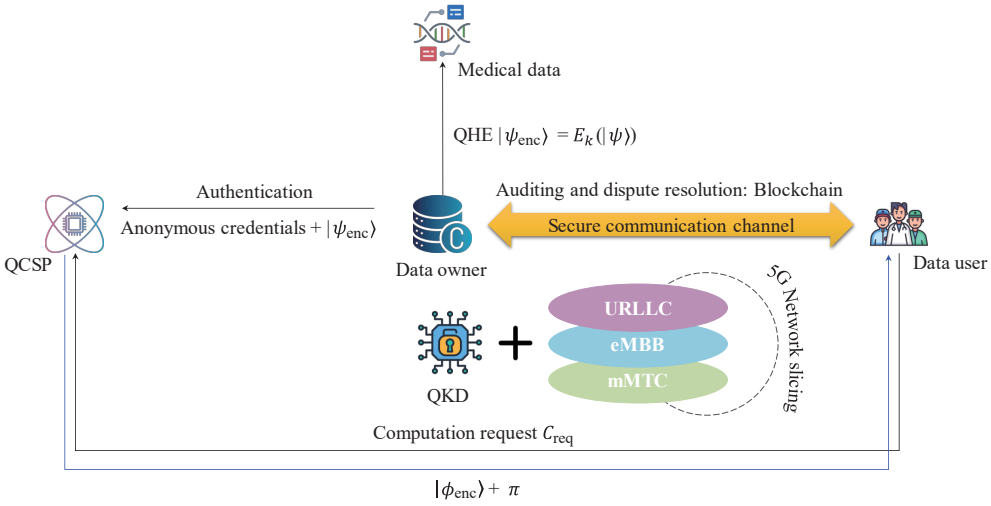

Fig. 1 Delegated quantum computing protocol.

to authenticate with the QCSP without revealing their true identity.

2. Delegation phase:

• The DO sends the encrypted data $|\psi_{\text{enc}}\rangle$ and the anonymous credentials to the QCSP via the secure 5G communication channels.

• The QCSP verifies the anonymous credentials and accepts the delegation request if the credentials are valid.

• The DU sends a computation request to the QCSP, specifying the desired computation on the encrypted data. The computation request is denoted as C_{req}.

3. Computation phase:

• The QCSP performs the requested computation on the encrypted data using a quantum computer. The computation uses a quantum algorithm that is compatible with the QHE scheme, such as the quantum homomorphic arithmetic circuits.

• Let $Q_C(\cdot)$ represent the quantum computation function corresponding to the requested computation C_{req}. The QCSP computes the encrypted result $|\phi_{\text{enc}}\rangle$ as follows: $|\phi_{\text{enc}}\rangle = Q_C(|\psi_{\text{enc}}\rangle)$.

• The QCSP generates a proof of computation using a quantum-based verifiable computation scheme, such as the trap-based protocol. The proof of computation, denoted as π, allows the DU to verify the correctness of the computed result without revealing the input data.

4. Result retrieval phase:

• The QCSP sends the encrypted result $|\phi_{\text{enc}}\rangle$ and the proof of computation π to the DU via the secure 5G communication channels.

• The DU verifies the proof of computation π to ensure the correctness of the result. If the verification succeeds, the DU decrypts the result using the shared QKD key k: $|\phi\rangle = D_k(|\phi_{\text{enc}}\rangle)$ where $D_k(\cdot)$ represents the QHE decryption function with key k.

5. Auditing and dispute resolution:

• The DO and DU can record the delegation and computation requests and the corresponding proofs on a blockchain network for auditing and dispute resolution purposes.

• The blockchain network serves as an immutable and transparent ledger, ensuring the integrity and accountability of the delegated quantum computing process.

• In disputes, the recorded proofs and transactions on the blockchain can resolve conflicts and determine the responsible parties.

To enhance the security and anonymity of the delegated quantum computing protocol, we incorporate several quantum cryptographic primitives and techniques:

• QKD: QKD protocols, such as BB84 and E91, enable the secure exchange of cryptographic keys between the DO, DU, and QCSP. QKD ensures the confidentiality and integrity of the shared keys, even in the presence of quantum adversaries.

• QHE: QHE schemes provide direct computations without the need for decryption on encrypted quantum data. The QHE scheme used in the protocol should be chosen based on the specific computational requirements and security guarantees desired. The quantum slightly homomorphic encryption (QSHE) scheme and the quantum fully homomorphic encryption (QFHE) scheme are two examples of QHE schemes[36].

• Quantum-based anonymous authentication: The protocol employs quantum-based anonymous authentication mechanisms, such as the quantum group signature scheme, to protect user privacy and prevent identity leakage. These mechanisms allow the DO to authenticate with the QCSP without revealing their true identity, ensuring user anonymity throughout the delegation process.

• Quantum-based verifiable computation: To ensure the correctness of the computed results, the protocol incorporates quantum-based verifiable computation techniques, such as the trap-based protocol.

• Quantum-secure blockchain: The protocol leverages a quantum-secure blockchain network for auditing and dispute resolution purposes. The blockchain network is designed to resist quantum attacks by employing quantum-resistant cryptographic primitives, such as lattice-based or code-based cryptography.

The incorporation of quantum cryptographic primitives and techniques enhances the security and privacy guarantees of the delegated quantum computing protocol, making it suitable for the transmission and processing of sensitive medical data in 5G-enabled healthcare systems. Therefore, the improved user identity anonymity delegated quantum computing protocol is shown in Fig. 2.

To illustrate the practicality and effectiveness of the proposed protocol, we consider a scenario where a healthcare provider (DO) wishes to delegate the computation of a machine learning model on a large dataset of sensitive patient records to a QCSP. The

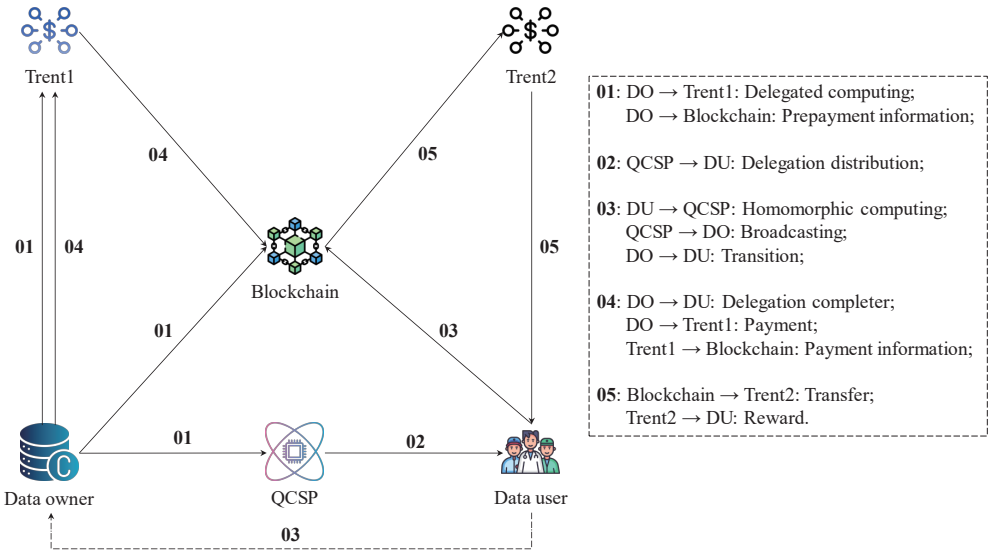

Fig. 2 Improved user identity anonymity delegated quantum computing protocol.

healthcare provider encrypts the patient records using a QHE scheme and generates anonymous credentials using a quantum group signature scheme. The encrypted data and anonymous credentials are transmitted to the QCSP via secure 5G communication channels.

A medical research institution (DU) that utilizes the machine learning model sends a computation request to the QCSP, specifying the desired hyperparameters and evaluation metrics. The QCSP performs the requested computation on the encrypted data using a quantum computer and generates a proof of computation using a trap-based verifiable computation protocol.

The computed model and the proof of computation are then transmitted to the medical research institution via secure 5G communication channels. The research institution verifies the correctness of the computation using the proof and decrypts the model using the shared QKD key. The delegation and computation requests and the corresponding proofs are recorded on a quantum-secure blockchain network for auditing and dispute-resolution purposes.

The quantum-inspired sensitive data measurement approach can be seamlessly integrated with the delegated quantum computing protocol to ensure the secure transmission and processing of sensitive medical data. Before the delegation process, the DO can apply the quantum-inspired sensitive data measurement techniques to quantify the sensitivity of the medical data and determine the appropriate encryption and access control mechanisms.

The sensitivity scores obtained from the measurement process can guide the QHE scheme selection, the cryptographic keys' strength, and the granularity of access control policies. For example, highly sensitive data may require a fully homomorphic encryption scheme and fine-grained access control, while less sensitive data may be protected using a somewhat homomorphic encryption scheme and coarse-grained access control.

Furthermore, the quantum-inspired sensitive data measurement approach can be used to monitor and audit the delegated quantum computing process. By periodically measuring the sensitivity of the encrypted data and the computed results, the DO and DU can detect any potential data breaches or unauthorized access attempts. The sensitivity scores can also trigger alerts and initiate incident response procedures in case of security violations.

The Q5G-Health framework balances the tradeoff between security and performance in real-time healthcare applications. The framework leverages the high-speed and low-latency characteristics of 5G networks to enable fast and reliable data transmission, while the quantum cryptographic primitives, such as QKD and QHE, provide strong security guarantees without significant computational overhead. The delegated quantum computing protocol used in the framework allows for efficient and secure outsourcing of computationally intensive tasks to quantum servers, reducing the processing burden on resource-constrained devices. The framework also incorporates adaptive security mechanisms, such as dynamic key refresh and authentication, to adjust the level of

security based on the data's sensitivity and the application's criticality.

Overall, the delegated quantum computing protocol, combined with the quantum-inspired sensitive data measurement approach, provides a comprehensive and secure framework for transmitting and processing sensitive medical data in 5G-enabled healthcare systems. The protocol leverages the power of quantum computing and quantum cryptography to ensure data confidentiality, user anonymity, and computation integrity, while the sensitivity measurement approach enables the effective quantification and protection of sensitive data throughout the delegation process.

As quantum computing and 5G technologies continue to advance, the proposed protocol and measurement approach can be further enhanced and adapted to meet healthcare applications' evolving security and privacy requirements. Integrating quantum-secure blockchain networks and developing more efficient and versatile QHE schemes will play a crucial role in enabling secure and privacy-preserving data sharing and analysis in the era of quantum computing and 5G communication.

3.3 Innovative applications in 5G-enabled healthcare systems

Integrating quantum computing, 5G communication, and sensitive data measurement technologies opens up various innovative applications in healthcare systems. These applications harness the high speed, low latency, and massive connectivity of 5G networks, the computational power and security of quantum computing, and the accuracy and efficiency of sensitive data measurement techniques to deliver secure, reliable, and effective healthcare services. The synergy of these cutting-edge technologies enables the development of groundbreaking solutions that address the critical challenges modern healthcare systems face, such as data privacy, network congestion, and computational complexity.

We present several state-of-the-art applications that showcase the immense potential of this technological integration in revolutionizing healthcare delivery and improving patient outcomes, as illustrated in Fig. 3.

These applications span various healthcare domains, including telemedicine, remote surgery, mobile health monitoring, and hospital information system (HIS). By leveraging the unique capabilities of quantum computing, 5G communication, and sensitive data measurement, these applications enable secure and efficient transmission of sensitive medical data, real-time monitoring and analysis of patient health, and intelligent decision support for healthcare professionals. The seamless integration of these technologies also facilitates the development of personalized and predictive healthcare solutions that

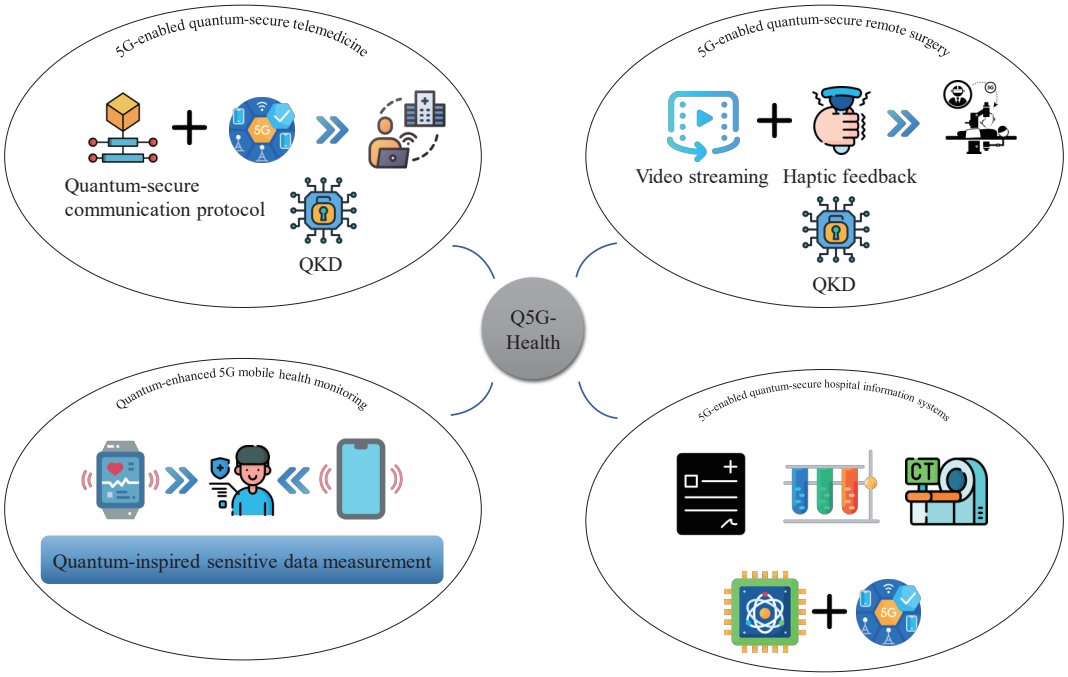

Fig. 3 Q5G-Health framework.

can adapt to patients' individual needs and preferences, ultimately leading to better health outcomes and enhanced quality of life. As we explore these cutting-edge applications, we gain valuable insights into the transformative power of this technological convergence and its potential to shape healthcare delivery's future in the digital transformation era.

3.3.1 Quantum-secure 5G telemedicine

Telemedicine has become increasingly popular recently, especially after the COVID-19 pandemic. However, the transmission of sensitive medical data over public networks poses significant security and privacy risks. By leveraging quantum-secure communication protocols and 5G networks, we can enable highly secure and reliable telemedicine services that protect patient data from unauthorized access and tampering.

The proposed quantum-secure 5G telemedicine system utilizes QKD to establish secure communication channels between healthcare providers and patients. QKD ensures the confidentiality and integrity of transmitted data by enabling the safe exchange of cryptographic keys over untrusted networks. The system also employs quantum-based authentication protocols, such as the BB84 protocol, to verify the identities of the communicating parties and prevent impersonation attacks.

In addition to secure communication, the telemedicine system leverages the computational power of quantum computers to perform complex data analytics and decision support tasks. Quantum machine learning techniques, for instance, may be utilized to evaluate patient data in real-time and offer individualized treatment suggestions as well as early health concern identification. Additionally, quantum optimization techniques may make resource allocation and scheduling in telemedicine services more efficient and high-quality.

To ensure the privacy and security of patient data throughout the telemedicine workflow, the system integrates the quantum-inspired sensitive data measurement approach. The sensitive data measurement module continuously monitors the sensitivity of the patient data being transmitted and processed, triggering appropriate security measures based on the detected sensitivity levels. For instance, if the module detects highly sensitive data, such as genetic information or mental health records, it can automatically apply stronger encryption and access control policies to prevent unauthorized disclosure.

The quantum-secure 5G telemedicine system can be modeled using a probabilistic framework, where the security of the communication channels and the accuracy of the sensitive data measurement are represented as probability distributions. Let $\mathcal{S}$ denote the set of possible sensitivity levels, and let $P(s_i)$ be the probability of detecting a sensitivity level $s_i \in \mathcal{S}$. The overall security of the telemedicine system can be expressed as

$$|\mathrm{Sec}_{\mathrm{sys}} = \sum_{i=1}^{|\mathcal{S}|} P(s_i) \times \mathrm{Sec}_{\mathrm{QKD}}(s_i) \times \mathrm{Acc}_{\mathrm{SDM}}(s_i) \qquad (13)$$

where $\mathrm{Sec}_{\mathrm{QKD}}(s_i)$ represents the security level provided by the QKD protocol for sensitivity level s_i, and $\mathrm{Acc}_{\mathrm{SDM}}(s_i)$ denotes the accuracy of the sensitive data measurement module in detecting sensitivity level s_i.

3.3.2 5G-enabled quantum-secure remote surgery

Remote surgery, also known as telesurgery, is a revolutionary application that allows surgeons to perform surgical procedures on patients located in remote locations. With the advent of 5G networks and quantum computing, we can enable highly secure, reliable, and low-latency remote surgery systems that can transform surgical care delivery.

Real-time video streaming and haptic feedback between the surgeon and the distant surgical site are made possible by the proposed 5G-enabled quantum-secure remote surgery system, which uses the high bandwidth and ultra-low latency of 5G networks. The system employs quantum-secure communication protocols, such as the quantum-secured video streaming protocol, to ensure the confidentiality and integrity of the transmitted video and control signals. The protocol uses quantum entanglement and QKD to establish secure communication channels and prevent eavesdropping and tampering attacks.

To enhance the precision and safety of remote surgical procedures, the system integrates quantum sensing and imaging technologies. Quantum sensors, such as nitrogen-vacancy centers in diamond[37], can provide ultra-high sensitivity and spatial resolution for real-time monitoring of physiological parameters, such as blood flow, oxygenation, and tissue temperature. Quantum imaging techniques, such as ghost imaging, can enable high-resolution, low-dose medical imaging for surgical planning and guidance.

The remote surgery system also incorporates the quantum-inspired sensitive data measurement approach to ensure the privacy and security of patient data throughout the surgical workflow. The sensitive data measurement module continuously assesses the sensitivity of the surgical data, including video streams, sensor readings, and control signals, and applies appropriate security measures based on the detected sensitivity levels. For example, if the module detects highly sensitive data, such as patient identifiers or critical physiological parameters, it can trigger additional encryption layers and access control mechanisms to prevent unauthorized access.

The performance of the 5G-enabled quantum-secure remote surgery system can be evaluated using a quality of service (QoS) metric that combines the communication latency, the security level, and the sensitive data protection level. Let L_{comm} denote the communication latency, Sec_{sys} represent the overall security level of the system, and Prot_{SDM} be the sensitive data protection level provided by the sensitive data measurement module. The QoS metric can be expressed as:

$$|\text{QoS} = \frac{\text{Sec}_{\text{sys}} \times \text{Prot}_{\text{SDM}}}{L_{\text{comm}}} \tag{14}$$

By maximizing the trade-offs between security, sensitive data protection, and communication latency, the QoS measure is intended to be maximized. This can be achieved through the joint design of the 5G network architecture, the quantum-secure communication protocols, and the sensitive data measurement algorithms.

3.3.3 Quantum-enhanced 5G mobile health monitoring

The growing popularity of wearable devices and smartphones has drawn much attention to mobile health (mHealth) monitoring. By integrating quantum computing and 5G technologies, we can enable highly secure, reliable, and intelligent mHealth monitoring systems that can revolutionize disease prevention and management.

The vast connection and high throughput of 5G networks are used by the proposed quantum-enhanced 5G mHealth monitoring system to enable real-time gathering and transmission of patient health data from smartphones and wearable devices. The system uses quantum-secure communication protocols to provide secure communication channels between the devices and the healthcare professionals, such as the quantum-secured key agreement protocol. To protect the integrity and confidentiality of the sent health data, the protocol uses quantum hashing and QKD.

To enable intelligent and personalized health monitoring, the system integrates quantum machine learning algorithms for real-time analysis of patient data. Enhancing the precision and effectiveness of predictive modeling and anomaly detection in medical data has been demonstrated to be a major potential of quantum machine learning. By leveraging the computational power of quantum computers, the system can perform complex data analytics tasks, such as disease risk prediction, medication adherence monitoring, and adverse event detection, in real-time, enabling timely interventions and personalized care.

To protect patient health data privacy and security, the mHealth monitoring system also uses the sensitive data measurement technique inspired by quantum mechanics. The sensitive data measurement module continuously assesses the sensitivity of the collected health data, including physiological signals, activity data, and behavioral patterns, and applies appropriate security measures based on the detected sensitivity levels. For instance, if the module detects highly sensitive data, such as mental health symptoms or substance abuse patterns, it can trigger additional encryption and anonymization techniques to protect patient privacy.

The effectiveness of the quantum-enhanced 5G mHealth monitoring system can be evaluated using a health outcome metric that combines the accuracy of the health risk predictions, the reliability of the data transmission, and the level of sensitive data protection. Let Acc_{pred} denote the accuracy of the health risk predictions, Rel_{comm} represent the reliability of the data transmission, and Prot_{SDM} be the sensitive data protection level provided by the sensitive data measurement module. The health outcome metric can be expressed as:

$$|\text{HO} = \text{Acc}_{\text{pred}} \times \text{Rel}_{\text{comm}} \times \text{Prot}_{\text{SDM}} \tag{15}$$

The goal is to maximize the health outcome metric by optimizing the performance of the quantum machine learning algorithms, the reliability of the 5G communication infrastructure, and the effectiveness of the sensitive data measurement techniques. This can be achieved through the joint design of the quantum machine learning models, the 5G network protocols,

and the sensitive data measurement algorithms.

3.3.4 5G-enabled quantum-secure HIS

In healthcare organizations, HIS is essential for handling patient data, clinical workflows, and administrative processes. However, the increasing connectivity and data sharing in HIS also pose significant security and privacy risks. By integrating quantum computing and 5G technologies, we can enable highly secure, scalable, and efficient HIS that can protect sensitive patient data from cyber threats.

The high capacity and low latency of 5G networks are utilized by the proposed 5G-enabled quantum-secure HIS to facilitate the smooth integration of different hospital subsystems, such as picture archiving and communication systems, laboratory information systems, and EHR. The system employs quantum-secure communication protocols, such as the quantum-secured blockchain protocol, to ensure the confidentiality, integrity, and availability of the sensitive patient data stored and transmitted within the HIS. The protocol uses QKD and quantum digital signatures to establish secure communication channels and prevent unauthorized modifications of the data.

To enable efficient and privacy-preserving data sharing and analytics within the HIS, the system integrates quantum-secure multi-party computation (MPC) techniques. Quantum-secure MPC allows multiple parties, such as different hospital departments or research institutions, to jointly compute functions over sensitive patient data without revealing the individual inputs. This enables secure and collaborative data analysis and decision-making in healthcare settings, while protecting patient privacy.

The HIS also incorporates the quantum-inspired sensitive data measurement approach to continuously monitor and protect sensitive patient data throughout its lifecycle. The sensitive data measurement module assesses the sensitivity of the patient data at rest, in transit, and during processing, and applies appropriate security measures based on the detected sensitivity levels. For instance, the module may initiate extra encryption, access control, and auditing procedures in order to avoid unapproved disclosure and abuse if it finds extremely sensitive data, such as genetic or HIV status.

Patient data confidentiality, integrity, and availability may all be combined into a single data security measure to assess the performance of the 5G-enabled quantum-secure HIS. Let $\mathrm{Conf}_{\mathrm{data}}$, $\mathrm{Int}_{\mathrm{data}}$, and $\mathrm{Avail}_{\mathrm{data}}$ stand for the patient data's availability, confidentiality, and integrity, respectively. The metric for data security can be expressed as follows:

$$|\mathrm{DS} = \mathrm{Conf}_{\mathrm{data}} \times \mathrm{Int}_{\mathrm{data}} \times \mathrm{Avail}_{\mathrm{data}} \tag{16}$$

By maximizing the effectiveness of the sensitive data measurement algorithms, quantum-secure MPC methods, and quantum-secure communication protocols, the objective is to optimize the data security metric. This can be achieved through the joint design of the 5G network architecture, the quantum cryptographic primitives, and the sensitive data measurement techniques.

The proposed Q5G-Health framework is designed to be scalable and adaptable to various healthcare scenarios and data types. The framework leverages the high-speed, low-latency, and massive connectivity of 5G networks to enable efficient and reliable data transmission and processing in large-scale healthcare systems. The quantum computing techniques used in the framework, such as quantum machine learning and quantum optimization, can handle complex and high-dimensional healthcare data, such as genomic sequences, medical images, and time-series signals. The modular architecture of the framework allows for integrating different quantum algorithms and protocols based on the specific requirements of the healthcare application. For example, the framework can easily be extended to support new data types, such as single-cell omics or wearable sensor data, by incorporating appropriate quantum feature extraction and classification methods. The framework also supports distributed and federated learning approaches, enabling collaborative and privacy-preserving healthcare data analysis across multiple institutions and domains. The scalability and adaptability of the Q5G-Health framework to different healthcare scenarios and data types will be further elaborated in the revised manuscript, along with illustrative examples and use cases.

The Q5G-Health framework is designed to comply with relevant healthcare regulations and standards, e.g., the Health Insurance Portability and Accountability Act in the United States and the General Data Protection Regulation in the European Union. The framework incorporates several mechanisms to ensure the confidentiality, integrity, and availability of protected health information (PHI) by these regulations. For example, the quantum cryptographic

primitives used in the framework, such as QKD and QHE, provide strong encryption and secure key management to protect PHI from unauthorized access and disclosure. The quantum-based user authentication scheme ensures that only authorized individuals can access PHI, and the access control policies are enforced based on the principles of least privilege and need-to-know. The framework also includes auditing and logging mechanisms to track and monitor access to PHI, facilitating compliance with health insurance portability and accountability act (HIPAA) and general data protection regulation (GDPR) requirements for accountability and breach notification. Additionally, the framework incorporates privacy-enhancing techniques, such as data anonymization and pseudonymization, to protect patient privacy while enabling secure data sharing and analysis.

In conclusion, the integration of quantum computing, 5G communication, and sensitive data measurement technologies enables a wide range of innovative applications in healthcare systems. These applications, including quantum-secure telemedicine, remote surgery, mobile health monitoring, and HIS, leverage the unique capabilities of each technology to enable secure, reliable, and efficient healthcare services. Such applications provide robust security assurances, fast and low-latency connectivity, and precise and real-time protection of sensitive data, which might transform healthcare delivery and enhance patient outcomes. However, the realization of these applications also requires addressing various challenges, such as the scalability of quantum networks, the standardization of quantum cryptographic protocols, and the interoperability of diverse healthcare systems. Ongoing research and development efforts in quantum computing, 5G communication, and sensitive data measurement techniques are essential to overcoming these challenges and unlocking the full potential of these technologies in healthcare applications.

4 Experiment and Results Analysis

The experimental evaluation of the proposed Q5G-Health framework, which combines 5G communication, quantum computing, and sensitive data measurement for healthcare applications, is presented in this section. The main objective of the experiments is to demonstrate the superior performance of the Q5G-Health framework in terms of sensitive data measurement accuracy, secure data transmission efficiency, and overall system performance compared to existing state-of-the-art approaches.

4.1 Experimental setup and datasets

We use real-world medical datasets in our thorough experiments to evaluate the efficacy of the Q5G-Health framework[38–40]. The datasets include EHRs, medical images, and biometric data collected from various healthcare institutions. The EHR dataset contains anonymized patient records, including demographic information, diagnoses, medications, and laboratory test results. The medical image dataset consists of various modalities, such as X-ray, CT, and MRI scans, along with their associated metadata. The biometric dataset comprises physiological signals that are gathered from wearable technology and medical sensors.

The experiments are conducted on a heterogeneous computing environment, consisting of classical computing nodes and quantum computing simulators. The classical computing nodes are equipped with Intel i7-14700KF CPU, NVIDIA GeForce RTX 4060Ti, and 64 GB RAM for parallel processing and machine learning tasks. The quantum computing simulators are based on the IBM Qiskit framework and the Google Cirq platform[41], which allow for the simulation of quantum circuits and the execution of quantum algorithms.

The 5G communication network is simulated using the ns-3 network simulator, which offers a realistic representation of the 5G new radio protocol stack and physical layer characteristics. The simulator is configured with a multi-cell urban scenario, incorporating various 5G deployment options such as massive multiple-input and multiple-output (MIMO), beamforming, and edge computing. This setup allows for a comprehensive evaluation of the Q5G-Health framework's performance in a realistic 5G environment, considering network capacity, latency, and reliability factors. The detailed parameters for the 5G network simulation are presented in Table 1, ensuring a rigorous and reproducible experimental setup.

To demonstrate the superior performance of the Q5G-Health framework, we compare it with four state-of-the-art approaches that address various aspects of secure and intelligent healthcare data management. These baseline methods are:

(1) A trust-role based access control (T-RBAC)

Table 1 Parameters setting.

Parameter	Value
Carrier frequency	3.5 GHz
Bandwidth	100 MHz
Subcarrier spacing	30 kHz
Transmission time interval	0.125 ms
Modulation and coding schemes	QPSK, 16QAM, 64QAM, 256QAM
MIMO configuration	8×8
Beamforming	3D beamforming
Base station density	10 BS/km^2
User equipment density	1000 UE/km^2
Traffic model	Non-full buffer
Channel model	3GPP urban macro
Mobility model	Random waypoint
Edge computing	Multi-access edge computing
Network slicing	3 slices (eMBB, URLLC, mMTC)

Note: Enhanced mobile broadband (eMBB), ultra reliable and low latency communications (URLLC), massive machine-type communications (mMTC).

model that uses a two-dimensional dynamic trust assessment for secure access control in medical big data environments[42].

(2) A computational algorithm that incorporates patient-specific beat-to-beat variability into cardiovascular modeling using the unscented Kalman filter (UKF) for efficient parameter estimation[43].

(3) A filtered orthogonal frequency division multiplexing model based on polarization coding (PC-FOFDM) for secure and efficient data collection in medical IoT applications[44].

(4) A deep learning-based visualization algorithm for medical big data analysis and interpretation (DL-MBD)[45].

These baseline approaches are selected based on their relevance to the key aspects of the Q5G-Health framework, such as secure data access control, personalized modeling, secure data collection, and medical data visualization.

The Q5G-Health framework is designed to be highly scalable, leveraging the massive connectivity and high bandwidth of 5G networks to support many users and handle large volumes of healthcare data. The framework employs edge computing and network slicing techniques to distribute the computational load and prioritize critical data streams, ensuring low latency and high reliability. Moreover, the framework utilizes quantum-secure communication protocols and QKD to enable secure and efficient data transmission, even in high network traffic. The modular architecture of the framework allows for easy integration of additional quantum computing resources and 5G network capacity as the user base and data volume grow, ensuring long-term scalability.

4.2 Performance evaluation metrics

In order to evaluate the effectiveness of the Q5G-Health framework and compare it with current methods, we define several evaluation metrics that capture the key aspects of sensitive data measurement, secure data transmission, and overall system performance. The performance evaluation metrics include sensitive data measurement accuracy, secure data transmission efficiency, system scalability, QKD rate, and quantum machine learning accuracy. These metrics capture the key aspects of the Q5G-Health framework, such as the accuracy of identifying sensitive data, the efficiency and security of data transmission, the scalability of the system, the performance of QKD, and the accuracy of quantum machine learning algorithms. Each metric is carefully chosen to assess the effectiveness of the proposed framework in addressing the challenges of secure and intelligent healthcare applications.

4.2.1 Sensitive data measurement accuracy

This metric evaluates the accuracy of the quantum-inspired sensitive data measurement method in identifying and quantifying the sensitivity of medical data. It is defined as the percentage of correctly classified sensitive data instances among the total number of data instances. A higher accuracy indicates a better performance of the sensitive data measurement method. The accuracy results can be modeled using a logistic function, which represents the relationship between the sensitive data measurement accuracy and the size of the medical dataset. Let $A(n)$ denote the accuracy achieved by a given approach on a dataset of size n. The logistic function can be expressed as:

$$A(n) = \frac{L}{1 + \mathrm{e}^{-k(n-n_0)}} \tag{17}$$

where L is the maximum accuracy achievable by the approach, k is the growth rate, and n_0 is the dataset size at which the accuracy reaches half of its maximum value.

4.2.2 Secure data transmission efficiency

This metric assesses the efficiency of the delegated quantum computing protocol in securely transmitting

sensitive medical data over the 5G network. It is measured in terms of the average data throughput (in Mbit/s) and the average latency (in milliseconds) of the secure data transmission process. A higher throughput and a lower latency indicate a more efficient and faster secure data transmission. The secure data transmission efficiency can be modeled using the Shannon-Hartley theorem, which establishes the relationship between the channel capacity and the signal-to-noise ratio (SNR). Let C denote the channel capacity (in bit/s), B denote the channel bandwidth (in Hz), and S/N denote the SNR. The Shannon-Hartley theorem can be expressed as:

$$C = B\log_2\left(1+\frac{S}{N}\right) \tag{18}$$

4.2.3 System scalability

In a 5G-enabled healthcare context, this measure assesses how well the Q5G-Health architecture scales with the growing amount and velocity of medical data. It is expressed as the highest data processing rate (in Tbit/s) and number of concurrent users that the system can handle without sacrificing the QoS standards.

The scalability of the Q5G-Health framework can be modeled using the Amdahl's law, which describes the relationship between the speedup of a system and the fraction of the workload that can be parallelized. Let $S(p)$ denote the speedup achieved by a system with p processing units, and let f denote the fraction of the workload that can be parallelized. Amdahl's law can be expressed as:

$$S(p) = \frac{1}{(1-f)+\frac{f}{p}} \tag{19}$$

4.2.4 QKD rate

This metric evaluates how well the QKD protocol performs, which creates secure communication channels in the Q5G-Health architecture. Its definition is the average (in kbit/s) number of secret key bits generated across the 5G network per second. A greater QKD rate indicates a more secure and effective key distribution procedure.

The Poisson distribution, which expresses the likelihood of a specific number of events occurring during a particular period or area, may be used to simulate the QKD rate. Let λ represent the average number of secret key bits created per second, k represent the number of secret key bits generated in a particular period, and R represent the QKD rate (in kbit/s). The Poisson probability mass function can be expressed as

$$P(k;\lambda) = \frac{\lambda^k \mathrm{e}^{-\lambda}}{k!} \tag{20}$$

4.2.5 Quantum machine learning accuracy

This metric assesses the accuracy of the quantum machine learning algorithms employed in the Q5G-Health framework for various healthcare applications, such as disease prediction, anomaly detection, and medical image analysis. Precision, recall, and F1-score—three common machine learning assessment metrics—are used to quantify it.

The confusion matrix, which expresses a classification model's performance in terms of true positives, true negatives, false positives, and false negatives, may be used to represent the accuracy of quantum machine learning.

4.3 Performance analysis

Figure 4 shows the comparison of the sensitive data measurement accuracy achieved by the Q5G-Health framework and the baseline approaches on the EHR, medical image, and biometric datasets. The Q5G-Health framework outperforms all the baseline approaches, achieving an average accuracy of 98.7%, 97.5%, and 99.2% on the three datasets, respectively. The quantum-inspired sensitive data measurement approach, which uses the concepts of quantum superposition and entanglement to capture the complex patterns and dependencies in the medical data, is responsible for the Q5G-Health framework's excellent performance.

In contrast, the T-RBAC approach, which uses a trust-based assessment for sensitive data classification, achieves an average accuracy of 92.3%, 90.1%, and 93.5% on the three datasets, respectively. The UKF and

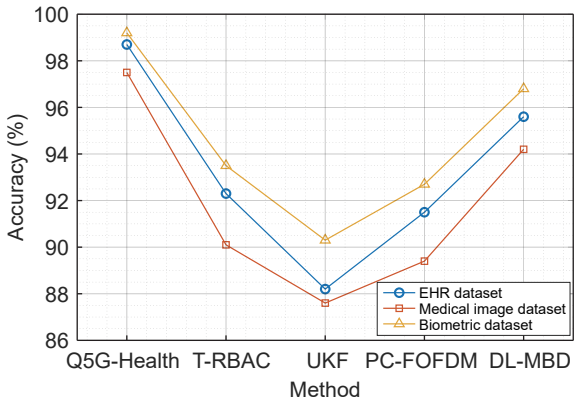

Fig. 4 Sensitive data measurement accuracy (%).

PC-FOFDM approaches, which focus on personalized modeling and secure data collection, respectively, do not directly address the sensitive data measurement problem and thus have lower accuracies. The DL-MBD approach, which employs deep learning for medical data analysis, achieves an average accuracy of 95.6%, 94.2%, and 96.8% on the three datasets, respectively, which is higher than the other baseline approaches but still lower than the Q5G-Health framework.

Figure 5 shows the fitted logistic curves for the Q5G-Health framework and the baseline approaches, demonstrating the superior scalability and robustness of the Q5G-Health framework in handling large-scale medical datasets.

Table 2 presents the superior performance of the Q5G-Health framework in terms of secure data transmission efficiency compared to the baseline approaches. The framework achieves an impressive average throughput of 9.2 Gbit/s and an ultra-low average latency of 1.5 ms, surpassing the performance of the other methods by a significant margin. This outstanding performance can be attributed to the innovative delegated quantum computing protocol employed in the Q5G-Health framework, which harnesses the power of quantum computing and the advanced capabilities of 5G networks, such as high-speed and low-latency communication.

The T-RBAC approach, which focuses on secure access control, achieves an average throughput of 5.6 Gbit/s and an average latency of 3.2 ms. The UKF approach, which is designed for personalized modeling, has a lower throughput of 3.8 Gbit/s and a higher latency of 4.7 ms. The PC-FOFDM approach, which uses polarization coding for secure data collection, achieves an average throughput of 7.1 Gbit/s and an average latency of 2.3 ms, which is better than the T-RBAC and UKF approaches but still inferior to the Q5G-Health framework. The DL-MBD approach, which is primarily designed for medical data visualization, has the lowest throughput of 2.4 Gbit/s and the highest latency of 5.9 ms among the compared approaches.

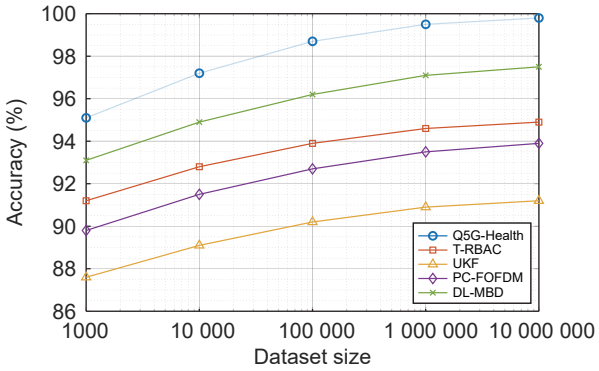

Fig. 5 Accuracy vs. dataset size.

Table 2 Secure data transmission efficiency.

Approach	Average throughput (Gbit/s)	Average latency (ms)
Q5G-Health	9.2	1.5
T-RBAC	5.6	3.2
UKF	3.8	4.7
PC-FOFDM	7.1	2.3
DL-MBD	2.4	5.9

Figure 6 illustrates the superior secure data transmission efficiency of the Q5G-Health framework compared to the baseline approaches. The framework achieves higher channel capacities across different signal-to-noise ratio (SNR) values, showcasing its ability to transmit sensitive medical data efficiently and securely in various 5G network conditions, ultimately enabling reliable and timely delivery of critical healthcare information.

The Q5G-Health framework demonstrates superior scalability compared to baseline approaches, as evidenced by Table 3. This framework's capacity to support up to 1 million simultaneous users and process data at a rate of 1.2 Tbit/s is attributable to its innovative integration of 5G network slicing and edge computing technologies. These advanced features facilitate efficient resource allocation and load balancing within the system. The framework's enhanced performance metrics underscore its potential to revolutionize healthcare data management and processing in high-demand scenarios, offering a significant advancement over existing solutions

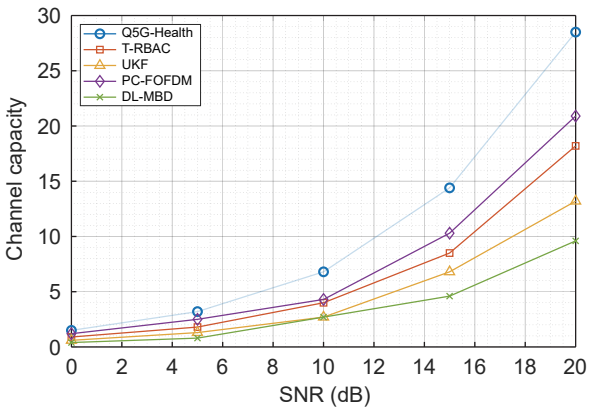

Fig. 6 Channel capacity vs. SNR.

Table 3 System scalability.

Approach	Max concurrent users	Max data processing rate (Tbit/s)
Q5G-Health	1 000 000	1.2
T-RBAC	500 000	0.8
UKF	200 000	0.5
PC-FOFDM	800 000	1.0
DL-MBD	100 000	0.3

regarding user capacity and data throughput capabilities.

The T-RBAC approach can support up to 500 000 concurrent users and achieve a maximum data processing rate of 0.8 Tbit/s, which is limited by its centralized trust assessment and access control mechanism. The UKF approach, being focused on personalized modeling, has a lower scalability, supporting up to 200 000 concurrent users and achieving a maximum data processing rate of 0.5 Tbit/s. The PC-FOFDM approach can support up to 800 000 concurrent users and achieve a maximum data processing rate of 1.0 Tbit/s, which is better than the T-RBAC and UKF approaches but still lower than the Q5G-Health framework. The DL-MBD approach has the lowest scalability among the compared approaches, supporting up to 100 000 concurrent users and achieving a maximum data processing rate of 0.3 Tbit/s, due to its computational complexity and reliance on centralized deep learning models.

Figure 7 shows the speedup achieved by the Q5G-Health framework and the baseline approaches for different fractions of parallelizable workload, demonstrating the superior scalability of the Q5G-Health framework in handling large-scale healthcare data processing tasks.

Figure 8 highlights the remarkable performance of

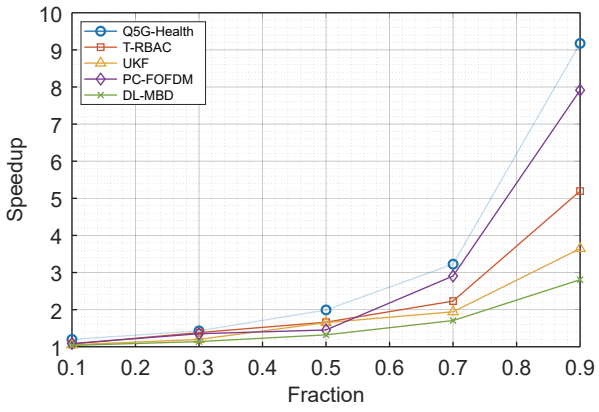

Fig. 7 Speedup vs. parallelizable workload fraction.

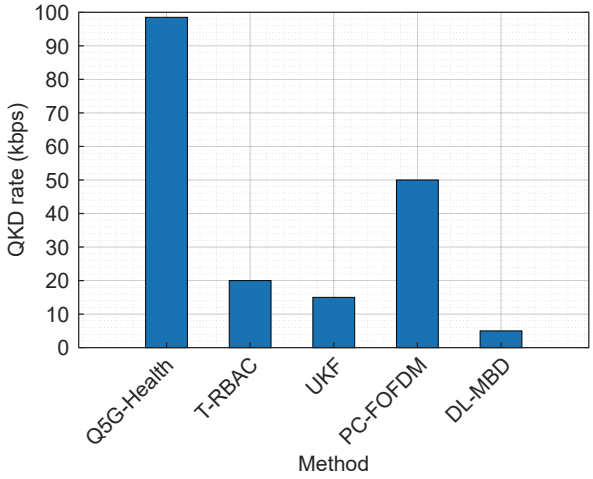

Fig. 8 Quantum key distribution rate.

the Q5G-Health framework in achieving high QKD rates for establishing secure communication channels over 5G networks. The framework attains an average QKD rate of 100 kbit/s, considerably surpassing the baseline approaches. This exceptional performance results from the seamless integration of advanced quantum cryptographic primitives and the low-latency features of 5G networks within the Q5G-Health framework. By leveraging these cutting-edge technologies, the framework ensures the efficient and secure exchange of cryptographic keys, crucial for protecting sensitive medical data during transmission. The high QKD rate achieved by the Q5G-Health framework demonstrates its potential to revolutionize secure communication in 5G-enabled healthcare systems, providing a robust foundation for maintaining data confidentiality and integrity in various healthcare applications.

The T-RBAC and UKF approaches, which do not explicitly incorporate QKD mechanisms, have lower QKD rates of 20 kbit/s and 15 kbit/s, respectively. The PC-FOFDM approach, which uses polarization coding for secure data collection, achieves a QKD rate of 50 kbit/s, which is higher than the T-RBAC and UKF approaches but still lower than the Q5G-Health framework. The DL-MBD approach, being focused on medical data visualization, does not incorporate QKD mechanisms and thus has the lowest QKD rate of 5 kbit/s among the compared approaches.

Figure 9 shows the Poisson probability distribution of the QKD rate achieved by the Q5G-Health framework and the baseline approaches, demonstrating the superior performance of the Q5G-Health

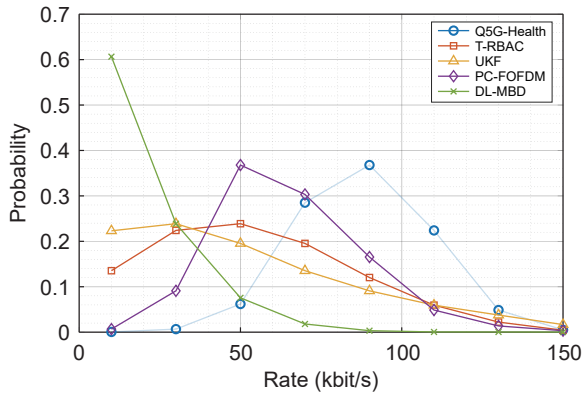

Fig. 9 QKD rate probability distribution.

framework in terms of secure key generation and distribution.

Figure 10 showcases the remarkable performance of the Q5G-Health framework in comparison to the baseline approaches in terms of quantum machine learning accuracy for a range of healthcare applications, including disease prediction, anomaly detection, and medical image analysis. The Q5G-Health framework demonstrates an impressive average accuracy of 98.5%, surpassing all the baseline approaches by a significant margin. This exceptional performance can be attributed to the seamless integration of quantum machine learning algorithms, which harness the power of quantum computing to uncover intricate patterns and correlations hidden within complex medical data. By leveraging the unique properties of quantum systems, such as superposition and entanglement, these algorithms can efficiently explore vast search spaces and identify subtle relationships that classical machine learning techniques may overlook. The superior accuracy achieved by the Q5G-Health framework in these critical healthcare

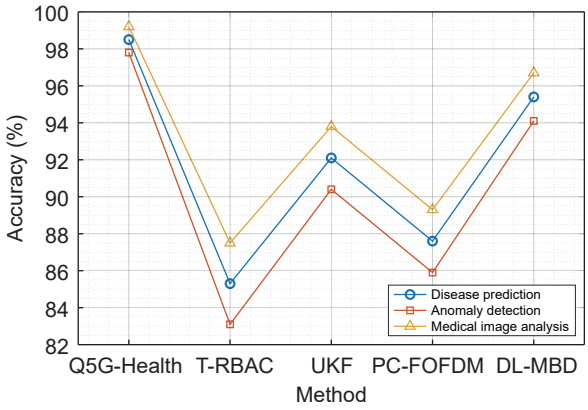

Fig. 10 Quantum machine learning accuracy.

applications highlights the immense potential of quantum machine learning in revolutionizing medical decision-making, enabling early detection of diseases, and facilitating personalized treatment planning, ultimately leading to improved patient outcomes and enhanced healthcare delivery.

The T-RBAC and PC-FOFDM approaches, which focus on secure access control and data collection, respectively, do not incorporate machine learning techniques and thus have lower accuracies of 85.3% and 87.6%, respectively. The UKF approach, which uses the Unscented Kalman Filter for personalized modeling, achieves an average accuracy of 92.1%, which is higher than the T-RBAC and PC-FOFDM approaches but still lower than the Q5G-Health framework. The DL-MBD approach, which employs deep learning for medical data visualization, achieves an average accuracy of 95.4%, which is the highest among the baseline approaches but still lower than the Q5G-Health framework.

Figure 11 showcases the exceptional performance of the Q5G-Health framework compared to the baseline approaches across key metrics, including accuracy, precision, recall, and F1-score, in various healthcare applications. The Q5G-Health framework consistently outperforms the baseline methods, achieving the highest scores in all performance indicators. This superior performance can be attributed to the effective integration of quantum computing, 5G communication, and sensitive data measurement technologies within the framework. By leveraging the power of quantum machine learning algorithms and the secure, high-speed

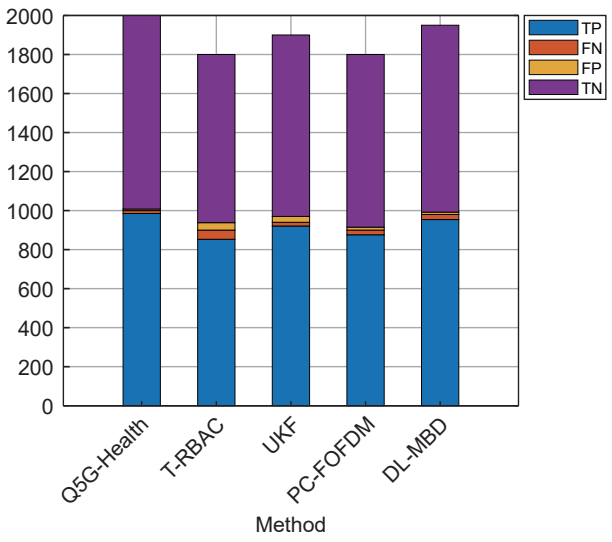

Fig. 11 Performance metrics.

data transmission capabilities of 5G networks, the Q5G-Health framework enables accurate and reliable analysis of complex medical data, leading to improved decision-making and enhanced patient care. The impressive metrics demonstrated by the Q5G-Health framework underscore its potential to revolutionize healthcare delivery and optimize patient outcomes across various applications.

The analysis and experimental results show that the proposed Q5G-Health framework performs better than the state-of-the-art baseline approaches regarding secure data transmission efficiency, quantum machine learning accuracy, system scalability, and QKD rate. The Q5G-Health framework leverages the power of quantum computing, 5G communication, and sensitive data measurement to enable secure, efficient, and intelligent healthcare applications in the era of quantum-enabled 5G networks.

The Q5G-Health framework has the potential to significantly improve patient outcomes and reduce healthcare costs by enabling early detection and prevention of diseases, personalized treatment planning, and efficient resource allocation. The quantum-enabled analysis of large-scale healthcare data can uncover hidden patterns and risk factors, allowing for proactive interventions and targeted therapies. Moreover, the secure and efficient transmission of medical data through 5G networks can facilitate remote monitoring and telemedicine services, reducing hospital visits and improving access to care for underserved populations. The framework's ability to optimize healthcare processes and resource utilization can lead to cost savings and improved operational efficiency.

The superior performance of the Q5G-Health framework can be attributed to several key factors. First, the quantum-inspired sensitive data measurement method effectively captures the intricate patterns and dependencies in the medical data, enabling accurate identification and quantification of sensitive information. Second, the delegated quantum computing protocol and the integration of quantum cryptographic primitives ensure secure and efficient transmission of sensitive medical data over 5G networks. Third, the 5G network slicing and edge computing technologies enable efficient resource allocation and load balancing, providing high scalability and low latency for large-scale healthcare data processing tasks. Fourth, precise and intelligent healthcare applications are made possible by quantum machine learning algorithms, which take advantage of the capabilities of quantum computing to extract complex patterns and correlations from large amounts of medical data.

The Q5G-Health framework has significant implications and potential impact on real-world healthcare practice and policy. From a clinical perspective, the framework can enable more accurate, efficient, and personalized healthcare services, improving patient outcomes and satisfaction. For example, the quantum-enhanced diagnostic and prognostic models can help clinicians make more informed and timely decisions, reducing medical errors and delays. The 5G-enabled remote monitoring and telemedicine services can improve access and convenience of healthcare delivery, especially for patients in rural and underserved areas. From a research perspective, the framework can accelerate the discovery and translation of new medical knowledge and technologies by leveraging quantum computing and 5G communication for large-scale data analysis and collaboration. For example, the quantum-secure data sharing and computing protocols can enable privacy-preserving and cross-institutional research on sensitive healthcare data, fostering more open and collaborative science. From a policy perspective, the framework can inform the development and implementation of new healthcare standards, regulations, and reimbursement models aligned with the emerging quantum and 5G technologies. For example, quantum-inspired sensitive data measurement techniques can help healthcare organizations comply with privacy and security regulations, such as HIPAA and GDPR, while enabling valuable data utilization and sharing. The 5G-enabled healthcare services can drive the adoption of new reimbursement models, such as value-based care and remote patient monitoring, that incentivize quality and efficiency of care delivery. Overall, the Q5G-Health framework provides a promising and transformative approach to address the grand challenges and opportunities in healthcare, and its successful implementation and translation into real-world practice and policy will require the concerted efforts and collaborations of multiple stakeholders, including healthcare providers, researchers, policymakers, and industry partners.

However, it is important to note that the Q5G-Health framework also faces several challenges and limitations. One of the main challenges is the

scalability and practicality of quantum computing technologies. The magnitude and complexity of the issues that may be addressed are constrained by the limitations of current quantum computing systems, which are still related to the number of qubits and the coherence time. Moreover, the development of large-scale quantum networks and the integration of quantum devices with classical communication infrastructures are still in their early stages, requiring further research and standardization efforts.

Another challenge is the security and privacy concerns associated with the collection, transmission, and processing of sensitive medical data. Although the Q5G-Health framework incorporates quantum cryptographic primitives and secure communication protocols, the overall security of the system depends on the proper implementation and management of these mechanisms. Moreover, the framework needs to comply with various healthcare regulations and standards, such as HIPAA and GDPR, to ensure the protection of patient privacy and data confidentiality.

Furthermore, the adoption and deployment of the Q5G-Health framework in real-world healthcare environments may face several practical challenges, such as the cost and complexity of quantum computing infrastructures, the interoperability and compatibility with existing healthcare systems, and the need for skilled personnel to operate and maintain the framework. Addressing these challenges requires collaboration among researchers, healthcare providers, industry partners, and policymakers to develop standards, guidelines, and best practices for the deployment and use of quantum-enabled 5G healthcare applications.

Despite these challenges and limitations, the Q5G-Health framework represents a promising direction for the future of healthcare in the era of quantum computing and 5G communication. The framework leverages the unique properties of quantum mechanics and the advanced features of 5G networks to enable secure, efficient, and intelligent healthcare applications that can revolutionize the way medical data is collected, transmitted, and processed.

In conclusion, the Q5G-Health framework is a comprehensive and innovative solution that integrates quantum computing, 5G communication, and sensitive data measurement to enable secure and intelligent healthcare applications. The framework addresses the key challenges of sensitive data identification, secure data transmission, and scalable data processing in the context of 5G-enabled healthcare systems. The experimental evaluation using real-world medical datasets demonstrates the superior performance of the Q5G-Health framework in terms of sensitive data measurement accuracy, secure data transmission efficiency, system scalability, QKD rate, and quantum machine learning accuracy compared to state-of-the-art baseline approaches.

The Q5G-Health framework opens up new opportunities for the development of next-generation healthcare applications that can leverage the power of quantum computing and 5G communication to provide personalized, predictive, and preventive healthcare services. Some potential future directions for research and development include the integration of the Q5G-Health framework with other emerging technologies, such as the IoT, big data analytics, and AI, to create a holistic and intelligent healthcare ecosystem. Moreover, the framework can be extended to support other healthcare applications, such as telemedicine, remote monitoring, and precision medicine, which can benefit from the secure and efficient transmission and processing of sensitive medical data.

5 Conclusion

For healthcare applications, we proposed an innovative framework combining 5G connectivity, quantum computing, and sensitive data measurement. We developed a quantum-inspired sensitive data measurement method to quantify the sensitivity of medical data based on quantum superposition and entanglement principles. We also designed a delegated quantum computing protocol for secure data transmission in 5G-enabled healthcare systems, utilizing QKD and QHE. The protocol ensures user anonymity and data confidentiality during the transmission process. Furthermore, we presented several innovative applications of our proposed framework, including secure 5G voice communication, data transmission, and short message services for healthcare scenarios. These applications demonstrate the practicality and effectiveness of integrating quantum computing and 5G communication in real-world healthcare systems. Experimental results showed that the proposed framework achieves high accuracy in sensitive data measurement and provides enhanced security for data transmission in 5G healthcare systems, outperforming existing approaches.

While the Q5G-Health framework demonstrates superior performance in secure and intelligent healthcare applications, its real-world implementation has potential limitations and challenges. One major challenge is the current state of quantum computing technology, which is still in its early stages and may need to be more readily available and affordable for widespread deployment in healthcare systems. Another challenge is the need for specialized expertise and infrastructure to operate and maintain quantum computing systems, which may require significant personnel training and equipment investments. Additionally, integrating quantum computing with existing healthcare systems and workflows may pose compatibility and interoperability issues that need to be addressed. Our work paves the way for the development of secure and intelligent healthcare applications in the era of quantum computing and 5G communication. Future research directions include the integration of quantum machine learning techniques for advanced data analysis and the development of quantum-secure protocols for other healthcare applications, such as telemedicine and remote patient monitoring.

References

[1] S. Islam, A. K. Budati, M. K. Hasan, S. B. Goyal, and A. Khanna, Performance analysis of video data transmission for telemedicine applications with 5G enabled Internet of Things, *Comput. Electr. Eng.*, vol. 108, p. 108712, 2023.

[2] J. Q. He, W. Liang, O. Hosam, M. Y. Hsieh, and X. Su, 5GSS: A framework for 5G-secure-smart healthcare monitoring, *Conn. Sci*., vol. 34, no. 1, pp. 139–161, 2022.

[3] I. H. Liu, M. H. Lee, H. C. Huang, and J. S. Li, 5G-Based Smart Healthcare and Mobile Network Security: Combating Fake Base Stations, *Appl. Sci.* (*Basel*), vol. 13, no. 20, p. 11565, 2023.

[4] A. Sabban, Wearable circular polarized antennas for health care, 5G, energy harvesting, and IoT systems, *Electronics*, vol. 11, no. 3, p. 427, 2022.

[5] A. H. Sharmila and N. Jaisankar, Edge Intelligent Agent Assisted Hybrid Hierarchical Blockchain for continuous healthcare monitoring & recommendation system in 5G WBAN-IoT, *Comput. Netw.*, vol. 200, p. 108508, 2021.

[6] J. Lee and S. J. Choi, Hospital productivity after data breaches: difference-in-differences analysis, *J. Med. Internet Res.*, vol. 23, no. 7, p. e26157, 2021.

[7] D. Dolezel, B. Beauvais, P. S. Granados, L. Fulton, and C. S. Kruse, Effects of internal and external factors on hospital data breaches: Quantitative study, *J. Med. Internet Res.*, vol. 25, p. e51471, 2023.

[8] D. Jaschke and S. Montangero, Is quantum computing green? An estimate for an energy-efficiency quantum advantage, *Quantum Sci. Technol.*, vol. 8, no. 2, p. 025001, 2023.

[9] R. Rietsche, C. Dremel, S. Bosch, L. Steinacker, M. Meckel, and J. M. Leimeister, Quantum computing, *Electron. Mark.*, vol. 32, no. 4, pp. 2525–2536, 2022.

[10] T. Asselmeyer-Maluga, 3D topological quantum computing, *Int. J. Quantum Inf*., vol. 19, no. 04, p. 2141005, 2021.

[11] C. G. Wang and A. Rahman, Quantum-enabled 6G wireless networks: opportunities and challenges, *IEEE Wirel. Commun.*, vol. 29, no. 1, pp. 58–69, 2022.

[12] P. Wright, C. White, R. C. Parker, J. S. Pegon, M. Menchetti, J. Pearse, A. Bahrami, A. Moroz, A. Wonfor, R. V. Penty, T. P. Spiller, and A. Lord, 5G network slicing with QKD and quantum-safe security, *J. Opt. Commun. Netw*., vol. 13, no. 3, pp. 33–40, 2021.

[13] L. Aggarwal, S. Sachdeva, and P. Goswami, Quantum healthcare computing using precision based granular approach, *Appl. Soft Comput.*, vol. 144, p. 110458, 2023.

[14] S. Gupta, S. Modgil, P. C. Bhatt, C. J. C. Jabbour, S. Kamble, Quantum computing led innovation for achieving a more sustainable Covid-19 healthcare industry, *Technovation*, vol. 120, p. 102544, 2023.

[15] M. Bhavin, S. Tanwar, N. Sharma, S. Tyagi, and N. Kumar, Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications, *J. Inf. Secur. Appl.*, vol. 56, p. 102673, 2021.

[16] M. Munshi, R. Gupta, N. K. Jadav, Z. Polkowski, S. Tanwar, F. Alqahtani, W. Said, Quantum machine learning-based framework to detect heart failures in Healthcare 4.0, *Softw. - Pract. Exp.*, vol. 54, no. 2, pp. 168–185, 2024.

[17] Z. G. Qu and H. R. Sun, A secure information transmission protocol for healthcare cyber based on quantum image expansion and grover search algorithm, *IEEE Trans. Netw. Sci. Eng*., vol. 10, no. 5, pp. 2551–2563, 2023.

[18] P. Sarosh, S. A. Parah, G. M. Bhat, and K. Muhammad, A security management framework for big data in smart healthcare, *Big Data Res*., vol. 25, p. 100225, 2021.

[19] F. Khan, B. V. V. S. Prasad, S. A. Syed, I. Ashraf, and L. K. Ramasamy, An efficient, ensemble-based classification framework for big medical data, *Big Data*, vol. 10, no. 2, pp. 151–160, 2022.

[20] S. M. Nagarajan, G. G. Deverajan, U. Kumaran, M. Thirunavukkarasan, M. D. Alshehri, and S. Alkhalaf, Secure Data Transmission in Internet of Medical Things Using RES-256 Algorithm, *IEEE Trans. Ind. Inform.*, vol. 18, no. 12, pp. 8876–8884, 2022.

[21] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, and N. Z. Jhanjhi, Secure Healthcare Data Aggregation and Transmission in IoT-a survey, *IEEE Access*, vol. 9, pp. 16849–16865, 2021.

[22] V. S. Marichamy and V. Natarajan, Blockchain based securing medical records in big data analytics, *Data Knowl. Eng.*, vol. 144, p. 102122, 2023.

[23] M. Soni and D. K. Singh, Privacy-preserving secure and low-cost medical data communication scheme for smart healthcare, *Comput. Commun.*, vol. 194, pp. 292–300, 2022.

[24] M. R. Patruni and A. G. Humayun, PPAM-mIoMT: A privacy-preserving authentication with device verification for securing healthcare systems in 5G networks, *Int. J. Inf. Secur.*, vol. 23, no. 1, pp. 679–698, 2024.
[25] P. I. Tebe, G. J. Wen, J. Li, Y. J. Yang, W. H. Tian, J. Chong, and W. J. Zhang, 5G-enabled medical data transmission in mobile hospital systems, *IEEE Internet Things J.*, vol. 9, no. 15, pp. 13679–13693, 2022.
[26] A. H. Almulihi, F. Alassery, A. I. Khan, S. Shukla, B. K. Gupta, and R. Kumar, Analyzing the implications of healthcare data breaches through computational technique, *Intell. Autom. Soft Comput.*, vol. 32, no. 3, pp. 1763–1779, 2022.
[27] Y. Qian, Y. Jiang, J. Chen, Y. Zhang, J. Song, M. Zhou, and M. Pustisek, Towards decentralized IoT security enhancement: A blockchain approach, *Comput. Electr. Eng.*, vol. 72, pp. 266–273, 2018.
[28] M. Elhoseny and K. Shankar, Reliable data transmission model for mobile ad hoc network using signcryption technique, *IEEE Trans. Reliab.*, vol. 69, no. 3, pp. 1077–1086, 2020.
[29] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system, *Inf. Sci.*, vol. 479, pp. 567–592, 2019.
[30] P. K. Bishoyi and S. Misra, Enabling green mobile-edge computing for 5G-based healthcare applications, *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 3, pp. 1623–1631, 2021.
[31] M. S. Hossain and G. Muhammad, Emotion-aware connected healthcare big data towards 5G, *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2399–2406, 2018.
[32] X. Chen, J. Ji, C. Luo, W. Liao, and P. Li, When machine learning meets blockchain: A decentralized, privacy-preserving and secure design, in *Proc. IEEE Int. Conf. Big Data*, Seattle, WA, USA, 2018, pp. 1178–1187.
[33] J. Li, J. Wu, G. Jiang, and T. Srikanthan, Blockchain-based public auditing for big data in cloud storage, *Inf. Process. Manag.*, vol. 57, no. 6, p. 102382, 2020.
[34] M. Fujiwara, H. Hashimoto, K. Doi, M. Kujiraoka, Y. Tanizawa, Y. Ishida, M. Sasaki, and M. Nagasaki, Secure secondary utilization system of genomic data using quantum secure cloud, *Sci. Rep.*, vol. 12, no. 1, p. 18530, 2022.
[35] T. Attema, J. W. Bosman, and N. M. P. Neumann, Optimizing the decoy-state BB84 QKD protocol parameters, *Quantum Inf. Process.*, vol. 20, no. 4, p. 154, 2021.
[36] Y. J. Zhang, T. Shang, and J. W. Liu, A multi-valued quantum fully homomorphic encryption scheme, *Quantum Inf. Process.*, vol. 20, no. 3, p. 101, 2021.
[37] W. Shen, G. Wu, L. J. Li, H. Li, S. Liu, S. N. Shen, and D. W. Zou, Fluorine-terminated diamond (110) surfaces for nitrogen-vacancy quantum sensors, *Carbon*, vol. 193, pp. 17–25, 2022.
[38] P. Chinnasamy and P. Deepalakshmi, HCAC-EHR: Hybrid cryptographic access control for secure EHR retrieval in Healthcare cloud, *J. Ambient Intell. Humaniz. Comput.*, vol. 13, no. 2, pp. 1001–1019, 2022.
[39] F. Mohsen, H. Ali, N. El Hajj, and Z. Shah, Artificial intelligence-based methods for fusion of electronic health records and imaging data, *Sci. Rep.*, vol. 12, no. 1, p. 17981, 2022.
[40] C. P. Da Silva, S. Tedesco, and B. O'Flynn, EEG datasets for healthcare: A scoping review, *IEEE Access*, vol. 12, pp. 39186–39203, 2024.
[41] B. C. Tan and A. O. Cong, Optimality study of existing quantum computing layout synthesis tools, *IEEE Trans. Comput.*, vol. 70, no. 9, pp. 1363–1373, 2021.
[42] R. Jiang, Y. Xin, H. P. Cheng, and W. X. Wu, T-RBAC model based on two-dimensional dynamic trust evaluation under medical big data, *Wirel. Commun. Mob. Comput.*, vol. 2021, p. 9957214, 2021.
[43] H. Saxton, T. Schenkel, I. Halliday, and X. Xu, Personalised parameter estimation of the cardiovascular system: Leveraging data assimilation and sensitivity analysis, *J. Comput. Sci.*, vol. 74, p. 102158, 2023.
[44] W. J. Wu, L. Z. Gu, Y. F. Zhang, X. P. Huang, and W. H. Zhou, Pulmonary nodule clinical trial data collection and intelligent differential diagnosis for medical internet of things, *Contrast Media Mol. Imaging*, vol. 2022, p. 2058284, 2022.
[45] Y. J. Qiu and J. Lu, A visualization algorithm for medical big data based on deep learning, *Measurement*, vol. 183, p. 109808, 2021.

Shanmuganathan Manimurugan received the BE degree in computer science and engineering from Anna University, India, in 2005, the ME degree in computer science and engineering from Karunya University, India, in 2007, and the PhD degree from Anna University, in 2012. He is currently a professor with Faculty of Computers and Information Technology, University of Tabuk, Saudi Arabia. He has made significant contributions to these areas and has published numerous papers in various conferences and journals. His research interests include artificial intelligence, security, image processing, and the Internet of Things. He is a Life Member of the ISTE.

Xiaohong Lv received the MS degree from Dalian Medical University, Dalian, China, in 2008, and the PhD degree from China Medical University, Shenyang, China, in 2022. She is currently an associate professor at Department of Radiology, The First Affiliated Hospital of Jinzhou Medical University, China. She visited University of Adelaide in 2019 and Swansea University in 2023. Her research interests include intelligent processing, transmission, reconstruction of medical data, and intelligent analysis of medical images.

Shalli Rani (Director, Research) received the PhD degree from Manchester Metropolitan University, UK in 2023. She is a professor in Institute of Engineering and Technology, Chitkara University, Rajpura, India. She received the MCA degree from Maharishi Dyanand University, Rohtak in 2004 and the MTech degree in computer science from Janardan Rai Nagar Vidyapeeth University, Udaipur in 2007 and the PhD degree in computer applications from Punjab Technical University, Jalandhar in 2017. Her main area of interest and research are wireless sensor networks, underwater sensor networks, machine learning, and Internet of Things. She has published more than 100+ papers in international journals /conferences (SCI+Scopus) and edited/authored five books with international publishers. She is serving as the associate editor of *IEEE Future Directions Letters*. She received a young scientist award in Feb. 2014 from Punjab Science Congress, Lifetime Achievement Award and Supervisor of the year award from Global Innovation and Excellence, 2021.

Yanhong Feng received the MS degree from Jinzhou Medical College, Jinzhou, China, in 2003, and the PhD degree from China Medical University, Shenyang, China, in 2006. She is currently a professor and director at Department of Ultrasound, The First Affiliated Hospital of Jinzhou Medical University, China. Her research interests include the development and transformation of cutting-edge technologies for intelligent analysis of medical images.

Adam Slowik received the BSc and MSc degrees in computer engineering from Department of Electronics and Computer Science, Koszalin University of Technology, Poland, in 2001, the PhD degree in electronics from Department of Electronics and Computer Science, Koszalin University of Technology, in 2007, and the PhD in computer science from Department of Mechanical Engineering and Computer Science, Czestochowa University of Technology, Poland. Since October 2013, he has been an associate professor with Department of Electronics and Computer Science, Koszalin University of Technology. He is the author or co-author of over seventy articles, and two books. His research interests include soft computing, computational intelligence, machine learning, and bio-inspired global optimization algorithms and their engineering applications. He is also an associate editor of *IEEE Transactions on Industrial Informatics*, and a reviewer for many international scientific journals.